Conficker Virus

Alok Kashyap[1], Ajay Rastogi[2]

[1]*Student, College of Computing Sciences And Information Technology,Teerthanker Mahaveer University, Moradabad*

[2] *Assistant Professor, College of Computing Sciences And Information Technology,Teerthanker Mahaveer University, Moradabad*

[1]alokkashyap03@gmail.com

[2]ajayrastogimbd@gmail.com

Abstract— **In this research paper we are discussing conficker virus. it is a worm for computer. Your Windows PC can infected by conficker worm. The Conficker is the most recent prevalent, renowned worm/bot. According to many research reports, it has infected 6.9 million to 14.9 million hosts and the victims are still growing even now. we analysed Conficker infections and we studies various interesting facets about this malware. The Conficker is a computer worm that vented on the Internet. This Conficker virus is automatically spread itself to other computers across a network interaction. Having many ways to remove the conficker virus. if you have a doubt that your computer infected by the Conficker worm,than you have to download the Conficker worm removal tool.**

this tool burns onto a CD. and run it on the infected computer. In this research paper we are tells about to conficker virus, than how to remove it, how to know you, is it in your computer. We can well known that computer & network security is an challenge. Attackers are incremented exploiting and defenders does respond to them over updates, service packs and doing other defensive measures. This reseach paper contain the details about to study of the coevolution of the Conficker Worm and associated defences against it. We observe that Conficker has some very different victim distribution patterns compared to many previous generation worms/botnets, suggesting that new malware spreading models and defence strategies are likely needed. We measure the potential power of Conficker to estimate its effects on the networks/hosts when it performs malicious operations.

Keywords— **Conficker, Botnet, Botnet Defence, Conficker removal tool.**

I. INTRODUCTION

Conficker worm [1] first appeared in November 2008 and rapidly spread in the world within a short period. It exploits a NetBIOS vulnerability in various Windows operating systems and utilizes many new, advanced techniques such as a domain generation algorithm, self-defense mechanisms, updating via Web and P2P, and efficient local propagation [2]. As a result, it has infected millions of victims in the world and the number is still increasing even now [3].

It is clear that the complex nature of Conficker makes it one of the state-of-the-art botnets, and therefore the analysis of Conficker is very important in order to defend against it. A full understanding of Conficker can also help us comprehend current and future malware trends. Existing research of Conficker analysis mainly falls into two categories. The first focuses on analyzing the Conficker binary and its behaviour.[4]

A preliminary version of this paper appeared in [5]

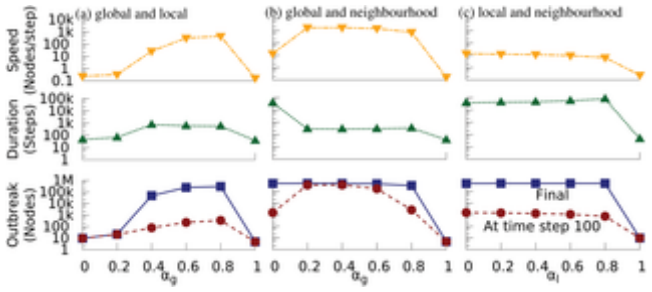
In this direction, SRI researchers [6] and the Honeynet project [8] already provided excellent reports that analyzed Conficker in great detail. The second research category mainly focuses on analyzing the network telescope data [7] or DNS sinkhole data [9] to reveal the propagation pattern and victim distribution characteristics of Conficker on the Internet. There are very few studies in this direction, which is probably because it is very hard to obtain large scale real-world data of victims and the amount of data should be large enough to cover victims' global behaviour. CAIDA [7] and Team Cymric [9] provided some initial reports which contain some very basic statistics on the scanning pattern and propagation information of Conficker. However, for a worm/bot that has infected so many victims and has so much potential to damage the Internet, it deserves a much deeper study. Such study is necessary because by analysing this state of-the-art botnet, we can gain more knowledge of current malware, e.g., how it differs from previous generation malware and whether such differences represent future trends or not. These deeper investigations could also provide new insights in developing new detection and defence mechanisms for current and future malware. In this paper, we attempt to provide a deeper empirical measurement

study of Conficker. We have collected a large-scale data set which contains almost 25 million Conficker victims with the help of Shadowserver.org (details on data collection are discussed in Section III). We believe such scale is large enough to uncover Conficker's global patterns. We provide an extensive measurement of various distribution patterns of Conficker victims. Furthermore, we use a comparison- and cross-check-based methodology in our measurement study. We study the similarities and differences between Conficker and several other publicly reported worms/botnets. Then we analyse how these differences may affect existing reputation based detection approaches. We also investigate possible aspects that may be useful for Conficker and future malware defence. In short, this paper makes the following contributions:[4]

• We provide a large-scale empirical study of almost 25 million Conficker victims. By analyzing this data, we reveal many interesting aspects that were previously unknown and show that Conficker victims exhibit a very different distribution pattern from many previously reported botnets or worms. This difference could be a new trend or some ignored facts that are potentially important for future malware defence. Detailed information is in Section IV.[4]

It contain this figure which is defining graph of the Conficker worms.

