UWE Bristol | University of the West of England

FINANCIAL SERVICES & INSURANCE INDUSTRIES BASED ON APT38 & SILENCE

Critical Systems Security - UFCF7P-15-M

PRANEETHRAJ

ID: 21071235

Section 1: EXECUTIVE SUMMARY

The assets of well-off companies and governments have always attracted attackers (PT, 2019). Due to the main centralized architecture and one point of reach for every organization makes the financial sector most attractive and highly rewarding area for the hackers. In this study we are concentrating on two most groups who attacked on the financial sectors, they are Silence and APT38. Silence is **Russian-speaking cybercriminal group**. APT38 who run campaigns with 26 unique malware families, also resources say it is **North-Korean state-sponsored.**

Section 2: IT and OT

IT	OT
IT is dynamic because it contains number of exploitable variants. IT teams are responsible for safeguarding every layer of security, it's a never-ending cycle as software gets updated now and then.	OT is deterministic, here system is designed for specific task and contains specific set of code to perform actions based on content. Here it's a yes or no clear process, there is no in-between states.
Data drives everything, its about digital information storage, transmit, and manipulate. Only concern is smooth flow of business.	Process is king, its overall On, off, control of different hardware. Environment is same for everyday process and action.
Attack surface or points are very huge, Gateway to attack is everywhere and BOTs contribute 60% of the traffic.	Less attack types as limited gateway, which is usually known to developers.
CIA traid is followed very strictly and privacy is top priority.	Control system are top priority as it manages operations. Ignoring this might cause serious damage to the environment. Last thing is confidentiality.
Updates, security updates need to be delivered as soon as some issue found and that vulnerability must be patched.	Critical infrastructure cannot be paused / shut from security updates every now and then. In fact, design itself will have no disruption, no slowdowns. So, updates are not viable solution.

Table (GE, No date) (Security Delta, No date)

Section 3: OVERVIEW & LANDSCAPE OF GROUPS.

APT38: Operating against 38 countries worldwide from 2014 in association with groups like: Nickel Gladstone, Chollima (MITRE,2021). Groups resources are worth around $500,000 according to FireEye. The TTP's were overlapping the other operations which is known as "Lazarus" actor known to be "TEMP.Hermit" (MANDIANT, 2018). It is also recorded that the group gained access for 155 days to 2 years according to its campaigns (Positive technologies 2019).

SILENCE: Is a financially motivated threat actor targeting banks, Insurance companies, and news agencies in different countries (MITRE, 2021). Active since 2016, residing in Russia, Ukraine, Poland and Kazakhstan. They use free Sysinternals Suit and other self-developed tools including its own framework, ATM theft toolkit etc. (Positive Technologies, 2018). Investment on malware toolkit is around $2500. NirCmd was used to penetrate and control the target machines. Tools, money mules accounted for 15 to 50% of the stolen $930,000. (GroupIB, 2020)

A) Kill Chain and TTP's:

Mitre Kill Chain was followed to understand the depth of attack groups.

APT38

Reconnaissance to Execution: APT38 have used tool named Mimikatz, a credential dumper, capable of obtaining windows account credentials (Mitre, 2021). **Initial access** was drive by compromise, phishing attack by Spearphishing attachment. **Execution**: Once user opens mail it falls to the process of Native API. Attackers deceive to execute different types of code, run binary files, scheduled task and tools to escalate privileges (Mitre, 2021)

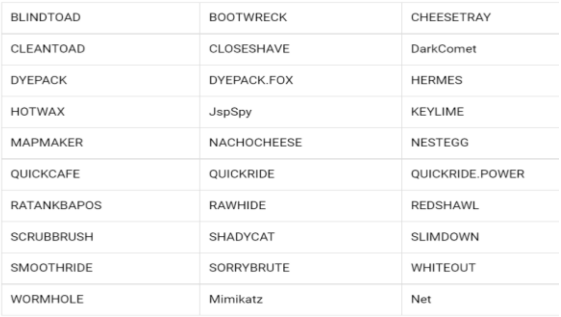
Persistence and Privilege Escalation: Used Windows API to execute code in victim's system (Mitre, 2021).Different applications like PowerShell, Windows Command line Shell, Malicious File which gathered credentials and map the victim's network topology (Mandiant Un-usual Suspects, 2018).

Defense Evasion: Disable or modify system firewall here this group had put firewall exemptions on specific ports, including ports 443, and 9443**, Impair command history logging:** terminal commands which resulted in executing them without leaving the execution. **Clear windows Event Logs**: To hide the activity of an intrusion, alert notifications, error, warning, information, success Audit and Failure Audit. Overall **cleared logs** from the system which could lead to their origin.

