Conficker Working Group: Lessons Learned

June 2010 (Published January 2011)

Disclaimer

This report was produced by The Rendon Group based upon work supported by the Department of Homeland Security under Air Force Research Laboratory Contract No. FA8750-08-2-0141. This report is published in the interest of scientific and technical information exchange. Any opinions, findings, conclusions or recommendations expressed in this report are those of the author(s) and do not necessarily reflect the views of the Department of Homeland Security or the Conficker Working Group.

TABLE OF CONTENTS

Executive Summary

In November 2008, Conficker A, the first of five variants of the malware, rapidly began infecting computers which had failed to install a Microsoft patch released just weeks earlier. In late December 2008, Conficker B added new mechanisms for distribution including USB storage devices.

Conficker was malware intended to create a botnet. Until recently, botnet controllers would instruct malware to connect with a few dozen fixed domains in order to control the machines. As security experts improved and blocked these domains, the malware authors expanded their sophistication, targeting many more domains. With early versions of Conficker, the infected computer would reach out to 250 pseudo-randomly generated domains per day from eight Top Level Domains (TLDs) to attempt to update with new code or new instructions.

With millions of computers under its control, many security experts speculated as to what the author would attempt to do. The worst case scenarios were bleak. The worm, properly instructed, could credibly threaten critical infrastructure on the Internet. Even the more benign uses could cause severe problems for the public or private sector.

In an unprecedented act of coordination and collaboration, the cybersecurity community, including Microsoft, ICANN, domain registry operators, anti-virus vendors, and academic researchers organized to block the infected computers from reaching the domains – an informal group that was eventually dubbed the Conficker Working Group (CWG). They sought to register and otherwise block domains before the Conficker author, preventing the author from updating the botnet. Despite a few errors, that effort was very successful.

Conficker C was released in February 2009 and managed to update nearly a million computers from Conficker A/B to Conficker C, despite the CWG's efforts. The new features present in the C variant showed that the author was adapting to the Working Group's methods and trying to break them. Starting on April 1, 2009, the C version of the code would generate 50,000 pseudo-random domains per day from over 116 domains all over the world.

In fighting Conficker A/B, the security community proved they could coordinate to block 250 domains per day, already an unprecedented effort. With Conficker C, they faced the challenge of organizing in less than three weeks to coordinate with over 100 countries and block over 50,000 domains per day. Even with the large task in front of them, the group managed an impressive amount of success in blocking the domains generated by Conficker C.

In coordinating to stop the botnet threat, the CWG became a model for cyber defense. Thanks to this effort, we can glean a number of valuable lessons to guide how future efforts may be initiated, organized and managed.

The Conficker Working Group sees its biggest success as preventing the author of Conficker from gaining control of the botnet. Nearly every person interviewed for this report said this

aspect of the effort has been successful. The blocking of domains continues and the Working Group has indicated they will maintain their effort.

Chief among the reasons for CWG's success in this area was their ability to obtain cooperation from ICANN and the ccTLDs. Without these organizations, the group would have been able to do little to scale the registration of international domains to block Conficker C from using domains to update. Processes are now in place that may make future coordination efforts easier, and many countries are reviewing domestic regulations, which would hopefully streamline their internal processes for dealing with such threats.

The Working Group sees its biggest failure as the inability to remediate infected computers and eliminate the threat of the botnet. While remediation efforts did take place, millions of the A/B variations of Conficker remain on infected computers. Members of the group recommended a greater focus on remediation from the start and more coordinated communication with ISPs. However, some indicated that total remediation may not have been a realistic goal.

Commercial competition and personal motivations play a role in how well these ad-hoc organizations function, and while some used these tensions to explain the errors of the group, the Working Group is also evidence that differences can be overcome to cooperate against a threat. Indeed, the number, scope and sophistication of cyber threats are increasing more rapidly than the number of people vetted within the cybersecurity community capable of fighting them.

The Conficker Working Group teaches us that private sector collaboration, public-private information sharing, support to law enforcement, resources and legislative reform are among the many urgent requirements if the cyber security community is to stay ahead of impending threats. This and other lessons learned and recommendations are detailed in the following pages.

Recommendations

The following summary of recommendations was written in collaboration with the Conficker Working Group core membership following the circulation of the first draft of the paper.

Strategy:

- Focus on the larger overall threat environment and develop a strategy for dealing with that global issue, vs. the "whack-a-mole" approach of battling one incident after another.
- Establish the mindset of a "long term battle" at the outset to help manage burn-out and fatigue.
- Work to expand the size, skills, technological advantage and communications networks of cybersecurity defenders to match the growing threat.
- Identify resources (monetary and otherwise) used for cybersecurity efforts and work towards an allocation model that is effective at the strategic level.

Group Structure:

- Utilize a trust model; the scope of the working group needs to be a manageable size to be

effective and include those directly affected, and yet large to enough to expand to include a broader universe of those impacted.
- Employ a more goal-outcome oriented structure vs. an ad-hoc approach.
- Create a leadership team with a formalized decision-making process.
- Incorporate a consensus model without hierarchy to allow the group to adapt and respond to fast changing conditions.
- Form sub-groups for division of labor and specialization; communication among sub-groups is essential.
- Gain the participation and support of key governing and regulatory bodies such as ICANN.

Operations:
- Utilize an infrastructure with a central set of resources that enables clear and effective communication. This would include resources like an organized mailing list hierarchy, a wiki, real-time chat room, and data sharing. It might also include a voice communication system of some kind (conference bridge, etc.)
- Formulate a plan to rotate responsibilities and reduce roles when support members are added.
- Strike a balance between task accountability and responsibility and the need to hold an individual accountable in a group comprised of volunteers with limited time.
- Assign (hire) a small accountable staff of 2-3 people to help manage and direct the roles and tasks of the large group of volunteer experts, and to keep track of ongoing details and priorities.
- Maintain clear records of events, decisions and outcomes from the beginning that will provide an effective learning experience.

Data Usage:
- House collected data at a trusted neutral sinkhole.
- Establish agreed upon rules regarding data sharing, usage, and attribution early on.
- Establish mechanisms to monitor such agreements.

Relations with Government:
- Establish an early warning alert procedure so that cybersecurity experts can alert the US Government through official channels when an issue is detected. Relying on social networks to notify the US Government is not sufficient or prudent.
- Improve cooperation between the private sector and the US government and governments around the world so that information sharing and efforts become a two-way exchange.
- Clarify the role of private sector cooperation with law enforcement, which is a vital part of cybersecurity efforts that governments must lead.

Relations with Stakeholders:
- Formalize communications with stakeholder groups vs. relying on social networks.
- Establish guidelines for publishing of research that considers the needs for operational security.

I Introduction

This paper was commissioned by the Department of Homeland Security's Science and Technology (S&T) Directorate to document the creation, workings and processes of the Conficker Working Group and to provide lessons learned and recommendations for best practices. The paper is the result of in depth interviews with 15 members of the Working Group to obtain their overview of the activities of the Working Group and their opinions on lessons learned and open source research to identify how the broader cyber community dealt with and how the media covered the Conficker worm.

This draft of the paper has been reviewed by those interviewed and other core members of the Conficker Working Group. They have provided commentary, edits and corrections as necessary. They have also recommended and collaborated on a summary of recommendations that has been placed after the executive summary.

Conficker is an Internet worm that has infected millions of computers since it first appeared in November 2008 as one of the largest currently active botnets in cyberspace. The intent of the author[1] of this worm remains unclear. However, the potential for the Conficker botnet to do significant damage to individual Internet users, corporations, governments or even critical Internet infrastructure leads many to rank it one of the largest and most serious cybersecurity threats of the past decade.

The Conficker Working Group (CWG) was created as, and remains, an ad-hoc organization formed by private sector corporations, groups and individuals to counter the Conficker malware threat. The group is likely the largest single collaborative cybersecurity effort ever taken on by private industry and individuals without any official sponsor or structure. It required the cooperation and coordination of software companies, academic researchers, anti-virus vendors, law enforcement, ICANN and a number of Top Level Domain administrators. In spite of the difficulty of the task, the group has been largely successful in its main goal of preventing the author of the malware from using it to do significant damage in the cyber domain.

Many participants and observers feel the collaboration model created by the Working Group may be as significant as the effectiveness of the effort itself. Groups created since the CWG, many of which overlap in membership, are looking to this group as a model for successful collaboration.

The first section of this paper looks at the Conficker malware and botnet. The second provides a narrative of the Conficker Working Group's activities. The third analyzes the effort, provides lessons learned and recommendations based on interviews with the members of the Conficker Working Group.

Where specific names of individuals, organizations or companies are necessary for the explanation of events or recommendations, they are included. Otherwise, more generic terms, such as working group member or interviewee, are used.

---

[1] Throughout the report, the malware author is referred to in the singular. However, as discussed later, it is uncertain whether there are one or many authors, whether they are male or female, and whether they were acting alone or as part of a criminal organization or nation-state.

II Conficker Worm and Botnet

Conficker is a type of computer malware known as a worm that targets a flaw within the Microsoft Windows operating system. Once it infects a computer, it can link the infected computer to a remote computer controlled by the malware author and then download additional instructions to the infected computer. Conficker uses a number of methods to self-propagate and evade defensive efforts to counter the malware or remediate the computer. Each of the five variations of Conficker improved upon its capabilities and adapted to the efforts of the cybersecurity community to defend against it.

This section outlines the basic technical aspects of Conficker and the differences among the variations so that the reader may understand how the worm spread, why the cybersecurity community took various actions and what made this piece of malware so dangerous in the opinion of many experts. The full technical details of Conficker have been well documented by a number of organizations inside and outside the Conficker Working Group, including Microsoft, the Honeynet Project, SRI International, various anti-virus vendors and an assortment of websites. For readers interested in a more thorough discussion of the technical aspects of the worm, the following are recommended references:

* http://www.microsoft.com/security/worms/Conficker.aspx
* http://mtc.sri.com/Conficker/
* http://www.honeynet.org/papers/conficker
* http://www.f-secure.com/v-descs/worm_w32_downadup_al.shtml
* http://www.symantec.com/connect/sites/default/files/the_downadup_codex_ed1.pdf
* http://en.wikipedia.org/wiki/Conficker
* http://lastwatchdog.com/faq-downadup-conficker-worm/

Overview of the Arrival of Conficker

On October 23, 2008, Microsoft released a critical security patch for Windows. According to the announcement[2]: "The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit."

According to Microsoft's Security Intelligence Report (SIR)[3] released a year later in October 2009:

> "Like the worms that plagued the Internet earlier this decade, malware that exploited the vulnerability would be able to spread without user interaction by taking advantage of the

[2] http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx

[3] http://www.microsoft.com/downloads/details.aspx?FamilyID=037f3771-330e-4457-a52c-5b085dc0a4cd&displaylang=en

protocols computers use to communicate with each other across networks. For this reason, and because actual attack code that exploited the vulnerability was known to exist in the wild at the time, the MSRC took the unusual step of releasing MS08-067 "out of band" rather than wait for the next scheduled release of Microsoft security updates, which takes place on the second Tuesday of every month. Security Bulletin MS08-067 happened to be released on the last day of the eighth annual meeting of the International Botnet Task Force in Arlington, Virginia, a suburb of Washington, D.C., where attendees agreed to closely monitor developments around what appeared to be the first legitimately "wormable" vulnerability to be discovered in Windows in several years."

Releasing MS08-067 during the International Botnet Task Force meeting in Washington, DC in October 2008 ensured widespread knowledge of the dangers of this vulnerability spread quickly through the cybersecurity community.

According to SRI International, an independent, nonprofit research institute, Chinese hackers had created software packages to use the exploit patched by MS08-067 as early as mid-September 2008[4]-[5]. Another report suggests that an infection of the Gimmiv Trojan, which utilized the same exploit as Conficker, was found as early as August 20, 2008, on a South Korean computer. Gimmiv would go on to infect a small number of computers in Vietnam and Malaysia in late September 2008.[6] After the patch was released, at least two other pieces of malware attempted to use the MS08-067 vulnerability before Conficker was released (W32.Kernelbot.A and W32.Wecorl).

Conficker's Design

Conficker is a Dynamic Link Library (DLL), Microsoft's implementation of the shared library concept in the Microsoft Windows and OS/2 operating systems, that uses a Remote Procedure Call (RPC) buffer overflow to push the code onto a Windows machine. Conficker then directs the infected computer to communicate with another address space (commonly on another computer on a shared network) without the programmer explicitly coding the details for this remote interaction (which is why it is defined as "self-propagating").

A patch for the Windows Operating System existed for weeks before the worm was released, and downloading the software update prevents Conficker from infecting a computer. However, many computer owners do not regularly patch their software or run routine maintenance on their computers. One security firm, Qualys, estimated 30% of computers running the Windows Operating System remained unpatched as of January 2009, over two months after the patch was released and over a month after the first version of Conficker was released. Additionally, millions of computers running counterfeit versions of Windows were vulnerable without access to the security patch.

---

[4] http://mtc.sri.com/Conficker/

[5] One interviewee for this paper said a separate Microsoft patch MS06-040 released in 2006 was closely related to the same exploit addressed by MS08-067.

[6] http://blog.threatexpert.com/2008/10/gimmiva-exploits-zero-day-vulnerability.html

While others had designed basic ways to exploit the Microsoft vulnerability, many security researchers described Conficker's concept and design as "elegant" because of the worm's:

* Multiple methods of self-propagation
* Ability to infect a computer and wait for further instruction
* Use of multiple defensive mechanisms to prevent its removal
* Adaptation by the author in releasing new versions
* Quick turnaround from the date the patch was released.

Conficker's Evolution

Conficker, also known as Downup, Downadup and Kido, was released and first detected in November 2008. The original version released is now known as "Conficker A."

