# Conficker Summary and Review

Dave Piscitello, ICANN Senior Security Technologist 7 May 2010

**Abstract**

This report provides a chronology of events related to the containment of the Conficker worm. It provides an introduction and brief description of the worm and its evolution, but its primary focus is to piece together the post-discovery and -analysis events, describe the containment measures chronologically, and describe the collaborative effort to contain the spread of the worm. The author captures lessons learned during a containment period spanning nearly a year and describes recent activities that attempt to apply the lessons learned so that the security and DNS communities can be better prepared for future attacks that exploit the global DNS.

This report represents the work of the author, on behalf of the ICANN Security Team. The author is responsible for errors or omissions. While members of the Conficker Working Group, ICANN SSAC, individual security researchers, and certain ICANN registries were invited to comment or review the report, none of these organizations were asked to formally endorse this work product.

## Introduction

The Conficker worm first appeared in October 2008 and quickly earned as much notoriety as Code Red[1], Blaster[2], Sasser[3] and SQL Slammer[4]. The infection is found in both home and business networks, including large multi-national enterprise networks. Attempts to estimate the populations of Conficker infected hosts at any given time have varied widely, but all estimates exceed millions of personal computers.

The operational response to Conficker is perhaps as landmark an event as the worm itself. Internet security researchers, operating system and antivirus software vendors discovered the worm in late 2008. These parties as well as law enforcement formed an ad hoc effort with ICANN, Top Level Domain (TLD) registries and registrars around the world to contain the threat by preventing Conficker malware writers from using tens of thousands of domain names algorithmically-generated daily by the Conficker infection.

Conficker malware writers made use of domain names rather than IP addresses to make their attack networks resilient against detection and takedown. Initial countermeasures – sinkholing or preemptive registrations of domains used to identify Conficker's command and control (C&C) hosts – prevented the malware writers from communicating with Conficker-infected systems and thus, presumably

prevented the writers from instructing the botted hosts to conduct attacks or to receive updates. The Conficker malware writers responded to this measure by introducing variants to the original infection that increased the number of algorithmically generated domain names and distributed the names more widely across TLDs. To respond to this escalation, parties involved in containing Conficker contacted more than 100 TLDs around the world to participate in the containment effort.

The combined efforts of all parties involved in the collaborative response should be measured by more criteria than mitigation alone. The containment measures did not eradicate the worm or dismantle the botnet entirely. Still, the coordinated operational response merits attention because the measures disrupted botnet command and control communications and caused Conficker malware writers to change their behavior. The collaborative effort also demonstrated that security communities are willing and able to join forces in response to incidents that threaten the security and stability of the DNS and domain registration systems on a global scale.

## Conficker Background

This section draws heavily from an excellent paper on the Conficker worm published at the Honeynet Project by authors Felix Leder and Tillmann Werner[5]. The description here largely tracks and distinguishes among Conficker variants when changes affected the worm's use of the DNS. It discusses the worm in general terms. Those interested in a very technical analysis of Conficker's infection – armoring and update processes, variants of the domain name generation algorithms, signatures that can be used by intrusion detection systems to detect Conficker, and disinfection issues – are encouraged to read the full paper. Leder and Tillmann have also produced a short video on the structure of Conficker and maintain a list of disinfectants and scanners at the Containing Conficker web page[6]. Lists of domain names generated by Conficker variants may be of particular interest to the domain name community and can be obtained there as well. Another source for this summary is an SRI Technical Report by Phillip Porras, Hassen Saidi, and Vinod Yegneswaran, which analyzes the Conficker package, processing, and protocol in considerable detail.

Conficker is called a *worm* because the first discovered variant attached to a program (executable), was self-replicating, and (importantly) used a network as the delivery mechanism. This combination of characteristics distinguishes worms from viruses[7]. Conficker is actually a *blended threat*[8] because it can be delivered via network file shares, mapped drives and removable media as well. The Conficker infection is a type of software called a Dynamic Link Library (DLL). A DLL cannot execute alone but must be loaded by or into a running application. The Conficker DLL launches with *rundll* on Windows, which lets it run as a standalone process. A Conficker installer loads its DLL into a Windows application by exploiting the MS08-067 vulnerability in the Windows Operating System[9]. This vulnerability allows Conficker malware writers to use what is called a *buffer overflow* to "inject" code into the Windows Server Service.

A buffer overflow is a method of exploiting software programming that fails to check boundaries before writing information into memory. The attacker discovers that a program is vulnerable to a buffer overflow by attempting to write more information into memory than the programmer had allocated to store information. Specifically, the attacker seeks to write information into memory that is adjacent to the memory he overruns. This adjacent memory may contain data or it may contain executable code; in either case, the attacked application will not operate as anticipated when it encounters the malicious code the attacker injected. In the case of Conficker, the attacker injected executable code that gives the attacker remote control over the infected computer and in particular, remote code execution privileges. Using the injected code, the attacker can add or change code to make the infected host computer do whatever it chooses.

