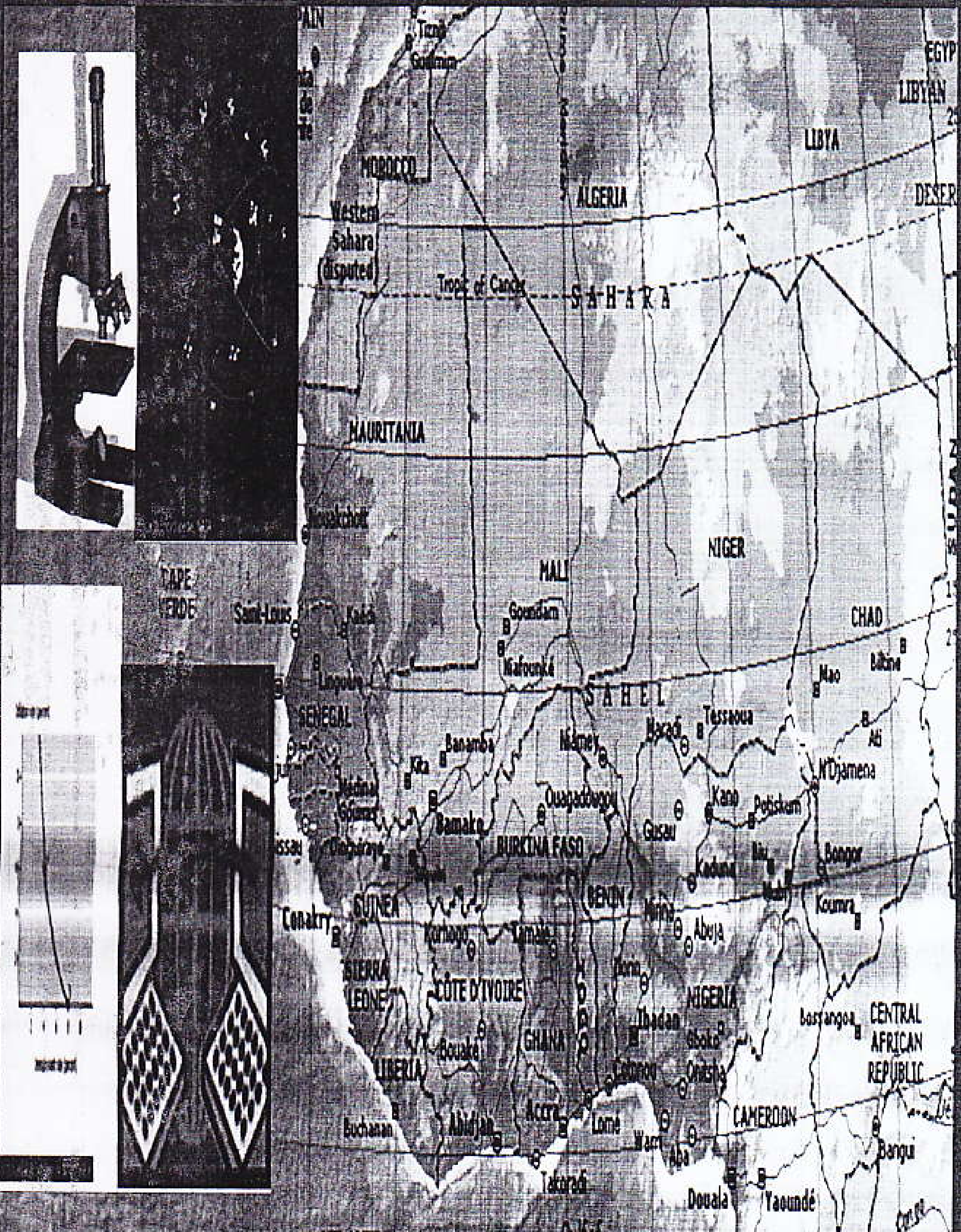
ISSN 1116 - 7711

VOL. 1 NO. 1 JANUARY, 2011

WEST AFRICA JOURNAL OF SCIENCE, TECHNOLOGY AND SOCIAL SCIENCES

www.wajostech.org



CONFICKER: AN ENVIABLE THREAT TO A COMPUTER AND INTERNET SYSTEM

[1]ADEBAYO O.S., [2]AMIT MISHRA , [3]MABAYOJE M.A., [4]ABIKOYE O.C. AND [5] OLAGUNJU MUKAILA.