There have been five main variations of Conficker. This paper uses the terms utilized by SRI and used generally by the members of the Conficker Working Group, A, B, B++, C and E. Others, Microsoft in particular, have labeled them Variations A, B, C, D and E. The various versions of Conficker, described below, are all still residing in millions of computers around the world. Thus, Conficker is still able to continue infecting additional computers and, perhaps more importantly, can still be altered by its creator to attack additional computers and the Internet infrastructure in new and possibly more dangerous ways.

Conficker A

On November 21, 2008, Conficker A was released and began attempting to infect computers that had not been patched. Conficker A particularly focused on other computers that were connected within an intranet. This ability meant Conficker spread rapidly within corporations that had many computers networked and were slow to patch their machines.

Conficker A generated a daily list of 250 domains from five Top Level Domains (TLDs: .com, .net, .org, .info and .biz) and attempted to connect to them to receive new instructions. The worm attempted to connect to the list every three hours. Numerous researchers broke the domain generation algorithm with relative ease. However, the author of Conficker used encryption to prevent the botnet from being hijacked by someone who registered a domain.

The methods used by Conficker's author to spread the worm and counter security measures have been used previously in other malware and were known to researchers when the Conficker author attempted them. However, Conficker's early success in infecting computers came from combining multiple methods of distribution, multiple counter-measures and releasing it so soon after the Windows vulnerability was announced. As noted above, several researchers described it as "elegant" in its construction.

One of the methods used by the worm to avoid detection by computer users and network administrators is to limit its use of computer resources and network bandwidth. Many computer

users can identify malware when their computer slows down dramatically or ads pop up on their screen without reason. Conficker does a better job than most malware of hiding in the background[7].

One oddity of Conficker A was that it began its program by checking for a Ukrainian keyboard. This led some analysts to suspect the author was Ukrainian or had ties to Ukraine and originally wanted to avoid violating any local laws.

Conficker B

Conficker Version B was released on December 29, 2008, and began attempting to connect with new domains on January 1, 2009. Version B used much of the code from Version A. It updated the domain generation algorithm to include three additional country code top level domains (ccTLDs: .cn, .ws and .cc). It added several methods of distribution including scanning for weakly passworded shares (people who use the password "password" or "123456" or "computer") and removable storage devices such as USB devices. The ability to infect USB devices spread Conficker B more quickly and allowed it onto computers that would otherwise not have been infected (including some computers inside the US Government). The infected USB device would also harm those trying to clean the malware from their computers: people who saved files onto USB drives before cleaning their computer would reinstall the worm when they reconnected the USB device. Companies would re-infect their entire networks if they were not careful with infected USB drives used by employees.

Conficker B avoided connecting to domains that were connected to cybersecurity researchers and known honeypots. Version B no longer did a keyboard check prior to executing. Version B patched several Windows APIs and disabled a preset list of popular anti-virus products if they were found on the machine. Version B's code also employed "anti-debugging features to avoid reverse engineering attempts."[8]

Unlike Version A, Conficker B included the GeoIP file within its code rather than reaching out to an external website. This served to adapt to security researchers shutting off access to the file, which Symantec said possibly slowed the infection early on[9].

Finally, Conficker B upgraded the encryption to include the MD6 cryptographic hash algorithm as a way of obscuring communications. The research on that algorithm was published on October 15, 2008, barely two months before Version B was published. That quick use of the encryption provided another indication that the author was following the cybersecurity community very closely and was quick to adapt the code.

---

[7] http://www.symantec.com/connect/sites/default/files/the_downadup_codex_ed1.pdf

[8] http://mtc.sri.com/Conficker/

[9] http://www.symantec.com/connect/sites/default/files/the_downadup_codex_ed1.pdf

Conficker B++

Conficker B++ was identified on February 16, 2009, (Microsoft calls this version "C"). According to SRI, 86% of the code is similar to Conficker B, but includes some new protocols[10]. It appears to be an initial response to the efforts of the Conficker Working Group to block domains. Most significantly, it created a way for the malware to update without connecting to a specific domain.

Conficker C

Conficker C is a major rewrite of the original Conficker code[11] (Microsoft calls this version "D"). First identified in late February 2009, it gave new urgency to the effort to block domains. If computers infected with Conficker A or B were upgraded to C, the results would be a much more dangerous botnet.

The Conficker C rewrite shows that the malware's creator was paying attention to the mitigation and remediation efforts of the Conficker Working Group and others (described below) and was adapting to counter those efforts. The rewrite responded to the defensive pre-registration of domains by increasing the number of domains contacted by infected computers from 250 to 50,000. (It actually only attempts to connect to 500 of the 50,000 possibilities.) The number of TLDs increased from less than 10 to over 100, adding numerous country code TLDs, which are far more difficult for security researchers to coordinate. The increase in domains also significantly increases the number of "collisions" in which computers attempt to access legitimate websites already owned and operated by others.

Some group members and observers believe the new domain strategy in Conficker C is actually a "red herring" meant to consume the time and resources of those trying to mitigate and remediate the malware. The real threat, they believe, is in the peer-to-peer (P2P) capability of Conficker C, which was not present in previous versions. The computers can connect to each other and update code over networks without connecting to domains, thereby negating the efforts of the CWG and others to contain the worm.

Conficker C also increases the malware's defenses. It disables safe mode on the computers it infects and prevents the user from visiting a list of websites, such as Microsoft or other key anti-virus vendors, which could help the user remove the malware. The worm deletes prior restore points to prevent the computer user from using a rollback function.

---

[10] http://mtc.sri.com/Conficker/

[11] http://mtc.sri.com/Conficker/addendumC/index.html

Conficker E

Conficker E, released on April 7, 2009, is a variation on Conficker C. Conficker E was designed to update computers that were already infected with Conficker C. It installed Waladec, a form of scareware that attempts to trick computer users into paying money for fake anti-virus software. Waladec was a separate piece of malware not created by Conficker's author. Rather, it appears the author of Conficker provided access to Conficker to a criminal group. It is unknown whether the author of Conficker profited from this use of his malware or what his relationship was/is with the criminal group.

Conficker E was programmed to uninstall itself on May 3 and revert to Conficker C. The move to uninstall the scareware and revert to Conficker C added to the speculation that this was a renting out of the botnet.

Variant	Detection Date	Infection Vectors	Update Propagation	End Action
Conficker A	21-Nov-08	Net BIOS; Exploits MS08-067 vulnerability in Server service	HTTP pull; Downloads from trafficconverter.biz; Downloads daily from any of 250 pseudorandom domains over 5 TLDs	Updates self to Conficker B, C or D
Conficker B	29-Dec-08	NetBIOS; Exploits MS08-067 vulnerability in Server service; Creates DLL-based AutoRun trojan on attached removable drives	HTTP pull; Downloads daily from any of 250 pseudorandom domains over 8 TLDs; NetBIOS push	Updates self to Conficker B++ or E
Conficker B++	20-Feb-09	NetBIOS: Exploits MS08-067 vulnerability in Server service; Creates DLL-based AutoRun trojan on attached removable drives	Blocks a selective list of DNS lookups to prevent remediation; Disables AutoUpdate	Updates self to Conficker C

Variant	Detection Date	Infection Vectors	Update Propagation	End Action
Conficker C	4-Mar-09	HTTP pull; Downloads daily from any 500 of 50000 pseudorandom domains 110 TLDs; P2P push/pull; Uses custom protocol to scan for infected peers via UDP, then transfer via TCP	Blocks DNS lookups; Does an in-memory patch of DNSAPI.DLL to block lookups of anti-malware related web sites; Disables Safe Mode; Disables AutoUpdate; Kills anti-malware; Scans for and terminates processes with names of anti-malware, patch or diagnostic utilities at one-second intervals	Downloads and installs Conficker E
Conficker E	7-Apr-09	NetBIOS; Exploits MS08-067 vulnerability in Server service	NetBIOS push; Patches MS08-067 to open reinfection backdoor in Server service; P2P push/pull; Uses custom protocol to scan for infected peers via UDP, then transfer via TCP	Updates local copy of Conficker C to Conficker D; Downloads and installs malware payload: Waledac spambot; SpyProtect 2009 scareware; Removes self on 3 May 2009 (but leaves remaining copy of Conficker D)

Info from Microsoft website, CWG website, Wikipedia

Attribution and Theories About the Conficker Worm

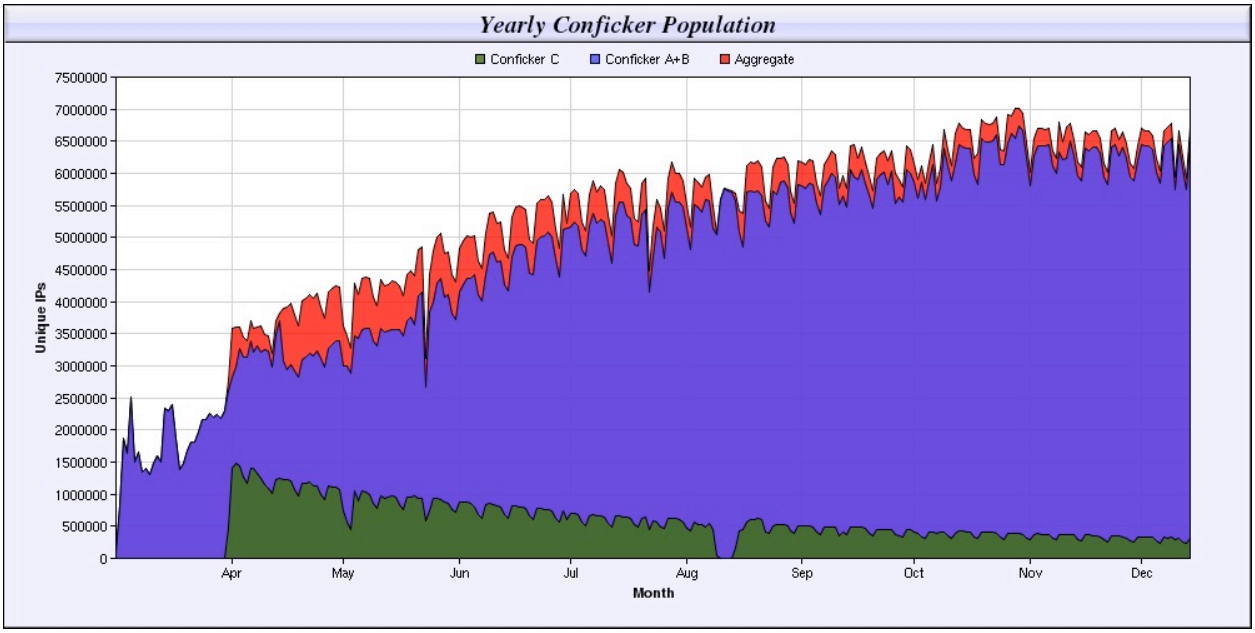
As of the writing of this paper, the author of Conficker has not been publicly identified. Several hints within the original code, including avoiding infecting computers using a Ukrainian keyboard, has led some researchers to believe the author lives in Eastern Europe. Others have suggested that a criminal organization or a nation-state may actually be behind Conficker, due to its sophistication and rapid adaptations. However, there is limited evidence in the public domain to support speculation that this malware was authored by a nation-state.

Scope of the Threat

Conficker is among the largest botnets in the past five years. It combined a number of the best tricks and traps within malware. Experts felt Conficker was dangerous because it was an open-ended tool that could be used for a variety of purposes, without signaling the author's true motivation. The ability of Conficker's author to rapidly update and distribute new versions of

code to adapt to changing security efforts made it unique and more difficult to contain. When the GeoIP system was renamed and moved[12], harming Conficker A's ability to spread, Conficker B was released. When the Conficker Working Group announced it would block domains, the author began incorporating P2P technology and vastly expanded the domains that could be registered, making the defenders' job significantly more difficult.

Numbers of infections:



http://www.shadowserver.org/wiki/uploads/Stats/conficker-population-year.png

One year after the original malware was released, between five and thirteen million computers from approximately 6 million unique IP addresses are infected by the A or B variants of Conficker.[13] The number of infections appears to have leveled off, but remediation efforts do not appear to be making a dent in the number of infected computers.

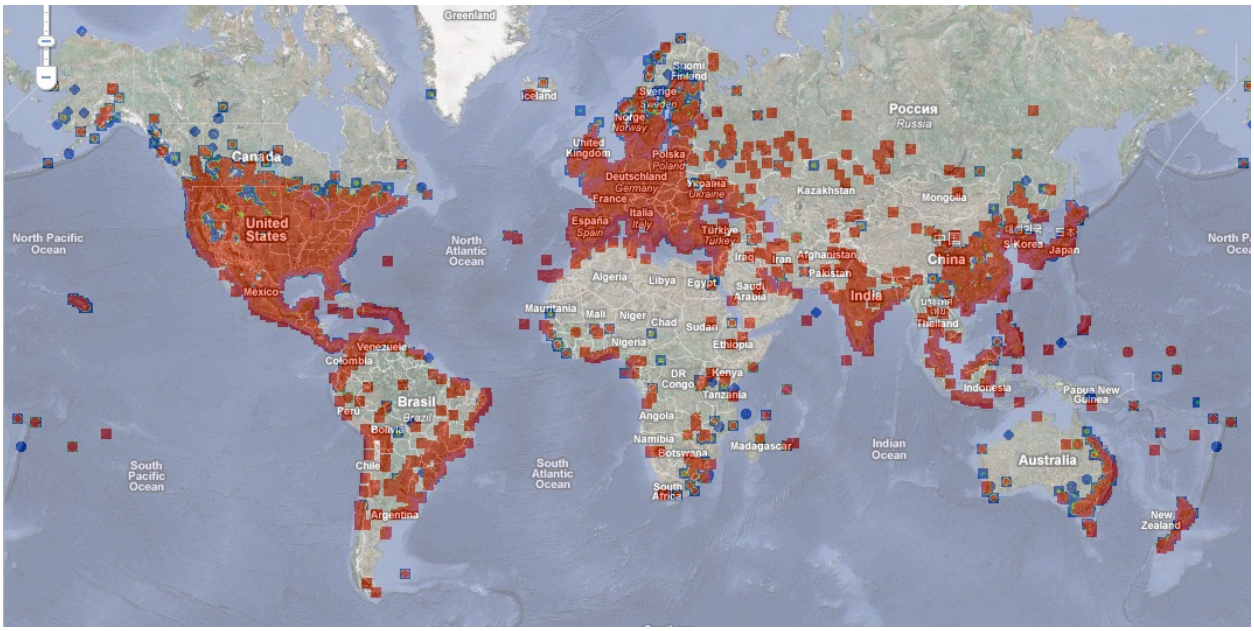
Conficker C has infected far fewer computers and the numbers of those computers have been declining. As of early December 2009, between 300,000 and 400,000 unique IP addresses were shown as infected. That is down from over a million unique IP addresses that were seen in April 2009.