To prevent detection, certain worms embed themselves in a benign manner on the infected computer, i.e., into a program or software that is expected to run on a computer running the Windows operating system. The worm then attempts to disable software that could detect or remove the infection. Conficker variants disable Windows Automatic Update, Windows Security Center, Windows Defender and Windows Error Reporting. Later variants also used DNS filtering to block antimalware programs from obtaining updates (e.g., virus signatures that would allow the resident AV software to detect and remove Conficker related malware). Conficker malware also resets the Windows System Restore point[10], which contains information that could be used to remove Conficker malware by restoring the infected computer's file system and registry to versions saved prior to the infection.

Early variants of the Conficker malware enlisted an infected machine into a Conficker botnet. Once enlisted, the malware running on infected computers uses a domain generation algorithm (DGA) to create a daily list of domain names. The Conficker malware writers used the same algorithm to generate an identical list. The writers then registered a small number of these domains and set up name resolution service for the selected subset of domains so that the domain names assigned to *Internet rendezvous logic points*[i] can be resolved to IP addresses by DNS resolvers. The Conficker malware writers did not appear to use the generated domain names routinely, presumably because they determined the names had been blocked. A later variant shifted the botnet from employing rendezvous logic points to a peer-to-peer network. Malware operating on infected hosts discover other bots by detecting attacks from another infected hosts, confirming the code the attacking hosts attempt to inject is the same as its own code, and connecting back to the attacker using HTTP so that hosts with matched infections can share files directly.

The Conficker-infected computers attempt to connect to HTTP servers operating on rendezvous logic points by contacting domains from the daily-generated list of domain names. If they are able to resolve a domain name and connect to an HTTP server, the botted machines are able to receive additional malware or instructions to perform certain actions using already-present executables. The worm uses strong cryptographic techniques (RSA and MD6) to control what code can be loaded onto an infected box. All code "loads" must be correctly signed or they will be rejected. Presumably, only the Conficker malware writer has the private signing key for updates. In some cases, the Conficker bot will be told to try various means of infecting other hosts (e.g., through anonymous network shares). In other cases, the Conficker bots can become an army that can be directed at will by rendezvous points to support a wide range of malicious or criminal activities.

*Botnets are extremely difficult to dismantle. Botnets can remain operational – and will continue to serve as platforms for numerous attacks - for as long as the botted*

[i] A rendezvous logic point is a server that is functionally similar to a command and control (C&C) server.

*computers remain infected and as long as the bots can remotely communicate with the rendezvous point(s).*

The following section offers a chronology of events that describe how the security, intelligence and DNS communities were able to disrupt communications between Conficker infected hosts and rendezvous logic points.

## Origin and Evolution of the Conficker Working Group

Prior to the formation of the Conficker Working Group, operating system and security software vendors (Microsoft, Symantec, F-Secure), other security research organizations (Shadowserver Foundation, Team CYMRU) and the intelligence community (US Federal Bureau of Investigation, US Secret Service and the US Department of Defense) had monitored and analyzed Conficker and had cooperated to contain the threat. F-Secure had begun "spot" sinkholing[ii] domain names that Conficker bots were attempting to contact to estimate the size of the botnet. Several operators of the Top Level Domains in which Conficker malware writers were registering domains (VeriSign, Afilias, NeuStar, PIR, and WS) were already involved at this point, and ICANN staff assisted the security researchers in contacting CNNIC to advise them of the threat and ask for their participation in the containment effort.

To support efforts to monitor Conficker traffic, analyze the infection, identify infected hosts and estimate the size of the botnet, Support Intelligence was registering 500 domain names identified as Conficker algorithmically generated domains per day across a small number of top level domains, through an ICANN accredited registrar, Alice's Registry, Inc. As part of the preemptive registration action, Support Intelligence configured name servers to resolve to IP addresses of sinkholing hosts under the control of security researchers and malware analysts.

Preemptive domain registrations had previously been applied with some success by FireEye Malware Detection Labs to thwart the Srizbi botnet in early November[11] and security researchers were hoping for similar success by applying the same technique. In the case of Conficker, preemptive registration was to serve two purposes: prevent Conficker infected hosts from communicating with C&C and direct traffic to sinkhole hosts where the Conficker bot traffic could be further monitored and analyzed. On 28 January 2009, a security researcher at Support Intelligence contacted ICANN staff regarding the Conficker threat. Support Intelligence's blocking activities were self-funded and the organization was seeking support from ICANN to obtain financial relief or reimbursement from registries for the domains it had and was continuing to register.

[ii] The "verb" *sinkhole* refers to an activity where traffic suspected to be associated with a bot net is redirected to a computer(s) operated by security researchers or law enforcement for observation or to divert an attack away from an intended target.

Discussions relating the ongoing Conficker response activities appeared on several security lists in parallel with these activities, which increased awareness of the global nature and scale of the threat. For example, personnel at registry operator Afilias were discussing Conficker monitoring, blocking, and funding issues with several relevant parties prior to Support Intelligence contacting ICANN. CERT-CC staff had contacted staff at domain name registry operator NeuStar to ask whether Neustar might arrange for some assistance from the BIZ registry to help contain Conficker. On 31 January 2009, Neustar received briefings describing Support Intelligence's preemptive registration initiative from Microsoft staff and other security researchers via private correspondence. Combined, these dialogs were essential in engaging resources to contain Conficker, but they were loosely coordinated in the sense that not all parties were kept informed at all times, information shared was not uniform, and that dissemination of information relied heavily on individual webs of trust.

