OIC-CERT Computer Emergency Response Team

OIC-CERT Journal of Cyber Security
Volume 4, Issue 1 (April 2022)
85 - 96

Study of Lokibot Infection Against Indonesian Network

Ariani[1] , Siti Rahmawati[2], and Rudi Lumanto[3]
[1,2,3]CSIRT.ID, Jakarta, Indonesia
[1]**ariani@csirt.id,** [2]**rahma@csirt.id, and** [3]**rudi@csirt.id**

ARTICLE INFO

Article History
Received 19 Oct 2021
Received in revised form 26 Mar 2022
Accepted 4 Apr 2022

Keywords:
malware; bot; malicious activity; Lokibot; information-stealer; malspam;

ABSTRACT

In recent years, malware has become the top cybersecurity threat. Of the many types of malware that need attention is malware that causes data leakage, one of which is Lokibot. In 2021, we observed that malware attacks also occurred massively on the Indonesian internet network. Among the types of malware in those attacks, Lokibot was the most significant. Our observations are a severe warning and must be taken seriously. However, analysis and studies related to Lokibot attacks on Indonesian internet networks are not yet available, so it is necessary to analyse this Lokibot attack to perform the correct preventive or mitigation actions. This analysis aims to provide a systematic description of the trend of Lokibot malware attacks in Indonesia and how to overcome them. We carry out the study using the descriptive-analytical method. With this analysis, we hope that Lokibot attacks in Indonesia will be better understood and serve as an introduction to further analysis in solving many cases of data leakage in Indonesia and other countries with similar cases.

I. INTRODUCTION

Malware and botnets are among the biggest threats to the internet today, and they are linked to most forms of internet crime. A botnet is a collection of compromised machines that run bot programs (read: compromised devices and programs will be malicious) controlled by a remote command and control infrastructure. Bots first appeared in 1989, particularly the Internet Relay Chat (IRC) bot. These bots were friendly and designed for gaming. Ten years later, in May 1999, the first malicious IRC bot named Pretty Park was discovered [1]. As technology evolves, these malicious bots develop into a botnet controlled by the internet. Rambrock et al. [2] said that botnets are the most significant threats on the internet.

ISSN 2636-9680
eISSN 2682-9266

Based on the data we collected through Open Source Intelligence (OSINT), malicious activity from bots is the most common type of malicious activity compared to phishing or spam. Using various bots, we analysed the malicious activity through OSINT based on Indonesia's malicious source and destination IP addresses. Our observation, from January to July of 2021, found that the bot that massively attacked the Indonesia network was Lokibot, shown in Fig. 1. Based on the chart, the total Lokibot is more than 25 million, which is not too different from ProxyBack, but from the chart Fig. 2 we found that the Lokibot is increasing significantly than Proxy Back.

Since July 2020, the US Cybersecurity and Infrastructure Security Agency (CISA) has warned of a significant increase in the use of Lokibot through phishing campaigns. It uses COVID-19 to lure target businesses with the infamous Lokibot information-stealer [3]. And since March 2021, a substantial increase in Lokibot activity from Indonesian IP addresses has begun.

We observed that the source IP address for the destination IP address is consistent with the same destination. After analysing the destination IP address, the IP address indicated it is a Command and Control (C&C) server, with ten or even hundreds of types of malware [3].

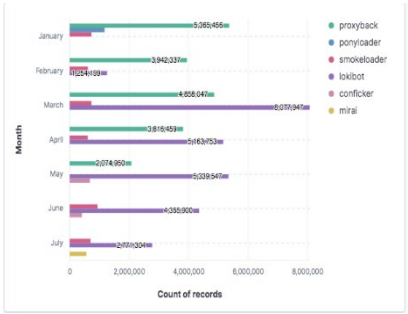

Fig. 1. Top 20 Malware (mid-year 2021)

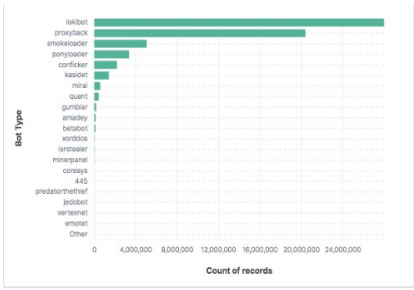

Fig. 2. Monthly Bot Trend (mid-year 2021)

With the global expansion of Lokibot and the rise of this malware, particularly in Indonesia this year, we need to know more and do analysis to help secure the network better and know how to overcome them.