[12] http://www.blackhat.com/presentations/bh-usa-09/HYPPONEN/BHUSA09-Hypponen-ConfickerMystery-PAPER.pdf

[13] http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking

The exact size of Conficker has been debated since the worm appeared. At its peak, Tom Gaffney of F-Secure estimated that 15 million machines were infected.[14] Others found that number to be too high, but nearly everyone today places the number above five million.

Infected computers appear in nearly every country in the world. Today's infections are heavily located in Asia, particularly India, as well as Brazil. One reason for this may be the prevalence of counterfeit Windows OS software in many parts of the developing world. Computer users with pirated software are far less likely to patch their computers. Some argue that Microsoft's policies on piracy make it harder for these users to patch their computers, making these computers more likely to be infected[15].



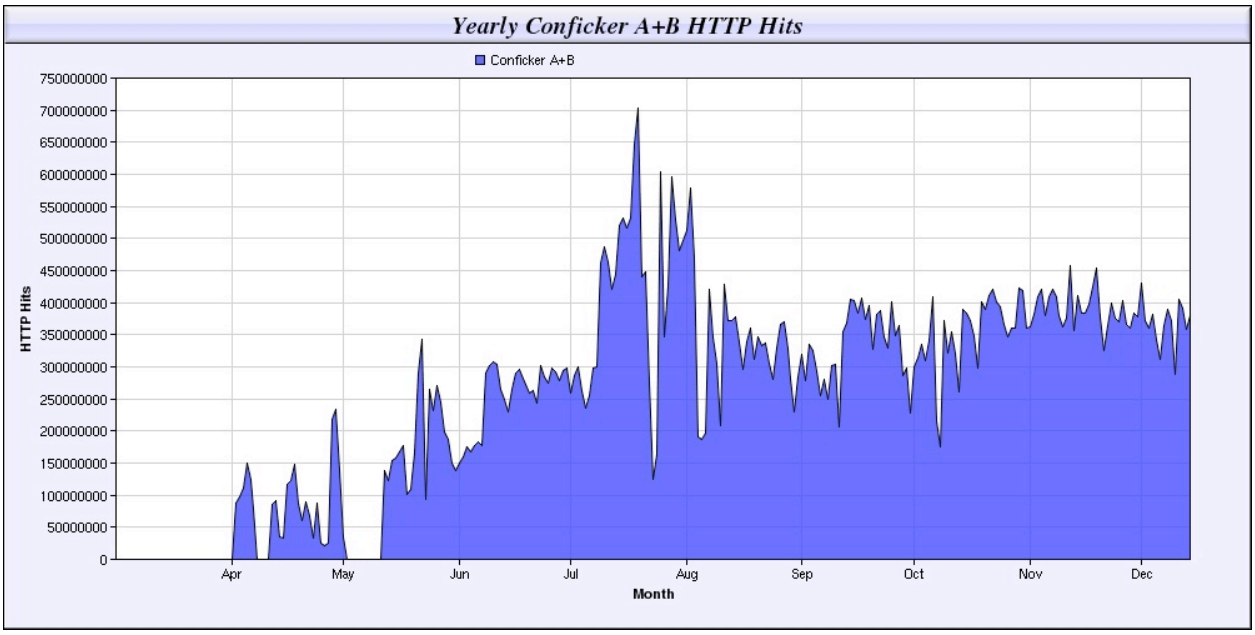
http://www.confickerworkinggroup.org/wiki/uploads/ANY/conficker_world_map.png

---

[14] http://www.telegraph.co.uk/technology/4338625/Conficker-Windows-virus-infects-15-million-PCs.html

[15] Microsoft does offer security updates even to pirated copies of Windows, but there are certain circumstances when the update will not work, for example if the user has not installed a minimum required service pack (in this case SP2 for XP) manually. There is also the issue of people not wanting to use Windows Update if they are using a grey market or pirated copy of Windows.

SOURCE: http://www.microsoft.com/uk/athome/security/update/genuine.mspx



http://www.shadowserver.org/wiki/uploads/Stats/conficker-http-ab-year.png

Researchers generally agree that this is one of, if not the single largest cyberthreats in recent memory. One member of the core group said it was "the most dangerous piece of malware we have ever faced." Others indicated that the media and public underestimated the importance of the threat.

However, researchers disagree as to how significant a threat Conficker is on the scale of all existing cyberthreats. As one researcher said, some malware currently in existence is doing far more tangible damage in terms of spreading spam, backing denial of service attacks or stealing identity information from individuals. Conficker's threat, on the other hand, comes from its potential, which was prevented from being fully realized due to the Working Group.

The *New York Times*[16] reported on March 19, 2009 that

> "Perhaps the most obvious frightening aspect of Conficker C is its clear potential to do harm," said Phillip Porras, a research director at SRI International and one of the authors of the SRI report. "Perhaps in the best case, Conficker may be used as a sustained and profitable platform for massive Internet fraud and theft." "In the worst case," Mr. Porras said, "Conficker could be turned into a powerful offensive weapon for performing concerted information warfare attacks that could disrupt not just countries, but the Internet itself."

[16] http://www.nytimes.com/2009/03/19/technology/19worm.html

Purpose of the Malware

Since the discovery of the Conficker worm researchers have debated the intent of Conficker. The worm was not designed to promote a specific type of attack (the way Srizbi would send spam). It essentially allowed the author to virtually "put his foot in the door" and wait for the right time to use the growing botnet.

A popular theory about the purpose of Conficker is that the worm would be used to spread other malware. This theory seemed to be somewhat confirmed with the release of Conficker E, which included Waladec used for spam and scareware. The scenario of renting out the botnet for spam was always among the most likely and least threatening of the potential uses for Conficker. However, to some it seemed a mundane and inelegant use for such an exceptional botnet, leading analysts to question whether Conficker E was a diversion to draw attention away from its true purpose. Others wondered if the author had been scared away from doing something more damaging because of the high level of attention from the media and security experts and simply fell back on making a quick profit as an alternative.

More worrying were theories that Conficker could be used for a significant cyberattack against critical infrastructure in the public or private sector. The author as a form of blackmail could conduct attacks or the author renting out the botnet could do them to whomever was willing to pay for the attack.

Going against the prevailing theory that the malware was written by an individual or criminal group, some believe Conficker was the work of a nation-state. At times, analysts described the possible "weaponization" of Conficker into an instrument of cyberwarfare. None of these theories were ever confirmed, but the obscure nature of Conficker's purpose has led security researchers to identify a variety of possible scenarios.

Some suggested that the author may never have intended to utilize Conficker and the entire botnet was a feint or a "head-fake." Among those with this theory, one suggested Conficker was used to distract the security community from other malware such as Zeus and Torpig, which continue to reap large profits for criminals. Another suggested that Conficker was an attempt to test the defenses of the cybersecurity community.

While the view that Conficker was a ruse and not a legitimate threat is not the prevailing view, it does come up in questions of why Conficker was never used for anything more devious than scareware. It is likely that the Conficker Working Group effort to counter the spread did make it more difficult for the author to act with impunity, but the author did not seem to have tried his or her hardest. As noted previously, it is possible the level of attention given to the malware scared off the author. It is also possible the author is waiting for a later date or is waiting for someone to pay for the use of the botnet.

On the more obscure side, some analysts posited that the author planned to sell the botnet for "cloud computing time." This seems unlikely, but the willingness of people to think outside the box was spurred by the lack of information about the purpose of the botnet. Paradoxically, it is possible the public speculation about Conficker's purpose may have given the author new ideas on the worm’s potential usage.

In addition to concerns that the author or authors may attempt to update Conficker and provide it new instructions, there is concern among some researchers that other organizations or nation-states could take over Conficker (using the term "hijack"). The processes for doing so are relatively complex and would require a considerable effort, but would be beyond the technical capabilities some cybersecurity experts, hackers and nation-states. Several individuals within and outside the Conficker Working Group expressed this concern during interviews and explained potential processes for hijacking Conficker.

As a footnote, over the course of 2009, criminals taking advantage of the public's fear of the Conficker botnet undertook several other malware efforts. For example, spam was sent encouraging the recipients to purchase a Conficker removal or protection kit, when in reality it was a scam to obtain money or to steal credit card information. Scareware is not just a successful business for cybercriminals; it undermines the public's trust in cybersecurity efforts.

III The Conficker Working Group

Using information from interviews, documents and the media, this section provides the narrative of how the Conficker Working Group formed and operated from November 2008 through summer of 2009.

The Cybersecurity Environment pre-Conficker

The threats in cyberspace are growing in number, scope and sophistication and have been for a number of years. Individual cybercriminals and organized "cybergangs" continue to improve their skills and have developed a variety of profit models to scam the public. While law enforcement efforts increase and arrests and property seizures have occurred, most cybercriminals feel they can act with relative impunity.

Prior to Conficker, collaborative efforts to combat specific pieces of malware had occurred on a number of occasions. In that, the Conficker Working Group was not unique. Groups of people in the anti-virus community, registry operators, academics and others would collaborate on an ad-hoc basis to share information and coordinate actions--but not on the scale of the Conficker Working Group. Additionally, there are several standing security collaboration groups where many of these individuals communicate (and there is broad overlap among these groups). Until recently, these groups were mostly email listserves of individuals who had been vetted by the group managers, but some groups have added social networking and collaboration technology such as wikis.

Several people interviewed expressed the view that the community had hit a turning point in 2007-08 and decided to take more proactive actions against cybercriminals. Some organizations, including registries, had begun actively "taking down" registered domains that were spreading malware without waiting for law enforcement. Several interviewees indicated the coordination against Conficker was part of an important broader shift in the cybersecurity community to be proactive rather than reactive.

Previous Efforts Against Malware: Srizbi

In late 2008, botnet called Srizbi was one of the world's largest of its kind, responsible for a significant amount of spam email.[17] Computers infected with the Srizbi trojan would connect to a control server, receive instructions and send the spam emails. The Srizbi botnet faced a significant setback when authorities took down the control servers at the McColo server facility. At that time, the security firm FireEye, coordinating with others including Microsoft and Verisign, registered the domains ahead of the botnet creators and kept them from regaining control of the infected computers. The effort was successful for about two weeks, but proved difficult for FireEye to sustain indefinitely due to lack of funding.[18] The trojan authors regained control.

FireEye did work afterwards to contact the ISPs that they had identified as infected through sinkhole servers. The hope was they could remediate some of the 100,000 infected computers and shrink the size of the botnet.

The effort against Srizbi failed. However, the attempt served as a proof of concept for the methodology of capturing domains, described by one interviewee as "defensive DNS." The lessons learned from the Srizbi effort became important to the effort that would become the Conficker Working Group. In cases where companies may not be able to fully stop an infection or prevent the authors from taking control, they still may be able to slow it down and hamper it.

Tracking Conficker and The Beginning of the Conficker Working Group

When Conficker first appeared on researchers' networks and honeypots in late November 2008, in the words of one interviewee, "It was hard to avoid." Companies that had honeypots (computers and networks designed to pick up malware in cyberspace in order to research it) were collecting numerous samples of the new malware. Companies with large numbers of domains and IP addresses were seeing infected computers trying to contact domains.

As a measurement of the initial speed of infection, according to a *New Scientist* article published on June 12, 2009[19]:

> For most of 20 November, about 3000 infected computers attempted to infiltrate [SRI's] telescope's vulnerable ports every hour -- only slightly above the background noise

[17] http://en.wikipedia.org/wiki/Srizbi_botnet

[18] http://www.computerworld.com/s/article/9121678/Massive_botnet_returns_from_the_dead_starts_spamming

[19] http://www.newscientist.com/article/mg20227121.500

generated by older malicious code still at large. At 6 pm, the number began to rise. By 9 am the following day, it was 115,000 an hour. Conficker was already out of control.

On November 22, 2008, days after Conficker was first identified, Microsoft issued a new security alert recommending immediate patching. On November 25, a day before the A variant would begin attempting to connect to 250 domains per day, they addressed the new malware on their blog.[20]

Throughout December, discussion of Conficker increased on a number of security lists[21] on which the private sector collaborates. By late December, SRI estimated 1-1.5 million computers were infected with Conficker A.

The release of the B variation of Conficker in late December,[22] which included new methods for distribution, "escalated" the threat according to the key participant in the Conficker effort from Microsoft. There were increased numbers of infections around the globe and increased calls from enterprise customers and individuals who had been infected or were concerned about infections. Microsoft's initial goal was to slow the infection rate down to "give time" to Windows users to patch their computers or utilize anti-virus software.