By this time, several organizations (Symantec/Kaspersky, eNom) had begun contributing funds to assist with payment of the fees Support Intelligence was incurring to contain Conficker. This financial aid helped pay for or recover registration fees to CCTLDs. Recognizing that the current method of preemptive registration was "fundamentally unsustainable" even with Microsoft's contributions and that the operational response imposed an unreasonable and precarious burden on a single individual, Neustar contacted ICANN's Chief Internet Security Advisor and the chairman of ICANN's Security and Stability Advisory Committee (SSAC).

On 3 February 2009, while attending an ICANN DNS SSR retreat, several parties already involved in the containment effort met in Atlanta to conduct a briefing for senior management from ICANN and gTLD registries. Participating were:

- ICANN senior management, general counsel, and security staff,
- Law enforcement (FBI/NCFTA),
- Security researchers (Microsoft, Support Intelligence, ISC), and
- GTLD registry operators (VeriSign, Afilias, NeuStar)

Participants reviewed how Conficker had been handled to date (see above), and discussed how to sustain the effort through February and March and how to manage public disclosure. The operators of the affected registries – initially, BIZ, COM, INFO, NET, and ORG – volunteered their participation and set about blocking domain names. The participants discussed ways that ICANN might assist in the preemptive registration effort. ICANN's security staff agreed to coordinate preemptive registrations with CCTLDs and to facilitate ongoing communications among the participants. ICANN senior management and general counsel agreed to consider declaring the Conficker response to be a special circumstance (exception case) and to manage contractual waiver aspects of the response so that the GTLD registries could continue their preemptive registration activities through 1 April 2009. The participants agreed to continue to conference regularly to report status and to explore mechanisms to contain or mitigate future, similar threats.

Based on traffic analysis and intelligence gathered related to Conficker available at the time of the meeting, participants agreed that the operational response plan put into action in Atlanta would have to continue for several months and a workflow emerged: researchers would generate the daily lists and contact the targeted registries, who would then take measures to block Conficker botnet operators from registering the domain names.

On 12 February, Microsoft published a press release announcing "partnership with technology industry leaders and academia to implement a coordinated, global response to the Conficker (a.k.a. Downadup) worm"[12] and offering a $250,000 reward for information leading to the arrest and conviction of Conficker's writers[13]. The announcement acknowledged the participation and cooperation of ICANN, registry operators (NeuStar, VeriSign, CNNIC, Afilias, Public Internet Registry) as well as Global Domains International Inc., M1D Global, AOL, Symantec, F-Secure, ISC, researchers from Georgia Institute of Technology, the Shadowserver Foundation, Arbor Networks and Support Intelligence. At this point, Arbor Networks joined to complement sinkhole operations. Following this announcement, the press began referring to the ad hoc partnership as the Conficker Cabal[14]. The partnership later preferred and continues to use the name Conficker Working Group.

From early February through mid-April, the staff from ICANN security, services, compliance and legal departments coordinated a series of calls with parties who agreed to collaborate as a DNS operational response team. The team, consisting of involved gTLD registry and registrar representatives, met to continue to share information and to discuss ongoing efforts to contain Conficker. The group was explicitly a voluntary collaboration that focused specifically on the Conficker situation, established mechanisms for vetting additional members to ensure trust in those involved and made no determinations related to any contractual matters. Many of these parties were also engaged in the broader security community Conficker working group. By this point the CWG had multiple functioning subgroups, including sinkhole operators, malware analyzers, DNS operators, remediation tool producers, etc.

On 20 February, Microsoft received reports of a Conficker.C variant[iii]. Security researchers determined by examining infection samples that this variant had a more aggressive domain generation algorithm. Cognizant that the security and domain name communities were blocking registrations, the Conficker malware writers seemed intent to test the level of commitment of the Conficker Working Group. In *Analysis of Conficker.C*[15], Parras, Saidi, and Yegneswaran describe Conficker.C as "a direct retort to the action of the Conficker Cabal, which recently blocked all domain

[iii] The labeling of Conficker variants becomes confusing at this point. One security researcher at SRI obtained a virus sample and labeled it B++ whereas other analysts labeled the variant C. The 8 March 2009 SRI analysis of Conficker.C thus describes the variant others in the community labeled D. Some members of the security community now refer to the 1 April 2009 variant as Conficker. C/D. A table comparing certain features of the Conficker variants appears in Appendix A.

registrations associated with the A and B strains." The Conficker.C variant introduced two functional changes. The first altered the control channel communications from a C&C to a peer-to-peer model. Conficker.C also changed the domain name generation algorithm and rendezvous logic point selection method: "Conficker.C now selects its rendezvous points from a pool of over 50,000 randomly generated domain name candidates each day. Conficker.C further increases Conficker's top-level domain (TLD) spread from five TLDs in Conficker A, to eight TLDs in B, to 110 TLDs that must now be involved in coordination efforts to track and block Conficker.C's potential DNS queries.

