The Rise of FusionCore An Emerging Cybercrime Group from Europe - CYFIRMA

Archived: 2026-04-02 10:54:35 UTC

Published On : 2023-04-03

EXECUTIVE SUMMARY

The CYFIRMA research team has identified a new up-and-coming European threat actor group known as FusionCore. Running Malware-as-a-service, along with the hacker-for- hire operation, they have a wide variety of tools and services that are being offered on their website, making it a one-stop-shop for threat actors looking to purchase cost- effective yet customizable malware. The operators have started a ransomware affiliate program that equips the attackers with the ransomware and affiliate software to manage victims. FusionCore typically provides sellers with a detailed set of instructions for any service or product being sold, enabling individuals with minimal experience to carry out complex attacks.

INTRODUCTION

In this research report, we will discuss previously undiscovered malware being sold by FusionCore, its respective capabilities and the level of sophistication of the threat actors. FusionCore was founded in 2022 by user “Hydra”, the

co-developer of the Typhon Reborn stealer. This malware developer has been in the stealer development and logs-selling business for a few years now, initially, being involved with the NoMercy infostealer, along with another associate that goes by the alias; “NecroSys”.

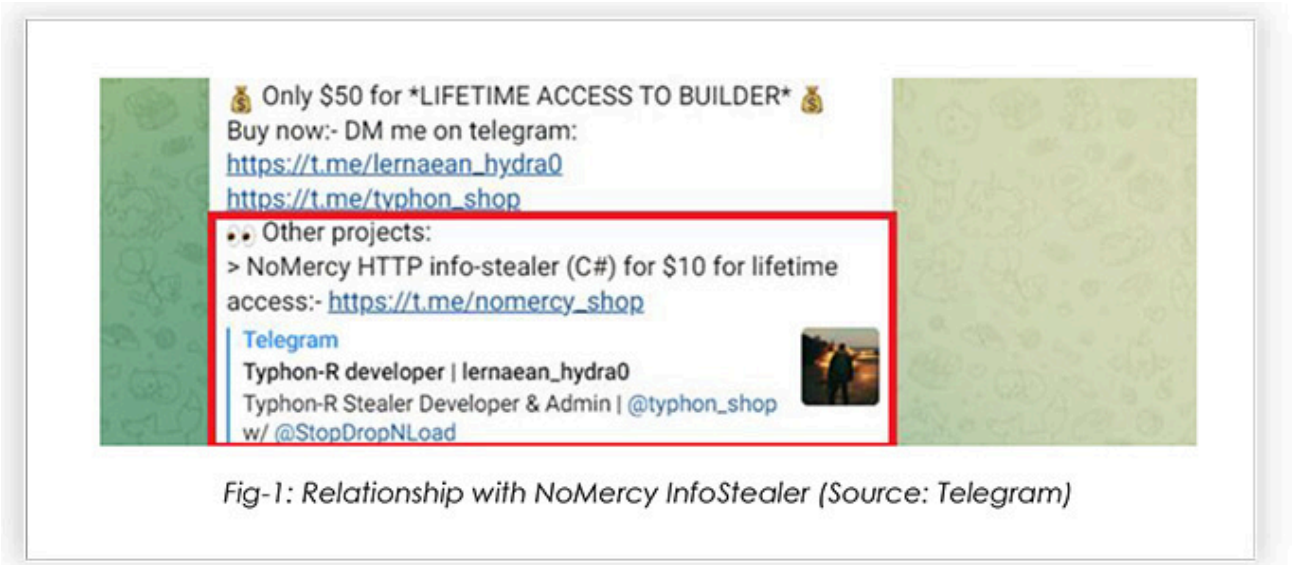

Fig-1: Relationship with NoMercy InfoStealer (Source: Telegram)

Researchers found the NoMercy stealer to be very crude and basic, and observations indicate that it was at the initial stages of development in early 2022. Based on the feedback from the threat actors, who were using the NoMercy infostealer, Hydra quickly realized that there is a high demand for all kinds of malware, not just infostealers. He decided to build a team that develops custom malware – and named the team FusionCore. Their malware catalogue includes, Typhon-R Stealer, RootFinder Stealer, RootFinder RAT, Cryptonic Crypter, RootFinder Ransomware, RootFinder Miner, Golden Mine, ApolloRAT, SarinLocker and KratoS dropper; with many new malwares already in the pipeline.

The other primary associates of FusionCore include, “NecroSys” (developer of SarinLocker, Typhon Stealer, Kratos Dropper, Ambien RAT), “DanielNusradin” (developer of RootFinder RAT, RootFinder Miner, RootFinder Stealer and RootFinder Ransomware), “InsaniumDev” (the developer of Golden Mine) and “SysKey” (group administrator, malware developer). Given the breadth of the threat actor group’s capabilities, translating into a range of lateral movements, a successful attack could result in significant financial and operational damage, as well as damage to the organization’s reputation among customers, investors, and partners. The CYFIRMA research team was able to obtain a few of the previously undiscovered malware samples being used by FusionCore operators. We will analyze them and share our findings with the community in our upcoming research reports.

FUSIONCORE GROUP PROFILE

FusionCore aliases are highly influenced by Greek and Roman mythology. Hydra named himself after a serpentine water monster Lernaean Hydra (the many-headed serpent who, when one of its heads was cut off, grew two more) in Greek Mythology. The Typhon stealer’s name is based on a monstrous serpentine giant, Typhon in Greek mythology. We have observed a trend within FusionCore’s primary operators to name their flagship malware after Greek mythological creatures. Most of the malware programs developed by FusionCore are written in C++, C# and Go. The operators are using open-source .NET obfuscators such as Obfuscar, NETShield and ConfuserEx to increase the

evasiveness of their crypter stub (software that can encrypt, obfuscate, and manipulate malware). The group highly relies on open-source software, with NBMiner and xmrig as part of their tool arsenal to enable cryptocurrency mining.

TIMELINE OF FUSIONCORE EVOLUTION

June 2022

After working on new features and evasion capabilities, Hydra started selling the Typhon-stealer, released on their new telegram channel.

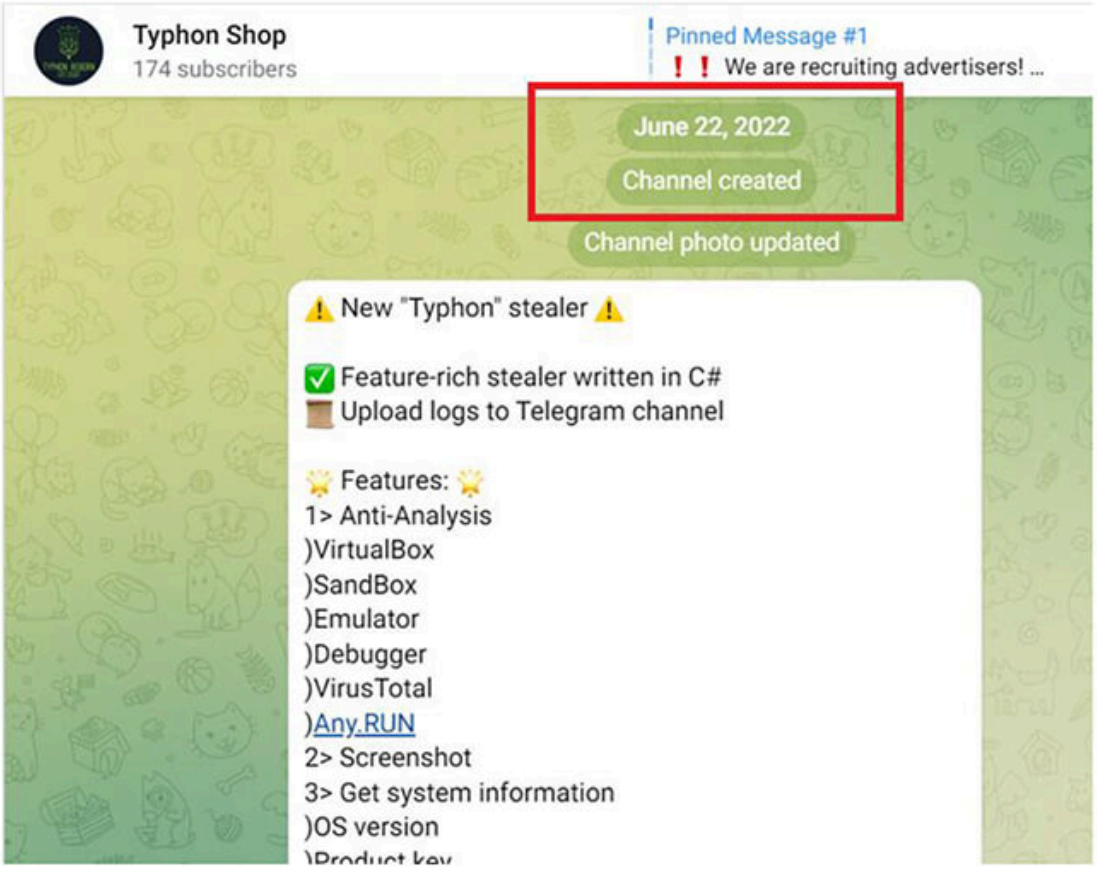

Fig-2: Typhon Stealer telegram channel creation in June 2022 (Source: Telegram)

July 2022

Typhon stealer was being updated frequently, based on user feedback.

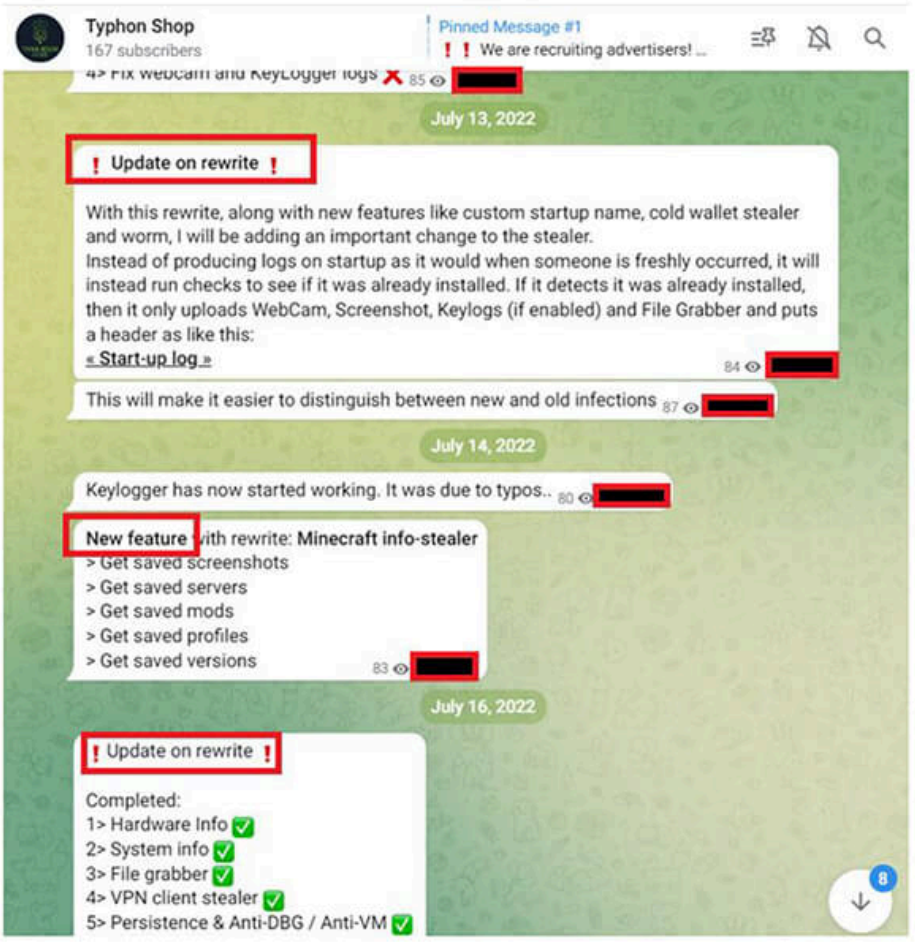

Fig-3: Frequent updates based on feedback from attackers, using the Typhon stealer (Source: Telegram)

July 2022

The MaaS operators were found to provide malware-spreading services across the globe, indicating that they likely have access to a private botnet, spanned across multiple geographies. The operators were found to charge a higher

price, to spread malware within Europe, than any other continent.

