Conficker by the numbers

Sebastián Bortnik
Security Analyst at ESET Latin America

This is a translation for ESET LLC of a document
previously available in Spanish by ESET Latin America
(see http://eset-la.com/centro-amenazas/2241-conficker-numeros).

English version edited and reviewed by the Research Team at ESET, LLC.

Table of Contents

1

Numbers have served humanity since the dawn of history. They integrate into a communication system that functions irrespective of linguistic barriers.

In this paper, we will tell the story of the Conficker worm from a numerical point of view. One year after its emergence as a threat, the Conficker worm exhibited soaring rates of propagation and infection, a significant number of variants, and development features that are both novel and highly dangerous. The numbers associated with Conficker over 12 months of activity are proof of the starring role this worm will have in malware history and of how much it is possible to learn from it.

08-067

On October 23rd, 2008, Microsoft published its security bulletin MS08-067. While the company's usual policy is to provide updates on the second Tuesday of each month, this patch appeared 10 days after "Patch Tuesday." According to Microsoft's normal procedures,[1] out-of-cycle updates are only published "*occasionally*." This confirms *a priori* the severity of a vulnerability that "*cannot wait until next month*."

The Microsoft MS08-067 server vulnerability was labeled *critical* for the majority of the operating systems it affected [2] (Windows 2000, Windows XP and Windows 2003) and *important* for the rest (Windows Vista and Windows Server 2008). In summary, remote code execution is possible on a vulnerable system "*if the user receives a specially crafted RPC request*."

On that day, Microsoft distributed a patch to its users in order to fix the vulnerability (also documenting provisional workarounds) and recommended its clients to "*run the update immediately.*" Conficker had begun.

250

Microsoft's security bulletin warned that the vulnerability could possibly be used in the crafting of a "wormable" exploit. [2]

Almost as predicted, *Win32/Gimmiv* came out on the same day the patch was It. was the first malware to exploit the MS08-067 vulnerability. The worm had primarily been designed to steal information, such as usernames and passwords used or stored by MSN Messenger, Outlook Express and Internet Explorer, as well as cookies stored in the system.[3] Despite its sudden and dramatic appearance, Gimmiv spread mainly throughout Asia and did not attain high infection rates, nor did it persist over time.

By mid-November of the same year, less than a month after the bulletin was published, the first variant of the Conficker worm had appeared, and was detected by ESET products as *Win32/Conficker.A*. Within a few weeks, the worm demonstrated that its developers had worked really hard, particularly on maximizing its infection rates. It was obvious by the end of the year that the Conficker worm was going to be highly successful at self-dissemination.

With the worm out "In the Wild" (ItW), security researchers analyzed the malware and immediately established that it was written by professionals, and incorporated some innovative propagation and update routines. (Self-replicating malware is formally described as being "In the Wild" (or as an "In-the-Wild virus" when it appears on the WildList. For more information, visit: http://www.wildlist.org/)

The new worm was spreading, as was Gimmiv, through the RPC protocol vulnerability previously mentioned. Its most conspicuously novel characteristic was its updating mechanism, making effective use of the creation of pseudo-random domain names.[4] When a system is infected with an active Conficker sample, the worm enters a never-ending loop, generating 250 pseudo-random domain names on a daily basis (taking the date and time of the system as referential values to "seed" the random function). During each loop, the malware contacts every single one of the generated 250 domains, looking via port 80 for a binary file on the corresponding servers. Whenever it finds an executable, it is downloaded and executed on the infected system.

This feature allows any person who knows the domain-creation algorithm to download and run a malicious file on all the systems infected with Conficker. At the same time, this feature makes it difficult for the hacker to restrict control of the system. As long as the system is infected, it will contact 250 different domains on a daily basis, from any of which a hacker might take control of the system.

On December 29th the first subsequent Conficker variant came to light. From that date on, the variant known as Conficker.B (and detected by ESET products as *Win32/Conficker.AA*) was not only able to spread across networks through the RPC vulnerability, but also through USB devices and shared folders with weak passwords, by means of dictionary attacks with a database of 248 possible passwords, in order to gain access to resources in other systems.[5]

Conficker.B also incorporated routines to protect itself from removal, closing processes associated with the most widely used antivirus products, by using a dictionary of 52 process names that are associated with those products. The worm searched active processes and informational resources, and blocked access to web sites whose names contained specific strings. This was done using another dictionary of 52 words, including, for instance, the words "windowsupdate," "eset" and "nod32").

With the appearance of this variant, it became possible to infect machines on which the Microsoft MS08-067 patch was already installed, using the additional infective methods. This was a significant contributing factor to Conficker's success in self-propagation.

Networks infected with Conficker suffered, among other inconveniences, from information leakage, heavy traffic through internal networks, saturation and denial of network services, and the use of the IP addresses used by companies where infected machines were present.

In January, ESET Latin America's Lab indicated that "*Conficker came to stay for a while*."[6] We were not mistaken. Conficker's infection rates kept on growing. And there was more to come.

