Time Detection of Malware Threads

Martin Strmiska[1], Pavel Mesicek[1], Libor Pekar[1] and Roman Jasek[1]

[1] Tomas Bata University, Zlin, Czechia
strmiska@utb.cz

Abstract. Malware is an unwanted software that performs actions in computers or computer networks, which users might disagree with. One of the worst types of malware is ransomware that affects the victim's data by modifying, deleting, or blocking the access to them. Frequent malware attacks on organizations led to a change in malware detection from external identification (companies were dependent on other organizations or their products) to internal identification. Based on this, the time needed to detect ransomware (dwell time) has significantly decreased. Nowadays, internal detection prevails over the external one. The dwell time differs based on the continent. In the paper, the malware and ransomware descriptions with their variants are provided, and the concept of dwell time is described. Moreover, attention is not only paid to the reduction of dwell time within the recent years but also to how the most used vector attacks are connected.

Keywords: Malware, detection, dwell-time, Ransomware, cybersecurity, phishing, Remote Desktop Protocol.

1 Introduction

A computer attack is any attempt to destroy, change, steal property, or gain unauthorized access to a property by using computer systems. One of the most problematic attacks is malware that spreads mainly due to software engineering. In this case, the attacker gets control over a computer or a computer network. Attackers manipulate users in order to infect their devices. It is often much easier to exploit users' weaknesses than it is to find a network to attack. For the identification of malware, it is essential to detect it just in time. This detection is called dwell time. Dwell time is calculated as the number of days the attacker is present in a victim's network before being detected.

A recent study (Fireeye, 2021) shows that 59% of the security incidents investigated by Mandiant last year were initially detected by the organizations themselves, which is an improvement of 12% from the prior year. Pervasive ransomware campaigns drove down the median dwell time as threat actors sought to capitalize on shifting trends in the workspace and a global crisis.

The purpose of this research is to summarize attacks which have been the most frequent over the last few years. In addition, the paper demonstrates how global dwell time has decreased and highlights the importance of internal notifications. The paper also shows a possible use of dwell time as a well-timed analysis of threads and prevention.

Focusing on the ransomware field, we present important considerations regarding how attacks are carried out, but we also want to point out that very often it is not the fault of the technology but poor-quality work of information technology (IT) department or social engineering.

The paper is organized as follows. The first part of the article describes malware, including its variants and a detailed description of ransomware and other terms for this work. The second part, the results section, explains the concept of dwell time, its reduction within the recent years and what attack vectors are most used and how they are related. The last paragraph of this article is a conclusion that briefly summarizes the whole paper.

2 Theoretical Background

2.1 Malware

Malware is malicious computer software that may perform an action that the user might disagree with, such as opening pop-ups, sending spam, or causing system breakdowns. Malware mainly spreads via a computer network. There are several types of malware such as computer viruses, computer worms, a Trojan horse, adware, spyware, ransomware, and others [2, 3,17].

A computer virus can spread without the user's awareness. Its behavior is similar to any other's biological virus, and it may create its copies enabling further transmission. Those copies hide in files or programs [15].

A computer worm is a type of computer virus inside an infected file and enters a device or a computer network. Once inside the device, it distributes itself. Its goal is to gain information, make a freeway for a hacker, or cause harm (for example, making it impossible to use some of the programs) [15].

A Trojan horse is a virus pretending to be beneficial for the user; often, it offers a helpful feature, a free program, tool, or entertainment. In fact, it is used to open the back door to overtaking control over an attacked device, gain user's personal information and send them to hackers, download and launch another malware inside the attacked system. [16]

An Adware is an unpleasant advertisement application popping up while visiting some websites. They are not threading but annoying and often offending [6, 18].

A Spyware is a virus collecting information about user's browsing history on the internet or personal data (for instance, credit card numbers, passwords, etc.) [6].

A Ransomware is a computer program that blocks a computer system or may encrypt data inside the system. Further, it demands ransom from the victim (user) in exchange for returning the stolen data. Some forms of a ransomware encrypt files on the storage device; others lock the system and try to make the victim pay with a denunciative message [3].

A Dwell time is detection time; in other words, it is the time between when an attack takes place and when it is discovered [6, 18].

A Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft company that offers to the user, who has a graphical user interface (GUI), connection to another computer via a computer network [3, 9, 13].

A Virtual Private Network (VPN) is an instrument for the safe interconnection of several computers when connecting to an unreliable public network [10, 11].

2.2 Ransomware as a Malware

Ransomware is a sophisticated malware program created by hackers with knowledge of computer systems. Devices may be infected when opening a virus-infected e-mail, web browsers, or visiting webs where the virus is. It also spreads similarly to computer worms or computer viruses. For example, WannaCry is the most common type of ransomware all around the globe. WannaCry has infected almost 125 000 organizations in more than 150 countries. It might appear on a mobile phone as well. Amongst ransomware that infects android phones is Doublelocker, Charger, Jisut, Lockerpin, Simplocker. [3, 22]

Encrypting ransomware is a damaging program encrypting data on a hard drive based on which a ransom is demanded. The most used ones are Gpcode, Archiveus, Krotten, and Cryzip. The oldest was the AIDS trojan owned by Joseph Popp. [21]

Non-encrypting ransomware is not as damaging as the encrypting ransomware; it only "blackmails" the user. In 2011, a new ransomware worm appeared. It pretended to be a Windows notification, informing Windows users about the urgency to restart their computer. The users had to call an international phone number and insert a six-digit code so they could reactivate the computer. However, even though the malware was claiming the call to be free; the opposite was true [3, 19, 20].

3 Results

Just as cyber-attacks are becoming more sophisticated, so are the methods by which companies and individuals can defend themselves. The time when companies depended only on external products and companies is long gone. Recently, they have understood that their business depends on cybersecurity, and they cannot afford financial losses. Especially with the threat of ransomware. It is not only about investing in products but also in people, who are the most vulnerable part of companies [5].

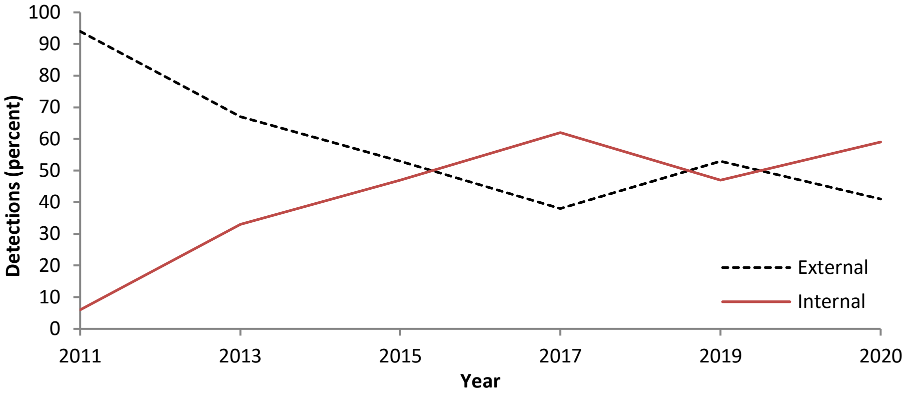

Fig. 1. Illustrates the results of a study dealing with the percentage of internal and external announcements varied over the years.

Improvements of internal departments in recent years have had a major impact on reducing global dwell time. The impact of external and internal notifications only started to be measured in 2015. From the beginning of the measurement, there is a clear evidence that internal departments detect a cyber-attack much earlier than external services. A significant difference is evident from the recent years, with the detection rate almost doubling between 2019 and 2020 [1].

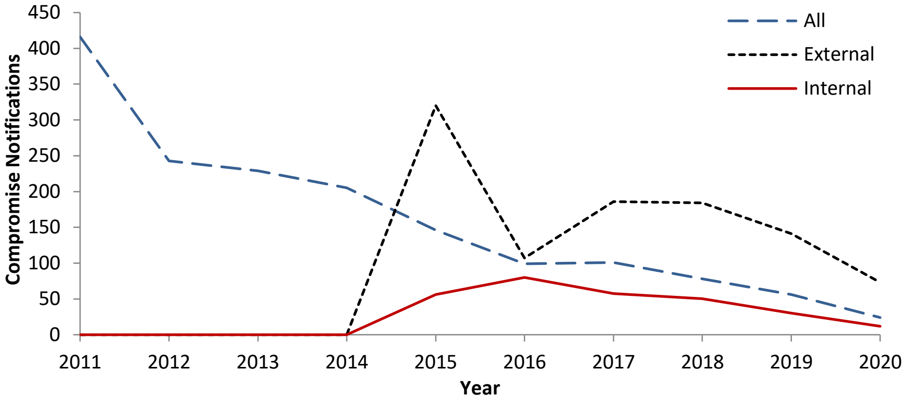

Fig. 2. Illustrates the results of reducing global dwell time between 2011-2020.