[1] Department of Mathematics and Computer Science, Faculty of Applied and Natural Sciences, Ibrahim Badamosi Babangida University, PMB 11 Lapai, Niger State-Nigeria.
olawalebayo@yahoo.com

[2] Department of Mathematics and Computer Science, Faculty of Applied and Natural Sciences, Ibrahim Badamosi Babangida University, PMB 11 Lapai, Niger State-Nigeria.
i.amitmishra@gmail.com

[3, 4, 5] Department of Computer Science, Faculty of Communication and information Sciences, University of Ilorin, PMB 1515 Ilorin, Kwara State-Nigeria.
services100ng@yahoo.com
mabayoje.ma@unilorin.edu.ng

ABSTRACT

The fear of Computer worms and virus have became the beginning of wisdom for most computer users just as they both pose threats to the computer and its all activities, organs and usefulness of computer system. Most of the computer and internet users cannot also differentiate between Computer Virus and Worms and therefore risk a high damage to their system by performing various kinds of activities that are harmful to their system. The categories, damages, symptoms, preventions of a Conficker worm among others are discussed in this paper.

Keywords: *Computer, Conficker, Damages, Internet, Symptoms, Threat, Users, Virus.*

1.0 INTRODUCTION

The threats by a virus and worms to a computer and internet system have considerably been a source of concern to the computer and internet users. The work or research over the year can easily be destroyed in a second by these elements. Communication over the internet can be easily blocked, various form of theft activities has been carried out due to the vulnerabilities of a computer and internet system [1]. A **computer virus** is a computer program that can copy itself and infect a computer. The term "virus" is also commonly but erroneously used to refer to other types of malware, adware, and spyware programs that do not have the reproductive ability. A true virus can only spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance because a user sent it over a network or the Internet, or carried it on a removable medium such as a floppy disk, CD, DVD, or USB drive. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer [1], [2].

As stated above, the term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, adware, and spyware programs that do not have the reproductive ability. Malware includes computer viruses, worms, trojans, most rootkits, spyware, dishonest adware, crime ware, and other malicious and unwanted software, including true viruses. Viruses are sometimes confused with computer worms and Trojan horses, which are technically different. A worm can exploit security vulnerabilities to spread itself automatically to other computers through networks, while a Trojan is a program that appears harmless but hides malicious functions. Worms and Trojans, like viruses, may harm a computer system's data or performance. Some viruses and other malware have symptoms noticeable to the computer user, but many are surreptitious and go unnoticed [1], [3].

A computer worm is a self-replicating Malware computer program. It uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. This is due to security shortcomings on the target computer. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer [4], [6] and [7].

Due to the alarming rate of widely frauds in the banking sectors through the ATM machine, duping of people of all forms on the internet, among others allegedly being perpetrated by the fraudsters through the vulnerabilities of internet system, there should be strict measures of various form in order to regulate and eradicate the threats being posed by these people through the aid of computer worms and virus. Computer worms assist the fraudster by installing itself on the host computer and collecting important information for its end user (hacker).

2.0 LITERATURE REVIEW

2.1 Definition of a Conficker

Conficker, also known as **Downup**, **Downadup** and **Kido**, is a computer worm targeting the Microsoft Windows operating system that was first detected in November 2008. It uses flaws in Windows software and Dictionary attacks on administrator passwords to co-opt machines and link them into a virtual computer that can be commanded remotely by its authors. Conficker has since spread rapidly into what is now believed to be the largest computer worm infection since the 2003 SQL Slammer, with more than seven million government, business and home computers in over 200 countries now under its control. The worm has been unusually difficult to counter because of its combined use of many advanced malware techniques [1],[8] and [11].