With this latest escalation in domain name manipulation, Conficker.C posed a significant challenge to those hoping to track its census and contain the threat it posed. The Conficker.C variant also highlighted the weakness of blocking name registrations as a countermeasure. The measure does not scale. By introducing increasingly large numbers of possible registrations and spreading these across a large number of TLD registries, the Conficker writers increased the likelihood of oversight or error, and also increase the number of organizations that had to collaborate.

Leder and Werman note in their report that the new Conficker variant improved the domain generation algorithm measurably, but at the same time revealed information that the writers should have taken care to hide: "Conficker.C contains code that will start to look for updates after 1 April 2009 local time... It is this hardcoded date value within the code that has generated such a high degree of press speculation about what the Conficker botnet will or more likely won't happen on April Fools day." Hard coding the date into the Conficker.C variant was not very clever and in fact, shows that even in the virus world those who fail to study history are doomed to repeat it: hard coding IP addresses of infection code had earlier provided security researchers with the means to block communications between bots and C&Cs.

At this point, the CWG faced several uncertainties and challenges. CWG members and others had made several repair and removal tools available, but the group could not enforce remediation or determine how many hosts infected by prior Conficker variants remained infected and had been upgraded by the Conficker malware writers from the original A variant (and thus could be further upgraded to Conficker. Considerable efforts to make the public aware of the threat were underway, but the CWG had to anticipate that Conficker.C would infect additional (new) hosts. The CWG focused certain of its monitoring activities on determining whether any of the algorithmically generated domains duplicated names already registered in a TLD and other efforts to continue to identify the domain names Conficker generated and make these available to TLDs so that they could be blocked.

ICANN security staff and ICANN regional liaisons contacted the list of CCTLD operators that security researchers had identified as targets for Conficker registrations, supplied each operator with a tailored list of names Conficker

malware writers would attempt to register, and advised them to join security mailing lists where DNS response issues related to the Conficker worms are discussed; however, certain CCTLD operators would not block the names on the list without a court order. ICANN staff also contacted the Chair of the ccNSO and the managers of the Regional ccTLD groups (CENTR, APTLD, AFTLD, LACTLD) to assist in calling attention to the anticipated event.

The anticipated April 1 update event received considerable public attention[16]. The Conficker Working Group, complemented now by a number of CCTLDs, prepared for the event. ICANN security staff and Conficker Working Group members recognized that 100% awareness or timely participation across such a large number of registry operators was doubtful. Cooperation among the various registries operators, although unlikely to fully stop Conficker, would enable the anti-virus community and those involved to better track and understand the spread of the worm and then to use that information to help disinfect systems.

By 30 March 2009, security researchers involved in The Honeynet Project had sufficiently analyzed Conficker.C to positively identify the infection[17]. Detection signatures were made available and quickly included in free and for-fee network scanners (NMAP, Tenable Security's Nessus, McAfee Foundstone Enterprise, and Qualys). Given the number of systems that remained infected and not patched, security researchers conceded that that number of systems still infected with earlier Conficker variants and still not patched to mitigate the MS08-67 would be updated on 1 April 2009 with the Conficker.E variant and that the extent and success of the update could not be predicted.

The intent of the Conficker.E variant was to remove all but the core malware functionality and upgrade contacted hosts with the new P2P communications ability. According to Microsoft Malware Protection Center[18], the Conficker.E variant "executes a self-termination routine when the date is May 3 2009. The worm deletes its main executable component on this date. However the DLL payload component (detected as Worm: Win32/ Conficker.E.dll) remains to continue participating in P2P communication among infected peers." On 21 September 2009, SRI released a Conficker P2P Protocol and Implementation Analysis[19]. In the report, the authors describe the new P2P scan-based discovery method Conficker malware writers would now use to join an infected host into the Conficker P2P network, the means by which peers share malware executables, and more.

## Ongoing Conficker Working Group Activity

Efforts continue to block registration of Conficker domains. Traffic analysis efforts have been helpful in developing a better understanding of the distribution of the worm and intended applications of the Conficker botnet [20]. Microsoft and security vendors continue to study methods for detection and removal of known variants.

Security researchers continue to publish and distribute Conficker scanners, signatures for intrusion systems, and general information. Efforts to target outreach to particularly infested networks continue.

The Conficker infection rate remains high for B and C variants but declining for C/E. Remediation continues to pose challenges. Security researchers continue to track Conficker. An October 2009 snapshot by the Shadowserver Foundation estimates the number of systems infected with Conficker A/B/C variants at approximately seven million[21]. The Conficker Working Group maintains visual timeline and chronology of Conficker at [22] to track historical, current and future events.

Activities to detect Conficker variants and remediate Conficker-infected hosts will undoubtedly continue for some time. This is inevitable given the millions of infected computers and historically marginal success in remediating malware. Lessons learned during the Conficker containment period are discussed in a later section of this paper. Security and DNS communities are working to devise long-term and sustainable approaches for dealing with not only Conficker but also future, similar threats. These, too, are discussed in a later section of this paper.