The chart shows a significantly decreasing global dwell time and highlights the importance of internal notifications. In particular, thanks to internal departments, the current global dwell time is only 24 days.

As already mentioned, the global dwell time is 24 days, but this low figure is mainly due to America, where the dwell time is 17 days. In 2019, it was 60 days; this is the only world region that has reduced dwell time very significantly. Europe, the Middle East, and Africa had had a slight deterioration compared to 2019 where they had a dwell time of 54 days and in 2020 the dwell time was 66 days. The Asia-Pacific had an even more significant drop in values than Europe, the Middle East and Africa. From also 54 days in 2019, its dwell time dropped to 76 days in 2020.

There is another factor that significantly decreases the global dwell time and that is the threat of ransomware. According to Group-IB, the number of ransomware attacks grew by more than 150% in 2020 [7]. Other cyber-attacks that do not behave so conspicuously on the network are estimated to have a detection time of 45 days. Ransomware, on the other hand, is very aggressive and therefore has a detection time estimated to be 5 days. Ransomware can also be considered as one of the main reasons why internal notifications have such a low dwell time [4].

From the previous paragraph, it is obvious that companies need to focus on protection against ransomware. As for 2021, it is necessary to significantly improve the security policy. The most used vector to gain access was through Remote Desktop Protocol since more than half attacks were carried out through it. Phishing was responsible for 29% and exploitation of public-facing applications for 17%. Nevertheless, all factors are related [8].

RDP is often attacked because of short or dictionary passwords, disabled account locking, failure to use two-factor authentication, disabled network authentication, untrusted certificates, and use of known logins such as administrator, support printer, etc. However, none of these things are merely the fault of the RDP but also the poor-quality work of the Information Technology (IT) department or poor knowledge or improvidence of a company’s workers. Because of these two factors, the statistic of the RDP is so high [9, 13].

What is also worth mentioning is that IT administrators rely strongly on the Virtual Private Network, which is an important security system that should be set up well. The first mistake is that users commonly use the same password for the VPN as for the domain. Another mistake is that attackers can easily guess passwords since the VPN is accessible from all over the world. Vulnerabilities have also already been proven for VPNs, especially with Palo Alto, FortiNet and Pulse Secure [9, 10, 11, 12, 14].

4 Conclusion

Malware has become more advanced and greater in numbers over the last years since it also attacks computers, phones, and other smart devices. It shows that internal notifications involved in global dwell time attacks are prevailing. In 2020, internal notifications accounted for almost 60% of all announcements. Our results show how ransomware has changed global dwell time in recent years. We would like to point out that we did not have access to the hardware from the project when we published this paper. For one of our many future extensions, we plan to send targeted phishing e-mails that we craft ourselves. These e-mails would contain a link that will not be malicious in real, but simply report clickthrough rates to us, the researchers. Subsequently, we would like to send out a questionnaire asking why the questioned people will have decided or have not decided to click on the link and what exactly they have found suspicious.

Acknowledgement

The paper was supported by Internal Grant Agency of Tomas Bata University in Zlín under the project number IGA/CebiaTech/2021/006.