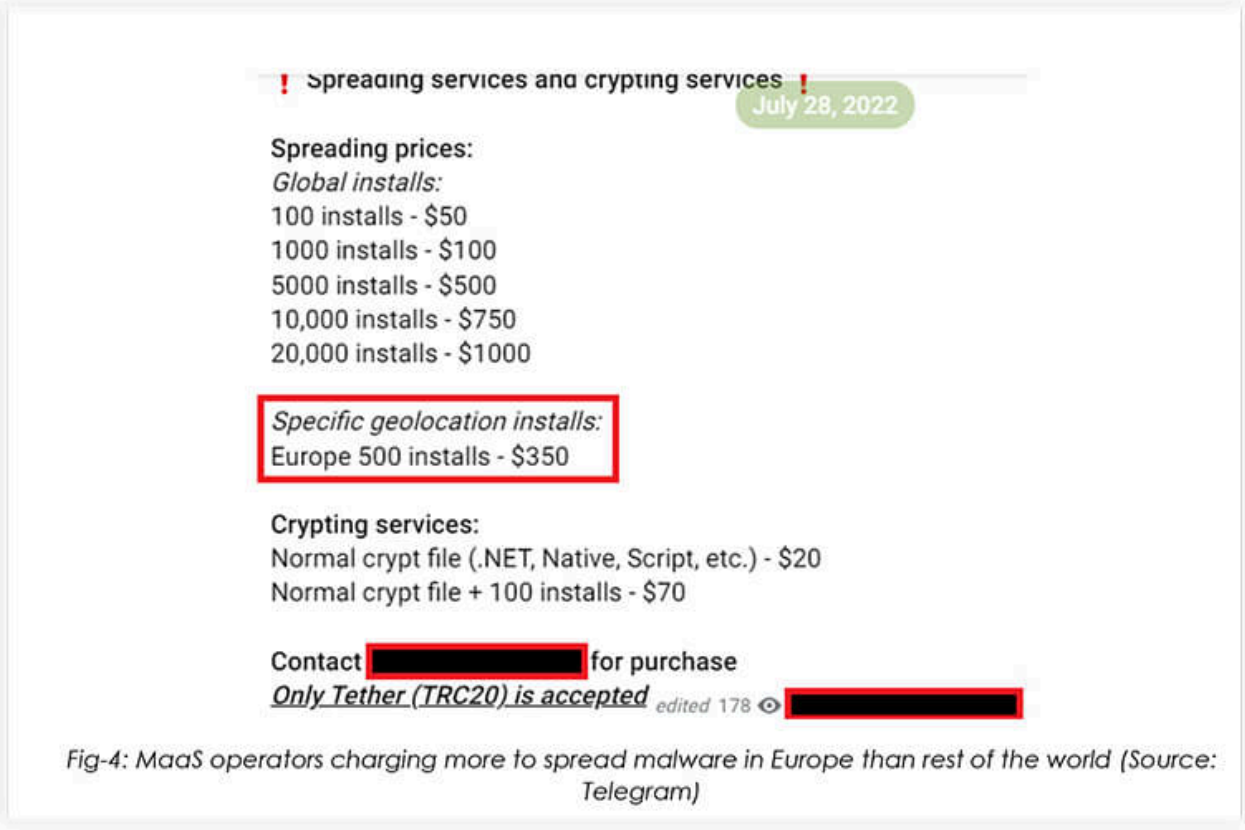

Fig-4: MaaS operators charging more to spread malware in Europe than rest of the world (Source: Telegram)

September 2022

FusionCore's telegram channel was created for streamlining MaaS operations:

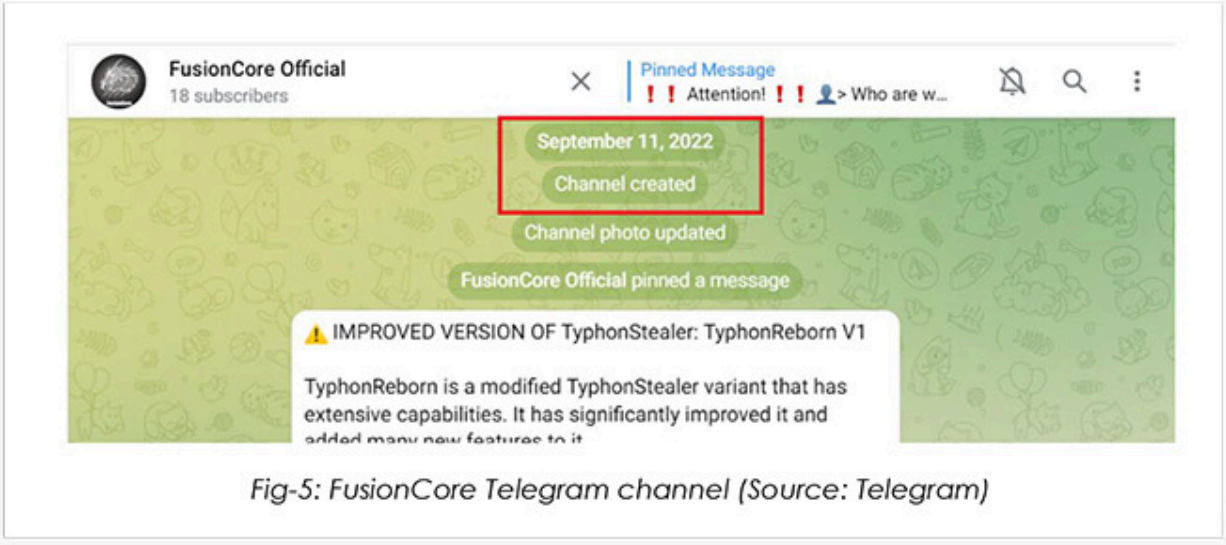

Fig-5: FusionCore Telegram channel (Source: Telegram)

Due to a lack of buyers, Hydra was willing to recruit a Russian-speaking advertiser, who would advertise the products on underground forums, channels, etc. with a 25% commission for the marketer on the revenue.

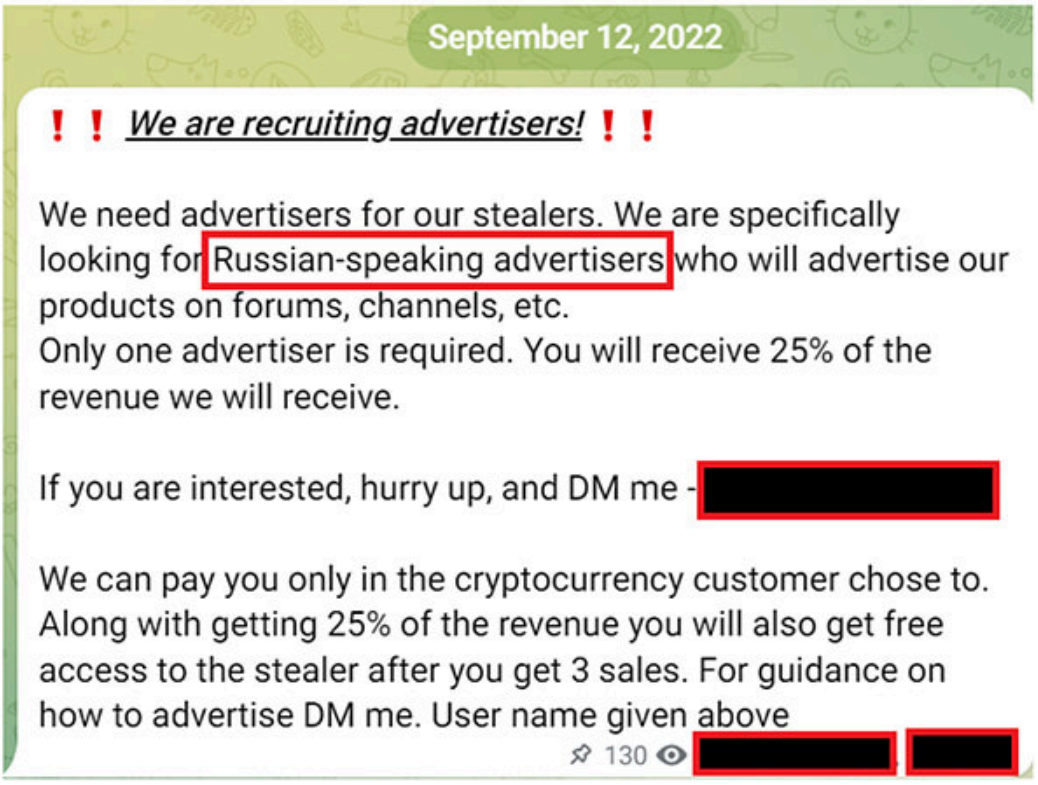

Fig-6: Announcement to recruit Russian-speaking advertisers (Source: Telegram)

October 2022

Another malware developer in FusionCore that goes by the alias NecroSys came in advertising a soon-to-be-released

ransomware written in C#, called SarinLocker.

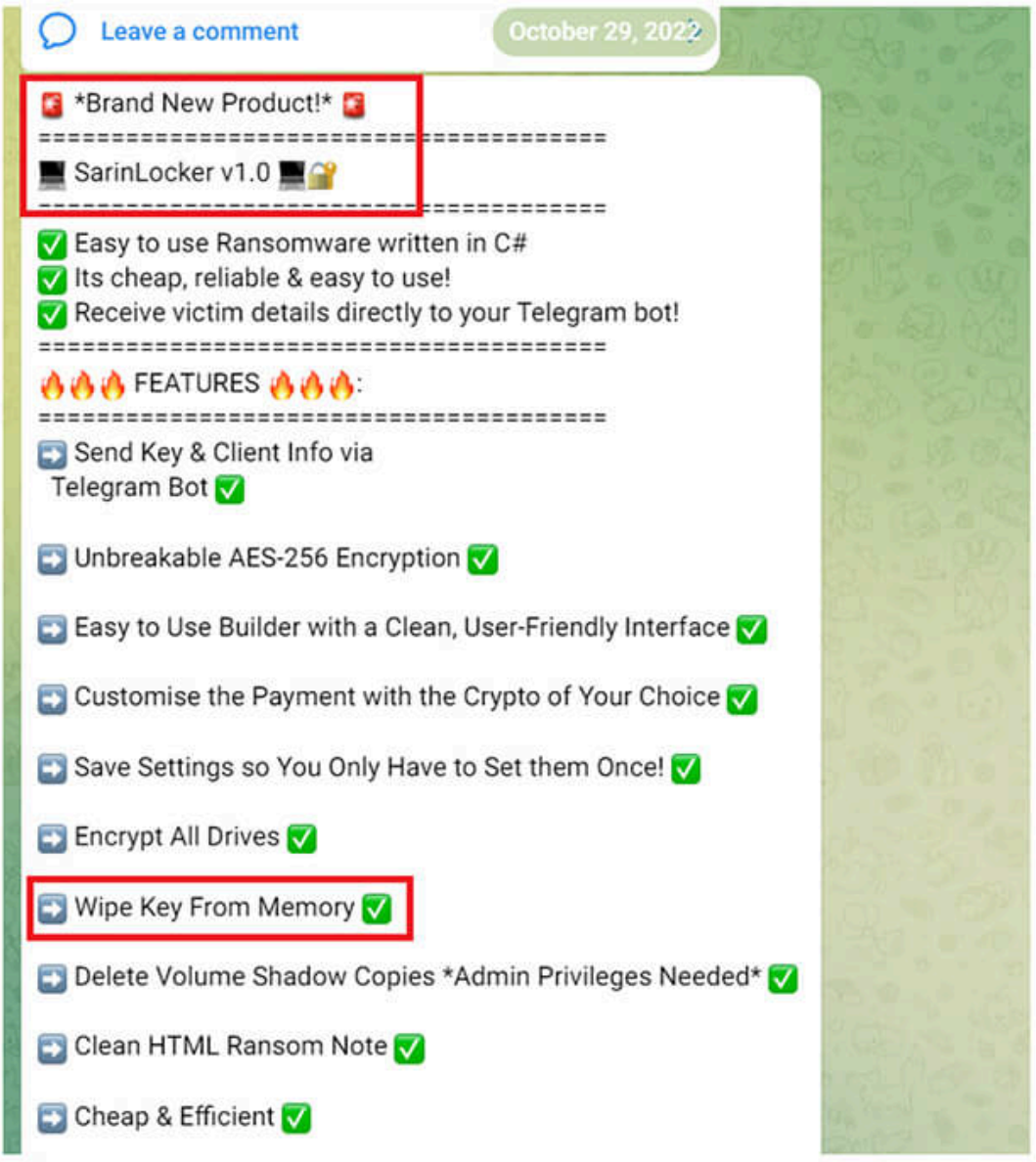

Fig-7: SarinLocker v1.0 under development (Source: Telegram)

November 2022

The group admin, SysKey announced the official launch of the webshop for FusionCore.

