Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 05, May-2023

A Study of the Latest Attack Vectors in Cyber-Security and Their Applications

Karan Chawla
Ashoka University
Gurugram, Haryana, India

***Abstract*—Cybersecurity is the practice of preventing and responding to assaults on computer systems, networks, hardware, and software. Your sensitive data is vulnerable to more complex and dynamic assaults that use cutting-edge techniques to get over well-established data protection measures by combining social engineering and artificial intelligence (AI). The world is getting more and more dependent on technology, and as we create new technologies that will eventually connect to our connected devices via Bluetooth and Wi-Fi, this dependency will only grow. Adversaries have the ability to establish persistence and increase privileges by executing malicious code when asked by Image File Execution Options (IFEO) debuggers. Using IFEOs, a developer may link a debugger to an application. An attacker can start a covert instance in the form of a virtual desktop and operate it secretly behind the scenes while the naive victim uses the computer as usual, as opposed to gaining control of the victim's desktop. For the purpose of removing any traces that the endpoint has been remotely operated, the hVNC creates a brand-new Windows desktop. Since this virtual desktop has its own associated explorer.exe process, victims are unable to monitor processes that are initiated in the context of the new desktop. The backdoor, referred to as "Domino," has been in use since at least October 2022 and has the capacity to gather essential system data, send data to its command-and-control (C&C) server, and start a loader to install the final payload on the compromised systems. The Domino software shares code with the Lizar virus. This review paper assesses three latest types of cyberattacks namely the IFEO injection used in the stack rumbling technique by the Chinese APT group, hVNC attach and the Domino Malware used by the Lizar group where each of these have a high threat to payload ratio.**

Keywords*— *Domino Malware, backdoor, hVNC, IFEO, Cyber-Security, Debugger.

I. INTRODUCTION

The practice of defending against and recovering from cyberattacks on computer systems, networks, devices, and software is known as cybersecurity. Your sensitive information is exposed to assaults that are increasingly sophisticated and dynamic as hackers employ cutting-edge strategies that combine social engineering and artificial intelligence (AI) to circumvent long-standing data protection precautions.

As we create new technologies that will eventually connect to our linked devices via Bluetooth and Wi-Fi, the globe will become more and more dependent on technology, which will only lead to an increase in that reliance. The benefits of cybersecurity are growing. Fundamentally, there is no indication that technology will play a different function in our society. Data leaks involving identity theft are now freely reported on social media platforms. Social security numbers, credit card numbers, and bank account numbers are just a few examples of the private data that is currently kept on the cloud by services like Dropbox or Google Drive.

Everyone, whether they are individuals, small organizations, or massive corporations, uses computers on a daily basis. When we combine this with the expansion of cloud services, inadequate cloud service security, cellphones, and the Internet of Things (IoT), we now have a wide spectrum of potential security vulnerabilities that weren't there a few decades ago. We still need to understand the differences between cybersecurity and information security, despite the fact that the two sectors of competence are becoming more similar. Governments all across the world are paying more attention to cybercrime.

Since it protects against data theft and loss, cybersecurity is essential. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal data, information relating to intellectual property, and computer networks utilised by the government and industry. Your company cannot protect itself against data breach operations without a cybersecurity programme, making it an unavoidable target for thieves.

Both inherent risk and residual risk are increasing as a result of improved global connectivity and the usage of cloud services like Amazon Web Services to store private and sensitive data. The likelihood of a successful cyber-attack or data breach against your company is increasing due to widespread improper configuration of cloud services and more intelligent hackers.

Business executives cannot only rely on standard cybersecurity tools like firewalls and antivirus software because hackers are growing more cunning and their strategies are becoming more resistant to traditional cyber defenses. To keep secure, it's crucial to cover all aspects of cybersecurity.

Cyber risks might originate at any level inside your company. To inform personnel about typical cyberthreats including social engineering schemes, phishing, ransomware attacks (think WannaCry), and other malware aimed to steal intellectual property or personal data, workplaces must offer cybersecurity awareness training.

Because of the prevalence of data breaches, cybersecurity is important across all sectors, not only those with strict regulations like the healthcare sector. Following a data breach, even small organizations run the danger of incurring irreparable reputational harm.