II. RELATED WORK

Many researchers have researched botnets. However, on average, the research related to botnets discusses the characteristics of botnets or how to identify botnets, not a research specifically on one type of botnet. In comparison, discussion on specific types of botnets is mostly done in blog articles. Correia et al. [4] researched botnets and C&C servers

in general. The article stated that botnets are mostly used as illegal activities and become a source of massive exploitation because they recruit new vulnerable systems to expand their reach, called zombies. Due to their large numbers and varying capabilities and resilience, botnets pose a significant and growing threat to corporate networks and the internet itself. Researchers who conducted research on botnets include Mills et al. [5], Zobal et al. [6], and Duncan et al. [7], published their articles on the internet. Hence, research on Lokibot were only be available in 2018 and above.

The trend of the tasks of this bot, on average, is to carry out information theft and remote administration tools [8]. As this article discusses Lokibot, Lokibots fall into information-stealing bots category such as Predator Pain, Pony, KeyBase, ISpySoftware, ISR Stealer, Tesla Agent, Zeus, and Atmos. Related to Lokibot, these bots spread throughout the monitoring period in 4 different campaigns with 160,000 samples delivered [6].

Hoang also broke down malicious activity caused by Lokibot in the report he wrote [9]. The article presents the results and findings of a dynamic and static analysis of Lokibot's behaviour, techniques, targets, and demolition methods. Apart from that, the article also reveals features used to prevent and mitigate threats.

The steps of the technique used by Lokibot are presented on the MITRE ATT&CK and CISA websites [9] [3] in 2020 when Lokibot infected the network significantly by initially exploiting the vulnerability in CVE-2017-11882 [10]. It contains a keylogger component as a credential stealer from browsers, email clients, file-sharing programs, remote connection programs [11].

Another study on Lokibot was conducted by Sharma et al. [12] due to increased information stealer attacks during the COVID-19 pandemic. Their paper analysed the COVID-19 pandemics from the perspective of cyber-attacks where cybercriminals take advantage of the premise of the COVID-19 pandemic to carry out information-stealing attacks with 404 keyloggers to the latest attack, namely Lokibot.

Based on previous reviews, we know that Lokibot information-stealing malware has become a popular threat of data breach incidents with common behaviour, techniques, targets, and demolition methods. Research on Lokibot is new because Lokibot itself is one of the bots that recently occurred due to a vulnerability in Windows and increased during the COVID-19 pandemic.

III. METHODOLOGY

The methodology used is descriptive-analytic. We describe

ISSN 2636-9680
eISSN 2682-9266

the available problems based on concepts and theories derived from several works in books and articles. We map it to discuss the existing problems obtained from data sources and references. Then we analyse it through several questions as guidance for explaining the problem. Our flow on this process review shows in Fig 3.

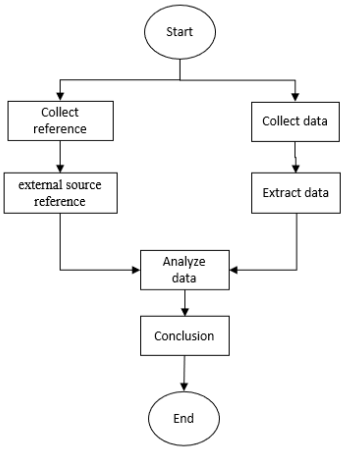

Fig. 3. Methodology Flowchart

We use Elastic as our environment to extract data and source our analysing process with external source reference. The evidence data we use as a reference is the data we collected from Open Source Intelligence (OSINT) originating from Indonesian IP addresses so that the conditions may differ from other case studies. Still, the core of this analysis is about the Lokibot pattern.

A. General Information

Lokibot is a piece of malware that emerged in 2015, designed to collect credentials and security tokens from infected Windows machines. It exploits security holes in remote code execution control. At first, Lokibot was not a well-known bot malware, but as Lokibot's activity increased, it even stuck to Emotet (malware downloader). Lokibot also uses a very simple codebase that makes it easy for lower-level cybercriminals to use it. Lokibot collects information and credentials from several applications such as browser applications, Thunderbird, FTP, SFTP, cryptocurrency wallets, and others in terms of data theft. However, Lokibot can create a backdoor that allows hackers to install additional software. And then, it will download ransomware such as the Jigsaw ransomware variant. It shows that another feature of Lokibot is its ransomware capabilities.