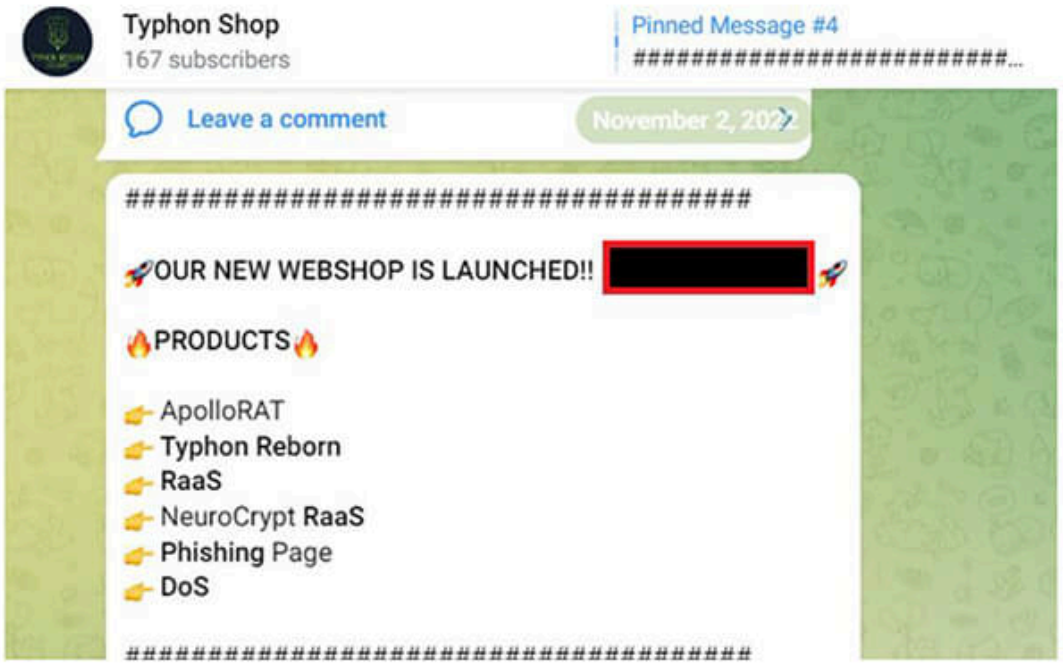

Fig-8: Telegram announcement stating official marketplace launch (Source: Telegram)

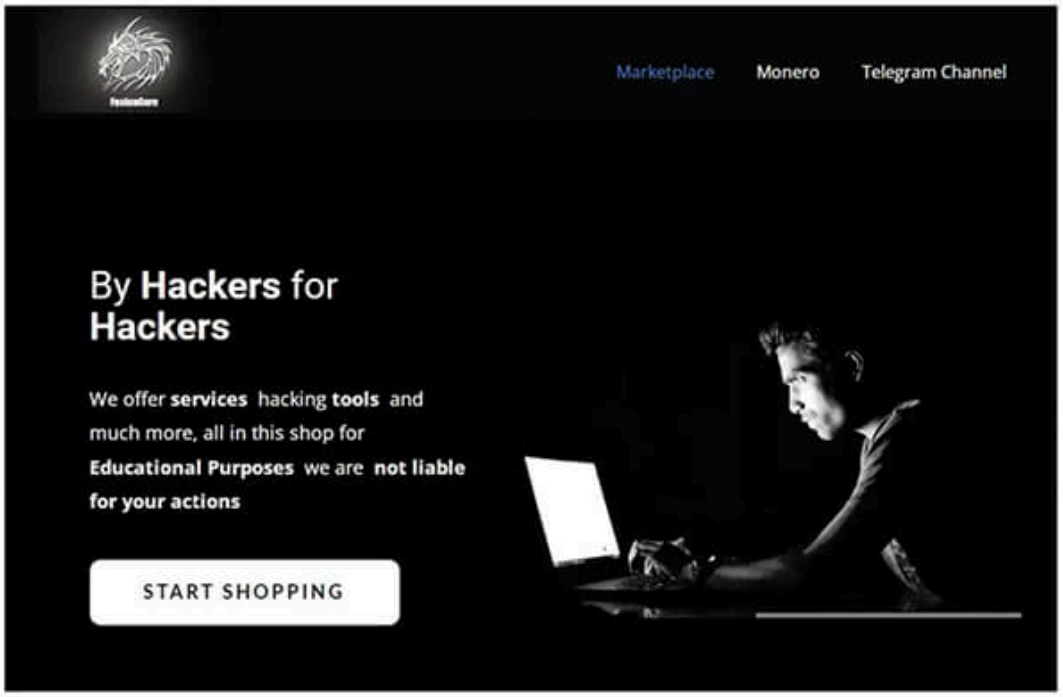

Fig-9: Web shop – FusionCore (Source: Surface Web)

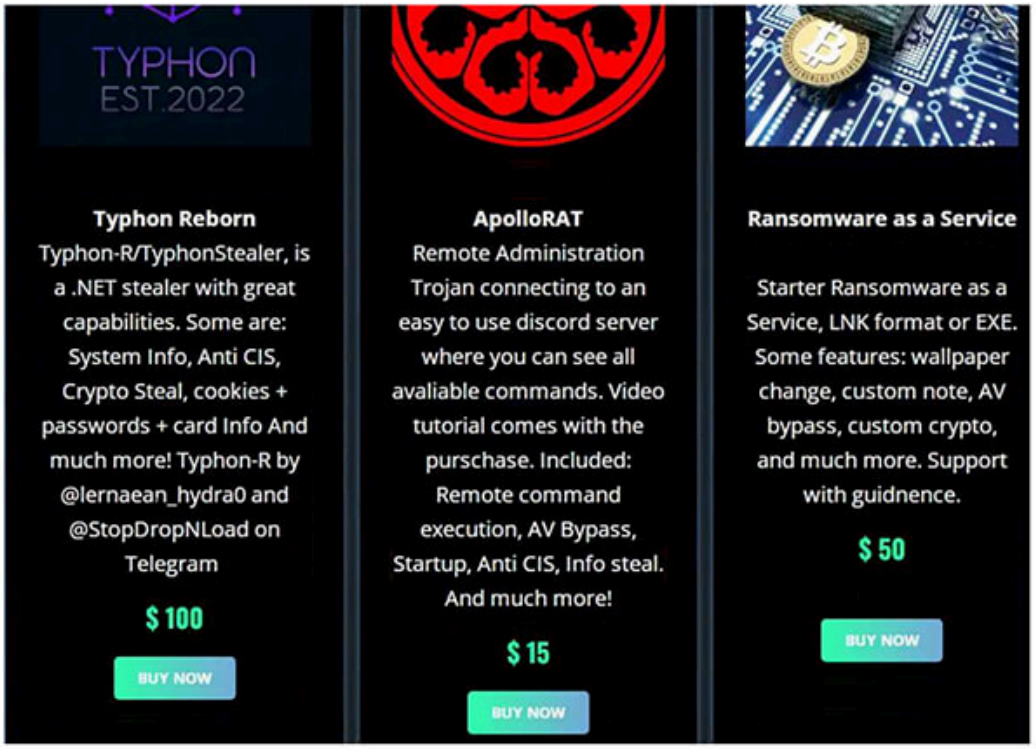

Fig-10: FusionCore malware and services (Source: Surface Web)

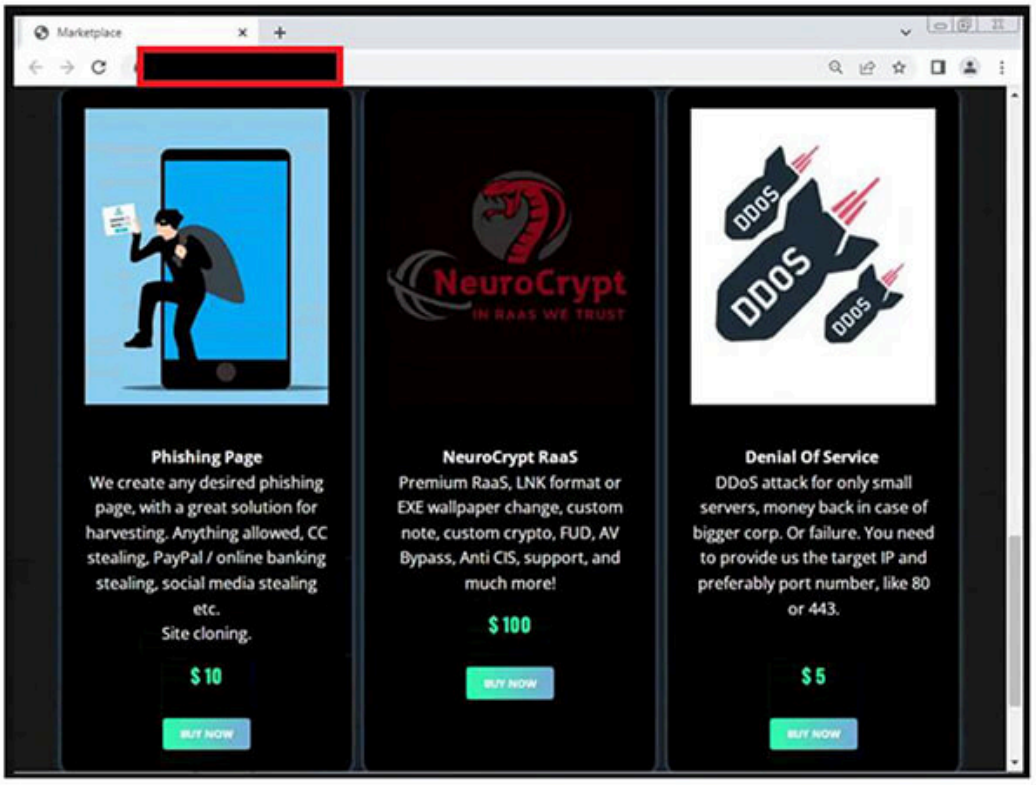

Fig-11: FusionCore malware and services (Source: Surface Web)

November 2022

The operators released an announcement, regarding the upcoming tools and related features:

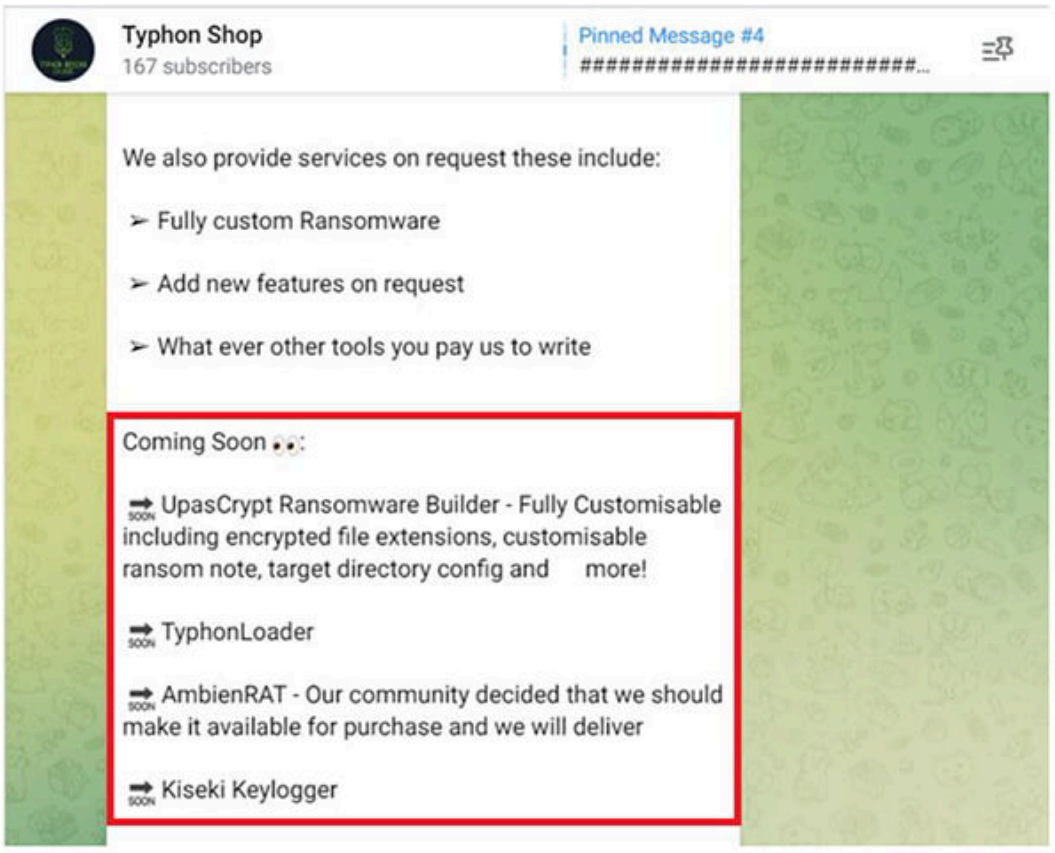

Fig-12: Upcoming malware by FusionCore (Source: Telegram)

January 2023

The MaaS operators were looking to expand their team with the addition of an experienced malware developer.