## The Importance of Roles in Conficker Working Group

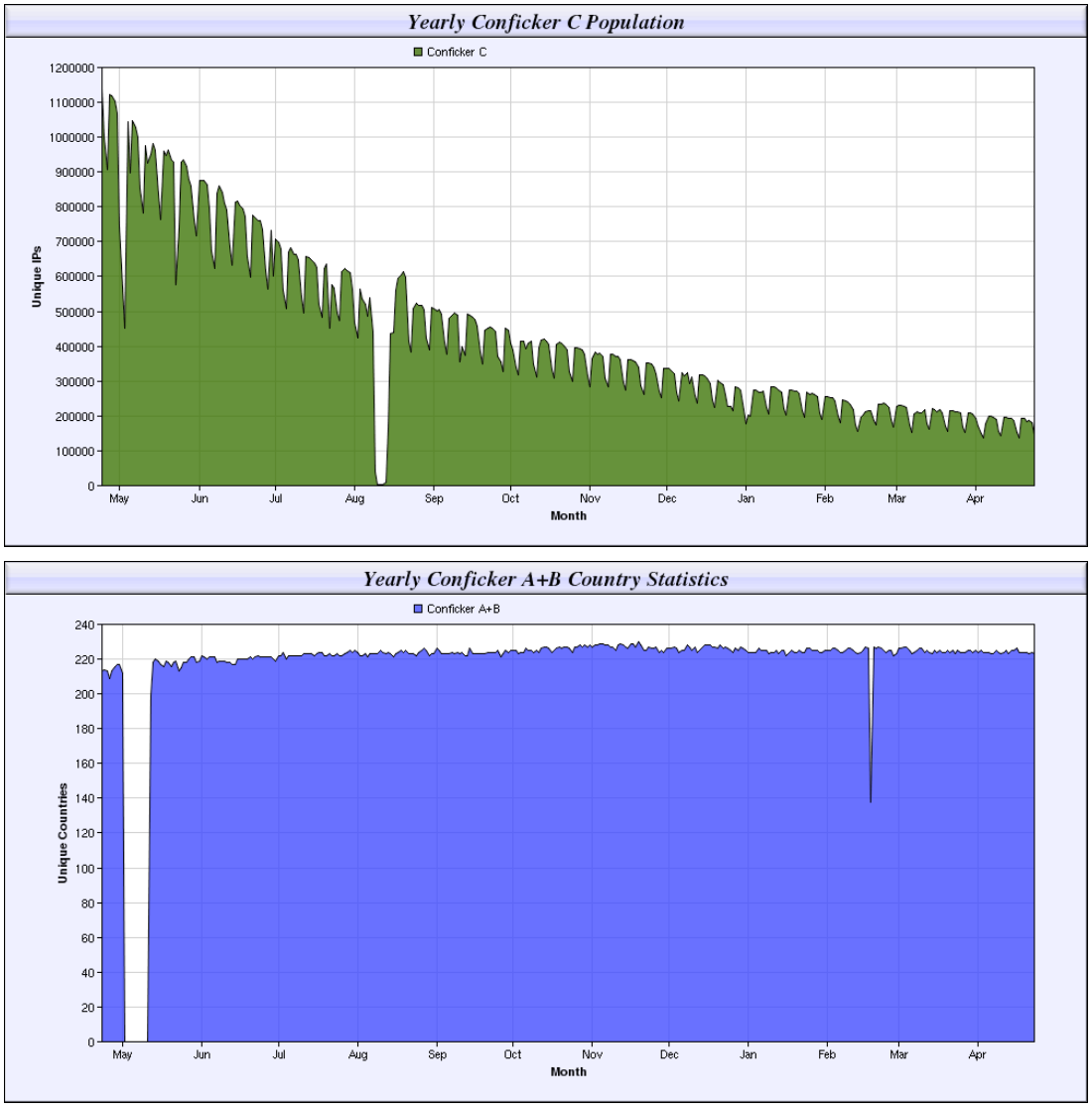
All the actions related to mitigating the Conficker worm were not directly nor entirely within the remit of any individual CWG participant. Throughout the chronology of Conficker events, all the collaborating parties performed roles that were appropriate to their organizations' core competencies: malware researchers reverse engineered the dropper/installer, traffic analysis engineers identified the loci of infestations, ICANN facilitated communications between registries and parties who compiled the C&C domain lists, and registry operators blocked registrations of Conficker domains. The collaborating parties tried to adhere to the best practices of public disclosure of security incidents and events by maintaining a low profile, protecting sensitive information, and sharing only information that the ad hoc partnership agreed to share.