Meanwhile, public word of the infections was beginning to spread and the media were picking up on the new malware threat. An infection of UK Ministry of Defense computers in early January 2009 brought mainstream media attention and also helped focus attention on the issue in government circles. The French and German militaries both dealt with significant infections that were made public. Microsoft continued to keep their website updated with information about the infection.[23]

On January 11, 2009, Microsoft released a security tool update to scan and clean early versions of Conficker. This was a significant development that would help responsible companies and individuals remove the malware from their machines and networks. However, this security update, like the MS08-067 patch before it, would not reach those who do not or could not update their computers on a regular basis.

Early on, several researchers were paying for and registering the vulnerable domains by hand, one-by-one[24]. Some were discussing the possibility of doing so in a comprehensive way. Others were getting access to domains so they could sinkhole the data and learn more about the infection.

---

[20] http://blogs.technet.com/mmpc/archive/2008/11/25/more-ms08-067-exploits.aspx

[21] Due to security/privacy concerns, specific names of other lists will not be mentioned in this paper

[22] http://blogs.technet.com/mmpc/archive/2008/12/31/just-in-time-for-new-years.aspx

[23] http://blogs.technet.com/mmpc/archive/2009/01/22/centralized-information-about-the-conficker-worm.aspx

[24] Among those groups, one interviewee pointed to the early efforts of F-Secure and the registry .ws. Both had used various data and shared that data with others, which helped determine the scope of the threat in the early months.

The large-scale coordination began in the final days of January and first days of February 2009. Throughout January, security researchers, registries, Microsoft and the Shadowserver foundation discussed the potential for managing the worm. On January 28, Shadowserver set up the Conficker email listserve. The initial membership of the listserve was small and nearly everyone knew each other.

In late January, T.J. Campana at Microsoft contacted Rodney Joffe of Neustar, the registry operator that manages .biz domains. Microsoft wanted Neustar's assistance to register or block .biz domains that would be contacted by Conficker-infected computers. Joffe requested that ICANN [25]waive their mandatory registration fees with the domains as the issue was related to the security of the DNS system. According to ICANN, this was the first time they had received such a request. ICANN agreed to waive the fee and later agreed to waive all fees related to registering Conficker domains. Since that time, ICANN has instituted a formal process for registry operators to request a fee be waived when dealing with an attack on the DNS system. Many interviewees said ICANN's willingness to change its policy on the fees and its creation of a formal system to waive fees for future events was a key part to the success in combating Conficker and set an important precedent that may help counter future threats. Most registrars cooperating with the Conficker Working Group did not charge the group for registering the domains.

On February 4, 2009, SRI released its analysis of Conficker A and B binary code. At the time, nobody from SRI was yet a member of the Working Group, but the analysis was widely circulated among the group members.

Sinkholing of Data. As domains were registered, they were pointed at six sinkhole servers to collect information about the scope and spread of the malware. Originally, a number of individual groups and organizations ran sinkhole servers[26]. In early February, the group decided to centralize the data at Georgia Tech, which offered server space to hold the data and bandwidth to manage it[27]. This was seen as a neutral site, where companies could share data and have

---

[25] From the ICANN bylaws (www.icann.org): The mission of The Internet Corporation for Assigned Names and Numbers ("ICANN") is to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems. In particular, ICANN:

1. Coordinates the allocation and assignment of the three sets of unique identifiers for the Internet, which are
    a. Domain names (forming a system referred to as "DNS");
    b. Internet protocol ("IP") addresses and autonomous system ("AS") numbers; and
    c. Protocol port and parameter numbers.
2. Coordinates the operation and evolution of the DNS root name server system.
3. Coordinates policy development reasonably and appropriately related to these technical functions.

[26] The early sinkholes were important in estimating the size and scope of infection. For example, F-Secure's efforts to sinkhole data in December and January assisted in early population estimates.

[27] Terrabytes of storage were required and they diverted resources from other projects related to cybersecurity to do so.

access controlled. Various access agreements were granted with some companies placing restrictions on the usage of their data.

Registering of Domains. Technologically, pre-registering (infected, affected, suspicious?) domains was not that hard. Once the malware code was reverse engineered, they were able to replicate the domain generation algorithm. From there, members of the Conficker Working Group could create lists of domains that must be registered and get them to the appropriate registries or authorities. Those registries learned how to automate the process. The difficulty lied in the coordination of efforts and associated legal frameworks, as well as research of domains already registered and double-checking of the lists.

Some Conficker A/B domains were already registered. Sometimes, the name was coincidentally registered by a legitimate website owner. In some cases, malware authors had registered the addresses and were utilizing them. Some security researchers working outside the CWG had registered domains to learn more about Conficker. Each of these instances needed to be researched. If the domain were as suspect, the registrars would often "take down" the domain. Domains that were spreading malware other than Conficker were found and taken down during the process. There were rare instances of a website administrator criticizing the fact that his or her website had been wrongfully shut down. However, these incidents did not result in significant problems for the Conficker Working Group. It appears all cases were resolved and misidentified websites were restored promptly.

The effort to coordinate the registration of domains and initial structure for the Conficker Working Group came together at the Global DNS Security, Stability, and Resiliency Symposium in Atlanta on February 3-4, 2009.[28]

The conference was coincidentally organized to discuss potential threats to the DNS infrastructure. At the conference, members of the registry community, law enforcement and ICANN met to discuss the Conficker threat and the attempts to register domains to stop it. Those who met at the conference formed the core membership (leadership) of the Conficker Working Group that was subsequently more formally organized. ICANN became more involved after that meeting. A number of the Working Group participants interviewed pointed to this meeting as the real start of the organization, even though some actions had taken place in January.

Participating at the meeting (via ICANN):

* ICANN senior management and general counsel (Paul Twomey, Doug Brent, John Jeffrey),

* ICANN security staff (Greg Rattray, John Crain, Geoff Bickers, Dave Piscitello),

* Law enforcement (Tom Grasso, FBI/NCFTA),

* Microsoft (TJ Campana),

* GTLD registry operators (Pat Kane and Ken Silva, VeriSign; Ram Mohan and Greg Aaron, Afilias; Rodney Joffe and Jeff Neuman, NeuStar),

---

[28] http://www.gtisc.gatech.edu/icann09

* Security researchers (Paul Vixie, ISC; Chris Lee, Shadowserver; David Dagon, Georgia Tech)

* SSAC Chairman Steve Crocker, Shinkuro.

The registries of the Top Level Domains that were affected by Conficker A and B played an important role in getting the effort to register domains off the ground and determined the makeup of the group early on. Three companies (Verisign, Neustar and Afilias) managed the TLDs .com, .net, .org, .info, and .biz. This made the participation and cooperation of these three companies vital to the effort to register the domains and maintain the effort over time. Additionally, the early participation of .ws helped block a significant number of domains and shared their data with the Working Group. The group was mindful of the failure to maintain the previous battle against Srizbi due to costs.

Among the other top issues discussed was the need to block .cn domains, which would require the cooperation of the Chinese government and the registry operator responsible for the .cn domain (who are connected to the government). Getting China's cooperation was a concern, but turned out to be easier than expected. A fair amount of effort went into preparing the request to the administrators of the .cn domain name (who have strong ties to the government). Chinese authorities responded rather quickly (once a local holiday was over) and agreed to pre-register the domains. Due to China's Internet architecture, once the country made the decision to cooperate with the effort, they easily shut down all potential affected domains. According to some analysts, they even took over domains that were already registered by someone else without researching them first, something that could not be done in most countries without facing significant protest. China chose to sinkhole its own data. Attempts to share the data between China and the US would prove to be a point of conflict in the group.

There were few formal contacts with the US government as an institution, but a large number of connections through personal channels. Several researchers within the Conficker Working Group, without coordinating with others, communicated through their own social networks with the FBI, DHS, DoD and various intelligence agencies. Questions were asked about how law enforcement could help and whether the group could help law enforcement. Later, law enforcement agencies from a number of countries placed representatives on the Working Group lists so they could follow developments, but these agencies were unable or unwilling to formally contribute to the group (though collaboration with specific individuals may have occurred).

On February 12, 2009, the Conficker Working Group was publicly announced and Microsoft offered a $250,000 reward for information leading to the arrest of the worm's creator.[29] The Microsoft reward offer received far more attention than the cooperation of the Working Group. The announcement named as key contributors to the Working Group ICANN, NeuStar, VeriSign, CNNIC, Afilias, Public Internet Registry, Global Domains International Inc., M1D Global, AOL, Symantec, F-Secure, ISC, researchers from Georgia Tech, the Shadowserver Foundation, Arbor Networks and Support Intelligence.

[29] http://www.microsoft.com/presspass/press/2009/feb09/02-12ConfickerPR.mspx

According to the Microsoft SIR report[30], "On the day the Working Group was announced, the group had successfully registered every Conficker domain name for the next 10 days, a genuine—if temporary—victory over the Conficker operators."

On February 12, Microsoft also posted information about the spread of the malware and the domains that it may target.[31]

On February 16, Conficker B++ (called Conficker C by Microsoft) was released. It appeared to be a direct challenge to the Conficker Working Group's efforts to stop its spread. Code within the new variant would allow it to update with a strategy beyond connections to a domain.

On a CWG conference call in late February, the CWG discussed how long domains should be registered, how long the effort should continue, and a potential endgame. These issues were not resolved on the call, but they were constant questions throughout the process. Interestingly, during the call, the group discussed whether the Conficker Working Group should take on other malware using domain generation algorithms or if it should also take on other unrelated malware. It does not appear this discussion went beyond this call, with some members recognizing the group's ad-hoc nature may not translate well to a more permanent organization handling other issues.

Conficker C was released in late February and was officially recognized as a significant new Conficker version as the result of very quick analysis done by researchers, particularly SRI and the Honeynet project, within weeks of the release. SRI released an initial analysis of the worm by March 8. The importance of the ability to quickly analyze the malware should not be understated. It is easy to take the malware analysis for granted in this process because it worked so smoothly and effectively at a few key moments when it was needed. As several interviewees stated, if it had taken six months to analyze the malware and reverse engineer the code that produced the target domain names, it would have been far too late.

Throughout March, ICANN assisted in contacting the over 100 ccTLDs affected. The process for contacting the ccTLDs was done on the fly using the contacts available. Never before had ICANN attempted to coordinate an emergency effort with all the ccTLDs.

The ccTLDs have a broad range technical capacities and resources, with some coordinating regularly with the cybersecurity community and others having more limited interactions. The cultural and language differences at times also made collaboration difficult. Misunderstandings happened as the group attempted to communicate the need to collaborate quickly. Some ccTLDs said they needed to consider domestic regulations. Some claimed they needed court orders if they were to block a domain that had already been registered. One ccTLD accused ICANN of "threatening" them if they did not cooperate, certainly a misunderstanding but an example of the tension this effort was creating.

---

[30] http://www.microsoft.com/downloads/details.aspx?FamilyID=037f3771-330e-4457-a52c-5b085dc0a4cd&displaylang=en

[31] http://blogs.technet.com/msrc/archive/2009/02/12/conficker-domain-information.aspx

In the end, in spite of the difficulties, the vast majority of ccTLDs cooperated with the effort. A few indicated that registering the domains in the manner requested would violate domestic regulations. There were several other countries in which local laws were not clear; the Conficker effort may have spurred local ccTLDs to clarify their regulations.

The exercise of trying to contact all the ccTLDs helped ICANN learn about weakeness in their system, which they are in the process of fixing. They are currently following up on recommendations to identify a specific security contact for each ccTLD and processes for sending messages. While reforms are ongoing, should the need arise again, ICANN feels they will be far more prepared thanks to the Conficker effort.

Increasing coordination across industry and academia combined with adding the ccTLDs to the Working Group meant hundreds of additional people were placed on the e-mail listserve being used by the Working Group. By late March there were at least 300 people on the e-mail list. It had become unweildly for making major decisions. There was also concern among some members that the worm's author may be listening to conversations on the main list.

Partly spurred by the rapidly increasing size of the group and partly due to the increasing demands across all aspects of the Working Group, in mid-March, the group split into various subgroups. The suggestion to split into subgroups had been made earlier, but the growing size made the need more urgent. See Appendix for explanation of subgroup activities.

Daily Operations of Conficker Working Group. Throughout February and March, the day-to-day tactical operations occupied a considerable amount of the group's time. Every day, domains had to be registered. The group would also check on the domains being contacted by Conficker that day and double-check their status. Where collisions occurred (where Conficker-infected computers would attempt to contact a domain that was already owned by someone else), the website would have to be researched. If the website could not be verified as legitimate, the registrar or registry would take the domain down. The website would also be taken down if, as occurred surprisingly often, the website was being used to spread other malware and spam separate from the Conficker effort.

There were a minimal number of instances where a legitimately operated website was shut down and the owner complained. In those cases, the group would discuss and return the website operation to the owner within a short period of time. Considering the rapid and ad-hoc nature of the operation, the error rate appears to be surprisingly low. Some might question the authority of the Working Group members and registries in general to take down domains without any regulatory oversight but it was essential to the containment of the botnet.

Regular reports continue to be produced within the CWG on the number of computers infected and the amount of data contained in the sinkhole servers and distributed to the listserves. At least three reports are distributed to the listserve or a smaller subset of individuals on a daily basis and others are produced as requested by a member of the Working Group. Members of the Working Group also watch for anomalies within the statistics that could indicate the worm was changing in some way they had not detected through other methods.

Considering the heavy workload during February and March, it is also important to note that while some companies had staff working on various aspects of the Conficker threat, many of the Working Group members had full-time jobs separate from or only partially related to their activities on the Conficker Working Group. Many worked on nights and weekends to accomplish these tasks.