Figures



II. SPREAD CONFICKER WORM

The Conficker virus is spreades your computer by through any removeable drives. The Conficker worm does infected by copying itself in the Windows system folder. It influence also spread through file sharing and through removable drives, like as USB drives , specially those with non-strong passwords. The virus enhances a file to the removable drive so that when the drive is used, the AutoPlay dialog box will show one supplementary option. In these following screenshot of the Autoplay dialog box, below Install or execute program, the first option Open folder to view files Publisher not stated was added by the worm. The option that is underlined, the Open folder to view files using Windows Explorer, is the option that Windows provides and the option you should use.

III. HISTORY

NAME

The origin of the name Conficker is thought to be a combination of the English term "configure" and the German pejorative term Ficker (engl. fucker).[10] Microsoft analyst Joshua Phillips gives an alternate interpretation of the name, describing it as a rearrangement of portions of the domain name trafficconverter.biz[11] (with the letter k, not found in the domain name, added as in "trafficker", to

avoid a "soft" c sound) which was used by early versions of Conficker to download updates.[15]

Discovery of Conficker

The first variant of Conficker, discovered in early November 2008, propagated through the Internet by exploiting a vulnerability in a network service (MS08-067) on Windows 2000, Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 Beta.[14]While Windows 7 may have been affected by this vulnerability, the Windows 7 Beta was not publicly available until January 2009. Although Microsoft released an emergency out-of-band patch on October 23, 2008 to close the vulnerability,[12] a large number of Windows PCs (estimated at 30%) remained unpatched as late as January 2009.[13] A second variant of the virus, discovered in December 2008, added the ability to propagate over LANs through removable media and network shares.[18] Researchers believe that these were decisive factors in allowing the virus to propagate quickly.[15]

Conficker virus Impact in Europe

Intramar, the French Navy computer network, was infected with Conficker on 15 January 2009. The network was subsequently quarantined, forcing aircraft at several airbases to be grounded because their flight plans could not be downloaded[16]

The United Kingdom Ministry of Defence reported that some of its major systems and desktops were infected.[17] The virus had spread across administrative offices, NavyStar/N* desktops aboard various Royal Navy warships and Royal Navy submarines, and hospitals across the city of Sheffield reported infection of over 800 computers [18]

An infection of Manchester City Council's IT system caused an estimated £1.5m worth of disruption in February 2009. The use of USB flash drives was banned, as this was believed to be the vector for the initial infection.[19]

A memo from the Director of the UK Parliamentary ICT service informed the users of the House of Commons on 24 March 2009 that it had been infected with the virus. The memo, which was subsequently leaked, called for users to avoid connecting any unauthorised equipment to the network.[20]

In January 2010, the Greater Manchester Police computer network was infected, leading to its disconnection for three days from the Police National Computer as a precautionary measure; during that time, officers had to ask other forces to run routine checks on vehicles and people.[21]

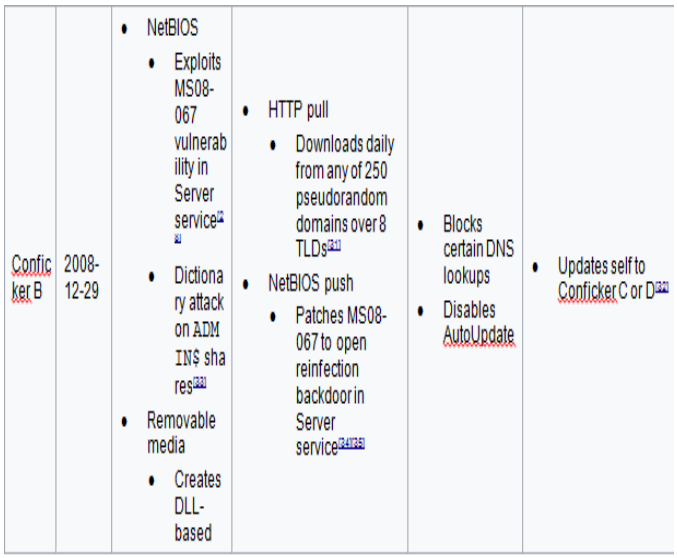
Operation of Conficker

Although almost all of the advanced malware techniques used by Conficker have seen past use or are well known to researchers, the virus' combined use of so many has made it unusually difficult to eradicate.[22] The virus' unknown authors are also believed to be tracking anti-malware efforts from network operators [23] and law enforcement and have regularly released new variants to close the virus' own vulnerabilities. [24]