2.2 History of Conficker

The origin of the name Conficker is thought to be a portmanteau of the English term "configure" and the German word *Ficker*, which means "to have sex with" or "to mess with" in colloquial German Microsoft analyst Joshua Phillips gives an alternate interpretation of the name, describing it as a rearrangement of portions of the domain name traffic converter.biz, which was used by early versions of Conficker to download updates [12] , [13] and [16].

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. 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, a large number of Windows PCs (estimated at 30%) remained unpatched as late as January 2009. A second variant of the worm, discovered in December 2008, added the ability to propagate over LANs through removable media and network shares. Researchers believe that these were decisive factors in allowing the worm to propagate quickly: by January 2009, the estimated number of infected computers ranged from almost 9 million to 15 million. Antivirus software vendor Panda Security reported that of the 2 million computers analyzed through ActiveScan, around 115,000 (6%) were infected with Conficker.

Recent estimates of the number of infected computers have been more notably difficult because of changes in the propagation and update strategy of recent variants of the worm [15],[20] and [21].

3.0 CONFICKER: ITS OPERATION, CATEGORIES AND DETECTION

3.1 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 worm's unknown authors are also believed to be tracking anti-malware efforts from network operators and law enforcement and have regularly released new variants to close the worm's own vulnerabilities.

3.2 Categories of Conficker

Five variants of the Conficker worm are known and have been dubbed Conficker A, B, C, D and E. They were discovered 21 November 2008, 29 December 2008, 20 February 2009, 4 March 2009 and 7 April 2009, respectively. See appendix for details

4.0 METHODS OF SPREADING OR DISTRIBUTION OF CONFICKER

Conficker can be 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. 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, a large number of Windows PCs (estimated at 30%) remained unpatched as late as January 2009.

A second variant of the worm, discovered in December 2008, added the ability to propagate over LANs through removable media and network shares. Researchers believe that these were decisive factors in allowing the worm to propagate over LANs through removable media and network shares.

5.0 SYMPTOMS OF CONFICKER WORM

The specific target of this viral attack is the Windows OS. If your computer is acting a little quirky lately you might want to find out if your PC has the CF worm.

Below are some basic examples of how to know if you have the Conficker worm on your computer. Due to the unique nature of the Conficker worm, there are some very prominent symptoms that your computer will have if the CF virus is present.

1. Locking-Out of Directory

If you find that you cannot access some directories on your computer, this might be a strong sign that you possibly have the Conficker worm on your PC.

This symptom is especially prominent if you are the computer's administrator.

2. Performance of Unscheduled Tasks

If a computer starts resetting restore points or account lock-out policies are resetting automatically, then this can be a sign that your PC has been infected.

3. It Disabled Windows Services Operation

Certain Windows services such as Windows Defender, Automatic update, error reporting and the Domain Name System have been disabled without your request.

This is a very strong sign that the Windows OS has been compromised.

4. **Anti-virus Software Sites Access are being denied**

If you are trying to access Websites that provide Internet security software and either cannot gain access or the load time is extremely long, this may be another indicator that the Conficker Worm is present in your computer.

6.0 PROTECTION AGAINST DANGEROUS COMPUTER WORMS

1. Worms spread by exploiting vulnerabilities in operating systems. All vendors supply regular security updates (see "Patch Tuesday"), and if these are installed to a machine then the majority of worms are unable to spread to it. If a vendor acknowledges vulnerability, but has yet to release a security update to patch it, a zero day exploit is possible. However, these are relatively rare.
2. Users need to be wary of opening unexpected email, and should not run attached files or programs, or visit web sites that are linked to such emails. However, as with the ILOVEYOU worm, and with the increased growth and efficiency of posing attacks, it remains possible to trick the end-user into running a malicious code.
3. Anti-virus and anti-spyware software are helpful, but must be kept up-to-date with new pattern files at least every few days. The use of a firewall is also recommended.
4. In the April-June, 2008, issue of IEEE Transactions on Dependable and Secure Computing, computer scientists describe a potential new way to combat internet worms. The researchers discovered how to contain the kind of worm that scans the Internet randomly, looking for vulnerable hosts to infect. They found that the key is for software to monitor the number of scans that machines on a network send out. When a machine starts sending out too many scans, it is a sign that it has been infected, allowing administrators to take it off line and check it for viruses.