II. IFEO INJECTIONS

By running malicious material that is prompted by Image File Execution Options (IFEO) debuggers, adversaries may create persistence and escalate privileges. A developer can connect a debugger to an application using IFEOs. A debugger that is contained in an application's IFEO is prepended to the name of the programme when a process is launched, essentially starting the new process within the debugger. IFEOs can be directly set using the registry or the GFlags tool under Global Flags. When a specific programme silently departs (i.e., is prematurely terminated by itself or another, non-kernel-mode process), IFEOs can also make it possible for an arbitrary monitor programme to be launched. A Registry key that configures "cmd.exe" or similar programme that gives backdoor access, as a "debugger" for an accessibility software, may be updated on Windows Vista and later, as well as Windows Server 2008 and later. The procedure for accessibility features is comparable to this one. The "debugger" programme will run with 'system' privileges once the Registry has been updated when the proper key combination is pressed at the login screen while using a keyboard or when connecting through Remote Desktop Protocol. These settings may also be abused to get privilege escalation, similar to how Process Injection is used, by causing a malicious executable to be loaded and run in the context of numerous processes on the machine. By continuously triggering invocation, installing IFEO mechanisms may also offer Persistence. By registering erroneous debuggers that reroute and inadvertently deactivate different system and security apps, malware can also utilise IFEO to impair defences. A recent cyber-attack used the 'stack rumbling' technique to disable software security.

The threat actor was observed using Windows Defender binaries to sideload DLLs and using the 'Bring your own vulnerable driver' (BYOVD) and 'stack rumbling' techniques to disable protection software. The assaults often begin with the deployment of the Behinder web shell, which offers backdoor capabilities, remote code execution, and a Socks5 proxy, through the exploitation of vulnerable public-facing apps, Internet Information Services (IIS), and Microsoft Exchange servers. It has been shown that some individuals sideload DLLs and launch malware like Croxloader (a modified Cobalt Strike loader) and SPHijacker (a tool for disabling security products) by exploiting legal Windows Defender executables. In order to stop security apps from operating, SPHijacker uses a vulnerable Zemana driver and stack rumbling to crash the program as soon as it is launched. To do so, it adds a new value to the IFEO registry key that is significant enough to cause a stack overflow and terminate the target programme. About 30 antivirus-related processes are the target of the technique, which results in a permanent DoS condition. "It is known that the IFEO register offers a variety of choices for creating processes. The technique known as IFEO injection can be used to stop the process execution flow in addition to attaching a debugger to an executable file.

III. HVNC ATTACK

Form-grabbing, screen-capture, web injections, and other dangerous features are all available in top-tier financial malware like Dridex, Neverquest, and Gozi. The hidden virtual network computing (hVNC) module, which enables attackers to get user-grade access to a compromised PC, is one significant component. Although it is well known that banking Trojans have remote control capabilities, little is known about how to use them. Malware uses hidden virtual network computing as a strategy to secretly take control of a victim's computer. Taking a look at an abstract of the VNC paradigm to better grasp how hidden VNC functions, one can see that there are two components to a VNC connection: a server and a client. The victim's computer serves as the server in this scenario, while the attacker acts as the client. The server transmits screen shots of the controlled endpoint's desktop to the client through the VNC connection. The client supplies the controller's keystrokes, mouse motions, and mouse clicks during that session. Attacker commands are executed by the victim's endpoint, and the attacker is able to observe the changes to the screen through the never-ending stream of screenshots. This gives the actor the ability to remotely manage what happens on the infected device. The victim can view everything the attacker does while using a standard VNC connection. That, of course, doesn't work for con artists. VNC in secret mode. Remote VNC access is not always harmful. It is employed as a reliable remote assistance solution in several settings. Cybercriminals just take advantage of the remote user-grade access that VNC provides. VNC is frequently used in financial malware to get around fraud safeguards. In the past, con artists faked their IP addresses using proxies. They did, however, have to come up with techniques to spoof fingerprints from whole devices when security measures improved. VNC can help in this situation. A transaction has a higher chance of success if it comes from a recognised user device. Previously, fraudsters had to access the account from the victim's own computer without leaving a trace in order to make fraudulent transactions seem legitimate to the victim's bank. The user would see the cursor moving on its own and get suspicious if they were using conventional VNC or other typical remote-control software. To solve this issue, cybercriminals created covert VNC. Instead of taking over the victim's desktop, an attacker can launch a covert instance in the form of a virtual desktop and operate it covertly behind the scenes while the unwary victim uses the computer as usual. The hVNC builds a fresh Windows desktop in order to erase any evidence that the endpoint has been remotely managed. Victims cannot observe processes started in the context of the new desktop since this virtual desktop has its own associated explorer.exe process.