The Upgrade to Version C. On March 5, 2009, a number of machines upgraded to Conficker C. On March 7, the Working Group was concerned they would lose control of the botnet on April 1 when C would begin contacting additional domains. However, they knew that only a small percentage of machines had upgraded. On March 10 and 17, by mistake two domains that should have been registered were not and more machines were upgraded. Mistakes such as this were largely due to human error, including individual mistakes in generating the list of domains that would be reached by Conficker, though some structural factors also played a role. While the errors created tension in the group, they also spurred the broader cooperative effort to get ccTLDs involved in the effort to stop the worm.

In a March 19 e-mail to the group, one member wrote: "We've lost the battle from a/b to c". Later analysis indicated that was not fully the case. In fact, many Working Group members today still believe the fight against A/B remains the more important effort. Still, the comment is reflective of the mood of the group at that moment, which appeared somewhat demoralized by the botnet upgrade to Variant C.

Once the computers were infected, the Conficker C variant attempted to reach 500 URLs from a list of 50,000 from 116 different Top Level Domains. The new variant also employed a peer-to-peer update mechanism, which many believe was a larger and more credible threat.

With 110 ccTLDs to coordinate with, the task looked nearly impossible. It had been difficult to coordinate 250 domains per day inside eight TLDs. Yet the group decided to tackle the much larger task. Working Group members discussed ways to scale the mass pre-registration effort for the ccTLDs. Several technological solutions were found. There was some concern, however, that working with the ccTLDs would be difficult.

The Working Group created a briefing that was delivered through ICANN and other channels to each of the ccTLDs. The briefing (known among the group as the ccTLD "go pack"; a public version is attached in the Appendix) explained the threat, why coordination was essential and what the ccTLD would need to do to assist.

Working with the ccTLDs required reaching out at times through the registry operators. Some of the same registries who manage the generic TLDs also manage technical requirements for various ccTLDs. For example, Afilias manages the .info domain, which was affected by Conficker A/B. The company also manages the domains for about a dozen countries including Honduras (.hn), Belize (.bz) and India (.in).

On March 2, the Sophos Threat Lab blog[32] reported that Conficker was set to connect to a domain owned by Southwest Airlines on March 13. Collisions were a regular occurrence, though usually not with such a prominent company. The blog suggested that if Southwest Airlines did not change its domain settings, its entire website could get slowed or even shut down due to millions of Conficker-infected computers attempting to reach it. Southwest redirected its servers the next day to a Working Group sinkhole. While this event was averted, it was one of the more publicized collisions that occurred between real domains and the list randomly generated by Conficker.

Public Relations and April 1. As the Working Group worked on combating Conficker, there was increased media attention to the botnet and the efforts to combat it. This was both an opportunity and a threat to the Working Group. The opportunity was to get needed information to the public including network administrators and inform them of actions they could take to secure their computer. The increased attention also presented an opportunity to learn more about the author and potentially arrest him or her. Unfortunately, the media attention also created tension within the Working Group, made some suspicious about others' motives and diverted time and resources away from the more pressing work to get domains registered.

The first signs of the tension appeared on February 6 when an article at SearchSecurity.com suggested that OpenDNS and Kaspersky Lab were planning to pre-register domains.[33] This article preempted the February 12 announcement of the Conficker Working Group and caused some on the e-mail distribution lists to claim others were trying to take credit for everyone's work. Leadership in the group discouraged talking publicly about the worm. On February 9, a group member convinced a reporter to avoid discussing the Working Group over security concerns.

Microsoft, which had taken the lead on the public relations effort during the first few months, requested that the group hold off until the February 12 announcement and held a conference call with the Working Group on February 11 to coordinate the message and address concerns. There was an understanding that the Working Group was reaching into unprecedented territory in terms of cooperation and they wanted credit as a group, not as individual organizations.

Maintaining discipline in a group in which everyone is a volunteer is not easy or even realistic. A number of individuals spoke with the media. Others felt mildly offended, as if those speaking to the media after people had agreed to avoid it had violated their trust. For those who were to speak to the media, the group discussed details that should and should not be released. They were more willing to talk openly about the size, scope and details of the A/B infection. They were more reluctant to discuss the C variant until the malware researchers had published more about the worm.

---

[32] http://www.sophos.com/blogs/sophoslabs/v/post/3457

[33] http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1347175,00.html

Some of the negative consequences were unavoidable. Every group faces personality conflicts. This is particularly true for an ad-hoc organization with a minimally defined leadership that includes anti-virus companies, registry operators and registrars who compete in the commercial space and researchers who compete in the academic space.

At one point, people questioned why they could not talk to the media when they knew others in the group were briefing the government or private sector clients on the threat. This issue was never fully resolved.

April 1, 2009, the date that Conficker C would begin contacting domains, became the focus of the media hype about Conficker. The upgrade to Conficker C was a significant concern for the Conficker Working Group and one that had spurred far greater collaboration and effort. However, April 1 was only the first day of Conficker C's activity. The chance of the malware author striking on the first day, when the security community's attention was so heavily focused, was highly unlikely.

Despite the media hype, nothing happened on April 1. All of the domains were successfully blocked. Conficker remained active at the same level as usual, but did not attempt to update itself in any meaningful way.

There was knowledge among the Working Group members that April 1 was not necessarily the big day for Conficker C. In fact, FAQs by F-Secure, republished by the Conficker Working Group and given to all interested media, specifically said April 1 was the beginning of a new stage of the malware, but no major events were planned for that day.

Internally, the Working Group was not particularly concerned about an April 1 catastrophe either. In fact, the Working Group had discussions about the problem of overblown expectations in the media over the April 1 date and the fact that it would deter their efforts if and when nothing significant happened on April 1st (a very prescient prediction).

Still, the media focused heavily on the April 1 event. The numbers of articles in the print media increased as did coverage on television news. The weekly show "60 Minutes" ran a segment on the threat. Some in the Working Group criticized the media coverage as failing to provide the proper information.

If there was a positive side to the April 1 hype, it spawned several communications efforts aimed at the public. A number of cybersecurity experts and anti-virus vendors released information leading up to April 1 to better inform the public about the malware threat[34]. The attention also likely led to improved computer security in general, always a goal for many of the members of the group.

[34] One excellent example is the FAQ from the F-Secure blog, which is republished on the Conficker Working Group website http://www.f-secure.com/weblog/archives/00001636.html

Immediately after April 1, one member of the Working Group created an "eyechart" that would help a computer user determine if he or she was infected[35]. It was a small step, but received media coverage and was an example of communications with the average computer user that some members of the Working Group felt was lacking, even within the recent media hype. A variant of the eyechart was used on two major portals in South Korea to facilitate self-remediation.

Eyechart created to test for Conficker:

After April 1. While nothing happened on April 1, 2009, and media attention faded, the release of Conficker E on April 8 certainly got the attention of security researchers. Conficker E used the C variant's P2P capabilities to infect computers with Waladec and a form of scareware for one month. Afterward, the version would revert itself to the C version. Members of the Working Group offered up various theories mentioned in the previous section, but none of them were confirmed.

As of the writing of this report, Conficker E was the last act for Conficker's author. No new variants have been released since and it does not appear the author has attempted to update or send new instructions to the A/B variants or the C variants since that event.

No Endgame for Conficker. Questions about the "endgame" for the Working Group began as early as February, even before the addition of hundreds of additional group members. With the Conficker situation in a stalemate in April and May, the endgame became more urgent and in some ways more relevant for the Working Group. Top level domain administrators wanted to know how long they would have to direct resources to blocking this individual threat. There were also concerns that they would also be forced to deal with new threats. Nearly all of the ccTLDs agreed to continue blocking domains through the end of 2009, but did so with a mixed level of enthusiasm and concern.

[35] http://www.confickerworkinggroup.org/infection_test/cfeyechart.html

The Conficker Working Group had discussed remediation efforts previously, but now began a sub-group dedicated to remediation.

By May, the amount of discussion on the Conficker Working Group email lists had quieted significantly. There was an acknowledgement among the leadership that the work continued, but without new variants appearing, there was less of the "organized panic" as one person described the events of March. Symantec estimated publicly that the worm continued to infect 50,000 machines per day (some were reinfections).[36]

There were already indications that Conficker and the effort to counter it were having implications for the broader cybersecurity community. President Obama's cybersecurity report was released in late May and the president mentioned Conficker in a speech after the report was released:[37]

> "No single official oversees cybersecurity policy across the federal government, and no single agency has the responsibility or authority to match the scope and scale of the challenge. Indeed, when it comes to cybersecurity, federal agencies have overlapping missions and don't coordinate and communicate nearly as well as they should -- with each other or with the private sector. We saw this in the disorganized response to Conficker, the Internet "worm" that in recent months has infected millions of computers around the world.
>
> This status quo is no longer acceptable -- not when there's so much at stake. We can and we must do better."

The members of the Working Group understood President Obama's comment not to be directed at them, but rather the federal government. As discussed in sections below, the government's coordination with the Working Group was limited and contributed little to the private sector effort.

The Working Group fixed a problem creating discrepancies identified in the daily reports between the domains that had been registered or taken down and those that Conficker was generating that day. Several domains slipped through the system, only to be registered at the last moment when they were caught by people double-checking the domains. Systemically, this came from an error in the database generation that had since been fixed by the group working on malware reversal. It was an overall good sign that the group was able to recognize errors and correct them before they became significant problems that would lead to an update of the botnet.

---

[36] http://viewfromthebunker.com/2009/05/20/conficker-continues-to-spread/

[37] http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

ICANN held meetings in Sydney, Australia[38] in June 2009 and Seoul, South Korea[39] in October 2009 in which discussions about Conficker were prevalent. The repercussions of the worm have led to the discussions of new policies regarding DNS security.

Some of the ccTLDs have indicated that they will no longer cooperate with the effort to block the updating of version C[40]. For a variety of technical reasons, this remains less important than the blocking of the A/B variations, but it is still a symbolic loss. The cooperation of the ccTLDs was a major victory for the Conficker Working Group.

What Comes Next, The Group Debates. The Conficker Working Group has labored to maintain a stranglehold on all the A/B domains and as many C domains as they can. At this point, several million domains have been blocked since registration efforts began in January 2009. The only known slips in the domain registration effort were the two in March that allowed B to upgrade to C. Working Group members now pre-register the domains months in advance, but still double check the list of domains immediately before the day the Conficker-infected computers will contact them. Sometimes a domain is unregistered due to technical or human error or a domain that is registered outside of the Working Group appears suspect and they work to take it down.

When asked, most members believe the Working Group will remain intact, focused on Conficker as long as that threat remains. They stress that it remains important to block the A/B version from receiving instructions or updates. With millions of computers remaining infected with Conficker A/B, it could be taken over by the author again should the effort to block the domains wane. Fortunately, all of the registry operators and TLDs that began this effort and are necessary to block the A/B domains remain actively involved and willing to assist.

The group does not plan to take on additional tasks or attempt to counter new threats beyond Conficker. They continue to block tens of thousands of domains per day and in the words of one member, "It will remain in place while the threat is out there."

---

[38] http://syd.icann.org/

[39] http://sel.icann.org/

[40] Some TLD operators feel that they bore high costs in the time and resources they spent blocking domains and investigating "collisions," even though ICANN had waved the fees. Additionally, some remain concerned about the legal and regulatory framework in their countries.

IV Analysis and Lessons Learned (what worked, what didn't)

This section looks at what lessons can be learned from the efforts of the Conficker Working Group.

Interviews were not overly structured and the respondents provided a free flowing account of events and recommendations. For the purposes of standardization, every interviewee was asked the following seven questions:

* How did you (or your organization) become involved in the Conficker Working Group?
* In your opinion, what were the goals of the Conficker Working Group?
* Did the Conficker Working Group succeed at those goals?
* What worked?
* What did not work? Where were the breakdowns?
* If you could go 12 months into the past and give yourself a recommendation regarding the fight against Conficker, what would it be?
* What lessons should be applied to future groups?

Where possible, the interviewer followed up on answers for greater detail and insight.

1. How did you (or your organization) become involved in the Conficker Working Group?

This question provided insights into what brought each individual or organization into the Working Group from both a specific (social network, who knew whom) and generic (what was their interest/motivation/capability) approach.

Many of the core members of the Conficker Working Group knew each other prior to the effort or were within one degree of separation through various social networks. As one interviewee said, "we all knew each other." Many had worked on previous efforts to combat specific pieces of malware and were on the same security lists. One person noted that if you were to compare a list of the people involved in the Conficker Working Group effort with other efforts, 80-90% of the names would likely repeat.

As the group grew larger some of the trust models broke down. Individuals and organizations began entering the group who had limited connections to what had been a fairly closed social network built on trust and verification mechanisms.

One researcher was outside the official group and not on the email lists for over a month, although he was in regular contact with several Working Group members.

Another researcher, who joined the group over a month after it was officially formed, said early on "nobody invited us." This was not meant as a condemnation of the Working Group, but was a

sign that the informal and ad-hoc nature of the group's organization in the early stages managed to exclude potential stakeholders by unintended omission. In other words, the group was open to new members who could be verified through social networks, but did not focus on bringing in new people.

The same researcher also asked colleagues who were regular participants on similar efforts why they did not participate heavily in the Working Group. One, who manages a listserve, said he lacked time and wanted to focus on other malware. Another indicated, as above, that he "wasn't invited" and didn't consider becoming a member an option.

Social networks explain how specific people came together, but not the motivations of those individuals and organizations involved. Why would organizations and individuals become involved with the Conficker Working Group and what incentives would push them to collaborate with future organizations? This was a key question that a number of the group's organizers suggested that this research examine.

Responses to this question suggest individuals had several motivations for being involved in groups such as the CWG, including:

* General altruism for stopping a threat
* Cooperation rather than competition on a threat
* Coordination of research and sinkholing of data
* Public relations benefits
* Networking with other professionals
* Monetization of research and data
* Damage control
* Concerns of being on the outside

Core members of the Conficker Working Group put in many hours of unpaid time and effort, each indicating they wanted to stop a legitimate and potentially dangerous threat in cyberspace. Nothing in this section is to imply that they had other motivations. From a broader perspective, however, it is important to ask what motivates organizations and individuals to become involved and why they maintain their involvement over time. Not all threats rise to the level of Conficker and the most people who work as volunteers on cybersecurity threats have jobs and personal lives that would limit their involvement over time.

