International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

Notable security breaches exploited through Storm Worm Malware

Supun Dissanayake
University of Colombo School of Computing

Abstract:

Malicious Software (Malware) plays a vital part in security issues for internet users. They consist of potent ability to extract vital information from their prey. Thus, this research report investigates one of the most powerful malwares: Storm Worm. It identifies its history, effect and prevention mechanisms.

Key Words: Malware, Security, Forensics, Social Engineering, Computer Virus, Trojans, Rootkits

1. Introduction

Computer malware has been an influential component of the internet during last few decades and as the technology advances, their technicality, threat and damage are becoming more fearsome. Storm worm is regarded as one of the most sophisticated malware that the mankind has witnessed during the last decade. It was discovered on 17th January 2007; it was originated in Russia [1]. Furthermore, it has alternative names: "Small.DAM", "Peacomm", "Nutware" etc, given by various anti-virus companies [2]. Storm is extremely intricate due to its use of a combination of sophisticated techniques.

2. Infection Process

Social Engineering

In order to magnetize the attention of the victim, Storm sends emails with striking subject lines such as, "230 dead as storm batters Europe", "British Muslims Genocide" etc, with attachments to victims through bots. Then by using executable files such as "ReadMore.exe", "FullClip.exe", "FullVideo.exe" and disguising them as video and news files, the malware efficiently tries to deceive the victim and spread its content [3].

Installation and spread

For networking processes, Strom uses overnet protocol, which is based on Kademlia algorithm. Kademlia supports the decentralized structure of peer to peer botnets using its system of distributed hash tables [4]. After the malware installation, it adds itself into "services.exe" process; then Storm installs initial infection files such as "peers.ini" alongside "windows32.sys", which is a kernel mode driver component [3]. and commences its bootstrap process. Furthermore, these initiation files possess 146 nodes which are elements of the botnet; the corrupted computer connects to these nodes and becomes a peer. Then the latest bot explores the network, discovers encrypted URL with secondary injection payload, downloads it after decryption and executes it on the bot. Spam emails, DDoS attacks and all other malevolent botnet activities are resulted by this secondary injection code [5].

Trojans and Rootkits

According to Smith [6], it uses Trojans to open backdoors to the victims' system, which can be used to obtain the computers authority. This Trojan always disguises itself as a legitimate file and simultaneously carries a rootkit. The rootkit masks the software by differentiating the kernel code; thus, the anti-virus programs find it difficult to detect the malware. In order to remove evidence, the rootkit replaces the binary code that shows the system files and processes. Furthermore, it removes particular API calls related to the Storm and deletes entire files to hide the presence of malware. The coding of genuine drivers in the windows registry is also modified by the storm in order to activate the malware whenever the windows initiate.

3. Malicious Activities

Storm has been involved in many criminal activities. IBM suggested that Storm is making about $2 million per day thorough spam attacks and directing traffic [7]. According to Hypponen, "it's smaller and targeted" Trojan attacks are purely used to steal personal data for financial gain [8]. Moreover, Kevin Haley suggested that it makes money in the underground economy because it uses spam for illegal "pump and dump" schemes, which promotes cheap stocks in order to sell them for a large profit. Moreover, it can upload key logging software through Trojans to capture keystrokes and steal vital personal information [6].

4. Legal Aspects

There are many legal aspects involved with Storm Worm. Storm disobeys first, second and fifth principles of Data Protection Act-1998 [9]. According to the first principle, data should be processed fairly and lawfully, however, Storm deceptively obtains data and uses them without the users' acceptance. It employs data for unlawful purposes implying its negligence of the second principle. Moreover, once it takes over a computer, it uses its data perpetually implying that it exploits data longer than necessary by breaking the fifth principle.

It also breaches Computer Misuse Act-1990 [10] in its all three sections. It breaches into systems without authorization by breaking the section 1 and then it uses them to cause serious offences as depicted above. Thus, it breaks the section 2 of CMA. Moreover, its unauthorized modifications to computers and use of viruses break the third section of CMA.

Furthermore, companies must take individuals permission prior to sending emails. However, Storm sends spam emails without gaining permission; thus, it breaks Privacy and Electronic Communications Regulations-2003 [11].

5. Recommendations

Self-protection

It has been extremely difficult to stop Storms malicious activity since it uses a range of techniques. Due to its decentralized nature, Storm possesses multiple zombies. Hence, security experts cannot target a single server to demolish its activities. It only uses few zombies for spreading and for command and control purposes while the rest wait for instructions, thus even if some of them get caught, the network will still be unbroken and other zombies will gain control. It uses 40-bit encryption to hide its coding, it removes bots from the system for long periods to prevent detection and the core-code is replaced 10 times per hour; hence it is difficult to track and identify the malware. Moreover, fast fluxing hides websites that infect users and the public domain-name of compromised computers change frequently, making it complex for security experts to hunt down the malware [6].