Previous studies show that the most known Lokibot distribution is mostly through malspam campaigns with file attachments or phishing campaigns. The global conditions hit by the COVID-19 pandemic make malspam, with file attachments infiltrated by malware and sent with the subject of COVID-19, attack more people. Lokibot can also mimic popular game launchers to trick users into running it on their machines, automatically running scripts in C # scripts [15]. Another way of spreading is by using distribution media via an ISO file, which causes the target to be more unaware. Generally, the malware is

inserted into document file attachments [16].

B. Target Environment

When Lokibot first appeared in 2015, it targeted the Android system to get root privileges. In 2017, the spread of Lokibot was possible through pdf files or images that targeted the Windows operating system. The security vulnerability exploited at that time was CVE-2017-11882. Besides that, the victim system environment must have an internet connection for the binary to execute and communicate with its C&C server fully.

Lokibot has targeted over 100 financial institutions worldwide, earning more than USD2 million in revenue [17]. Along with the fact that Lokibot also attacks Android, it is possible that Lokibot also targets not only mobile banking, payment services,and crypto wallets, but also messaging and retail applications [18]. Lokibot does not target specific areas; any area can become its target.

Based on the data we collected, the average bot activity occurred during general working hours, with an average of more than 5000 activities and even up to 40,000 every hour. The Lokibot activity increased the most on certain days, as in Fig. 4. It means the Lokibot activity works several times. It shows bots have infected many computers. When people work and use the computer, the bot runs and communicates inconspicuously with the C&C server in the background without being noticed by computer users.

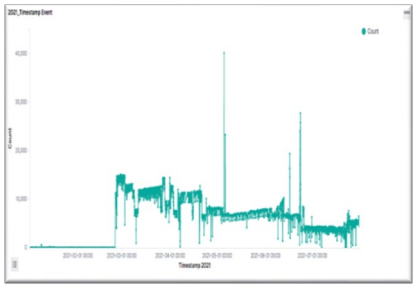

Fig. 4. Timestamp Lokibot on Data Case

C. Attack Technique Flow

Previous studies show that Lokibot is a large and complex malware with several wrappers packaged and is usually a follow-up payload from an exploit kit or provoked by malspam. Lokibot runs silently and does not affect system performance, making it very challenging for detection and prevention. Fig 5 shows the flow of the Lokibot attack technique [10] with the details of the method in TABLE 2 [11]. A simplifed explanation of the flow including the processes are as follows:

a) The attacker sends malspam to the user with malware instead of file attachment

b) When the user opens the file, it executes some process to unpack the package of compressed malware, and execute a file which communicates with the attackers to download bot.

ISSN 2636-9680
eISSN 2682-9266

c) After successfully downloding file, it will be decrypted and will execute the malware.

d) Finally, the Lokibot can communicate with the C&C server and execute commands, which are controlled by the C&C server.

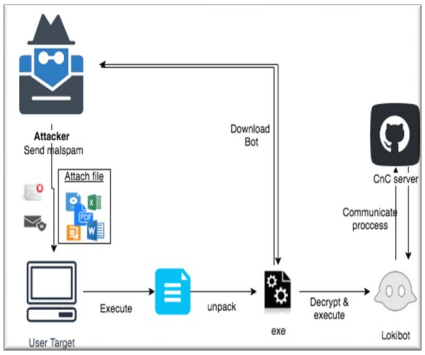

Fig. 5. Lokibot Process

IV. ANALYSIS AND RESULTS

In this analysis, we started by defining some questions, as shown in TABLE 1, then observed more deeply through the answer. Furthermore, we analysed it with comparative studies from previous work.

TABLE 1: Question List

No.	Subject	Questions
1	General Information	a. What is the Lokibot? b. How did it spread?
2	Target Environment	a. Who is the target of bot activity, such as target specification, exploited vulnerabilities? b. What are areas of the group targeted? c. When does the average Lokibot activity occur?
3	Attack Technique Flow	a. What is the flow of attack technique?
4	The Impact	a. What is the impact of Lokibot on victims and the global?
5	Condition-based on Data Case	a. What is the current condition based on case study data? b. Why so many Lokibot?