Several CWG members publicly expressed their surprise and gratitude for member willingness to engage in the Conficker containment[23]. Many security and registry organizations had not encountered circumstances such as those Conficker posed and thus did not have communications channels in place to coordinate containment efforts. CWG members indicated that ICANN's ability to facilitate and expedite communications with TLD registries accelerated processes that would under other circumstances have challenging if not impossible to obtain during the windows of opportunity Conficker afforded them. ICANN security staff and regional liaisons initially filled this gap by relaying information gathered by security researchers to TLD operators and later by introducing collaborators and providing direct contact information. Registry operators blocked Conficker domains and advised ICANN

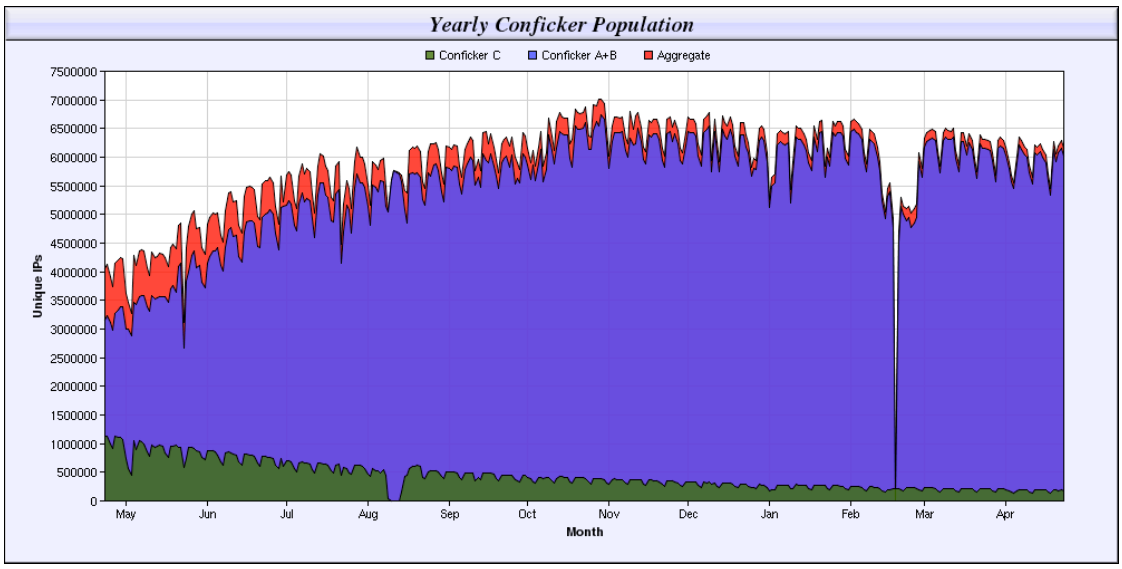
counsel and senior management of the measures they took to prevent the registration of auto-generated domains by the Conficker miscreants. These ad hoc methods provided some insight into how certain formal constructs might prove beneficial in future response efforts.

## Conficker Today

Infection tracking by the CWG shows that Conficker.C populations have diminished over the past year but that number of computers infected Conficker A+B is still large (graphs courtesy of Conficker Working Group[24]).




Over the past year, the Shadowserver Foundation has tracked the Conficker populations (A+B, C, and aggregate), which remain in the millions.




## Lessons Learned

Several lessons may be learned from the chronology and events related to containing the Conficker worm. Perhaps the most positive lesson learned is that DNS, security, and law enforcement can collaborate when an incident of global proportion is identified. A positive result from the ad hoc response was that the participants disrupted the botnet communications and thus prevented opportunities to put the botnet to misuse. The containment, however, was temporary, and the Conficker malware writers countered by making the containment measure increasingly difficult to coordinate and sustain.

The Conficker collaborative responses relied largely on volunteer efforts and goodwill, informal communications channels, interventional operational practices, informal agreements, and assumptions that response would be uniform and unilateral. Each of these dependencies exposed certain weaknesses:

*Ad hoc collaborative response may not be scalable or sustainable.* In the absence of (complementary) formal structures or commitments, certain problems that encumbered or confounded the Conficker response will persist. The Conficker response was a highly distributed effort that leveraged many volunteers as well as full time staff across multiple organizations to get the job done. We need to consider the fact that we cannot rely on having sufficient resources of the caliber that were engaged for Conficker to be available at a moment's notice as a real threat. As we study threats to the DNS, we need to also consider that we have not yet encountered a situation where resources might be needed for multiple, simultaneous incidents involving the global DNS.

*Like other malware writers, worm/botnet writers will adapt to countermeasures deployed to detect or contain them*. However, we still see evidence that while botnet writers have adapted to the containment, they still appear to prefer DNS to hard-encoded IP addresses and still use second level labels across multiple TLDs. The DNS is likely to continue to be part of malware writer toolkits. It is thus appropriate to consider ways to build on the successful elements of this incident response and improve those aspects that were not so successful.

*Informal communications may not be sufficient for all global incident response efforts, especially in situations where there is zero tolerance for error or omission*. Conficker demanded constant attention from responders. Conficker variants generated new domain lists daily. Security researchers monitored traffic and analyzed code samples continuously in anticipation of new variants. During the months of effort to contain Conficker, communications among responders could be characterized as having spikes, lags, and dormant periods where some parties were unable to respond or unresponsive. In certain cases, contact information available to parties was not accurate, or was not sufficient to reach a party with authority to act on behalf of the contacted organization. In other cases, ICANN staff determined that some registry contact information maintained by IANA was not accurate or was not the contact at a registry with authority to participate in incident response. Formal channels with agreed-upon or mandatory exchanges and exchange frequencies should be considered for future response efforts.