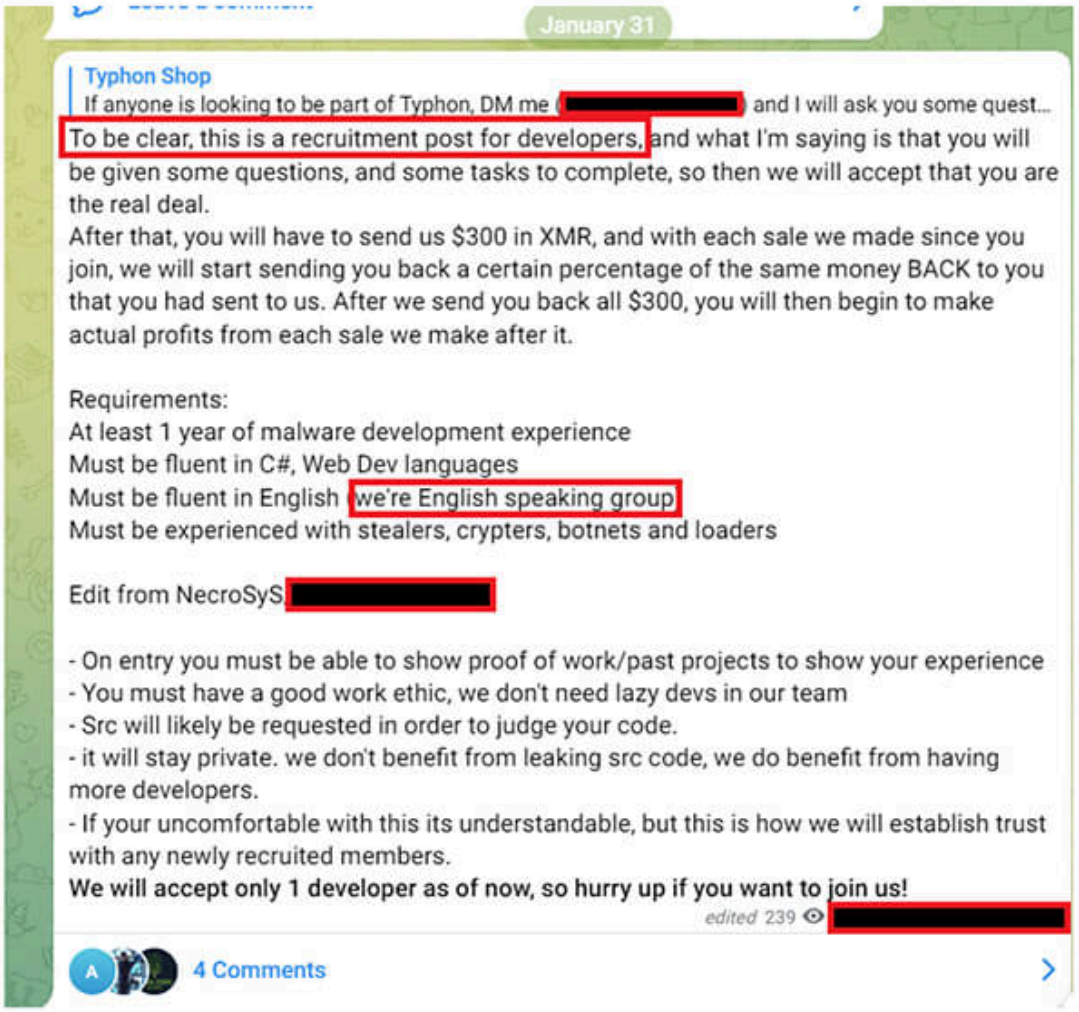

Fig-13: Recruitment announcement for malware developers (Source: Telegram)

Needless to say, the post gained traction from the malware developers' community.

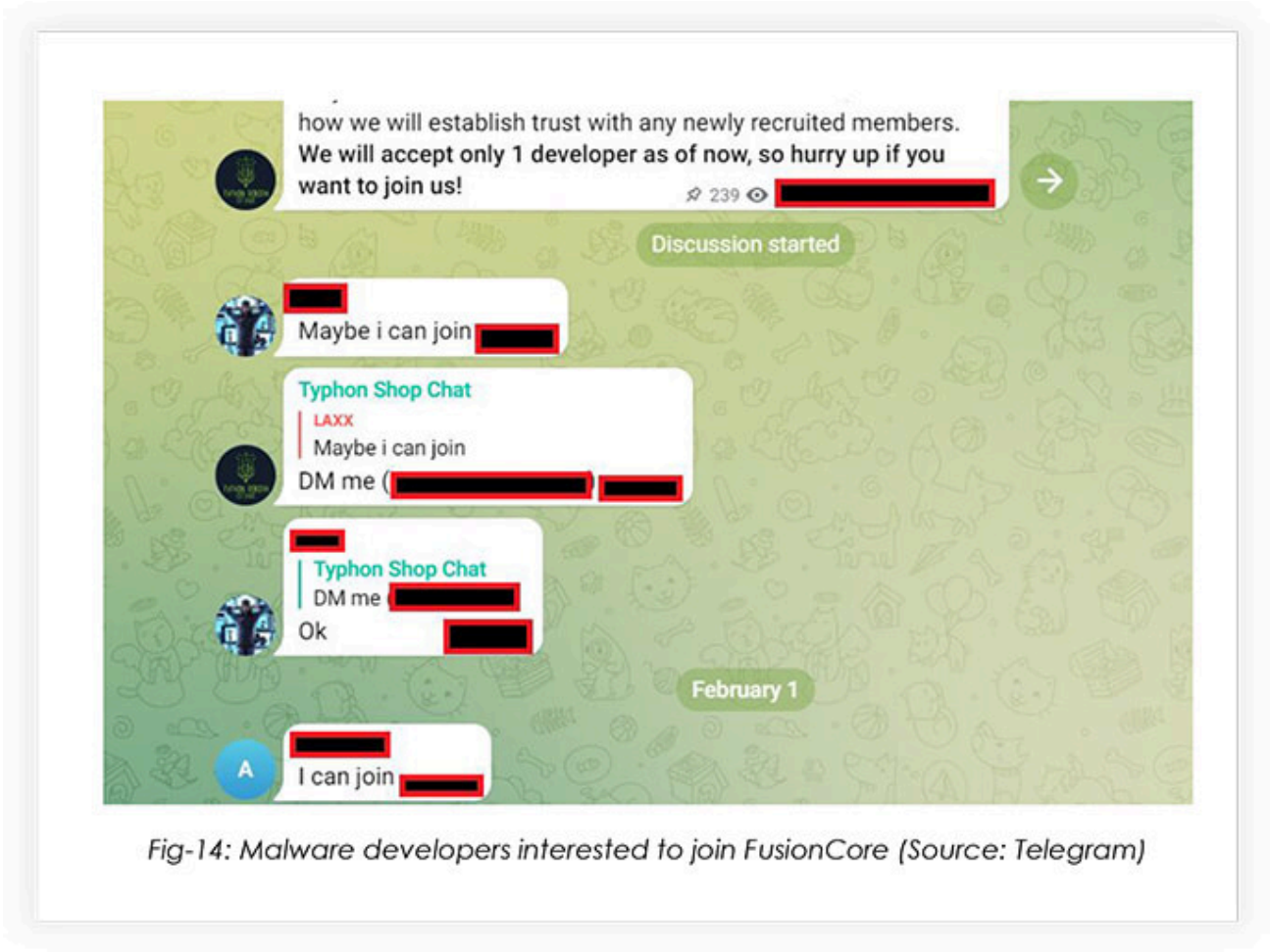

Fig-14: Malware developers interested to join FusionCore (Source: Telegram)

February 2023

Leveraging the poor Operations Security (OpSec) from the MaaS operators, the CYFIRMA research team has obtained the C2 panel snippet, shared by the attacker on 25th February 2023 on their telegram channel (now deleted). The snippet reveals public IPs that are being used by the FusionCore for testing grounds for the malware:

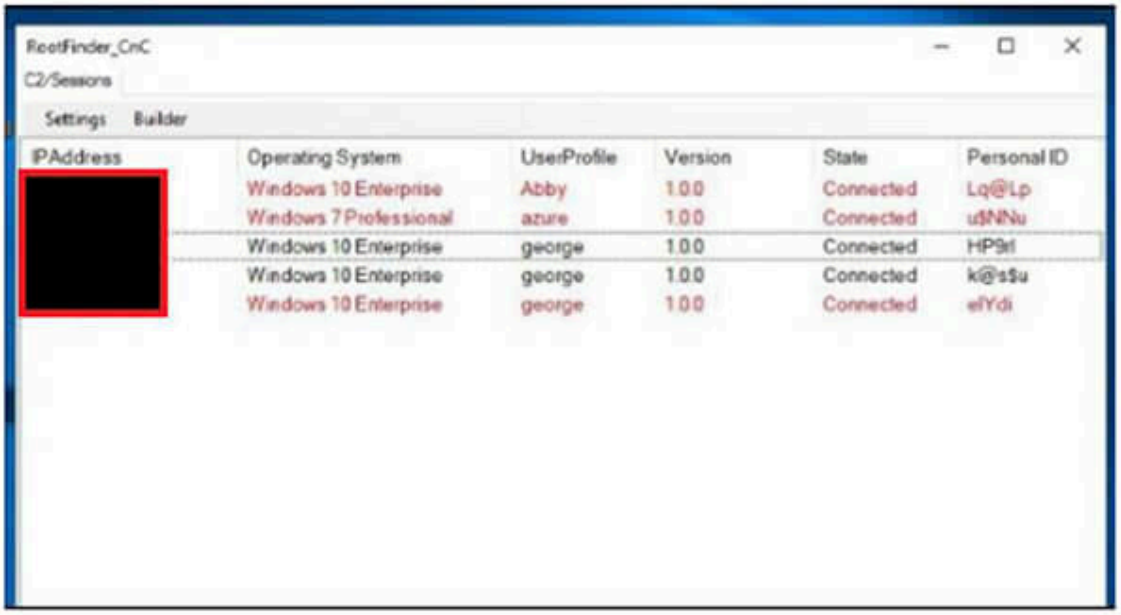

Fig-15: RootFinder RAT C2 panel (Source: Telegram)

The CYFIRMA research team will continue to monitor the infrastructure, as these are likely part of the botnet that the MaaS operators are using to provide malware- spreading services. The RootFinder telegram channel was deleted shortly, after the threat actors realized the operational error.

March 2023

Hydra shared a screenshot of the Typhon Reborn stealer dashboard (under development). Please take note that the dashboard is set to display Sweden time by default.

Fig-16: Typhon reborn stealer dashboard – under development (Source: Telegram)

On 26th March 2023, NecroSys made an announcement on the Typhon stealer telegram channel about an upcoming, fully native, and fully undetectable ransomware, named “VIPERA Ransomware”, that is designed to encrypt victim files in microseconds.

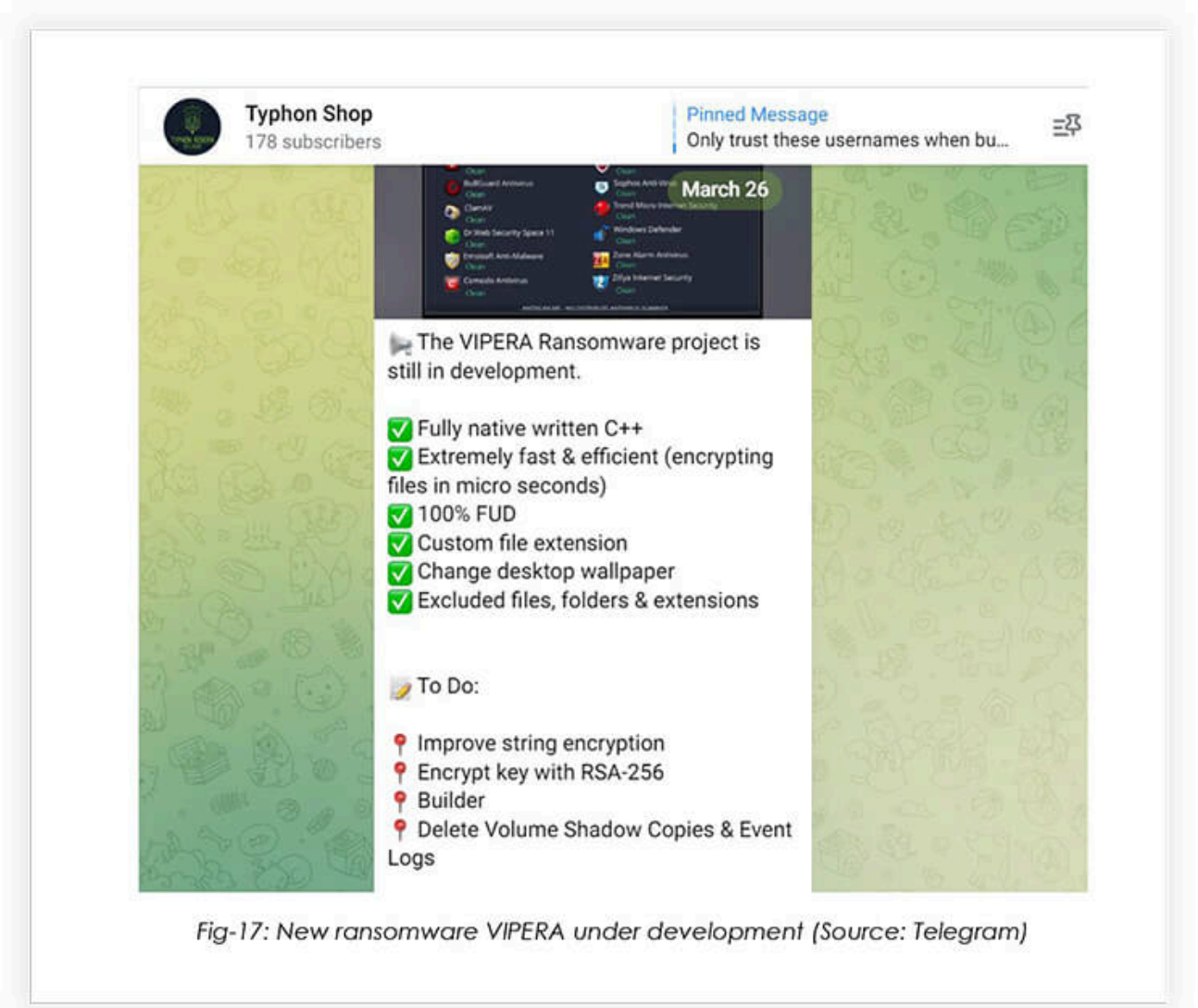

Fig-17: New ransomware VIPERA under development (Source: Telegram)

Based on the available information and discussions, it can be ascertained with medium confidence that the operators of FusionCore are operating from Europe. The group acts as both malware developers and threat actors, providing malware subscriptions as well as hacker-for-hire services. Using phishing as their primary attack vector for initial access, FusionCore specializes in a wide range of malware, which makes them capable of carrying out stealthy and persistent attacks.