With much of the Internet infrastructure controlled by the private sector, there is a common opinion that the market will work to take care of Internet security as a whole. This point of view suggests the government has a limited role to play in broader cybersecurity efforts such as the Conficker Working Group.

Yet, motives are important if the goal is to understand what is required to replicate the success of this structure. The early members of the Conficker Working Group self-organized to deal with a specific situation they all independently recognized as a threat to the larger community. No particular institutional mechanism created or called for the group.

The cybersecurity community was ripe for this sort of collaboration. The recent experience with Srizbi helped push the idea of defensive DNS. Conficker's method of going after the DNS system by bringing in the registrars and the ccTLDs was unprecedented. Again, existing social networks allowed stakeholders to connect with each other efficiently with trust and validation.

Several interviewees warned that Conficker was like no previous threat and the next threat will not be like Conficker. The same motivations that brought together the Conficker Working Group would result in a different formation in the future, with some similar actors and some different.

For that reason, many of the Working Group members indicated that a standing organization to handle these threats might not be the proper way to manage them.
However, as described in the answers to the recommendations question, there is a need for social networks, resources, and tools for collaboration and possibly for the group to operate.

2. In your opinion, what were the goals of the Conficker Working Group? 3. Did the Conficker Working Group succeed at those goals?

The Conficker Working Group did not set out with formal goals. While the generic goal was obvious (fight Conficker), they had not defined the exact endstate they were trying to achieve. When the group came together in January, they recognized they were attempting an unprecedented level of collaboration, but most did not expect the group to grow to the size that it did or last as long as it has.

In the press release[41] that launched the Working Group on February 12,

> Microsoft Corp. announced a partnership with technology industry leaders and academia to implement a coordinated, global response to the Conficker (aka Downadup) worm. Together with security researchers, ICANN and operators within the Domain Name System, Microsoft coordinated a response designed to disable domains targeted by Conficker. Together with security researchers, Internet Corporation for Assigned Names and Numbers (ICANN) and operators within the Domain Name System, Microsoft coordinated a response designed to disable domains targeted by Conficker. Microsoft also announced a $250,000 reward for information that results in the arrest and conviction of those responsible for illegally launching the Conficker malicious code on the Internet.

The interviewees agreed a key goal or the key goal was to prevent the author from updating the infected computers, control of the botnet and use of it to launch a significant cyber attack. However, some focused more on how Conficker affects the average computer user, while some worried about the bigger picture threat of the damage that could be caused by the botnet composed of five million computers.

---

[41] http://www.microsoft.com/presspass/press/2009/feb09/02-12ConfickerPR.mspx

Interviewees described the goal differently. Campana of Microsoft used the term "protect" with a focus on giving Microsoft customers time to update their computers to block or remediate the infection. Another member of the working group described it as "grabbing the bull by the horns and controlling it." A third described it as "preventing a disaster" that could occur if the author utilized the botnet to its full extent.

One person said, “the goal was hazy... need to define the goal and make preparations to get there.” One person indicated that the group in February believed they “could patch our way out of the problem,” meaning that they just needed to stall the botnet long enough for Microsoft and AV software to get the proper tools to their customers.

Preventing a major cyber attack. All but one person said the Conficker Working Group was a certain success or qualified success in terms of slowing the spread of malware and generally preventing the author from utilizing it for a significant cyber attack. One interviewee said, "we made one guy's life really hard for a while. Many malware authors look for a quick buck and face relatively little resistance. We made sure this guy [Conficker's author] would have to work for it.... We may have deterred him by making it a bit harder to implement."

More broadly, the effort may have “sent a message” to malware authors that the security community can coordinate at blocking their efforts to exploit domains. “They [the malware authors] were increasing the number of domains used for each botnet as the community got better at blocking them. Conficker’s increase to 50,000 [domains per day] was the natural Darwinian evolution of that battle.” That person went on with the metaphor, “Each side was playing increasingly better chess… the cooperation from the ccTLDs and ICANN’s decision to waive the fees tipped the chess board over and told them the game was over.”

Although the February 12 Microsoft press release focused on obtaining information leading to the arrest of the authors of Conficker and the US$250,000 reward that Microsoft offered, the issue barely came up in discussions among the Working Group members.. In interviews in which the goal was mentioned, it was seen as a failure but not one the CWG was responsible for.

The inability to attribute Conficker to an individual or group remains a key failure of the effort to combat Conficker and eliminate the threat, but as several interviewees stated, the responsibility for identifying and capturing criminals should fall to law enforcement agencies. Members of the Conficker Working Group said law enforcement had been cooperative from the beginning. The Group also expressed a willingness to assist law enforcement, but some expressed confusion over how they could best help and what the limits of their assistance should be. One person said that more private sector cybersecurity experts would be willing to help if they weren't concerned they would become part of a court case over chain of evidence issues. Two interviewees said governments could help by increasing the funding and research for cyber-forensic technologies and increasing the funding for investigations.

Remediation. At the same time, at least five million infected computers continue to exist and the author was never captured or even identified. For those who mentioned remediation as a goal, the words "absolute failure," "complete failure" and "barely even touched" were used. One said the group should never have taken on the task of remediation as it was an impossible goal.

Others said the task should have been taken on in a more comprehensive manner, though strategies to do so were limited. One member of the Working Group said he wished they had tackled remediation from the beginning and gone about contacting infected ISPs in a more comprehensive way[42].

Research. On the goal of research, the view was that creating a system to coordinate the sinkholing and sharing of data was successful. Coordinating the registration of domains was necessary to ensure a comprehensive defense. It also allowed for the centralization of data about the infected computers attempting to reach those registered domains. The researchers eventually created a structure that standardized the format of the data collected.

Several researchers did question whether that data was utilized as well as it could have been. Once sinkholed, it is unclear whether the group was doing everything they could to identify infected computers and answer questions about why the spread of the malware remained persistent.

Another concern among some of the interviewees is the need for collective research to counter the threat versus the trend among some in the security community towards monetization of data about affected computers. In other words, there are those who would register domains as a way to sinkhole data and then use that data to sell remediation services, which may or may not interfere in efforts to collectively tackle the problem. Also a concern, in the hands of cybercriminals, sinkhole data could provide them targets for exploitation. For these reasons, Georgia Tech was chosen as a neutral site and data sharing agreements were organized to ensure the maximum contributions to the research effort while maintaining security of the data and privacy for those who requested it.

Informing the Public. A few people indicated informing the public about the threat was a goal. Some members of the group feel more could have been done to provide information to the average computer user and to ISPs. There is a recognition that the media hype surrounding the April 1 deadline produced as one member said, "more heat than light," when it came to informing the public.

Beyond Conficker. At several points in March, April and beyond, the group did consider questions about goals in various e-mail exchanges. They raised questions about taking on additional tasks beyond Conficker (other malware that tapped into the DNS system or other malware in general). Several indicated Conficker was simply a portion of the large and growing problem of malware in general. There were concerns that addressing a single issue was playing in the margins of the larger cybersecurity problem.

On the issue of goals in general, one interviewee recommended defining the goal early, visualizing the endstate and then laying out the steps to get there; while that person said the

---

[42] In December 2009 the Shadowserver Foundation pushed forward a new effort to publicize infections by ASN as part of a new remediation effort. Their effort can be found here: http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker

organic and ad hoc creation of the Conficker Working Group functioned, the group could have been organized and functioned better had the goals been considered earlier. This suggests that even if future groups are formed ad-hoc, they should stop and consider their goals and scope.

4. What worked?

This question was asked allowing an open ended answer, although the researcher did follow up looking for "What worked from a management or organizational level?" where possible when answers focused more on goals achieved or technical details. At times, the answers for what worked and what did not overlaps with the answers for whether goals were accomplished.

Private Sector Collaboration. The Working Group structure itself was a successful example of private sector collaboration and a model for future efforts according to most of the membership. Collaboration on security threats has existed for years and there are constantly multiple (often overlapping) efforts to coordinate against various malware threats. Several interviewees described the CWG as a "shift" in the collaboration model. More than one interviewee said it was the first truly successful effort they were involved in after a decade of attempts to collaborate.

Informal Organization. While the lack of formal organization may appear to be a negative to some outside the group, many members of the group said the informal structure, "the meritocracy and self-policing" as one person said, were positive for the Working Group. They ensured that all voices were heard and no individual felt they were being overruled or taken advantage of by a rival company. The consensus model kept the coalition together and did not force polarizing decisions that could have split the group. Importantly, the lack of formal structure also allowed the group to adapt more easily as the malware changed and the group added more members.

Strong Social Networks That Facilitate Trust. The informal social networks that brought the group together appeared to work for most of the people in the core group. However, it also resulted in unintended omission of other potential stakeholders from which the group could have benefited. Biases could also emerge, as those not inside the social networds or who did not become members may be hesitant to state their objections.

Sub-Group Structure. The sub-group organization was successful and is already being used as a model for future groups. However, several people expressed the importance of communication between the sub-groups and the core group and the obligations the sub-groups have to the group as a whole.

Data Sinkholing. The coordination of the sinkhole effort was largely successful. Much of the data was sinkholed on servers and shared with most who requested access. With all the flaws considered (access, data format, who owns the infrastructure), this should be considered a model for future groups. The agreement to share data was important to many of the companies that participated.

Cooperation from ICANN and Top Level Domains. Members of the Working Group were especially pleased with the cooperation and coordination of ICANN and the ccTLDs in the

process. They view ICANN and ccTLD cooperation as a precedent that will help future efforts and discourage malware authors from believing they can easily exploit that portion of the DNS system. Several said they want this emphasized publicly to reinforce that message and thank those organizations for the job they did.

5. What did not work? Where were the breakdowns?

"Don't gloss over the failures." More than one interviewee insisted on the importance of articulating the mistakes or difficulties faced by the CWG, even before the question was asked. While the majority of those interviewed said the CWG was more successful than most efforts and saw an unprecedented level of cooperation, there was also an acknowledgment that the success was limited.

A number of the areas that the interviewees described as not working were the expected result of something that worked or a decision that was better than the alternative. The group needed to be inclusive to be successful in spite of the drawbacks of making it too big. A group of volunteers collaborating in an ad-hoc manner faced obvious difficulties in tasking and accountability of its membership. The split into subgroups meant glitches in management, communications and transparency within the group, but was widely praised as a better alternative than keeping all the discussion on the central email distribution list.

Remediation. The ability for the group to remediate infected computers was limited in its success, and was not a central goal of the group when it was first created. The focus of the group's efforts over the months of February and March was not on remediating computers, though certainly individuals and organizations conducted remediation activities outside the CWG process.

One person suggested that a reason remediation was hard is there are some financial models for groups that provide remediation to specific ISPs, while there are none to clean up cyberspace as a whole. That individual suggested there may be ways to incentivize remediation efforts if funds from the private sector or the government could be obtained.

Communication with ISPs. Several people pointed to uncoordinated communication between the Working Group and ISPs as a weakness. Members of the Working Group tended to coordinate through their own formal and informal social networks to reach out to ISPs, a process many felt could have been more systematic.

Collaboration with the US Government. The group as a whole saw little participation from the government. One person put it as “zero involvement, zero activity, zero knowledge.” Those interviewed did not necessarily express a clear consensus on what the government role should have been, with some expressing a desire for greater communication and collaboration while others indicated that they felt the private sector is more capable of managing the effort.

With that said, one area the U.S. Government did participate indirectly was through malware reversal. SRI's research is funded by the US government and played an important role in the process.

Information sharing with the US Government. Most participants who commented on the issue felt information sharing between the Conficker Working Group and the government was one way, with information flowing from the group to the government, but without receiving information in return. A few said they had two-way information sharing with the government, but that was not done at the group level but through personal contacts.

Public Relations. One interviewee said "public relations worked reasonably well through March 12," but then companies and individuals started straying from the talking points and putting out individual releases. Public Relations efforts at times did more to increase hype than to help deliver pertinent information. It is possible that statement is more a reflection of the media environment than anything that could have been said or done by the CWG. However, as one interviewee noted, more should have been done in terms of considering audiences in communications. Speaking with cybersecurity experts is different from speaking with ISPs or individual computer users. Each needs to receive a different message about the security of their systems and what they must do to protect or remediate their computers.

Lack of Accountability. There were breakdowns in the group's model. Computers were updated from Conficker B to C after the group failed to register three domains in March. Human error was the main cause. Groups must be prepared for error, hold people accountable and have backup systems in place. However, because the CWG was composed primarily of volunteers, many of whom had full time jobs, and it was still building new systems to register many domains, it was hard to find time to double-check lists and accountability was difficult to establish and enforce. A few suggested resources for a small staff (2-3 people) to do the day-to-day tasks may have prevented some of the errors, but some interviewees indicated that errors may have occurred anyway.

However, this also speaks to the tenuous model on which the CWG's strategy depends. They needed near perfection to prevent the botnet from updating and receiving instructions from the author. Interviewees said the author, if truly determined, would find an error in their preventative registration and exploit it.

Challenges of Sub-Groups. While praise for the sub-group model was nearly universal, several interviewees also pointed out the drawbacks inherent in this structure. In particular, the groups did not necessarily interact or communicate well with each other or the core group. As authorities in an all-volunteer group were limited, there was no formal mechanism to force the sub-groups to report back all of their activities to the core group. Certainly there were members of the core group on each of the sub-groups, but the segregation created by separating out the tasks broke down some of the initial benefits of bringing together a cross-disciplinary group.