A feature of malware known as LOBSHOT dubbed hVNC (Hidden Virtual Network Computing) enables attackers to sneakily access a victim's PC. The hVNC component is useful for getting around fraud detection tools. Additionally, LOBSHOT is used to commit financial crimes thanks to its information-stealing and banking trojan functionality. LOBSHOT first establishes a unique framework for each user that includes a variety of data, including the GUID of the computer, Windows edition, the name and username of the computer, information about the Windows desktop object, the number of active processes, the malware process ID, and parent process, as well as the screen resolution, display device information, DPI for the display(s), and handles to the desktop objects and windows. The user would see the cursor moving on its own and get suspicious if they were using conventional VNC or other typical remote-control software. To solve this issue, cybercriminals created covert VNC. Instead of taking over the victim's desktop, an attacker can launch a covert instance in the form of a virtual desktop and operate it covertly behind the scenes while the unwary victim uses the computer as usual. The hVNC builds a fresh Windows desktop in order to erase any evidence that the endpoint has been remotely managed. Victims cannot observe processes started in the context of the new desktop since this virtual desktop has its own associated explorer.exe process.

Another important feature of the virus is the hVNC module of LOBSHOT. At this point, the hacked system starts sending images of the hidden desktop to an interested client under the attacker's control. By controlling the keyboard, clicking buttons, and moving the mouse with the client, the attacker has full remote control of the target device. The attacker can provide different commands thanks to LOBSHOT's hVNC module. These include the Windows Run command, starting a new Windows process using a provided command, launching web browsers like Internet Explorer, Edge, and Firefox, stopping already-running explorer.exe processes, changing Windows sound settings, setting or retrieving clipboard text, and turning on the Start Menu.

IV. DOMINO BACKDOOR

The Visual C++ programming language was used to produce a 64-bit DLL known as the Domino backdoor. Once activated, the malware spreads infection by obtaining the login and hostname from the infected machine and making a hash of the data obtained. The backdoor then adds its current process ID to the hash. The virus then uses XOR to decode the configuration block and generates a 32-byte random key that is encrypted with the RSA key. After connecting to the C2 server successfully, the Domino backdoor makes additional efforts to gather the essential system data, encrypt it, and deliver it to the distant server. Therefore, the malware anticipates receiving the decrypted payload from C2, which it then further decrypts, loads, and executes in order to spread the infection.

The backdoor, known as "Domino," has been operational since at least October 2022 and has the ability to collect fundamental system data, transmit information to its command-and-control (C&C) server, and launch a loader to install the final payload on the compromised computers. The Lizar virus shares code with the Domino programme. The functionality, configuration architecture, and formats used for bot IDs are likewise comparable between the two malware families. Between March 2020 and late 2022, attacks used Lizar, also known as Tirion and DiceLoader, but Domino seems to have taken its place in more recent campaigns, according to IBM's security researchers. The Dave loader, which has been associated with the Conti/TrickBot gang and is still being maintained by former members of the criminal organization, has been used in Domino assaults from February 2023. According to IBM, this demonstrates that former CONTI members and current or former FIN7 engineers most likely worked together to acquire or utilise Domino. The Dave loader was also detected delivering IcedID and Emotet, both of which were used by former Conti affiliates to spread ransomware. The Dave loader has been used in conjunction with Cobalt Strike in assaults that may be linked to former Conti members.

Threat actors with a financial incentive typically work together with other hacking groups to boost their profits by using additional virus dissemination routes.