MALWARE OFFERED BY FUSIONCORE

SARINLOCKER

On 15th November 2022, NecroSys officially announced the release of SarinLocker v1.0, a ransomware which would use telegram for sending decryption keys and client information. It appends an extension SARIN.LOCKED on the encrypted files. The prices were really competitive, compared to other ransomware, as they were charging 20$ for a month, and 100$ for lifetime access.

Please take note that the ransomware has the ability to wipe the decryption key from the infected device’s memory – making it tougher to extract the key, during memory forensics.

The CYFIRMA research team was able to obtain a few of the malware samples, being used by FusionCore operators. We will analyze the obtained FusionCore samples and share our findings with the community in our upcoming research reports. Till then, security teams can find the IOC(s) at the end of this report to block as required.

Admin Panel

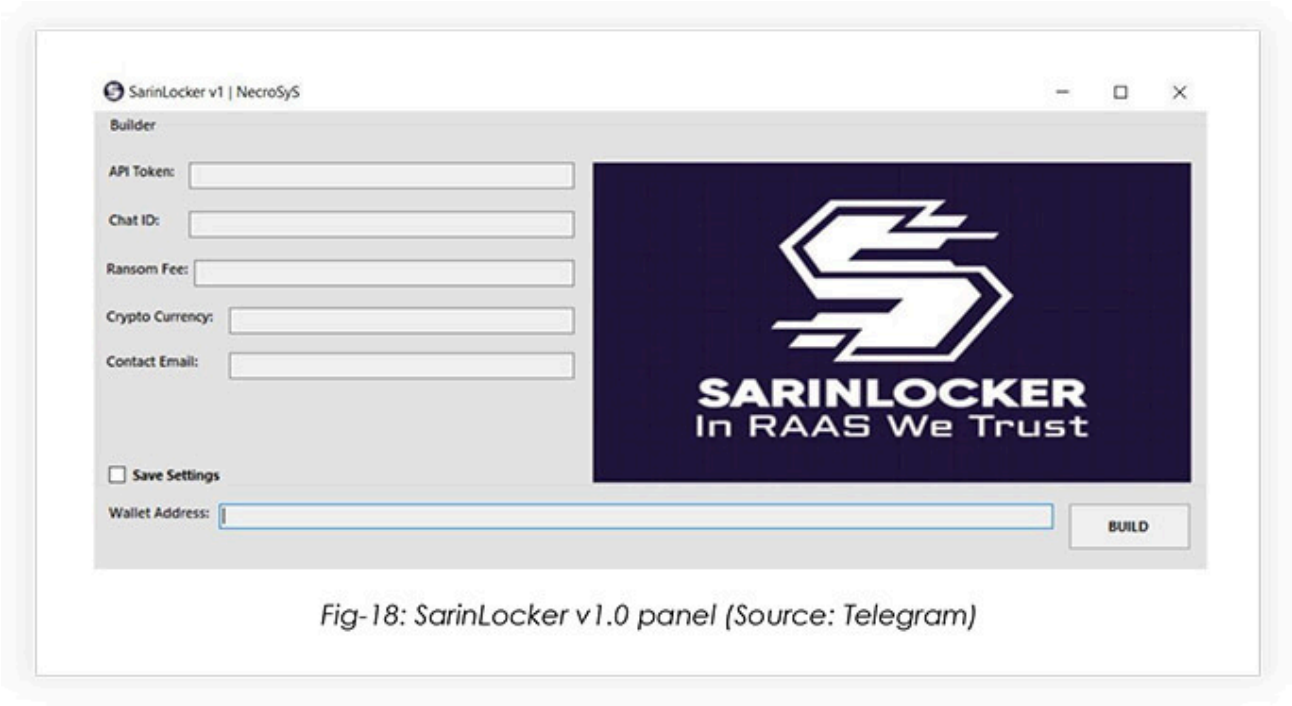

Fig-18: SarinLocker v1.0 panel (Source: Telegram)

Fig-19: SarinLocker post-encryption desktop wallpaper (Source: Telegram)

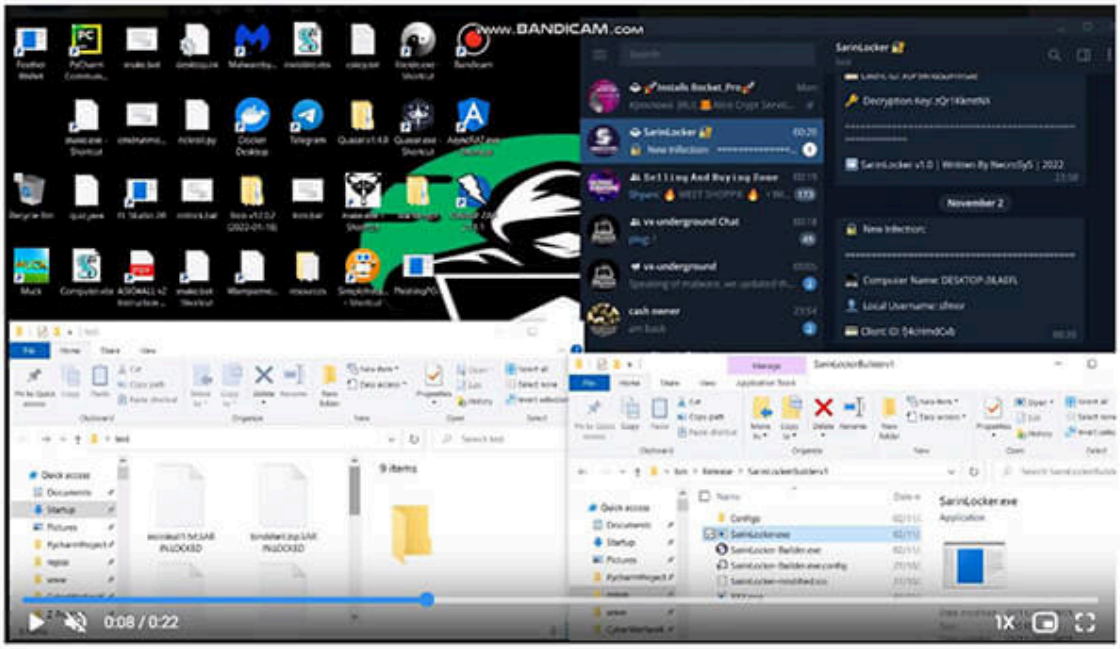

Fig-20: Demo video snippet showcasing the use of telegram bot (Source: Telegram)

In November 2022, a poll was posted on the Typhon stealer telegram channel, regarding the development of SarinLocker v2.0

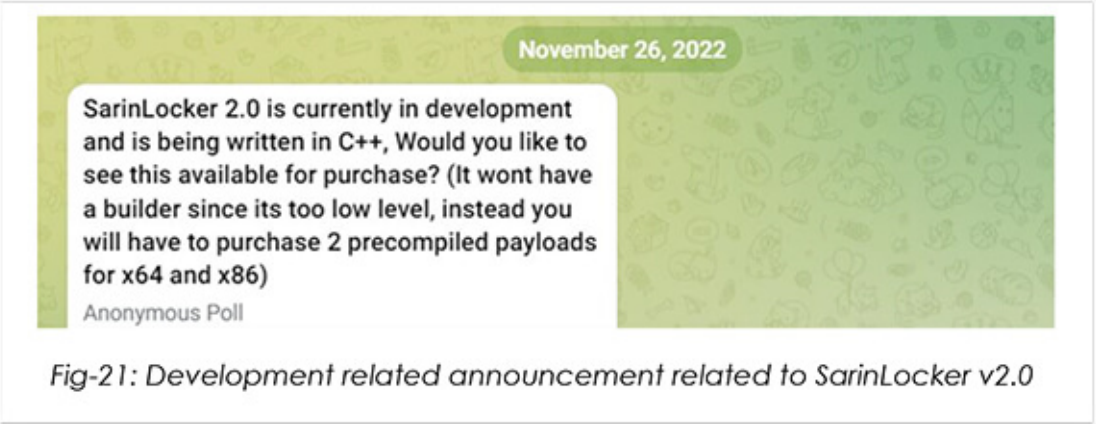

Fig-21: Development related announcement related to SarinLocker v2.0

Please take note that the malware developer states that there will be 2 precompiled payloads for x64 and x86 systems.

On 22nd December 2022, NecroSys announced the release of SarinLocker v2.0, which was written in C++. Amongst other changes, the new version would have a longer decryption key for victims, as the decryption key in SarinLocker v1.0 was short and could be brute-forced.

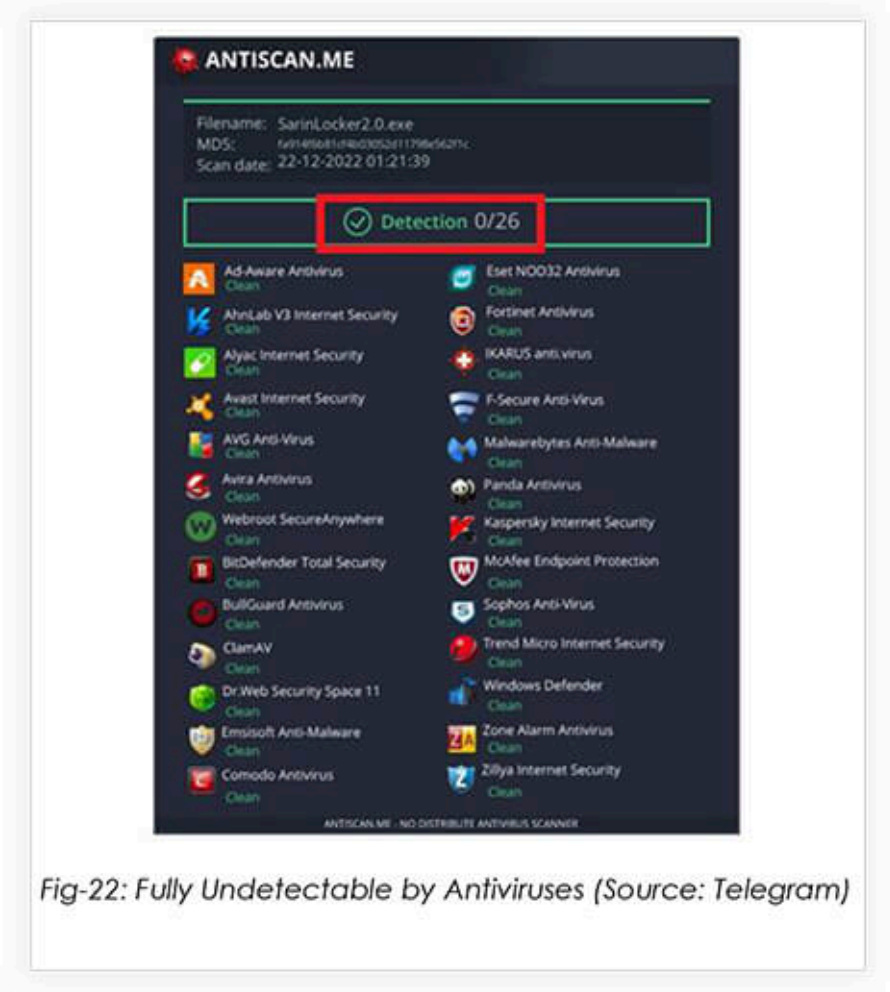

Fig-22: Fully Undetectable by Antiviruses (Source: Telegram)

ROOTFINDER STEALER

On 14th February 2023, Hydra started advertising a new information stealer, called the RootFinder Stealer on the Typhon Stealer telegram channel.