Lack of Tasking Authority. Many people had mixed feelings about the informal nature of the group when it came to assignments and tasks. While there were never formal contracts set out for individual roles and responsibilities, the responsibilities were clearer in early February when the

group was small. However, as one interviewee said, "it was a coalition of the willing... we couldn't force anyone to do anything they didn't want to do, because they'd quit."

Inclusion vs. efficiency There is an essential paradox to the size of the group that the CWG never quite resolved and which other groups currently face. On 11 February, a day before the group made a public announcement, there was a discussion about the proper size of the group, foreshadowing the issues that were to come as hundreds of individuals and organizations joined in March. The group needs participation in order to share information and collaborate on the solution. However, they lose a streamlined decision-making process and they lose some of the trust that can be maintained more easily within smaller organizations. Much of the private sector cybersecurity community relies on trust mechanisms to ensure their data and ideas are guarded. As problems grow, they must work with ccTLD operators and those ISPs infected with the malware, many of who fall outside the usual circle of known individuals.

The group acknowledged that paradox in the interviews. One member said "Yes, [the group] got too large," and followed it up by saying the addition of members in March "was a necessary expansion... important not to be exclusionary."

Regarding the necessity to share information with those who aren't vetted within the circles of trust, at least three people noted, "You can't control who gets infected." As one said, "At some point you have to give information to those you don't trust" in order to halt or remediate infections.

6. If you could go 12 months into the past and give yourself a recommendation regarding the fight against Conficker, what would it be?

This question is effective at identifying recommendations for future groups. Responses fit into three main areas: 1) the intensity and length of the effort to combat the malware, 2) the organization and goals of the group, and 3) the jobs of the specific individuals involved.

Understanding and preparing for the long-term implications of the effort. Some version of "preparing for a longer term effort" was the top answer given by the interviewees. One person indicated that a specific task related to malware reversal and encryption would take at least six months, but that they did not start on it because they believed that the coordinated effort would not continue that long.

Related to the long-term nature of the effort, several members of the group cited burnout as a key breakdown. The group was not prepared for the long-term effort and they could not maintain the momentum indefinitely, being the volunteer effort that it was.

This also becomes a key issue when dealing with the broader threat environment. One interviewee said the community was "overwhelmed" and "fatigued." Another said everyone was "wringing their hands" over the increased threats. If the cybersecurity community can be burned out by a single piece of malware, what happens when several major threats exist at the same time?

The endgame is important. None of the people working on cybersecurity wants to fight a never-ending battle against a single threat. Burnout on problems like these is not just possible but likely. That said, defining success as the full annihilation of a security threat may not be feasible. Instead, the community needs to define its success as managing the threats in a way that avoids burnout but the bigger picture in sight.

Consider the organization and split into subgroups earlier. As there was near unanimity on the importance of the sub-group model, the recommendation to split into sub-groups sooner was not surprising. Interviewees indicated that several working groups organized since Conficker have adopted the sub-group model from the start due to this lesson.

One core member said that he would have recommended "putting in place a more organized and better defined leadership group starting with the Atlanta meeting." Several indicated that defining the contributions and requirements of the members more in detail could have helped avoid some of the errors and tensions. "Early on, everyone knew what their jobs were," said one, indicating that the model broke down as the group grew in size.

Consider the motivations of those involved. A number of members said suggested the need to be more aware of and prepared for the motivations of those involved in the group. This is a sensitive topic and overall the group members have high regard and respect for one and other. One member said, "ego, pride and politics in the info security world... detracts from the effectiveness of cybersecurity efforts."

Some of the same people praised the broader sense of altruism in the group, in spite of criticizing motivations. One person said, "people put in hours of unpaid work on nights and weekends, often at the expense of their own free time or time with their family." Another said, "[whatever the other motivations], we all do this because we care about the security of the basic infrastructure and philosophy of the Internet."

Concerns over commercial competition certainly existed can be successfully overcome. Many companies joined the CWG with considerable reservations over the potential that their work in the group could undermine their position vis-a-vis their competitors in the cybersecurity space. Yet, largely, the concerns over commercial competition were overcome by the CWG.

7. What lessons from what worked or didn't work should be applied to future groups?

Asking about recommendations produced a wide variety of thoughts from the group membership. Some of the recommendations are implied in the answers to the other questions above. Others were directed more at the broader cybersecurity environment than at groups combating specific malware in the future. Not surprisingly, those interviewed provided recommendations that at times overlapped with previous reports including the recent White

House Cyberspace Policy Review[43] released in May 2009 and the General Accounting Office report on Cyber Security[44] released in March 2009.

The need for collaborative infrastructure.
The single most common recommendation related to the need for an infrastructure to help the private sector collaborate to counter threats in cyberspace as they appear.

There are already a number of standing informal groups within the private sector that provide secure email listserves or websites to discuss threats. These groups are growing capabilities.

No one recommended a standing organization to manage all threats. "Every threat is different" and "competition is good" were two common themes. The formation of small working groups within a large architecture of collaboration was the preferred model and the one the private industry is already implementing. One interviewee described the process as the need for the community to "self-organize and re-self-organize" as new threats emerge.

Groups managing threats will continue to rely heavily on volunteers and industry support. However, several interviewees said additional resources would assist. Some felt these resources should come from private industry while others thought there should be mechanisms for government funding depending on the threat.

When asked what specific resources were needed, one interviewee said a group as large as the Conficker Working Group could have used a full time project manager, some administrative support, and one or two technical staff to assist with the daily tasks, while volunteers continued to do a majority of the work. Others provided formulations that were strikingly similar, never exceeding 4-5 paid full time staff.

Organization and management of future groups. New groups handling specific malware are already being formed in the private sector and are looking to the Conficker Working Group as a model.

Per the lessons learned above, the group should have decision-making processes formalized early. Interviewees said the groups should (and will) run on consensus rather than a top-down structure, but they should not defer to certain individuals with experience in such a way that it would impede the decision-making process.

The suggestion to utilize the sub-group model from the start is already being implemented by a number of private sector groups focused on new malware threats. Two interviewees stressed and others mentioned that sub-groups should have a clear mandate and work closely with the leadership group to ensure information is shared.

On the issue of accomplishing tasks, one person said, "things took longer than they should" due

---

[43] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[44] http://www.gao.gov/new.items/d09432t.pdf

to the lack of resources or personnel dedicated to specific tasks. Another took a somewhat different view, "only tasks that are short and pointed get done... tasks that last more than a few days get lost."

As mentioned above, the lessons from coordinating sinkhole data and information sharing about the infected computers taken from Conficker should be brought forward. Shared data rather than data scattered across multiple networks allows for more comprehensive research and analysis.

As the private sector relies heavily on trust networks, interviewees noted the necessity of forming them ahead of time and instituting processes to vet individuals who are outside the usual social networks. One interviewee, describing the trust networks that exist, said the private sector cybersecurity community must fight against its natural tendency towards insular relationships and invite more people into the networks. Someone must reach out to organizations and encourage them to participate.

Greater cooperation between industry and government. There was significant disagreement among the group as to the amount and type of government cooperation. Regarding fighting malware such as Conficker, one person said, “It's not really the government's job,” while another said, “It sounds like the sort of thing government ought to be doing.”

In general, recommendations referred to cooperation between the private sector and the US government, but interviewees also stressed the importance of governments around the world. Several indicated that one reason the US government should have more of a supporting than a leading role in organizations like the Conficker Working Group is that it would complicate and politicize efforts at international cooperation.

When prompted about recommendations related to government actions, a number of individuals said there should be funds for assisting with collaboration infrastructure and organization. One interviewee said, “there aren’t many sticks the government could apply, but there are certainly carrots they could offer to encourage better collaboration [over competition].”

Government can play a role publicizing and raising awareness about the cybersecurity threat. For example the public needs to be reminded to update their computers to prevent malware from spreading in the first place. Individuals need to choose strong passwords. These are basic recommendations, but they are necessary. Communicating to the public about basic computer security can have a major impact on mitigating the effects of malware.

Every interviewee who discussed the issue said law enforcement activity must be a major component to defeating cyberthreats and must be strengthened.[45] One interviewee said, "Industry is essential, but can only keep a lid on the problem... law enforcement activity is essential to solving these threats." Others indicated that a law enforcement solution to a threat like Conficker might be the only effective method to ending it permanently.

---

[45] This also matches recommendations made by the GAO.

Information Sharing. On government involvement and information sharing: "They have people [on the lists], it's a one way street that doesn't work." Government must share information, not just consume information. As one interviewee said, the US government "should not just leech off the process." Also of concern on this issue, one person noted, "DOD and NSA don't have taxonomy for sharing info outward."

There should be guidelines for information publication and sharing before the event begins. At several phases in combating Conficker, time and energy was spent debating the rules and norms of what information could be publicly released about the botnet structure and expansion (depth, location of machines). This was particularly true for the Honeynet paper analyzing the Conficker worm, which the group debated and eventually requested to have a portion redacted.

The government must acknowledge the research done in the private sector and give it proper attribution. Many members of the group found it quite disrespectful that research they had done was presented verbatim in classified government briefings without proper attribution. However, as one person noted, plagiarism of the group's work is actually an academic security concern. Initial malware reversal research was done quickly and those doing the research needed secondary confirmation. Not having properly attributed reports can create circular reporting mistakes in which research is accidentally self-verified and not legitimately double-checked until it is too late.

Early warning and taxonomy. While no Working Group member mentioned this specific recommendation unprompted, the recommendation of the GAO that government "Bolstering cyber analysis and warning capabilities"[46] seems implied by the narrative of the CWG actions and several people discussed the issue tangentially.

A number of people recognized Conficker's threat in December and January. Members of US-CERT were not added to the Conficker Working Group list until mid-March.
A more formal early warning mechanism should be established between the informal networks of cybersecurity experts and the US government. The US government received information about Conficker through a number of informal channels, and as one interviewee stated, "informal communication worked." However, relying on informal mechanisms to inform the government of threats may not be the best practice and may have led to different parts of the government inconsistencies.

Potential legal and regulatory reforms. Several interviewees recommended legal reforms that would empower cybersecurity defenders. There were concerns over the potential application of anti-trust laws to organizations in which the private sector collaborates to take on a security threat. There were also concerns that laws that are meant to stop cyber crime but may do more to stop cyber defenders.

[46] http://www.gao.gov/new.items/d09432t.pdf

Rodney Joffe of Neustar wrote in Canada's National Post on October 23, 2009:[47]

> Finally, we must recognize that our laws are woefully inadequate and out of date. They don't begin to recognize the global nature of cyber crime. We have to understand how the criminals "game" our system, and make carefully considered changes. We need to bring international pressure to bear on governments that support or protect these criminals, and we have to make sure we don't make errors in legislation that end up hindering us from dealing with the problem. A prime example of a rule that must be reconsidered by Parliament is the law that was enacted to criminalize the placement and execution of computer programs on a computer without the owner's permission. While this law was designed to stop cyber criminals from doing what they now do with impunity, it has actually blocked computer scientists and government from releasing countermeasures — the equivalent of vaccines — to disable the malicious software.

Group members were aware their viewpoint on some cybersecurity laws and regulations may not be shared by everyone, but one person put it, "there needs to at least be a public discussion on the balance between security and privacy... more Congressional hearings may help." Another person suggested that the individuals and organizations who work on a number of cybersecurity efforts like the Conficker Working Group should potentially do more to push the debate at the national level: "We complain, but how many of us have picked up the phone to call members of Congress with our concerns? I certainly haven't.... Perhaps that's the next step." There was an indication that having a public debate and discussion on the topic was as important as obtaining their specific recommendations for regulatory reform.

Another discussion was raised by those studying Conficker's infection of medical equipment. Conficker managed to infect a number of computers related to hospital medical equipment that were connected to the Internet and improperly patched. Even after computers were remediated, they were then reinfected through USB channels. The patching process for medical equipment as well as the regulations governing USB drives in medical equipment should be looked at by proper regulatory agencies. This paper makes no recommendation other than to review the issue.

The strategic level. Cybersecurity experts are facing attacks that are increasing in number, size and sophistication. Consideration needs to be given to the larger threat environment and prioritize where the limited resources for cybersecurity should be allocated (and where they shouldn't). One person said that some individuals must stay focused on the strategic threat environment rather than the "latest bright shiny object," like Conficker. Another asked, "How many threats exist? What are the most immediately troubling? What have the potential for long-term damage? Nobody appears responsible for that."

Several interviewees were asked whether the cybersecurity community could have handled "two Conficker-level threats at the same time." The answers differed. One person said, "we would have found a way to do it." Another said, "No chance, one of them would have gotten past us." A third person suggested that the scenario had actually occurred: "One reason Zeus got so big was

---

[47] http://network.nationalpost.com/np/blogs/fullcomment/archive/2009/10/23/rodney-joffe-the-cyber-crime-epidemic.aspx

we were all working on Conficker."

A number of these security researchers expressed views from a “red team” point of view related to flaws that could come from Conficker. However, no one organization is responsible for documenting and preparing for those potential threats. One problem is a legitimate fear that documenting some of the threats could provide a roadmap for the malware authors.

Finally, "Take the fight to the enemy... Go on the offensive." was how one interviewee described a key strategic lesson learned from Conficker. Several people saw the Working Group's success as proof that actively countering malware was effective and necessary. "Playing only defense is no longer an option," said one. Another said, "The fight can't be won by just building bigger firewalls and better AV [anti-virus software] and intrusion detection."

V Conclusion: Moving forward

Calling Conficker a "test run" is not meant to minimize the threat that it posed and continues to pose. However, in many ways, Conficker did serve as a test run for the cybersecurity community to learn where their strengths and weaknesses were. One person said, “In some ways, we’re thankful for Conficker… It helped us get things done we couldn’t before.”