*Maintaining consistency, completeness and accuracy of information during the course of a long incident response effort is challenging*. During the Conficker response, parties initially used available rather than formal communications channels (e.g., security mail lists, teleconferences, private email, etc.) and relied on contact information at hand or passed hand to hand. The Conficker Working Group established communications channels as the containment effort grew, but sensitive information was not consistently classified, encrypted or signed. The nature and level of detail communicated among the participants was unintentionally but predictably not uniform. The ad hoc nature of these communications also resulted in different parties receiving information at different times, which made it difficult to maintain broad situational awareness. No individual or organization performed formal action tracking or auditing, and thus chronicling the incident response for post-incident review and analysis has been difficult. In particular, information that is potentially valuable in improving response to future global incidents may be lost or as yet undisclosed.

*Scaling trust is hard*. Volunteer efforts rely on personal webs of trust. Most participants in the Conficker response knew some or several other participants but it is unlikely that anyone knew everyone and unlikelier still that anyone could produce an accurate accounting of all parties to all information sharing during the course of the containment effort.

*Operational processes that rely on block lists at a registry level are not scalable. The* most obvious reason is that preemptive blocking scales poorly: in response to the blocking efforts, Conficker's writers increased the numbers of algorithmically generated domains and the numbers of TLDs. The operational burden to block domains increases in several ways; for example, distribution of names across larger numbers of TLDs, removal of the names from available pools can become expensive, non-compensated costs for registry operators. Registries also filtered domains to assure that all "collisions" between Conficker's DGA domains and domains that are already registered in TLDs were not adversely affected.

*Certain activities related to incident response raise contractual issues for ICANN, registries, and registrars.* In the case of Conficker, ICANN and GTLD registries were able to resolve matters relating to domain fees quickly. The community cannot rely on all contractual matters to be so easily handled for all future incidents. Regarding the ease by which Conficker-related contractual matters were resolve, one security expert observed (anonymously) that, "in the first example of breaking the rules, you're given some leeway. The second time, the stakes are higher, and you have to beware that a single mistake will be disproportionately highlighted."

*Certain countermeasures or preemptive actions cannot be implemented unilaterally by all TLD operators*. Some registry operators require court orders before they take a particular action in response to a global incident. In a scenario like Conficker, where lists of malicious domains are generated daily, even a one day delay to process a court order can inhibit the response.

We should refrain from concluding from these lessons learned that formal structures must replace voluntary ones. For example, establishing formal structures does not address the issue that some TLDs will not be willing to participate or to continue to participate in certain kinds of response indefinitely. Relying entirely on formal structures may exclude participation by certain individuals for a range of political, legal, or personal reasons. Rather, we should bear in mind that responses with inadequate resources will be more prone to error or omission than those given adequate resources. Effective response will inevitably and ultimately depend upon the support and participation of relevant stakeholders, notably those who have delegated responsibility for the various assets involved. In other words, while certain formal structures can complement and render ad hoc responses more effective, both may be necessary to deal with future events of the Conficker kind.

## Way Forward

Base on the lessons learned from the collaborative response to Conficker, one element of a way forward is to formalize relationships among parties that become involved when security events of a global nature occur. ICANN (the entity and community) has established certain formal relationships and structures and is working in concert with other organizations on others.

Within the specific context of global security events involving abuse of the DNS and domain registration services, and using Conficker as a learning experience, ICANN and the gTLD registries have developed an Expedited Registry Security Request Process (ERSR)[25]. Through this process, gTLD registries can now inform ICANN of a present or imminent security threat against the registry or the DNS infrastructure and request a contractual waiver for actions the registry might take or has taken to mitigate or eliminate the threat. The contractual waiver would provide exemption from compliance with a specific provision of the Registry Agreement for the time period necessary to respond to the threat. The ERSR allows a registry to maintain operational security during an incident while keeping relevant parties (e.g., ICANN, other affected providers, etc.) informed as appropriate.

The ERSR is intended to help registries deal with malicious activity involving the DNS of scale and severity that threatens systematic security, stability and resiliency of a TLD or the DNS. It can also be used in circumstances where a registry discovers unauthorized disclosure, alteration, insertion or destruction of registry data. The ERSR would also be an appropriate process for an event with the potential to cause a temporary or long-term failure of one or more of the critical functions of a gTLD registry as defined in ICANN's gTLD Registry Continuity Plan[26].

Today, many organizations support a variety of activities that are intended to improve Internet security awareness and respond to security incidents. ICANN security staff has studied incident and emergency response at national and international levels to understand how these activities might be coordinated, especially in circumstances where the DNS is central to global incidents or where events threaten the security, stability, or resiliency of domain name service at a global level. With the assistance of these organizations, ICANN has developed an operational concept plan and business case for a DNS-CERT[27].

As proposed in the concept plan, the DNS-CERT would act as a security coordination center to assist DNS operators and supporting organizations by providing information, expertise or resources to respond to threats to the security, stability and resiliency of the DNS efficiently and in a timely manner. Again, as proposed, the central purposes of the DNS-CERT would be to maintain situational awareness, facilitate information sharing, improve coordination within the DNS operational community, and improve coordination with the broader security and other affected communities.