References

1. FireEye, M-Trends 2020, https://content.fireeye.com/m-trends/rpt-m-trends-2020, last accessed 2021/7/6.
2. Shetty, N., Praveen, R.: A Survey Paper on Malware Detection Techniques. International Journal of Advanced Trends in Computer Science and Engineering, vol. 10, pp. 558–563. The World Academy of Research in Science and Engineering, Online (2021).
3. Malware | Detection, Prevention, Protection & Removal | Avast, https://www.avast.com/c-topic-malware, last accessed 2021/6/13.
4. Kovacs, E.: Breaches Detected Faster, But Ransomware Surge a Major Factor, https://www.securityweek.com/breaches-detected-faster-ransomware-surge-major-factor-fireeye, last accessed 2021/4/13.
5. Why Cybersecurity should be part of Internal Communication Strategies. https://kingeclient.com/why-cybersecurity-should-be-part-of-internal-communication-strategies, last accessed 2019/5/14.
6. Resource Center - Spyware and Adware. Hamilton College. https://my.hamilton.edu/offices/lits/rc/spyware-and-adware, last accessed 2018/3/23.
7. Leyden, J.: Ransomware attacks more than doubled last year as cybercrime operations scale up during coronavirus pandemic. The Daily Swig | Cybersecurity News and Views. https://portswigger.net/daily-swig/ransomware-attacks-more-than-doubled-last-year-as-cybercrime-operations-scale-up-during-coronavirus-pandemic, last accesed 2021/6/30.
8. Group-IB, Ransomware uncovered: Attackers' latest methods, https://go.group-ib.com/rs/689-LRE-818/images/Group-IB_Ransomware_Uncovered_whitepaper_eng.pdf.
9. Haller, M. (2020, Proč zabezpečení RDP pomocí VPN hackery nezastaví. https://martinhaller.cz/bezpecnost/proc-zabezpeceni-rdp-pomoci-vpn-hackery-nezastavi, last accessed 2020/2/24.
10. Tsai O., Chang M.: Attacking SSL VPN - Part 3: The Golden Pulse Secure SSL VPN RCE Chain, with Twitter as Case Study! https://devco.re/blog/2019/09/02/attacking-ssl-vpn-part-3-the-golden-Pulse-Secure-ssl-vpn-rce-chain-with-Twitter-as-case-study, last accessed 2019/9/2.
11. Tsai O., Chang M.: Attacking SSL VPN - Part 2: Breaking the Fortigate SSL VPN. https://devco.re/blog/2019/08/09/attacking-ssl-vpn-part-2-breaking-the-Fortigate-ssl-vpn, last accessed 2019/9/9.
12. Tsai O., Chang M.: Attacking SSL VPN - Part 1: PreAuth RCE on Palo Alto GlobalProtect, with Uber as Case Study! https://devco.re/blog/2019/07/17/attacking-ssl-vpn-part-1-PreAuth-RCE-on-Palo-Alto-GlobalProtect-with-Uber-as-case-study, last accessed 2019/7/17.
13. Securing Remote Desktop (RDP) for System Administrators. https://security.berkeley.edu/education-awareness/securing-remote-desktop-rdp-system-administrators, last accessed 2021/8/8.
14. Lakshmanan, R.: Pulse Secure VPNs Get New Urgent Update for Poorly Patched Critical Flaw. https://thehackernews.com/2021/08/pulse-secure-vpns-get-new-urgent-update.html, last accessed 2021/8/9.

15. Aycock, J. Computer Viruses and Malware. Springer, pp. 14–15.
16. Fortinet, What Is a Trojan Horse? Trojan Virus and Malware Explained | Fortinet, https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus, last accessed 2021/8/9.
17. Souri, A., Hosseini, R. A state-of-the-art survey of malware detection approaches using data mining techniques, Human-centric Computing and Information Sciences, vol. 8, pp. 1-22.
18. Zavrak, S. Adware: A Review. International Journal of Computer Science and Information Technologies, vol. 6, 2015.
19. Brewer, R. Ransomware attacks: detection, prevention and cure. Network Security, 2016(9), p. 59.
20. Forbes, Another Ransomware Campaign Threatens to Expose Victims' Data. https://www.forbes.com/sites/leemathews/2020/01/23/another-ransomware-campaign-threatens-to-expose-victims-data/#271fbefd770a, last accessed 2021/8/9.
21. eTrust, eTrust Spyware Encyclopedia - AIDS Information Trojan. http://www3.ca.com/se-curityadvisor/pest/pest.aspx?id=175, last accessed 2021/8/9.
22. BBC, Cyber-attack: Europol says it was unprecedented in scale - BBC News, https://www.bbc.com/news/world-europe-39907965, last accessed 2021/8/9.