Basic system information is gathered by the Domino backdoor and forwarded to the C2. The Domino loader is typically the AES-encrypted payload that the C2 returns. An encrypted payload is included in the resources of the loader and is decoded using AES. The payload that has been encrypted is a.NET info thief that calls itself the Nemesis Project. The Domino backdoor is designed to connect to a separate C2 address for domain-joined computers, indicating that Cobalt Strike or another more advanced backdoor might be downloaded for higher-value targets instead of the Project Nemesis information stealer.

It is known that fraudsters use phishing to spread the Domino virus by sending out phoney emails that look authentic and contain a link or attachment that, when clicked, installs the malware on the victim's machine. Domino malware may also be spread by other methods, such as phishing, social engineering, exploiting software flaws, P2P networks, illegal software, malicious advertisements, hacked websites, etc. The goal is to convince the victim to download and run malicious software.

In December 2021, Project Nemesis info thieves were unveiled and put up for sale on a number of Dark Web sites. It has the ability to gather information from a variety of online browsers and programmes, including Steam, Telegram, Discord, cryptocurrency wallets, VPN services, and more.

CONCLUSION

The 'stack rumbling' approach was recently utilised in a cyberattack to destroy software security. The threat actor was seen sideloading DLLs with Windows Defender binaries, disabling security software via "Bring your own vulnerable driver" (BYOVD), and stack rumbling. Attacks often begin with the installation of the Behinder web shell, which offers backdoor capabilities, remote code execution, and a Socks5 proxy, through the exploitation of shoddy public-facing apps, Internet Information Services (IIS), and Microsoft Exchange servers. For hVNC, Accessing VNC remotely isn't necessarily bad. It is used in many contexts as a dependable remote help option. Simply put, cyber criminals' profit from VNC's remote user-grade access. Financial malware typically takes advantage of VNC to get around fraud protections. In the past, con artists used proxies to mask their IP addresses. However, when security measures increased, they had to develop methods to fake fingerprints from whole machines. VNC can be useful in this scenario.

For the Domino Backdoor, Once launched, the virus spreads infection by getting the hostname and login from the compromised computer and hashing the data collected. The backdoor then updates the hash with its current process ID. The configuration block is then decoded by the virus using XOR, and a 32-byte random key is generated and encrypted using the RSA key. The Domino backdoor continues its efforts to collect the crucial system data, encrypt it, and send it to the remote server after connecting to the C2 server successfully.

REFERENCES

[1] Matthew P Barrett. 2018. Framework for improving critical infrastructure cybersecurity version 1.1. Technical Report.

[2] G Bell and M Ebert. 2015. Health care and cyber security: increasing threats require increased capabilities. KPMG (2015).

[3] Global Innovation Policy Center. 2019. Inspiring Tomorrow, US Chamber International IP Index (7th Edition).

[4] IP Commission. 2017. The Report of the Commission on the Theft of American Intellectual Property. http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf

[5] Carlos M Correa. 2016. The Current System of Trade and Intellectual Property Rights. In European Yearbook of International Economic Law 2016. Springer, 175–197.

[6] Kaspersky Daily. 2018. Top 5 most notorious cyber-attacks. https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/

[7] Julie Hirschfeld Davis and David E. Sanger. 2015. Obama and Xi Jinping of China Agree to Steps on Cybertheft. https://www.nytimes.com/ 2015/09/26/world/asia/xi-jinping-white-house.html

[8] A Mark Doggett. 2005. Root cause analysis: a framework for tool selection. Quality Management Journal 12, 4 (2005), 34–45.

[9] International Agency for Research Cancer. 2018. China's Fact Sheet. https://gco.iarc.fr/today/data/factsheets/populations/ 160-china-fact-sheets.pdf

[10] Chuck Grassley. 2019. Grassley on Chinese Espionage: It's called cheating. And it's only getting worse. https://www.judiciary.senate.gov/grassley-on-chinese-espionage-its-called-cheating_ and-its-only-getting-worse

[11] The White House. 2018. Statement from the Press Secretary Regarding the President's Working Dinner with China. https://www.whitehouse.gov/briefings-statements/ statement-press-secretary-regarding-presidents-working-dinner-china/

[12] Mazaher Kianpour, Stewart Kowalski, Erjon Zoto, Christopher Frantz, and Harald Øverby. 2019. Designing Serious Games for Cyber Ranges: A Socio-technical Approach. In 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 85–93.