A. The Impact

Lokibot presence is quite dangerous because it is easy to use and very effective in violating the privacy of individual users within large entities. The impact on the victim is that the attacker will retrieve the victim's credential information, and the attacker can misuse the exploited credential information.

The global harmful impact of Lokibot has never happened. Still, with the current pandemic condition where attackers use it to do mass distribution, the spread of malware by utilizing the COVID-19 pandemic campaign will be easier. In addition, because this Lokibot

also attacks Android, the impact of losing money is also very possible.

The impact will also cause data breaches that can destroy a person's privacy, whose value is comparable to a large financial loss.

TABLE 2: Lokibot MITRE ATT&CK enterprise techniques

Execution
• User Execution Malicious file
Privilege Escalation
• Process Hollowing
Defense Evasion
• Hide artefact: Hidden Files and Directories
• Obfuscated Files or Information: Software packing
• Process Hollowing
Credential Access
• Credentials from Web Browsers
• Input Capture: keylogging
Discovery
• System Information Discovery
• System Network Configuration Discovery
• System Owner/User Discovery
Collection
• Input Capture: keylogging
Command & Control
• Web Protocols
Exfiltration
• Exfiltration Over C2 Channel

B. Condition-based on Data Case

This study found more than 25 million activities carried out by Lokibot from February to July 2021. This number is quite an incredible number, and when viewed from the previous Fig 4, the Lokibot's activity is relatively consistent.

The source and destination IP addresses of the Lokibot data show that the destination IP address indicates a C&C server for some malware. As shown in

Fig. 6, one IP was found to communicate with several files such as exe, zip and apk.

When the Lokibot infects the target, the Lokibot command method uses a centralized model which operates on a client-server architecture. Then a command-and-control (C&C) server operates the entire botnet. In addition, the botnet goes to port 80, which is the HTTP protocol. An HTTP botnet is a web-based botnet in which bot herders use the HTTP protocol to send commands.

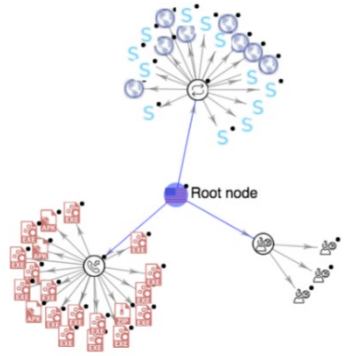

Fig. 6. Root Node C&C IP Address Relations

The destination IP address's reputation indicates that a new C&C server was recently added in late 2020 or early 2021. It is clear that the spread of malware increases when the C&C server also infects

ISSN 2636-9680
eISSN 2682-9266

new servers. In the previous malicious activity, most of the C&C servers used to communicate with the source IP addresses are mostly IP addresses that have been infected with malware and have been C&C servers for more than two years. Most destination IP addresses have bad reputation. Fig. 7 shows the reputation of the IP address that is the most destination IP address of malicious activity.

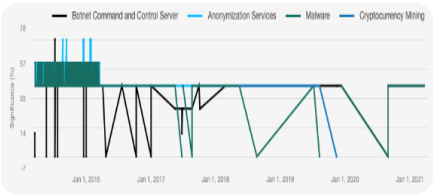

Fig. 7. Reputation is the most IP Destination of Malicious Activity

Most source IP addresses are also IP addresses with a fairly bad reputation, mainly because they indicate that they have been infected by malware for more than a year. Illegal activities that are carried out are spreaders of spam, phishing, or doing DOS on specific IPs. The source IP address that we monitored has several unique IP addresses of more than 15000 IP addresses leading to less than 120 unique destination IP addresses. It demonstrates that Lokibot has infected over 15000 computers or systems commanded and controlled by over 100 C&C servers.

Based on this data, we found that many types of malware had been spread and consistently persisted on computers with Indonesian IP addresses. Fig 8 shows an example of the most common source IP address of malicious activity with a bad reputation. Many of them have been infected by malware that has to send spam and the ability to execute command by C&C control, such as downloading another malware or other command.

Fig. 8. The reputation of some IP addresses in Indonesia

Indonesia's IP destination and IP address have a bad reputation; the IP destination is a C&C bot, and Indonesia's IP address is an infected system. The correlation is that IPs from outside of Indonesia drive the Lokibot's activity, which increases when the C&C server command the previous malware that has been stored on computers to download Lokibot so that more computers become infected.