6.1 How to remove a Conficker Worm?

The only concern of millions of individual who have recently found the Conficker worm on their computer is how to get rid of the worm. It is highly commendable to diagnose and detect the presence of the worm on the system since many people overlook the dormant but deadly virus until it is too late and their operating systems have been destroyed.

However, the fact that you have been observant and caught it out does not mean that your worries are over; in fact, they have probably just begun.

It is in fact advisable for an individual with more than one computer at home to avoid transferring any removable devices between the computers until the Conficker worm has been deleted. This is because the virus has a Variant B which will hide in removable devices and then attack during an auto-run function. So the first very initial action should be to control the reach of the Conficker virus within the home.

Next, because the Conficker worm will disable the anti-virus programs and automatic updates on the system, one need to out think the strand by downloading anti-virus software in once email.

The virus will prevent accessing any anti-virus websites that offer the security patch to eliminate the threat or download the software to destroy it. However, it will not prevent opening email so if an antivirus is downloaded to erase the Conficker virus from another source then one should be able to access and start the download to clean the system.

If this does not work, a computer might have to be taken to a computer expert who specializes in deleting viruses because one may need to have computer reformatted, which can be a dangerous job for a computer novice. Plus, if the job is not properly executed, one may risk losing vita data as well as re-infecting system again with the Conficker worm once reformatting is complete.

6.2 Removal and detection

Microsoft has released a removal guide for the worm, and recommends using the current release of its Windows Malicious Software Removal Tool to remove the worm, then applying the patch to prevent re-infection.

i) Third-parties

Third-party anti-virus software vendors AVG Technologies, McAfee, Panda Security, BitDefender, ESET, F-Secure, Symantec, Sophos, Kaspersky Lab Trend Micro and Sunbelt Software have released detection updates to their products and claim to be able to remove the worm.

ii) Automated remote detection

On 27 March 2009, Felix Leder and Tillmann Werner from the Honeynet Project discovered that Conficker-infected hosts have a detectable signature when scanned remotely. The peer-to-peer command protocol used by variants D and E of the worm has since been partially reverse-engineered, allowing researchers to imitate the worm network's command packets and positively identify infected computers en-masse.

Signature updates for a number of network scanning applications are now available including NMap and Nessus.. In addition, several commercial vendors have released dedicated scanners, namely eEye and Mcafee. It can also be detected in passive mode by sniffing broadcast domains for repeating ARP requests.

iii) US CERT

The United States Computer Emergency Readiness Team (US-CERT) recommends disabling AutoRun to prevent Variant B of the worm from spreading through removable media. Prior to the release of Microsoft knowledgebase article KB967715, US-CERT described Microsoft's guidelines on disabling Autorun as being "not fully effective" and provided a workaround for disabling it more effectively. US-CERT has also made a network-based tool for detecting Conficker-infected hosts available to federal and state agencies.

7.0 CONCLUSIONS

The degree of damages done to the computer and internet system by the computer worms and its cost implication is highly noteworthy. Conficker has since spread rapidly into what is now believed to be the largest computer worm infection since the 2003 SQL Slammer, with more than seven million government, business and home computers in over 200 countries now under its control.

The specific target of this viral attack is the Windows OS. Conficker worm makes computer to act a little quirky lately. Due to the unique nature of the Conficker worm, it has some very prominent symptoms which can be diagnosed and on which the solution can be proffered. The difference between a computer worms and virus should highly realise in order to know the appropriate solution for the system.

As part of technical approach to solving problems of worm, all vendors must supply regular security updates, and these must be installed to a machine to disallow the majority of worms from spreading to it. Users must be wary of opening unexpected email, and should not run attached files or program that is not trustworthy. Anti-virus and anti-spyware software that are helpful, but up-to-date with new pattern files at least every few days is another panacea for combating the Conficker worm.

REFERENCES

[1] Markoff, John (2009). "Worm Infects Millions of Computers Worldwide". *New York Times*. http://nytimes.com/2009/01/23/technology/internet/23worm.html.