Five variants of the Conficker virus are known and have been dubbed Conficker A, B, C, D and E. [25]They were discovered 21 November 2008, 29 December 2008, 20 February 2009, 4 March 2009 and 7 April 2009, respectively.[26]

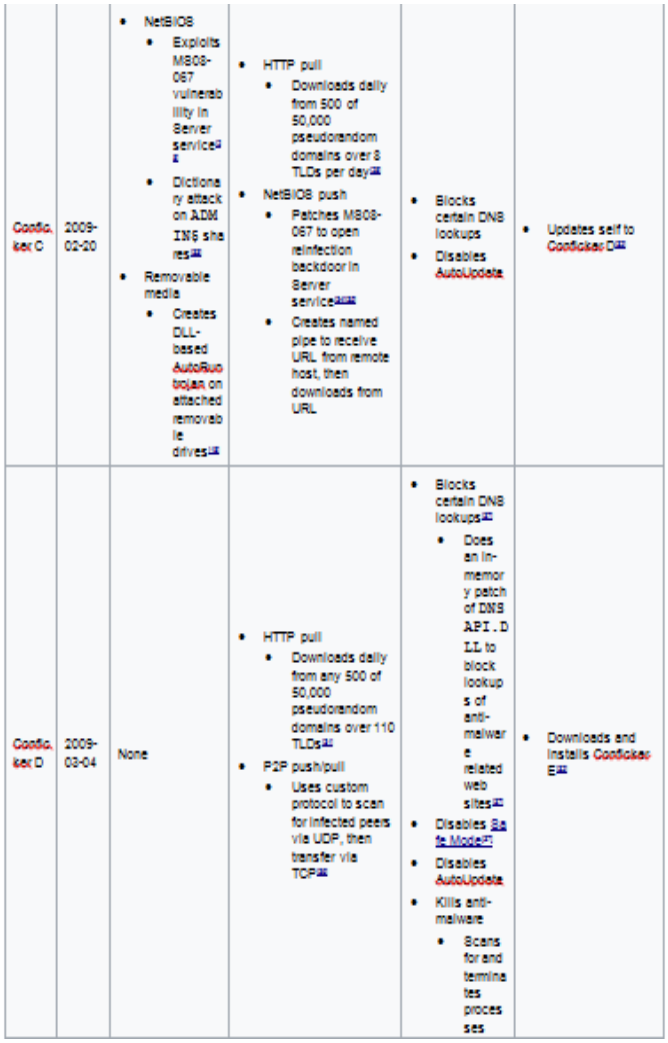
Variant	Detection date	Infection vectors	Update propagation	Self-defense	End action
Conficker A	2008-11-21	• NetBIOS • Exploits MS08-067 vulnerability in Server service[2][3]	• HTTP pull • Downloads from trafficconverter.biz • Downloads daily from any of 250 pseudorandom domains over 5 TLDs[31]	None	• Updates self to Conficker B, C or D[32]

[15]



Conficker B	2008-12-29	• NetBIOS
		  • Exploits MS08-067 vulnerability in Server service
		  • Dictionary attack on ADMIN$ shares
		• Removable media
		  • Creates DLL-based
			• HTTP pull
			  • Downloads daily from any of 250 pseudorandom domains over 8 TLDs
			• NetBIOS push
			  • Patches MS08-067 to open reinfection backdoor in Server service
				• Blocks certain DNS lookups
				• Disables AutoUpdate
					• Updates self to Conficker C or D

[15]



Conficker C	2009-02-20	• NetBIOS
		  • Exploits MS08-067 vulnerability in Server service
		  • Dictionary attack on ADMIN$ shares
		• Removable media
		  • Creates DLL-based AutoRun trojan on attached removable drives
			• HTTP pull
			  • Downloads daily from 500 of 50,000 pseudorandom domains over 8 TLDs per day
			• NetBIOS push
			  • Patches MS08-067 to open reinfection backdoor in Server service
			  • Creates named pipe to receive URL from remote host, then downloads from URL
				• Blocks certain DNS lookups
				• Disables AutoUpdate
					• Updates self to Conficker D

Conficker D	2009-03-04	None	• HTTP pull
			  • Downloads daily from any 500 of 50,000 pseudorandom domains over 110 TLDs
			• P2P push/pull
			  • Uses custom protocol to scan for infected peers via UDP, then transfer via TCP
				• Blocks certain 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
					• Downloads and installs Conficker E

[15]

CONFICKER VIRUS REMOVAL AND DETECTION

Microsoft has released a removal guide for the virus, and recommends using the current release of its Windows Malicious Software Removal Too.[27] to remove the virus, then applying the patch to prevent re-infection.[28]

Third-party software

Many third-party anti-virus software vendors have released detection updates to their products and claim to be able to remove the worm.[15]

IV. Conclusions

Our study uses data collected during the first day of the Conficker epidemic to parametrise a hybrid model to capture the worm's spreading behaviour. The study highlights the importance of mixing different modes of spreading in order to achieve large, rapid and sustained epidemics, and suggests that the trade-off between the different modes of spreading will be critical in determining the epidemic outcome.