The COVID-19 pandemic campaign has become an excellent opportunity for attackers to take advantage to spread Lokibot by sending malspam about the COVID-19 campaign. In addition, this is also due to the level of security awareness among the public, who are less aware of information security and cybersecurity.

During a pandemic, there are so many data breach incidents in Indonesia. There has yet to be a definitive report on the cause of that breach, which brings us to many possible causes, and one of them may correlate with the massive spread of Lokibot. As a credential information stealer malware, Lokibot is a dangerous potential threat.

Lokibot steals credential information from the infected computer so that the victim's loss is in the form of information and data breaches. A data breach is a threat that significantly impacts social life because it violates privacy and can also result in financial loss.

Based on the statistic bot in January-July 2021. Fig. 9 and Fig. 10 show the different numbers of Lokibot in Q1 and Q2 of 2021. We divide Q1 and Q2 with a diverse group that does not intersect. In early 2021, Lokibot showed 33% (more than 9 million activities), and in Q2 of that year, Lokibot increased to 57% (almost 15 million).

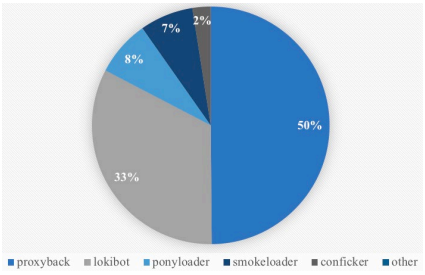

Fig. 9. Top 5 Bot Category in Q1

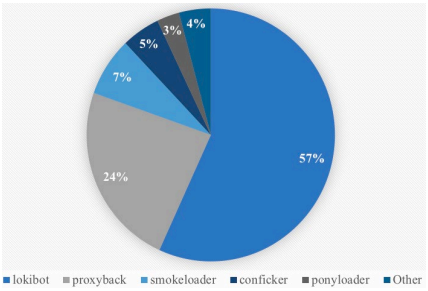

Fig. 10. Top 5 Bot Category in Q2

Lokibot's enhanced spread may be due to taking advantage of the COVID-19 campaign when the worldwide pandemic was on the verge of occurring. An example of the COVID-19 campaign to disseminate Lokibot is shown in Fig. 11 Lokibot's global ranking is still quite high. ANY.RUN [20] shows the global rank of Lokibot as one of information-stealer rank 4, which is more than 20k IoC, which means that Lokibot has propagated globally.

Users can prevent devices from becoming Lokibot zombies by increasing individual security awareness, consistently patching the system in use, using antivirus that continuously scans and is always updated, implementing perimeter protection such as employing IDS IPS on the network,

ISSN 2636-9680
eISSN 2682-9266

and so on. Another critical method of prevention is the policy established by the organization in terms of system management as administrative control.

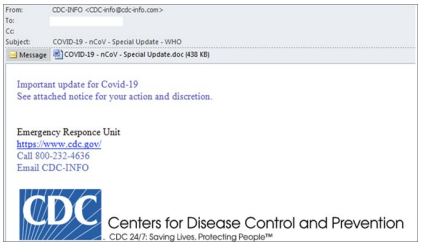

Fig. 11. Mail example Lokibot campaign **[12]**

Using safe mode, a user can clean dangerous programs and malicious browser add-ons that have been installed on the computer. Users with device administrator access can also remove hazardous programs running on Android, ensuring that users in an Android system are safer. Furthermore, because most antiviruses have been able to spot Lokibot, it is highly suggested that users use one.

V. CONCLUSION

This study reviewed and analysed the massive infection of Lokibot in Indonesia during the pandemic. Some important findings below ensure the need for immediate actions to prevent the escalated effects of Lokibot.

a. The Spread of Lokibot in Q2 reached about 57% compared with Q1(33%). It increased massively during the pandemic, especially in 2021, compared to another type of malware in Indonesia.
b. Much of the reputation of IP addresses in Indonesia has a bad history of becoming bots, which can be controlled by C&C servers that drive them to spread malware by sending malspam.
c. The massive spread of Lokibot is probably because of the COVID-19 malspam campaign.
d. The massive spread of Lokibot, with its core core function as a credential information stealer, is probably connected to many data breach incidents in Indonesia. This may be the topic for next issue and an important further work that needs to do done.