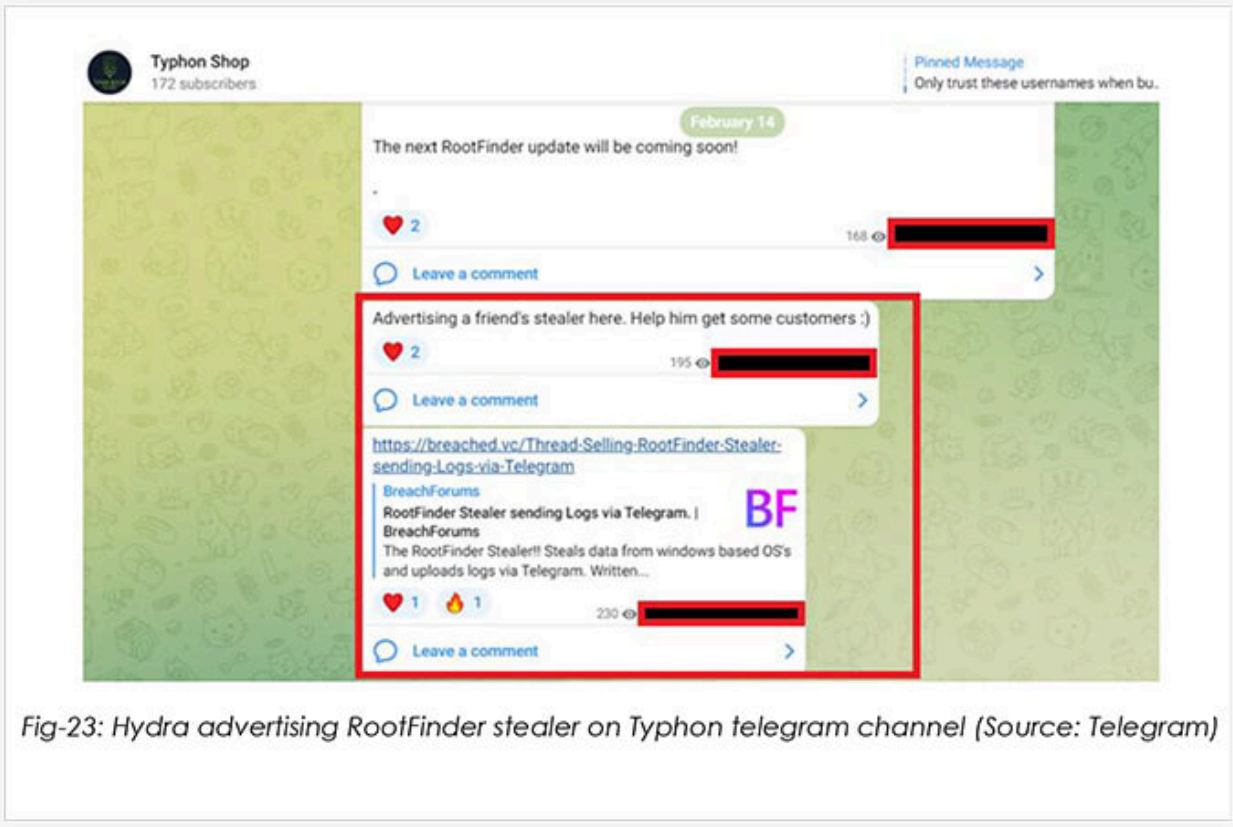

Fig-23: Hydra advertising RootFinder stealer on Typhon telegram channel (Source: Telegram)

The developer of RootFinder range of malwares (Stealer, RAT, Ransomware, Miner) is using the alias, Daniel Nusradin. We believe that the developer of RootFinder is a novice at this stage and is taking guidance from the more seasoned members of FusionCore on how to develop malware.

It is a variant based on the Redline and Typhon Stealer. The infostealer uses a telegram bot for receiving data from the infected device.

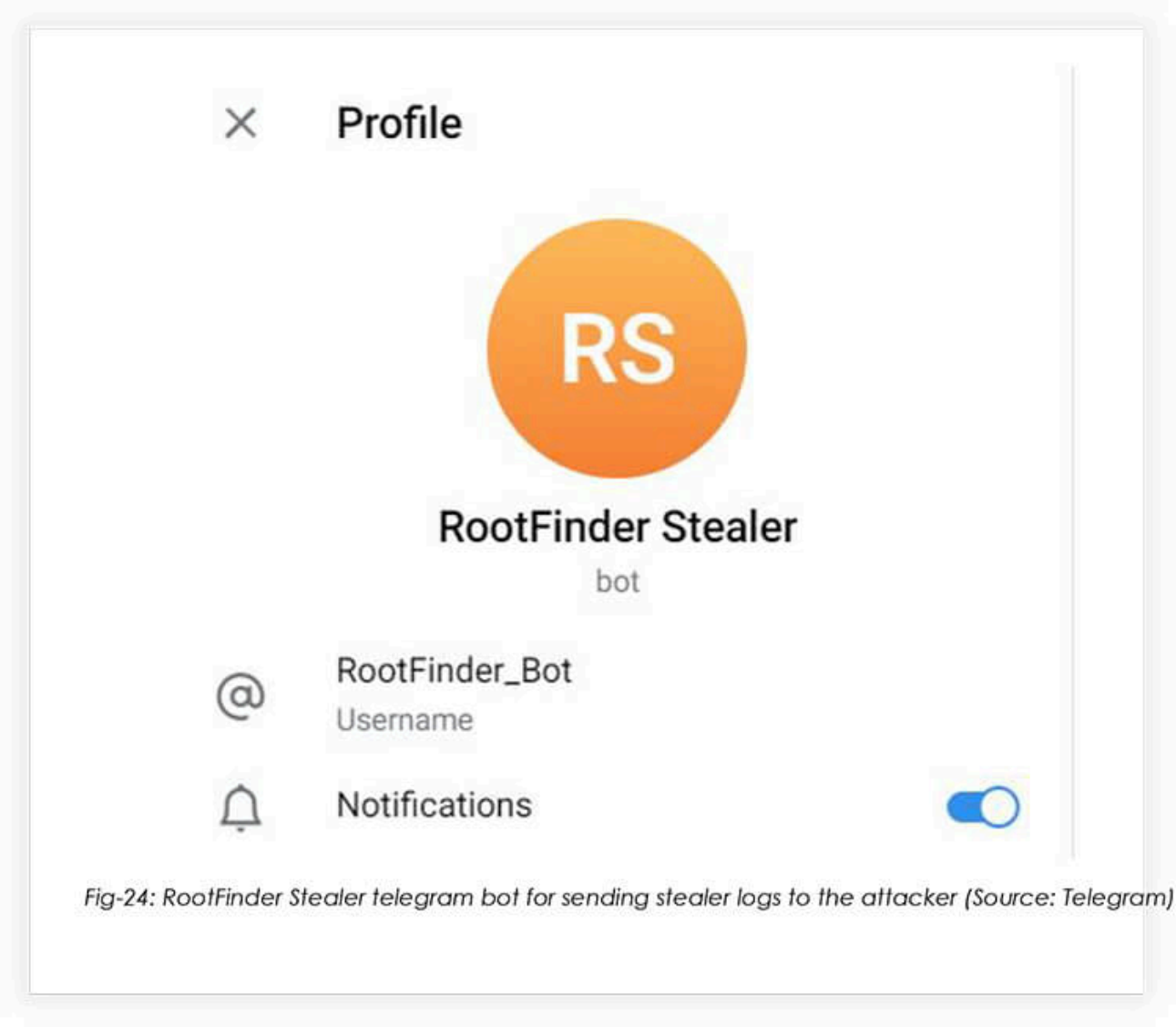

Fig-24: RootFinder Stealer telegram bot for sending stealer logs to the attacker (Source: Telegram)

Features:

- Grabs the victims' details (Date & Time, Computer User, Operating System, Operating System Version, DNS hostname, Installed Anti-Virus, And the Computer language)
- Harvests hardware information (HWID, RAM Sizə (in Megabytes), Memory Devices, BIOS Caption, BIOS Manufacturer, Graphics Card, CD-Rom path)
- Collects Network Information (Private IP address, External IP address, Subnet Scan, Mac Address)
- Data recovery (Passwords, Cookies, Autofills, Credit Cards, Search History)

ROOTFINDER RANSOMWARE

There's very limited information about the RootFinder ransomware. The ransomware's author seems inexperienced, with poor OpSec, so it's unlikely that the malware will become more sophisticated and widespread anytime soon.

Features:

- The Ransomware employs an encryption process that is completely undetectable and can encrypt files more quickly. The encryption method used is AES Encryption.
- The Ransomware is designed to be lightweight, with a size of only 26 KB.
- Upon installation, the malware connects to an HTTP Panel and transmits the personal installation key to the attacker.
- The Ransomware can generate unique decryption keys for each victim.
- Additionally, there is a separate application for affiliates that requests the Personal Installation Key. The attacker must provide the victim's Installation Key in the application to obtain the decryption key.
- Buyers(attackers) are registered to a web panel, enabling them to log in and access the ransomware admin panel.

CRYPTONIC

Cryptonic is a .NET crypter that's compatible with both .NET and Native Payloads. A crypter is a type of software that can encrypt, obfuscate, and manipulate malware, making it harder to detect by security programs. Cryptonic comes with an easy-to-use builder and each stub is unique. It is not for sale yet as the threat actors have not finished the development. However, anyone who is interested can purchase test crypts, that are being sold for $5 equivalent in XMR or ETH.

Fig-25: Favicon for Cryptonic (Source: Telegram)

Threat actors can use Cryptonic to make known malware undetectable by Antivirus engines. FusionCore demonstrated this by using Cryptonic on a previously known LockBit 3.0 sample:

Fig-26: Before Cryptonic, LockBit sample being detected by majority of antiviruses (Source: Telegram)

Fig-27: After using Cryptonic, the same LockBit sample becomes fully undetectable by antiviruses (Source: Telegram)

GOLDENMINE

GoldenMine is a cryptocurrency miner written in .NET. The miner is based on open- source tools, named NBMiner and XMRig. It can mine a wide variety of coins such as XMR, ETH, RVN, BEAM, and more, supporting both CPU & GPU mining.

Fig-28: GoldenMine advertisement (Source: Telegram)

Features:

- The miner's custom arguments are modified dynamically at the beginning of the process.
- The client allows for restarts, while miners are currently running.
- The client has the capability to detect if miners are being terminated or not.
- The client provides protection for miners(anti-analysis).

STRONTIUM STEALER

This infostealer is a relatively new addition to FusionCore's malware arsenal.

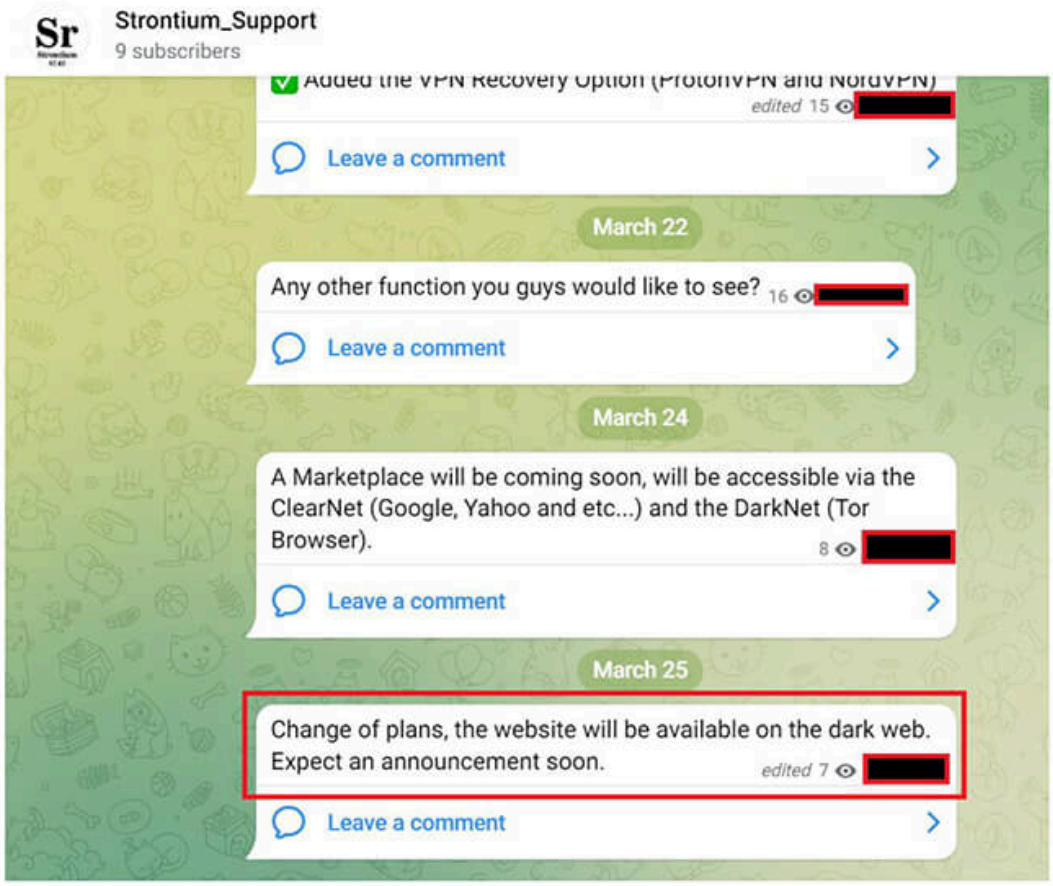

Fig-29: Announcement stating that a marketplace will be launched on the dark web. (Source: Telegram)