$250,000

On February 12, 2009, when Conficker was already an epidemic infecting millions of systems, Microsoft announced in a news release[7] that it would pay a reward of $250,000 for "*information that results in the arrest of those responsible for launching and spreading Conficker on the Internet*."

The offering of Microsoft's reward (which as of December 2009 has still not been collected by anybody, since the culprits have not yet been identified) is convincing evidence of the magnitude of Conficker's impact. Microsoft had taken similar actions, for instance, with major epidemics like the Slammer worm in 2003.[8]

In the same news release, the company announced that it would collaborate with other organizations, including the Internet Storm Center (ISC), Verisign and, above all, ICANN (Internet Corporation for Assigned Names and Numbers – http://www.icann.org), to block the domains used by Conficker. Greg Rattray, Chief of Internet Security at ICANN, suggested that: "*The best way to face threats like Conficker is by the security and domain name systems working together.*"

Conficker continued to affect computer users, and the most prominent companies and organizations within the security sector needed to join forces in order to defeat it. Despite efforts to block the domain names to which the infected machines would connect, the worm was still infecting systems, and new variants appeared during the months that followed.

April 1st, 2009

On March 4th, 2009 another Conficker variant emerged, which would draw attention to the worm from all technology-focused media. Although this variant did not represent a greater threat per se than the earlier versions of the worm, [9] it added a feature that made an enormous impression on the news media: a time bomb.

The variant known as Conficker.C (proactively identified by ESET products as *Win32/Conficker.X)* would remain dormant on infected systems until April 1st, 2009. On that day, it would begin to look for updates through a similar pseudo-random domain creation method; however, this new variant would generate 50,000 URL addresses to be checked daily (in contrast to the 250 of the earlier versions). This action on the part of the Conficker writers is clearly in reaction to the security community's work on blocking the domain names (as described above). Now they had to control 50,000 domains on a daily basis instead of 250.

On April 1, Conficker.C began its new update search cycle. Seven days later, the machines infected with this variant downloaded a new worm version – the most recent known variant at the time of writing – proactively detected by ESET's heuristics and subsequently named *Win32/Conficker.AQ*. [10] This threat incorporated, as the only feasible update mechanism, the use of a peer-to-peer network to establish communication between all systems infected and recruited into the botnet. This shows that the main motivation and purpose of the worm developers was the creation of a network of zombie computers.

These different variants of Conficker show the "professional" mind-set of its developers, who incorporated new propagation and infection mechanisms as months went by, in order to accommodate changes in circumstance. The infection rates, which will be presented in the next section, confirm this analysis.

12 x 11 x 03

In February 2009, ESET Latin America's Lab compared the Conficker infection rates shown in the following table: [11]

Date	Detection (Worldwide)	Detection (Latin America)
January 24th, 2009	5.08 %	8.07 %
February 18th, 2009	3.52 %	8.86 %

Table 1: Conficker infection rates worldwide

From these data, it was concluded that the values remained stable "*even though 20 days had gone by*" [11] between the two dates. Right in the middle of a rapid escalation of the Conficker epidemic – even though countless web sites were alerted

to the importance of updating and patching their operating systems, using antivirus software and setting up the systems so as to avoid worm propagation – users were still unprotected, and the spread increased, almost three months after the appearance of the worm. Detected numbers of Conficker infections remained stable, despite the fact that effective security counter-measures already existed. How much longer would users need to be able to protect themselves from this threat? Thirty days? Two months?

The answer can be summarized by the worldwide statistics of Conficker detection rates drawn from ESET's ThreatSense.Net [12] system:

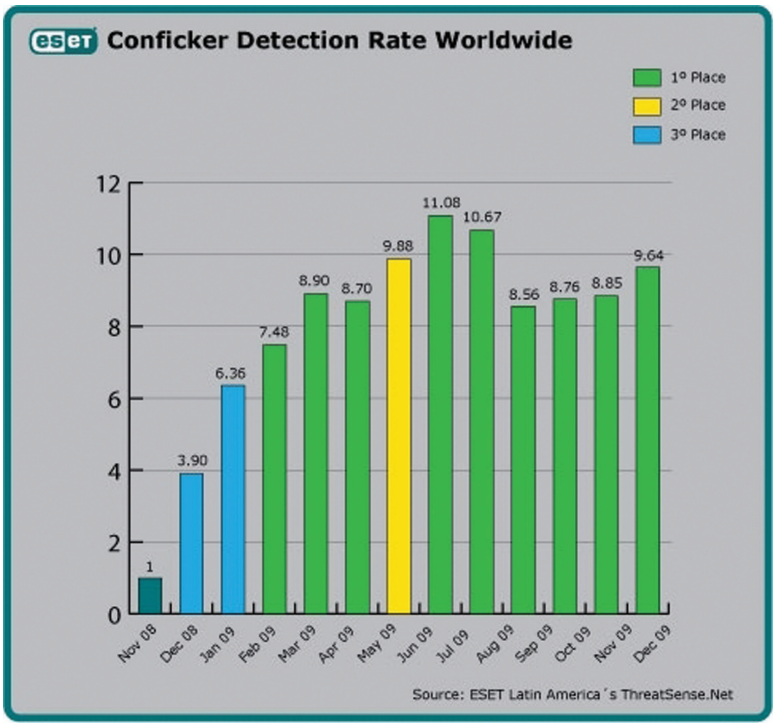

Fig. 1: Conficker worm detection

These numbers confirm that the Conficker infection rates remained stable during the worm's history. Over the whole year, we have seen a worldwide detection rate that allows us to estimate that the malware still remains present in 1-in-10 of the computer systems on which it had been detected.