We conclude that Lokibot has become popular because it has a great opportunity on global issues that spread malware significantly. The attacker takes advantage of phishing emails to steal information.

A further study requires an in-depth analysis of the specific method used. In terms of the appropriate analysis method to be implemented in the real case of malware, we will know how to mitigate using technical method, suggest decision-making method to be implemented in the real security

system, and how to increase the security awareness.

VI. REFERENCES

[1] C. Elliott, "Botnets: To what extent are they a threat to information security?," *Information Security Technical Report,* pp. 79-103, 2010.

[2] D. Ramsbrock and X. Wang, "The Botnet Problem," in *Computer and Information Security Handbook (Second Edition)*, 2013, pp. 223-238.

[3] "IBM X-Force Threat Activity Report," [Online]. Available: https://exchange.xforce.ibmcloud.com/. [Accessed June 2021].

[4] P. Correia, E. Rocha, A. Nogueira and P. Salvador, "Statistical Characterization of the Botnets C&C Traffic," *Procedia Technology 1,* p. 158 – 166, 2012.

[5] A. Mills and P. Legg, "Investigating Anti-Evasion Malware Triggers Using Automated Sandbox Reconfiguration Techniques," *Journal of Cybersecurity and Privacy,* pp. 19-39, 2020.

[6] L. Zobal, D. Kolar and J. Kroustek, "Exploring Current Email Cyber Threats using Authenticated SMTP Honeypot," in *17th International Joint Conference on e-Business and Telecommunications (ICETE 2020) - SECRYPT*, 2020.

[7] R. Duncan and Z. C. Schreuders, "Security implications of running Windows software on a Linux system using Wine: a malware analysis study," *Journal of Computer Virology and Hacking Techniques,* vol. 15, p. 39–60, 2019.

[8] Palo Alto, "SILVERTERRIER: The Rise of Nigerian Business Email Compromise," Canada, 2018.

[9] M. Hoang, "Malicious Activity Report: Elements of Lokibot Infostealer," Infoblox, Canada, 2019.

[10] H. Unterbrink, "A Deep Dive into Lokibot Infection Chain," 6 January 2021. [Online]. [Accessed July 2021].

[11] MITRE ATT&CK, "MITRE ATT&CK," 02 July 2020. [Online]. Available: https://attack.mitre.org/software/S0447/. [Accessed July 2021].

[12] crowdstrike, "Malspam in the Time of COVID-19," 2020. [Online]. Available: https://www.crowdstrike.com/blog/covid19-and-malspam/.

[13] M. Co and G. Sison, "Attack Using Windows Installer Leads to LokiBot," Trend Micro, 8 February 2018. [Online]. Available: https://www.trendmicro.com/en_us/research/18/b/attack-using-windows-installer-msiexec-exe-leads-lokibot.html. [Accessed July 2021].

[14] M. Kazem, "Trojan:W32/Lokibot," 25 November 2019. [Online]. Available: https://www.f-secure.com/v-descs/trojan_w32_lokibot.shtml. [Accessed July 2021].

[15] CISA, "Alert (AA20-266A)," 24 October 2020. [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-266a. [Accessed July 2021].

[16] R. Sharma, N. Sharma and M. Mangla, "An Analysis and

ISSN 2636-9680
eISSN 2682-9266

Investigation of InfoStealers Attacks during COVID'19: A Case Study," in *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*, India, 2021.

[17] I. Arghire, "Loki Bot Attacks Target Corporate Mailboxes," 30 August 2018. [Online]. Available: https://www.securityweek.com/loki-bot-attacks-target-corporate-mailboxes. [Accessed July 2021].

[18] R. Sobers, "81 Ransomware Statistics, Data, Trends and Facts for 2021," 6 July 2021. [Online]. Available: https://www.varonis.com/blog/ransomware-statistics-2021/. [Accessed July 2021].

[19] L. Loeb, "Android Banking Trojan 'Gustuff' Becomes More Dangerous," March 2019. [Online]. [Accessed July 2021].

[20] A. Remillano, M. Malubay and A. R. Macaraeg, "LokiBot Impersonates Popular Game Launcher," 14 February 2020. [Online]. [Accessed July 2021].

[21] any.run, "Lokibot," [Online]. Available: any.run, "Lokibot," [Online]. Available: https://any.run/malware-trends/lokibot. [Accessed September 2021]. [Accessed September 2021].