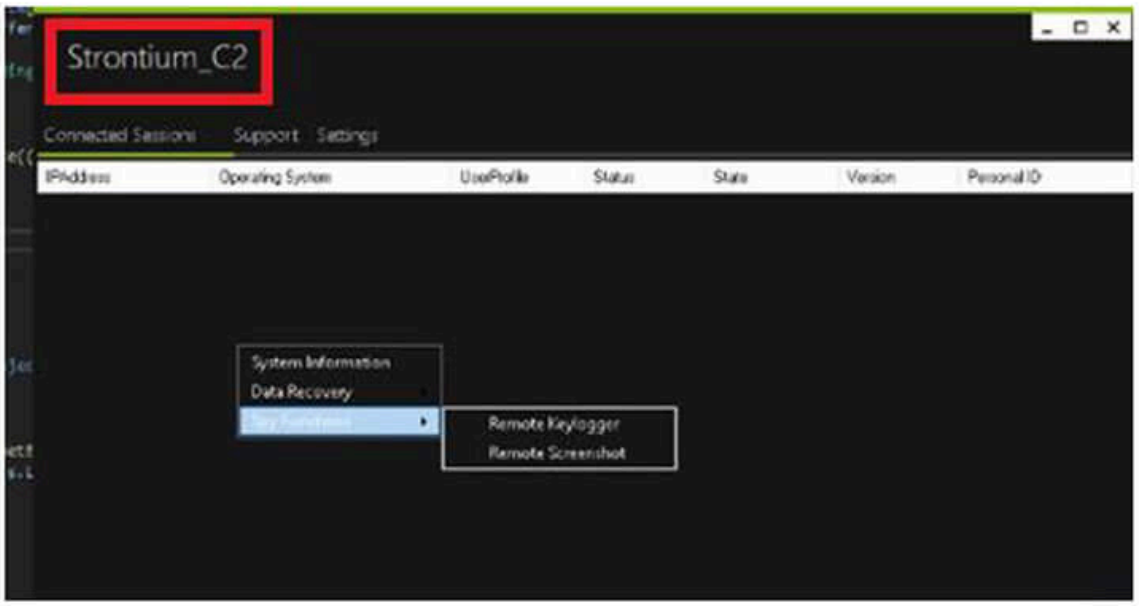

Fig-30: Admin Panel for the Strontium Stealer (Source: Telegram)

Fig-31: Keylogger Module in the Strontium Stealer (Source: Telegram)

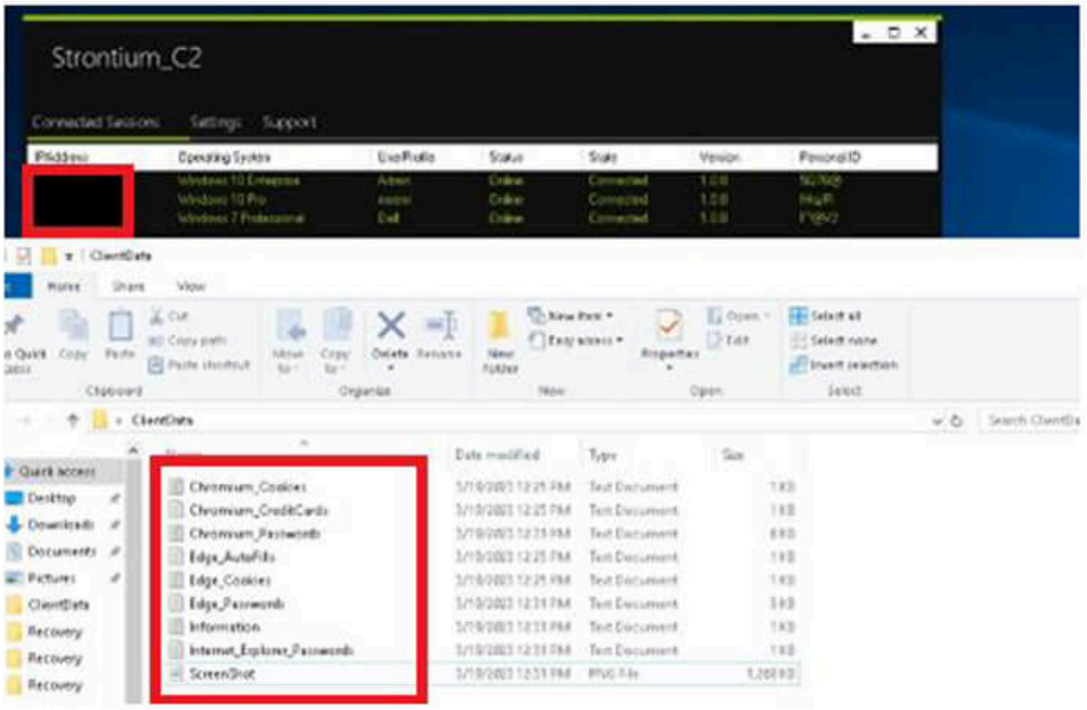

Fig-32: The malware can capture browser autofill, credit cards, cookies, credentials and screenshots. (Source: Telegram)

Date@Time	Actions	Save Location
3/18/2023 2:13:34 AM	Began the C2 listener.	No Save Location.
3/18/2023 2:13:42 AM	192.168.100.154:1102 has connected.	No Save Location.
3/18/2023 2:13:44 AM	Sent the *System Information* Command.	No Save Location.
3/18/2023 2:13:45 AM	The System Information is received.	C:\Users\user\Desktop\ClientData
3/18/2023 2:13:50 AM	Sent the *Remote Desktop* Command.	No Save Location.
3/18/2023 2:13:50 AM	The Screenshot is received.	No Save Location.
3/18/2023 2:13:54 AM	Sent the *Autofills* Command.	No Save Location.
3/18/2023 2:13:54 AM	The Autofills are received.	C:\Users\user\Desktop\ClientData
3/18/2023 2:14:00 AM	Sent the *Cookies* Command.	No Save Location.
3/18/2023 2:14:02 AM	Sent the *Passwords* Command.	No Save Location.
3/18/2023 2:14:02 AM	The Passwords are received.	C:\Users\user\Desktop\ClientData
3/18/2023 2:14:12 AM	Sent the *CreditCards* Command.	No Save Location.
3/18/2023 2:14:12 AM	The CreditCards are received.	C:\Users\user\Desktop\ClientData
3/18/2023 2:14:18 AM	192.168.100.154:1102 has disconnected.	No Save Location.

Fig-33: Strontium C2 server logs (Source: Telegram)

Features:

- The server and client components of the malware are lightweight. The client component is only 83KB in size.
- The malware can gather basic system information from the victim's computer.
- It is capable of stealing passwords, cookies, autofill data, and credit card information.

- The malware also includes spying functions such as activating a keylogger and taking screenshots of the victim’s desktop.
- The client component has an AntiAnalysis module to prevent security researchers from analyzing the malware.
- The connection between the malware and the C2 server is encrypted.
- The server component can generate an obfuscated client to evade detection by anti-virus software.
- The malware is designed to bypass majority of anti-virus programs.

EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) INSIGHTS

Threat Actor Profile: The members of FusionCore are young (possibly in their late teens), yet ambitious malware developers who have a wide variety of skills, depending on the type of malware that needs to be built. FusionCore is running a Malware-as-a-service model (MaaS), along with hacker-for-hire services, relying largely upon open-source tools, such as Obfuscar, NETShield, ConfuserEX, for increasing evasiveness in their malware toolkit.

Threat Landscape: FusionCore operators have started an affiliate program, named AnthraXXXLocker, and more affiliates are likely to join the group in the upcoming months. Furthermore, with the addition of new developers, FusionCore is set to enhance its malware arsenal in the coming future, adding to the already booming infostealer business, as well as dipping their toes into the extortion business.

Victimology: The targets of FusionCore would predominantly depend on the buyers and affiliates. Given they are a young up-and-coming group, they are willing to work with anyone, from anywhere. However, so far, the known targets of FusionCore include, Lindesberg Municipality in Sweden, and the Typhon Stealer was observed in a phishing attempt, against an infosec company in Asia Pacific.

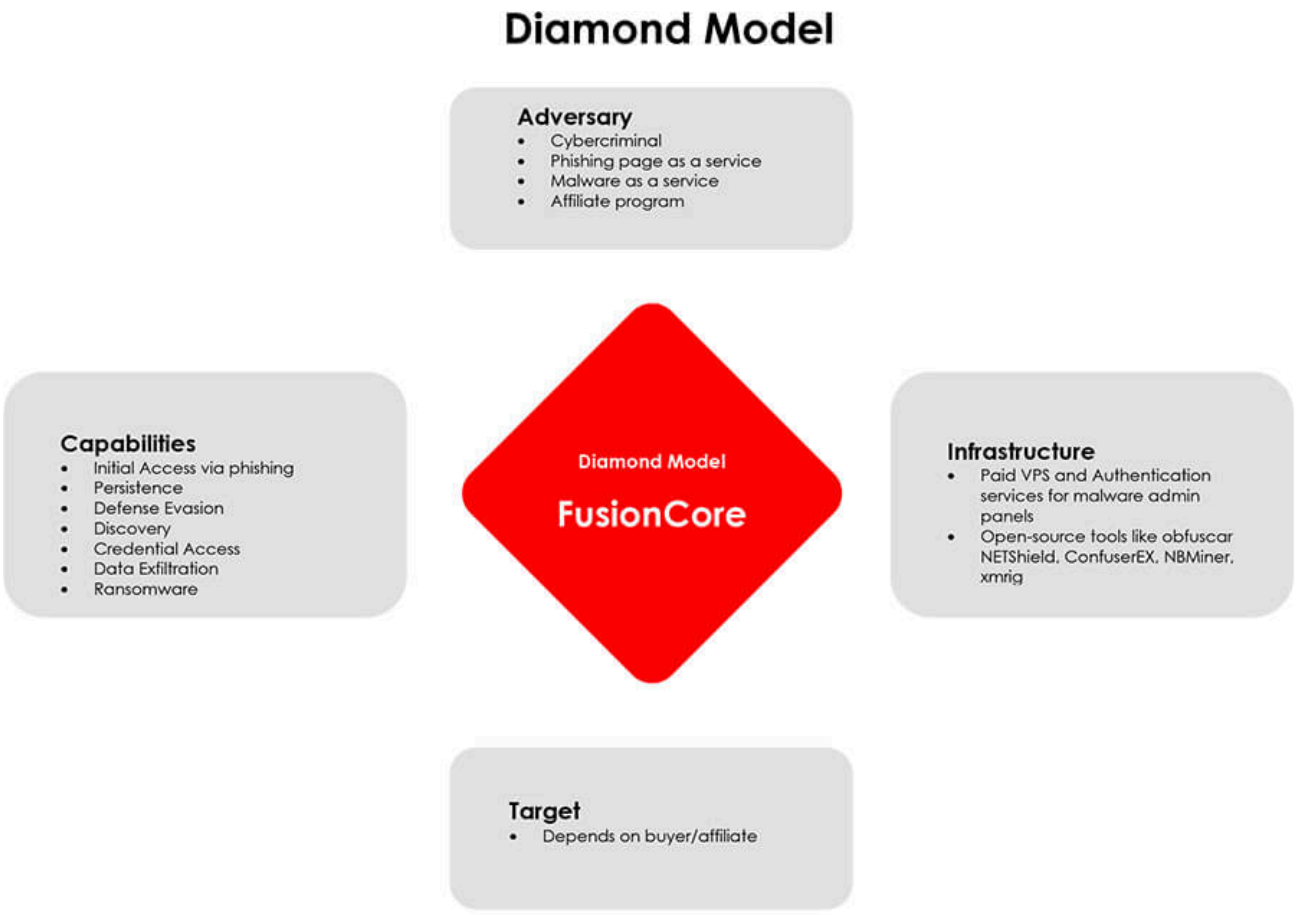

Fig-34: Diamond model for threat actor group; FusionCore

Impact Assessment: The threat actor group's diverse catalogue of malware presents a multifaceted risk to an organization, with the potential for financial losses due to data theft, operational disruptions caused by ransomware attacks, and reputational damage resulting from breaches of sensitive data.