In addition to these programs, ICANN's security team is studying how to improve and maintain accurate contact information in cooperation with the security community and registry operators. Staff will also study ways to improve and formalize monitoring responses to global incidents while they are in progress (e.g., auditing and tracking), methods to chronicle incident responses, and ways to coordinate post-incident review and assessment. These may be incorporated into the DNS-CERT program as it evolves, or they form be the bases for other initiatives

instigated by other organizations. ICANN will consider what if any role it should perform upon review of the initiatives.

## Concluding Remarks

In certain respects, the collaborative response to Conficker was a single volley in what is arguably an early battle of a long campaign. ICANN and other members of the CWG will continue to assist in remediation efforts related to the Conficker worm. Individual organizations will no doubt use their experiences to help define roles in future global incidents. The DNS and Internet security communities must also consider how they together might establish more formal collaborative response to future occurrences of Conficker and other threats to the DNS security, stability and resiliency of similar nature and scale.

Appendix A. Table of Conficker Variants

| Variant & date | Bot Evolution | DNS/Domain Abuse |
|---|---|---|
| Conficker.A 2008-11-21 | • Infects via MS08-67, anonymous shares<br>• Resets system restore point, disables security services<br>• HTTP callback to download files | 250 pseudo-randomly generated domains registered in 5 TLDs |
| Conficker.B 2008-12-29 | • Infects via MS08-67, anonymous shares, shares with weak passwords, network maps, removable media<br>• Reset system restore point<br>• Disables security software and security updates via DNS filtering | 250 pseudo-randomly generated domains registered in 8 TLDs |
| SRI Conficker.C a.k.a. Conficker.D 2009-02-20 | • Infects via MS08-67, anonymous shares, shares with weak passwords, network maps, removable media<br>• Disables security software and security updates via DNS filtering<br>• Changes bot from HTTP C&C to P2P<br>• Sets 1 April 2009 as activation date for new DGA | Tens of thousands of pseudo-randomly generated domains registered in 100+ TLDs |
| Conficker.E 2009-04-01 | • Initial exploit uses MS08-67<br>• Only installs if prior Conficker variants present<br>• Disables security software and security updates via DNS filtering<br>• Resets system restore point<br>• Updates to pure P2P network<br>• Self-terminates on 3 May 2009: remove all Conficker executables except DLL | |
| … | | |

## Citations


[1] Code Red (Computer Worm), http://en.wikipedia.org/wiki/Code_Red
[2] Blaster worm, http://en.wikipedia.org/wiki/Blaster_Worm
[3] Sasser (Computer Worm), http://en.wikipedia.org/wiki/Sasser_worm
[4] SQL Slammer, http://en.wikipedia.org/wiki/SQL_slammer_(computer_worm)
[5] Know Your Enemy: Containing Conficker, http://www.honeynet.org/papers/conficker
[6] Containing Conficker, http://iv.cs.uni-bonn.de/wg/cs/applications/containing-conficker/
[7] The Difference Between a Computer Virus, Worm and Trojan Horse, http://www.webopedia.com/didyouknow/internet/2004/virus.asp
[8] What is a Blended Threat? http://www.securityskeptic.com/blendedthreat.htm
[9] Microsoft Security Bulletin MS08-067 - Critical, 23 October 2008, http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
[10] How to Restore Windows XP to a previous state, http://support.microsoft.com/kb/306084
[11] Disconnecting from the Srizbi Botnet, http://www.fireeye.com/securitycenter/srizbi_notify.html
[12] Microsoft Collaborates With Industry to Disrupt Conficker Worm, http://www.icann.org/en/announcements/announcement-2-12feb09-en.htm
[13] MS puts up $250K bounty for Conficker author, http://www.theregister.co.uk/2009/02/12/conficker_reward/
[14] Conficker Cabal, http://www.confickercabal.com/
[15] Analysis of Conficker.C, http://mtc.sri.com/Conficker/addendumC/
[16] Alert: April 1 "Conficker" Computer Worm, http://www.cbsnews.com/stories/2009/03/26/tech/cnettechnews/main4894856.shtml
[17] Conficker Researchers Counter April 1 Update With Detection Scan, http://www.crn.com/security/216401818
[18] Microsoft Malware Protection Center - Win32/Conficker.E, http://www.microsoft.com/security/portal/Entry.aspx?name=worm:Win32/Conficker.e
[19] Conficker P2P Protocol and Implementation Analysis http://mtc.sri.com/Conficker/P2P/
[20] Conficker Infection Distribution, http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionDistribution
[21] Shadowserver Foundation Conficker statistics page, http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker
[22] Conficker Timeline, http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline
[23] Shadowserver Foundation Announces New Effort To Combat Conficker https://infosecurity.us/?p=6238
[24] Conficker Working Group Infection Tracking http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking
[25] Expedited Registry Security Request Process, http://icann.org/en/registries/ersr/
[26] gTLD Registry Continuity Plan, http://icann.org/en/registries/continuity/gtld-registry-continuity-plan-25apr09-en.pdf
[27] Global DNS-CERT Business Case, http://www.icann.org/en/topics/ssr/dns-cert-business-case-10feb10-en.pdf