Attack Prevention

There are few methods that can be undertaken to prevent attacks from the Storm. It is important not to open email attachments from unknown sources, especially when they are linked to another website. Also, updating windows and installing plug-ins for software prevent Storm Attacks since these updates are intended to prevent loopholes in the existing system. Moreover, it is important to install powerful antivirus software since they are specifically created to track down malware such as Storm Worm. Furthermore, host-based software firewall with filtering and notification facilities for outbound network connections will inform if there are any malicious activity related to the computer [12].

Conclusion

Overall, it accentuates the colossal strength of Storm as a malware. Its usage of various techniques makes it more influential compared to its peers. Usage of sophisticated self-protective methods makes it difficult to track down by the security experts. Furthermore, its malevolent activity directed towards financial gain and the damages that it had caused were immense. Thus, it breaks vital laws which denote its illegal nature. It is tremendously difficult to combat the Storm to end its existence, however, numerous methods can be undertaken to prevent its initial installation. Thus, according to The Telegraph [13], Storm Worm is ranked 10 in the "top 10 worst computer viruses of all time".

References

[1]. Leyden, J. (2008) **Storm Worm turns one** [Internet] Available from: <http://www.channelregister.co.uk/2008/01/18/storm_worm_botnet/> [Accessed 29 March 2014].

[2]. Holz, T., Steiner, M., Dahl, F., Biersack, E., Freiling, F.(2008) **Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm.** [Internet] Available from: <https://www.usenix.org/legacy/event/leet08/tech/full_papers/holz/holz.pdf> [Accessed 05 April 2014].

[3]. Hidalgo, J. **(2007) Trojan.Peacomm: Building a Peer-to-Peer Botnet | Symantec Connect Community.** [Internet] Available from: <http://www.symantec.com/connect/blogs/trojanpeacomm-building-peer-peer-botnet > [Accessed 05 April 2014]

[4]. Maymounkov, p., Mazi, D. (2002), **A peer-to-peerinformation system based on the xor metric. IPTPS '01: Revised Papers, First International Workshop on Peer-to-Peer Systems**, pp 53-65.

[5]. Grizzard, J., Sharma, V., Nunnery, C., Byung, H., Dagon, D., (2007), **Peer-to-peer botnets: overview and case study. In HotBots'07: Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets,** CA, USA, USENIX Association Berkeley**.**

[6]. Smith, B (2008), **Storm (Worm) is brewing,** [Internet] Computer, Vol. 41 Issue 2, pp.20-22, 3p, Available from: < http://ieeexplore.ieee.org.ezproxy.leedsmet.ac.uk/search/searchresult.jsp?action=search&searchField=Search_All&matchBoolean=true&queryText=%22ISSN%22:0018-9162+AND+%22Volume%22:41+AND+%22Issue%22:2+AND+%22Start%20Page%22:20 > [Accessed 30 March 2014].

[7]. Malik, H. (2008), **IBM Says Storm Worm Creators Making Millions, Daily** [Internet], Available from: < http://gizmodo.com/354741/ibm-says-storm-worm-creators-making-millions-daily/all> [Accessed 31 March 2014].

[8]. Kawamoto, D., (2007), **'Storm worm' rages across the globe-CNET News,** [Internet], Available from: < http://news.cnet.com/Storm-worm-rages-across-the-globe/2100-7349_3-6151414.html> [Accessed 31 March 2014].

[9]. ICO, (n.d.), **Data Protection** [Internet], Available from: < http://ico.org.uk/for_organisations/data_protection> [Accessed 05 April 2014].

[10]. SQA,(n.d.)m **Computer Misuse Act**, Available from:< http://www.sqa.org.uk/e-learning/ProfIssues02CD/page_07.htm> [Accessed 05 April 2014].

[11]. ICO, (n.d.), **Privacy and Electronic Communications Regulations,** [Internet], Available from: < http://ico.org.uk/for_organisations/data_protection> [Accessed 05 April 2014].

[12]. University of Utah, Office of Information Technology and the Information Security Office (2007), **Storm Worm Virus Advisory,** [Internet], Available From: < http://www.secureit.utah.edu/notices/notices/Ar

chive/stormworm.html> [Accessed 04 April 2014].

[13]. The Telegraph, (2009), **Top 10 worst computer viruses** [Internet], 18 March 2009, Available from: <http://www.telegraph.co.uk/technology/5012057/Top-10-worst-computer-viruses-of-all-time.html> [Accessed 05 April 2014].