The group's hacker-for-hire services and stealer capabilities offer a significant threat to the organization's digital assets, potentially leading to financial losses, due to stolen intellectual property or compromised customer data.

The use of crypters in FusionCore's malware suggests a sophisticated approach, increasing the potential impact of their attacks and the difficulty of detecting and mitigating them.

CONCLUSION

The members of the new FusionCore group are coming up with their own set of malwares, with the help of more seasoned malware developers present in the group. Their developing catalogue of tools suggests they have the ambition to create a suite, covering most, if not all of kill-chain, creating a one-stop shop for threat actors.

Due to the emergence of Malware-as-a-Service (MaaS), cyber-attacks have become more sophisticated than before. With the potential of a single data breach bringing down an entire system, attackers currently have a significant advantage. It is also imperative to have complete visibility onto the attack surface, as security teams cannot protect against what they cannot see.

MITIGATION STRATEGIES / RECOMMENDATIONS

Strategic Recommendations

- Conduct regular vulnerability assessments and penetration testing to identify and remediate vulnerabilities.
- Develop and implement an incident response plan, that includes clear procedures for containment, investigation, and recovery from security incidents.
- Review and update security policies and procedures to ensure they align with best practices and regulatory requirements.
- Foster a security-first culture, by promoting security awareness and accountability at all levels of the organization.

Management Recommendations

- Invest in ongoing security training and development for IT staff, to ensure they have the skills and knowledge necessary to protect the organization’s assets.
- Establish a security governance framework that includes clear roles and responsibilities for managing security risks.
- Engage with industry peers and partners to share threat intelligence and best practices for mitigating cybersecurity risks.
- Regularly review and update the organization’s risk management strategy to ensure it reflects the evolving threat landscape and business priorities.

Tactical Recommendations

- Implement network segmentation to limit the impact of successful attacks on critical systems.
- Deploy endpoint protection solutions to detect and prevent malware infections.
- Train employees on security awareness best practices to reduce the risk of successful phishing attacks.
- Monitor network traffic and user activity to detect and respond to suspicious behavior.

APPENDIX I

Indicators Of Compromise (IOCs)

No.	Indicator	Type	Malware
1	Fa914f6b81cf4b03052d11798e562f1c	MD5	SarinLocker v1.0
2	4cdd313daa831401382beac13bea4f00	MD5	SarinLocker v1.0
3	856707241a7624681d6a46b2fa279bd56aa6438a	SHA1	SarinLocker v1.0
4	1a0211f6bc0aab4889364024bd2ec9a3baa56e654d07586bb9c06b0c86f68eaf	SHA256	SarinLocker v1.0
5	97e4bd269be93b96d8c67c11fadcb75b	MD5	SarinLocker v2.0 payload (x64)

6	a5696381cbffc85c0509b2054484b4d4c56697d6	SHA1	SarinLocker v2.0 payload (x64)
7	563dfc726daaec005638ed3271657aa3e2a2529b7940cd0741d5a47e7e9b9c2c	SHA256	SarinLocker v2.0 payload (x64)
8	10aeadfd910bc5dab9e7d9d88abf5795	MD5	SarinLocker v2.0 payload (x86)
9	d9806de5917acdfa6f5c0c0f83cf7f4b42830e9d	SHA1	SarinLocker v2.0 payload (x86)
10	d41d03d804e6ccb7c749c74745df5187618f57b5c58d427d293a40f91a7e9736	SHA256	SarinLocker v2.0 payload (x86)
11	20.99.160[.]173	IPv4	RootFinder RAT
12	373bb4e17fbf239f2d02ea3fb3dfa352	MD5	RootFinder Stealer
13	bd93aa67e43350ea3c4833671d68709621a1304d	SHA1	RootFinder Stealer
14	575c5ad5a00e3ce13a75079666adfd254734f9c99555f4edf42ca3fa5d83f6f6	SHA256	RootFinder Stealer
15	925a12fa388efe3bad829e475ac12bfb	MD5	Builder
16	d9f6e37c8f58ac02c5415cab7e49c730	MD5	AnthraxxxLocker Ransomware Payload
17	b7f1a84fcc50733ef535891dc9253c3b3544f81f	SHA1	Builder
18	de03afb794e3017d1f6aa657a6ef82ca49c6fd08	SHA1	AnthraxxxLocker Ransomware Payload
19	05472bedb5a7613310b8088ca89b81e8390d39dddb8ed79dedd7311d2aaa6f80	SHA256	Builder
20	eed648bb9bd45a440b2ceadbbae04e69f9c7f098ab8980c019a6736e4f7bd10b	SHA256	AnthraxxxLocker Ransomware Payload

APPENDIX II

MITRE Mapping

No.	Tactics	Techniques/Sub-Techniques	Purpose	Used By
1	Execution TA0002	Windows Management Instrumentation T1047	Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines) Checks if Antivirus program is installed (via WMI) Queries sensitive processor information (via WMI, Win32_Processor, often done to detect virtual machines) Queries process information (via WMI, Win32_Process) Queries sensitive Operating System Information (via WMI, Win32_ComputerSystem, often done to detect virtual machines)	Typhon Reborn Stealer, RootFinder Stealer
		Command and Scripting Interpreter T1059	Accept command line arguments	Typhon Reborn Stealer, RootFinder Stealer
		Scripting T1064	Executes batch files	Typhon Reborn Stealer
2	Persistence TA0003	Registry Run Keys / Startup Folder T1547.001	Reference startup folder	Typhon Reborn Stealer, RootFinder Stealer
3	Privilege Escalation TA0004	Process Injection T1055	Spawn processes in suspended mode (likely to inject code)	Typhon Reborn Stealer, RootFinder Stealer
4	Defense Evasion TA0005	Masquerading T1036	Creates files inside the user directory	Typhon Reborn Stealer, RootFinder Stealer
		Process Injection T1055	Creates a process in suspended mode (likely to inject code)	Typhon Reborn Stealer, RootFinder Stealer
		Scripting T1064	Executes batch files	Typhon Reborn Stealer

		File Deletion T1070.004	Drops batch files with force delete using cmd (self deletion)	Typhon Reborn Stealer, RootFinder Stealer, SarinLocker
		Timestomp T1070.006	Binary contains a suspicious time stamp	Typhon Reborn Stealer
		Virtualization/Sandbo x Evasion T1497	Queries sensitive device information (via WMI, Win32_VideoController, Win32_Processor, Win32_ComputerSystem often done to detect virtual machines) Contains long sleeps (>= 3 min) May sleep (evasive loops) to hinder dynamic analysis Checks if the current process is being debugged	Typhon Reborn Stealer, RootFinder Stealer, SarinLocker
		Disable or Modify Tools T1562.001	Uses netsh to modify the Windows network and firewall settings Creates guard pages, often used to prevent reverse engineering and debugging Uses taskkill to terminate processes	Typhon Reborn Stealer, RootFinder Stealer, SarinLocker, Strontium
		Obfuscated Files or Information T1027	Encrypt or decrypt data via BCrypt Encrypt data using DPAPI Encode data using Base64	Typhon Reborn Stealer, RootFinder Stealer
		File and Directory Permissions Modification T1222	Set file attributes	Typhon Reborn Stealer, RootFinder Stealer, SarinLocker
		System Checks T1497.001	Reference anti-VM strings targeting VirtualBox Reference anti-VM strings targeting VMWare Reference anti-VM strings Reference anti-VM strings targeting Xen	Typhon Reborn Stealer, RootFinder Stealer, SarinLocker
		Reflective Code Loading T1620	Load .NET assembly	Typhon Reborn Stealer, RootFinder Stealer, RootFinder Miner, RootFinder RAT, RootFinder

				Ransomware, Cryptonic
5	Credential Access TA0006	OS Credential Dumping T1003	Tries to harvest and steal browser information artifacts	Typhon Reborn Stealer, RootFinder Stealer
		Input Capture T1056	Creates a DirectInput object (often for capturing keystrokes)	Typhon Reborn Stealer, RootFinder Stealer, RootFinder RAT, Strontium
6	Discovery TA0007	Application Window Discovery T1010	Sample monitors Window changes (e.g., starting applications)	Typhon Reborn Stealer, RootFinder Stealer, RootFinder RAT
		Query Registry T1012	Monitors certain registry keys / values for changes (often done to protect auto-start functionality)	Typhon Reborn Stealer, RootFinder Stealer, RootFinder RAT, Strontium, SarinLocker
		System Network Configuration Discovery T1016	Checks the IP addresses of the machine	Typhon Reborn Stealer, RootFinder Stealer, RootFinder RAT, Strontium, SarinLocker
		Remote System Discovery T1018	Reads the hosts file	Typhon Reborn Stealer, RootFinder Stealer
		Process Discovery T1057	Queries a list of all running processes	Typhon Reborn Stealer, RootFinder Stealer, RootFinder RAT, Strontium, SarinLocker
		System Information Discovery T1082	Queries information about the installed CPU (vendor, model number etc.) Queries the volume information (name, serial number etc.) of a device Queries the cryptographic machine GUID	Typhon Reborn Stealer, RootFinder Stealer, RootFinder RAT, Strontium, SarinLocker, RootFinder Miner, Cryptonic, Golden Mine

			Reads software policies Queries process information (via WMI, Win32_Process) Queries sensitive Operating System Information (via WMI, Win32_ComputerSystem, often done to detect virtual machines)	
		File and Directory Discovery T1083	Reads ini files	Typhon Reborn Stealer, RootFinder Stealer, RootFinder RAT, RootFinder Ransomware, SarinLocker
		Security Software Discovery T1518.001	Checks if Antivirus program is installed (via WMI) AV process strings found (often used to terminate AV products) May try to detect the virtual machine to hinder analysis (VM artifact strings found in memory)	Typhon Reborn Stealer, RootFinder Stealer, RootFinder RAT, Strontium, SarinLocker, RootFinder Miner, Cryptonic, Golden Mine
		System Location Discovery T1614	Get geographical location	Typhon Reborn Stealer, RootFinder Stealer, RootFinder RAT, Strontium, SarinLocker, RootFinder Miner, Cryptonic, Golden Mine
7	Collection TA0009	Data from Local System T1005	Tries to harvest and steal browser information (history, passwords, etc.)	Typhon Reborn Stealer, RootFinder Stealer, Strontium
		Input Capture T1056	Creates a DirectInput object (often for capturing keystrokes)	Typhon Reborn Stealer, RootFinder Stealer, Strontium
		Data from Information Repositories T1213	Reference WMI statements	Typhon Reborn Stealer, RootFinder Stealer
		Archive Collected Data T1560	.NET source code contains calls to encryption/decryption functions	RootFinder Stealer, RootFinder RAT,

				RootFinder Ransomware, Typhon Reborn Stealer
8	Exfiltration TA0010	Exfiltration Over Web Service/Exfiltration to Cloud Storage T1567.002	Exfiltrates data using Telegram API	Typhon Reborn Stealer, RootFinder Stealer, SarinLocker
9	Command and Control TA0011	Application Layer Protocol T1071	Uses HTTPS Performs DNS lookups Downloads files from webservers via HTTP	Typhon Reborn Stealer, RootFinder Stealer, RootFinder Miner, Golden Mine, Strontium, SarinLocker, RootFinder RAT
		Web Service T1102	Connects to an online service (for C&C)	Typhon Reborn Stealer, RootFinder Stealer, RootFinder Miner, Golden Mine, Strontium, SarinLocker, RootFinder RAT
		Encrypted Channel T1573	Uses HTTPS Uses HTTPS for network communication	Typhon Reborn Stealer, RootFinder Stealer, RootFinder Miner, Golden Mine, Strontium, SarinLocker, RootFinder RAT
10	Impact TA0040	Resource Hijacking T1496	Mine cryptocurrency	Typhon Reborn Stealer, RootFinder Stealer, RootFinder Miner, Golden Mine
		Data Encrypted for Impact T1486	Modifies user documents; Writes a notice file (html or text) to demand a ransom	SarinLocker, RootFinder Ransomware
		Inhibit System Recovery T1490	Deletes volume shadow copies	SarinLocker

Sigma Rule(s)

RootFinder Stealer

title: Suspicious Network Command

description: Adversaries may look for details about the network configuration and settings of systems they access or through information discovery of remote systems

tags:

– attack.discovery

– attack.t1016

logsource:

category: process_creation

product: windows

detection:

selection:

CommandLine|contains:

– ‘ipconfig /all’

– ‘netsh interface show interface’ – ‘arp -a’

– ‘nbtstat -n’

– ‘net config’

– ‘route print’

condition: selection

level: low