[13] Stewart Kowalski. 1996. IT insecurity: A multi-disciplinary inquiry. (1996).

[14] Nir Kshetri. 2010. The global cybercrime industry: economic, institutional and strategic perspectives. Springer Science & Business Media.

[15] 15. James Andrew Lewis. 2013. Significant cyber incidents since 2006. Center for Strategic and International Studies (2013).

[16] Aaron M Lien, George B Ruyle, and Laura Lopez-Hoffman. 2018. Q Methodology: A method for understanding complex viewpoints in communities served by extension. Journal of Extension 56, 2 (2018), 2IAW4.

[17] Keith E Maskus. 1998. The role of intellectual property rights in encouraging foreign direct investment and technology transfer. Duke J. Comp. & Int'l L. 9 (1998), 109.

[18] Jean-Frédéric Morin and Dimitri Thériault. 2019. Copyright Provisions in Trade Deals: A Bird's-eye View. (2019).

[19] Netwrix. 2019. 2018 IT Risks Report. http://www.netwrix.com/go/research

[20] World Health Organization Representative Organization. 2019. The situation in China. http://www.wpro.who.int/china/mediacentre/factsheets/cancer/en/

[21] South China Morning Post. 2019. FBI has 1,000 investigations into Chinese intellectual property theft. https://www.scmp.com/news/china/article/3019829/ fbi-has-1000-probes-chinese-intellectual-property-theft-director

[22] Samantha F Ravich. 2015. Cyber-Enabled Economic Warfare: An Evolving Challenge. Hudson Institute.

[23] Eric Rosenbaum. 2018. 1 in 5 corporations say China has stolen their IP within the last year: CNBC CFO survey. https://www.cnbc.com/2019/02/28/ 1-in-5-companies-say-china-stole-their-ip-within-the-last-year-cnbc. html

[24] Donald Trump. 2018. National Cyber Strategy of the United States of America. Washington, DC (2018).

[25] GC Wilshusen. 2012. Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage., Pub. L. No. Technical Report. GAO-12-876T.

[26] L. Martignoni, E. Stinson, M. Fredrikson, S. Jha, and J. C. Mitchell. A Layered Architecture for Detecting Malicious Behaviors. pages 78–97, 2008.

[27] T. Murata. Petri nets: Properties, analysis and applications. Proceedings of the IEEE, 77(4):541–580, 1989.

[28] H. Orman. The Morris worm: a fifteen-year perspective. volume 1, pages 35–43, 2003.

[29] A. Mantovani, S. Aonzo, X. Ugarte-Pedrero, A. Merlo, and D. Balzarotti. Prevalence and impact of low-entropy packing schemes in the malware ecosystem. In Network and Distributed System Security (NDSS) Symposium, NDSS, volume 20, 2020.

[30] T. K. Lengyel, S. Maresca, B. D. Payne, G. D. Webster, S. Vogl, and A. Kiayias. Scalability, fidelity and stealth in the drakvuf dynamic malware analysis system. In Proceedings of the 30th Annual Computer Security Applications Conference, ACSAC '14, page 386–395, New York, NY, USA, 2014. Association for Computing Machinery.

[31] N. Falliere, L. O. Murchu, and E. Chien. W32.Stuxnet dossier. White paper, Symantec Corp., Security Response, 2011.

[32] T. L´aszl´o and A. Kiss. Obfuscating C++ pro- ´ grams via control flow flattening. volume 30, pages 3–19, 2009.

[33] A. K¨uchler, A. Mantovani, Y. Han, L. Bilge, and D. Balzarotti. Does every second count? time-based evolution of malware behavior in sandboxes. In Proceedings of the Network and Distributed System Security Symposium, NDSS. The Internet Society, 2021.

[34] M. Egele, T. Scholte, E. Kirda, and C. Kruegel. A Survey on Automated Dynamic MalwareAnalysis Techniques and Tools. 44(2), Mar. 2008.