Acknowledgement

We would like to thank GOOGLE for his comments and i want a feedback to improve the research paper.

References

[1] M. S. Techcenter. Conficker worm. http://technet.microsoft.com/en-us/ security/dd452420.aspxJ.

[2] B. N. Online. Clock ticking on worm code. http://news.bbc.co.uk/2/hi/ technology/7832652.stm.

[3] UPI. Virus strikes 15 million PCs. http://www.upi.com/Top News/2009/ 01/26/Virus-strikes-15-million-PCs/UPI-19421232924206.

[4] http://faculty.cs.tamu.edu/guofei/paper/Shin_TIFS12_Conficker.pdf

[5] S. Shin and G. Gu. ”Conficker and Beyond: A Large-Scale Empirical Study”. In Proceedings of 2010 Annual Computer Security Applications Conference (ACSAC), Dec. 2010.

[6] SRI-International. An analysis of Conficker C. http://mtc.sri.com/ Conficker/addendumC/.

[7] CAIDA. Conficker/Conflicker/Downadup as seen from the UCSD Network Telescope. http://www.caida.org/research/security/ms08-067/ onficker.xml

[8] D. Watson. Know Your Enemy: Containing Conficker. http://www. honeynet.org/papers/conficker.

[9] J. Kristoff. Experiences with Conficker C Sinkhole Operation and Analysis. In Proceedings of Australian Computer Emergency Response Team Conference, May 2009

[10] *Phillips, Joshua, Malware Protection Center - Entry: Worm:Win32/Conficker.A, Microsoft, retrieved 2009-04-01*

[11] *Grigonis, Richard (2009-02-13), Microsoft's US$5 million Reward for the Conficker Worm Creators, IP Communications, retrieved 2009-04-01*

[12] *Microsoft Security Bulletin MS08-067 – Critical; Vulnerability in Server Service Could Allow Remote Code Execution (958644), Microsoft Corporation, retrieved 2009-04-15*

[13] *Leyden, John (2009-01-19), Three in 10 Windows PCs still vulnerable to Conficker exploit, The Register, retrieved 2009-01-20*

[14] Leffall, Jabulani (2009-01-15). "Conficker worm still wreaking havoc on Windows systems". Government Computer News. Retrieved 2009-03-29.

[15] *https://en.wikipedia.org/wiki/Conficker.*

[16] *Willsher, Kim (2009-02-07), French fighter planes grounded by computer worm, London: The Daily Telegraph, retrieved 2009-04-01*

[17] *Williams, Chris (2009-01-20), MoD networks still malware-plagued after two weeks, The Register, retrieved 2009-01-20*

[18] *Williams, Chris (2009-01-20), Conficker seizes city's hospital network, The Register, retrieved 2009-01-20*

[19] *Leyden, John (1 July 2009). "Conficker left Manchester unable to issue traffic tickets". The Register.*

[20] *Leyden, John (2009-03-27), Leaked memo says Conficker pwns Parliament, The Register, retrieved 2009-03-29*

[21] *"Conficker virus hits Manchester Police computers". BBC News. 2010-02-02. Retrieved 2010-02-02.*

[22] *Nahorney, Ben; Park, John (2009-03-13), "Propagation by AutoPlay", The Downadup Codex (PDF), Symantec, p. 2, retrieved 2009-04-01*

[23] *Markoff, John (2009-03-19), Computer Experts Unite to Hunt Worm, New York Times, retrieved 2009-03-29*

[24] *Phillip Porras, Hassen Saidi, Vinod Yegneswaran (2009-03-19), An Analysis of Conficker, SRI International, archived from the original on 2009-04-01, retrieved 2009-03-29*

[25] *Tiu, Vincent (2009-03-27), Microsoft Malware Protection Center: Information about Worm:Win32/Conficker.D, Microsoft, retrieved 2009-03-30*

[26] *Macalintal, Ivan; Cepe, Joseph; Ferguson, Paul (2009-04-07), DOWNAD/Conficker Watch: New Variant in The Mix?, Trend Micro, retrieved 2009-04-07*

[27] *Malicious Software Removal Tool, Microsoft, 2005-01-11, retrieved 2009-03-29*

[28] *Protect yourself from the Conficker computer worm, Microsoft, 2009-03-27, retrieved 2009-03-30*