[2] Protect yourself from the Conficker computer worm, Microsoft, 2009-04-09, http://www.microsoft.com/protect/computer/viruses/worms/conficker.mspx.

[3] Defying Experts, Rogue Computer Code Still Lurks", New York Times, 2009-08-26. http://www.nytimes.com/2009/08/27/technology/27compute.html.

[4] Grigonis, Richard (2009). *Microsoft's US$5 million Reward for the Conficker Worm Creators*, IP Communications,http://ipcommunications.tmcnet.com/topics/ip-communications/articles/50562-microsofts-5000000-reward-the-conficker-worm-creators.htm.

[5] Phillips, Joshua, *Malware Protection Center - Entry: Worm:Win32/Conficker.A*, Microsoft, http://www.microsoft.com/security/portal/Entry.aspx?Name=Worm:Win32/Conficker.a.

[6] Leffall, Jabulani (2009). "Conficker worm still wreaking havoc on Windows systems". Government Computer News. http://gcn.com/Articles/2009/01/15/Conficker-worm-still-lurks.aspx.

[7] Microsoft Security Bulletin MS08-067 – Critical: Vulnerability in Server Service Could Allow Remote Code Execution (958644), Microsoft Corporation, http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx.

[8] Leyden, John (2009). *Three in 10 Windows PCs still vulnerable to Conficker exploit*. The Register. http://theregister.co.uk/2009/01/19/conficker_worm_feed.

[9] Nahorney, Ben; Park, John (2009). "Propagation by AutoPlay". *The Downadup Codex*, Symantec.pp. 32.http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_downadup_codex_ed1.pdf.

[10] "Clock ticking on worm attack code". *BBC News Online* (BBC).http://news.bbc.co.uk/1/hi/technology/7832652.stm.'

[11] Sulivan, Sean (2009). "Preemptive Blocklist and More Downadup Numbers". http://f-secure.com/weblog/archives/00001582.html.

[12] Neild, Barry (2009). *Downadup Worm exposes millions of PCs to hijack*, http://edition.cnn.com/2009/TECH/ptech/01/16/virus.downadup/?iref=mpstoryview.

[13] Virus strikes 15 million PCs, UPI, 2009-01-26. http://upi.com/Top_News/2009/01/25/Virus_strikes_15_million_PCs/UPI-19421232924206.

[14] "Six percent of computers scanned by Panda Security are infected by the Conficker worm". Panda Security. http://www.pandasecurity.com/homeusers/media/press-releases/viewnews?noticia=9526.

[15] McMillan, Robert (2009), "Experts bicker over Conficker numbers", *Techworld* (IDG), http://www.techworld.com/news/index.cfm?RSS&NewsID=114307.

[16] Willsher, Kim (2009), "French fighter planes grounded by computer worm", http://telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html,

[17] Williams, Chris (2009), MoD networks still malware-plagued after two weeks, http://theregister.co.uk/2009/01/20/mod_malware_still_going_strong.

[18] Williams, Chris (2009), *Conficker seizes city's hospital network*, http://theregister.co.uk/2009/01/20/sheffield_conficker.

[19] Leyden, John (2009), "Conficker left Manchester unable to issue traffic tickets". http://www.theregister.co.uk/2009/07/01/conficker_council_infection/.

[20] Leyden, John (2009), "*Leaked memo says Conficker pwns Parliament*" http://theregister.co.uk/2009/03/27/conficker_parliament_infection.

[21] Markoff, John (2009), "*Computer Experts Unite to Hunt Worm*", New York Times, http://www.nytimes.com/2009/03/19/technology/19worm.html?_r=1&ref=us

BIOGRAPHY

Mabayoje, M. A. has MSc. and BSc. Computer Science, University of Ilorin, Nigeria (2009 and 2003). She teaches Computer Science in the University. She is a full member of Computer Professionals (Registration) Council of Nigeria (MCPN) and Science Association of Nigeria (SAN). Her research interests include Ontology, Information System, Knowledge Management, Database Retrieval System, and Software Engineering.