Even after Conficker, as stated near the beginning of this paper, the threats in cyberspace are growing in size, scope and sophistication. The researchers in the private sector and academia are working hard every day to prevent potential attacks. Combating Conficker required hundreds of man-hours. While the effort to combat no single other threat at the moment arguably reaches the scale of the CWG, the combined efforts to combat the next top 20 pieces of malware easily do so. Many of the same people who worked to combat Conficker are also working on those threats.

Several interviewees stressed that the malware authors learn and improve with each major engagement against the community and that it’s important that they do the same.

APPENDIX A – Conficker Working Group Background

Conficker Working Group Members

- 1and1
- Afilias
- AOL
- Arbor Networks
- Cisco
- ESET
- F-Secure
- Facebook
- Georgia Institute of Technology
- Global Domains International
- IBM-ISS
- ICANN
- Internet Storm Center
- Internet Systems Consortium
- IT-ISAC
- Juniper
- Kaspersky
- McAfee
- Microsoft
- Neustar
- NIC Chile
- SecureWorks
- Shadowserver
- Sophos
- SRI International
- Support Intelligence
- Symantec
- Team Cymru
- Trend Micro
- Verisign

Interviews

Interviews ranged from 30 minutes to 2 hours, with most lasting more than an hour. One member provided a written write up of their participation in lieu of an interview. Several individuals were interviewed twice. When appropriate, additional off the record discussions were held beyond the interviews. Several interviewees provided documents that were used to verify or clarify information within this report, but cannot be released publicly.

- Greg Aaron, Afilias
- T.J. Campana, Microsoft
- John Crain, ICANN
- Thomas Cross, IBM
- David Dagon, Georgia Tech
- Andre DiMino, Shadowserver
- Barry Greene, Juniper Networks
- Rodney Joffe, Neustarr
- John Kristoff, Team Cymru
- Chris Lee, Shadowserver
- Andre Ludwig
- Ramses Martinez, Verisign
- Jose Nazario, Arbor Networks
- Phil Porras, SRI International
- Rick Wesson, Support Intelligence

Subgroups

Subgroup description
Partly spurred by the rapidly increasing size of the group and partly due to the increasing demands across all aspects of the Working Group, in mid-March, the group split into various subgroups. The suggestion to split into subgroups had been made earlier by various people in the group (it was seriously considered around February 20th, but did not happen). However, with the group growing, the need became more urgent.

Nearly every interviewee said the decision to split into subgroups was necessary and largely successful. Each of the subgroups allowed for greater collaboration on specific details within the effort. They also allowed for a new round of vetting and a new level of trust in the lists. One drawback from the subgroup model was that many people, including some within the leadership, lost visibility over the entire strategic level of effort.

The group's activities were divided into the following subgroups:

- Core Management
- Malware analysis
- DNS registration
- Sinkhole data
- Remediation
- Public Relations

Core Management.
Core Management involved about a dozen individuals who made the key decisions for the organization. The group was largely self-selected. The official “core” group email listserve formed once the original Working Group general group became too large and unwieldy to make

decisions. There were a few disputes about who should be on or off the core group, but these were largely decided with a consensus of the members.

The leadership of the Core Group was chosen informally by the members. Early leadership decisions were deferred to Microsoft's representative on the Working Group, T.J. Campana. This was mostly due to Microsoft's role in patching the exploit. Later on, the official leadership role moved to Rodney Joffe. Both Campana and Joffe were praised by a number of the interviewees for their efforts. It should be noted that in leading the group, however, they did not function as CEOs or direct managers with specified authority over the organization. They served to guide the consensus model among the group and worked to resolve disputes when they occurred.

Malware Analysis.
The initial focus of the malware analysis was to break down the worm and reverse engineer it to determine what its effects were, how it was spreading, and plans for its future use. It was through various malware analysis efforts that cybersecurity experts managed to recreate the code that Conficker used to search for updates and begin DNS registration. Even after the initial studies were released, malware analysis continued in order to learn more about the worm and its potential functions.[48] It is important to note that members of the Conficker Working Group were not the only ones analyzing the code of the worm. In fact, many analyses occurred outside the group, but were then studied by those in the malware group to determine its contribution to the overall effort.

The Malware Group actually began with an intro e-mail outlining the group's goals:

1. The binary's logic (What it does, and how it does it)
2. The effects of that logic on infrastructure (Impacts of the logic on infrastructure, such as DNS queries, UDP traffic, etc.)
3. Any reasonable means to identify this threat on a system, or network (Think AV signatures, IDS signatures, points of correlation, etc.)
4. Provide a trusted arena for exchange of information to take place between the parties on this list

The DNS Registration Group took on the task of dealing with generic DNS questions and looking at specific issues as they were raised by the ccTLDs. The main participants of this group are responsible for generating and distributing the regular lists of domains that must be blocked to prevent Conficker from reaching them. ICANN is sending the lists to participating ccTLDs on a quarterly basis.

With the update to Conficker C, the Working Group found itself working with many more ccTLDs. Giving these groups their own listserve was essential to communicating and coordinating among them. Working with ICANN and others, the Working Group managed to contact and collaborate with nearly every TLD in the world to temporarily register domains and block Conficker from updating further or receiving new instructions.

---

[48] Most recent SRI report on Conficker C p2p capabilities released in September.

There is a regular discussion on this list of the "end-game" as TLDs tire of having to go through the task of registering domains (sometimes in the hundreds) to block this one worm. Many people expressed a desire to continue to block updates of C if at all possible, but indicated the effort to block the updates of A/B was more important. If more domains slipped through and additional A/B computers were to receive new instructions or update to C, it could make this problem far worse to manage.

Sinkhole Data.
In registering the various DNS addresses, the group rerouted Internet traffic to a sinkhole server. The sinkhole server collects data as the worm attempts to contact the various DNS addresses. It records the location and IP address of the various computers trying to connect. This data can be used to analyze the scope of the Conficker worm overall and identify specific companies and organizations that have been infected by the worm and need to remove it from their systems. It can also be used to identify new variants that are released into the system.

This group was responsible for managing the sinkhole data collection, the format of the data, access requests to the data and the actual hardware storing the information. It looked at questions related to the scope and spread of Conficker and tried to identify trends in the data to understand the spread of the botnet and potentially assist with remediation.

The data collection and storage were at times a controversial issue. The storage of the data was moved to GA Tech early on as it was seen as a mostly neutral site. Because of the sensitivity of the data, there were concerns about who could access it. While several organizations had access to the sinkhole data for research purposes, the widespread view among Working Group membership was that the data remains underutilized for research. The data did help define the scope of the problem and establishes numbers and trends on infected computers.

Remediation.
After the initial push towards April 1, the Working Group took on the additional task of discussing remediation efforts. These efforts included discussions of public relations to encourage individuals and companies to patch their computers, coordination with ISPs to help remediate infected computers, and novel ideas for getting the patch to individuals. This group has had several outside the box discussions of potential ways to remediate Conficker, but have been hampered by the lack of authority or resources to do so.

The remediation efforts were pushed by concerns that the DNS registration efforts may not be sustainable over time. They also hope they can dismantle Conficker to prevent the worm from being utilized in the future (Several working group members mentioned this concern in relation to a cyber attack in South Korea in 2009, which utilized malware that was initially launched five years ago and remains on computers today). Further, remediation is an exercise to learn how to stop future outbreaks.

Public Relations.
The Public Relations Group was in charge of handling media requests, talking points, and coordinating the various public relations efforts of the companies and individuals involved in the

Working Group. Many of the people working on public relations were not core group members, but the public relations personnel from their respective companies. Microsoft played a large role in the organization of the public relations effort. In general, the goal was to ensure that all members of the group, including the various cooperating TLDs, received credit for the work they had done to combat this security threat. Some interviewees indicated the biggest challenge for this group was the concern that one organization would take credit and get the glory before the others.

Other functions:

Trust verification.
There were a number of times the Conficker Working Group discouraged the publication of specific information about the Conficker Worm, its code, the IP addresses of those infected or the activities of the CWG themselves.

Financial.
There was no central financial structure for the Conficker Working Group. Various individuals and organizations provided resources.

Timeline[49]

Nov 21 – Conficker.A initial release
Dec 29 – Conficker.B released
Jan 1 – Conficker.B/C payload activiation date
Feb 4 – SRI conficker analysis published
Feb 12 – Microsoft offers $250,000 reward for identifying Conficker authors
Feb 16 – Bug in MD6 implementation announced on crypto list
Feb 20 – Conficker.C released
Mar 4 – Conficker.D released
Mar 8 – SRI Conficker.C analysis released
Mar 15 – Many hosts updated to Conficker.D through DNS
Mar 26 – F-secure blog post with Conficker facts
Mar 30 – Honeypot project KYE "Containing Conficker" released
Mar 31 – Nmap, Nessus, and other commercial scanners for Downadup.A/B/C/D released
Apr 1 – Conficker.D/E payload activation date
Apr 3 – SRI releases P2P scanner for Conficker.C
Apr 7 – Honeynet Conficker KYE (rev 2) released
Apr 8 – Conficker.E released
Apr 15 – Simple Conficker scanner V2 released
May 3 – Downadup.E scheduled to delete itself
Jun 2 – Symantec releases Downadup Codex v.2.0
Sep 21 – SRI releases Conficker C P2P Protocol and Implementation Analysis

[49] http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline

APPENDIX B - Terms and Acronyms

US-CERT – United States Computer Emergency Readiness Team is the operational arm of the National Cyber Security Division (NCSD) in the Department of Homeland Security (DHS). It is a public-private partnership tasked with providing response support and defense against cyber attacks in addition to disseminating cyber security information to the public.

CWG - Conficker Working Group was created as, and remains, an ad-hoc organization formed by private sector corporations, groups and individuals to counter the Conficker malware threat.

FBI - Federal Bureau of Investigation is an agency of the United States Department of Justice that serves as both a federal criminal investigative body and an internal intelligence agency. The agency worked closely with DHS, the private sector, and other US agencies to fully identify and mitigate the Conficker threat.

ISP - Internet Service Provider is a company that offers access to the Internet. The ISP can offer various data transmission technologies such as dial-up, DSL, or cable.

IP – Internet Protocol address is a numerical label that is assigned to computers participating in a network. IP addresses serve two principal functions in networking: identifying host information and location.

P2P - Peer to Peer is a distributed network of participants that make their resources, such as music, available to other network participants without the need for central coordination, such as a server or a host. Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model where only servers supply, and clients consume.

DNS - Domain Name System is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates binary information with domain names assigned to each of the participants.

Domain name - A domain name is an identification label that defines a realm of administrative autonomy, authority, or control in the Internet, based on the Domain Name System (DNS). In www.example.com, example is the domain name.

TLD - Top Level Domain is identified by what follows the last dot in a web address, such as .com, .gov, .edu. It is the highest level in the hierarchical Domain Name System of the Internet. Management of most TLDs is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN), which operates the Internet Assigned Numbers Authority (IANA) and is in charge of maintaining the DNS root zone.

gTLD - Generic Top Level Domain is the generic category of TLDs maintained by the IANA, such as .com, .info, .net, and .org.

ccTLD - country code Top Level Domain is a TLD used to identify a country, sovereign state or a territory associated with the domain.

ICANN - Internet Corporation for Assigned Names and Numbers is a non-profit corporation created to oversee a number of Internet-related tasks such as Internet Protocol (IP) address space allocation, generic (gTLD) and country code (ccTLD) top-level domain name system management, and root server system management functions.

IANA - Internet Assigned Numbers Authority is the entity that oversees global IP address allocation, root zone management for the Domain Name System (DNS), media types, and other Internet Protocol related assignments. It is operated by ICANN.

SRI International is an independent, nonprofit research institute that conducted extensive research and analysis on the Conficker threat.

Sinkhole server collects data when a worm attempts to contact various DNS addresses.

DLL - Dynamic Link Library is Microsoft's implementation of the shared library concept in the Microsoft Windows and OS/2 operating systems. Conficker is a DLL that uses a Remote Procedure Call (RPC) buffer overflow to push its code onto a Windows machine.

RPC - Remote Procedure Call is a technology that allows a computer program to cause a subroutine or procedure to execute in another address space, usually on another computer on a shared network, without the programmer explicitly coding the details for this remote interaction.

Botnet is a term for software robots, or bots, that run autonomously and automatically. The term is usually associated with malicious software. Zombie computers run the malicious software, usually installed via drive-by downloads exploiting Web browser vulnerabilities under a common command-and-control infrastructure.

Malware is short for malicious software. It is software designed to infiltrate or damage a computer system without the owner's knowledge.

Spyware is a type of malware that is installed on computers and collects information about users without their knowledge.

Adware is short for advertising software. It is any software package, which automatically displays or downloads advertisements to a computer. Some types of adware are also spyware and can be classified as privacy-invasive software.

Trojan horse is malware that appears to perform a desirable function for the user but instead facilitates unauthorized access to the user's computer system. Trojans allow a hacker remote access to a target computer system.

Scareware is scam software that often has limited or no benefit, sold to consumers with a perception of threat. A frequently used tactic involves convincing users that a virus has infected their computer, offering downloadable software to remove it for a price. The software is usually non-functional or malware itself. Some forms of spyware and adware also use scareware tactics.

Waladec is a form of scareware that attempts to trick computer users into paying money for fake anti-virus software.

Virus is a computer program that can copy itself and infect a computer. The term is commonly but erroneously used to refer to other types of malware, adware, and spyware programs that do not have the reproductive ability.

Intrusion detection is the act of detecting attempts to compromise the confidentiality, integrity or availability of a computer or resource. When Intrusion detection takes a preventive measure without direct human intervention, then it is an intrusion-prevention system.

Firewall blocks unauthorized access to a computer or computer network while permitting authorized communications.