In the threat reports released every month by ESET, the Conficker worm has been the most detected malware in nine out of the 13 months of 2008-2009 that have already passed at the time of writing. In any case, since its first appearance over a full month, it has always been among the top three threats, even where it wasn't at the number one spot. According to the Conficker Working Group, [13] there were more than 6 million public IP addresses infected by the Conficker worm as of October 15, 2009. Moreover, each one of them can represent many infected machines. The infection rates of the Conficker worm have not only been high, often ranking top of the list, but they have managed to remain consistent over time. The combination of these features is another reason to consider Conficker the most significant threat of 2009 and to merit its prominent place in the history of malware.

$9.1 billion

Since Conficker is being analyzed from a numeric perspective, we still need to determine its economic impact. In April 2009, the Cyber Secure Institute study[14] estimated that the losses generated by the worm might reach $9.1 billion. The same report estimated that, even assuming a conservatively low number of compromised computers (200,000 infected systems), the costs for each group in terms of the time, resources and effort used to fix this problem would reach $200 million.

These numbers are based on analysis of the study group as a whole, although a significant percentage of Conficker infections affected networks of corporations or organizations whose deficits may be even higher.

During its first year of life, Conficker was rumored to have managed to infect, among other organizations, the French Navy[15] and the UK Parliament.[16]

The future

When will the Conficker propagation rates drop? Almost a year after the worm's appearance, the answer to this question still remains uncertain, and if we tried to suggest concrete dates, it might lead to an answer that is as infinite as the title of this final section. Rodney Joffe, director of the Conficker Working Group, stated (when the epidemic was already under way) that it is *"almost impossible to completely remove Conficker."*[17] In further support of his statement, he pointed out that if the worm is removed from 99 out of 100 infected systems in a network, it will still try to reinfect the network from that remaining infected system. (Of course, this is true of many network-aware malicious programs.)

In some months from now, it might be possible to observe how the Conficker propagation rates decrease. However, the more pressing issue is to ask oneself what the community has learned from Conficker's existence.

The worm was detected nearly a month after the release of the remediative Microsoft patch; nevertheless, propagation rates remained high throughout the 12 months or so of its existence. If an epidemic of this kind does not give users the opportunity to learn how to manage security issues efficiently, this indicates that while today's problem may be Conficker, tomorrow there will certainly be another kind of malware creating similar problems.

Software updates are an essential method of enforcing security, since modern malware frequently makes use of exploitable vulnerabilities. In areas like Latin America, the high piracy rates clearly add to this problem, since the number of users who do not use legal software with all the necessary security updates installed is significant.

These cases where, despite the existence of protective technologies, computers continue to become infected, confirm what we regularly assert at ESET Latin America: that user education is a cornerstone of information security, and necessary in order to complement proactive detection technologies. Educated and properly trained users will not only be less frequently exposed to computer threats, but will also make better decisions concerning the use and deployment of security technologies. This is exactly what has failed to happen in the case of Conficker.

Because users are not properly trained and educated to deal with the complex current threat landscape with both awareness and responsibility, it is currently "*impossible*," in Rodney Joffe's own words, to find a 100 percent solution for the problem.

References

1. http://www.microsoft.com/security/updates/bulletins/default.aspx
2. http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
3. http://www.eset.com/threat-center/blog/2008/10/24/a-closer-look-at-gimmiva
4. http://mtc.sri.com/Conficker/
5. http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fConficker.B
6. http://blogs.eset-la.com/laboratorio/2009/01/16/conficker-atraves-autorun/
7. http://www.microsoft.com/Presspass/press/2009/feb09/02-12ConfickerPR.mspx
8. http://www.securityfocus.com/columnists/197
9. http://blogs.eset-la.com/laboratorio/2009/03/28/1-abril-comienza-conficker/
10. http://www.eset.com/threat-center/blog/2009/04/12/win32confickeraq-whats-in-a-name
11. http://blogs.eset-la.com/laboratorio/2009/02/18/novedades-conficker/
12. http://www.eset-la.com/threatsense.net
13. http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking
14. http://cybersecureinstitute.org/blog/?p=15
15. http://www.pcworld.com/article/159224/conficker_worm_sinks_french_navy_network.html
16. http://www.h-online.com/security/news/item/Conficker-infects-UK-parliament-740811.html
17. http://www.smh.com.au/technology/security/internet-meltdown-threat-conficker-worm-refuses-to-turn-20090922-fzlh.html

www.eset.com

ESETCBTNWP20100216