Credential Access and Discovery: Using brute force account was compromised. **Keylogging** was another technique used under malware named **KEYLIME** which captured keystrokes from victims' machine (Mitre, 2020) Other techniques like Browser bookmark, File and Directory, Network, Process, System Information, User Accounts. By using all these attackers were able to identify and pass through.

Exfiltration and Impact

Main part is impacts of all above steps Data Destruction, Data Encryption, System Shutdown under system level and on the user level Runtime Data Manipulation, Stored Data Manipulation, Transmitted Data Manipulation, Disk Structure Wipe (MBR) and this will cause the disaster for the company as well as different stakeholders.



BLINDTOAD	BOOTWRECK	CHEESETRAY
CLEANTOAD	CLOSESHAVE	DarkComet
DYEPACK	DYEPACK.FOX	HERMES
HOTWAX	JspSpy	KEYLIME
MAPMAKER	NACHOCHEESE	NESTEGG
QUICKCAFE	QUICKRIDE	QUICKRIDE.POWER
RATANKBAPOS	RAWHIDE	REDSHAWL
SCRUBBRUSH	SHADYCAT	SLIMDOWN
SMOOTHRIDE	SORRYBRUTE	WHITEOUT
WORMHOLE	Mimikatz	Net

Fig.1: Tools & Malwares Used (cloudsek,2021)

SILENCE

Reconnaissance to Execution: Even Silence used Spearphishing mail, but here initially used hacked server for information and compromised accounts for campaigns, then used emails to create self-signed certificate, then broadcasted emails to 85,000 users in which emails contained decoy Word documents weaponized with exploits for **CVE-2017-11882+CVE-2018-0802-8174** vulnerabilities.

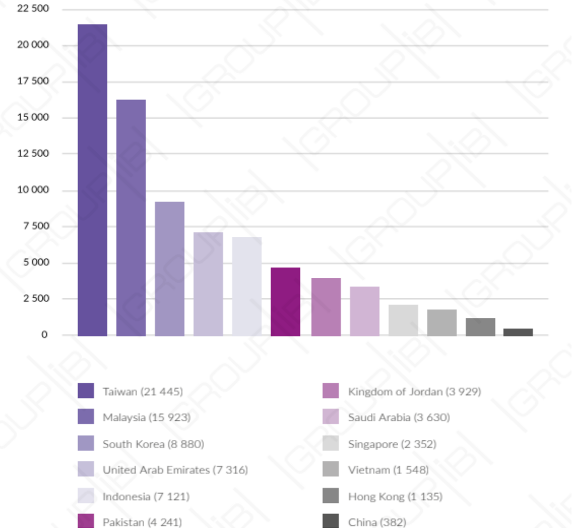


Fig.2: Recon emails spread for attack.

It also obtained & modified tools like Empire and PsExec(Mitre,2021) then leveraged API's like CreateProcess(), ShellExecute() to execute specific tasks (GroupIB,2019). After initial infection a loader called Silence.Downloader is installed and used to download other tools.

Defense Evasion, Credential Access and Discovery: Defense evasion was done by manipulating the name or location of legitimate files or resources when placing them. Credential materials was harvested by conducting Lateral Movement using Use Alternate Authentication Material.(Mitre, 2020). Silence had used the Farse6.1 utility (based on Mimikatz) to **extract credentials** from lsass.exe. (GroupIB, 2019). And finally, **discovery**, Silence has used Nmap to scan the corporate network, build a network topology.

Lateral Movement to Command and Control: The hackers remotely install Atmosphere on ATM's which contains a .DLL library after this get extracted, the dropper injects the library into the fwmain32.exe process which then enables the threat actor to remotely control the dispenser also a was able to control PIN pad. T1070.004 which was exploited for **lateral movement**(GroupIB, 2018), Using the unblocked server message block service like to access compromised computers, the group uses winexe, via SMB protocol(Mitre,2020) also it is standalone LPE exploits: CVE-2008-4250, CVE2017-0143 and 0263.(GroupIB,2019) Actions against systems were performed using valid user credentials which were gained using functions like CopyFromScreen & screencapture also leveraged peripherals or applications to capture video recordings for the purpose of gathering information. (Groupib,2019). Ingress Tool Transfer: was used to transfer tools to compromised environment through the **command-and-control channel**.

Exfiltration and Impact

Main part is impacts of all above steps Data Accumulation, Exploiting ATM. In an incident Silence.ProxyBot was uploaded to VirusTotal from an IP address in Sri Lanka. Later it used the same address for the CnC server. But then money withdrawal took place from ATMs but did **not leave any traces of transactions in the bank's systems. This suggests that a third party may have controlled the ATM dispenser remotely.** (SILENCE 2.2019)

B) Scale Of Operation & Campaigns

APT38

March-29-2022(LATEST): Through our investigation we were able to confirm Lazarus Group and APT38, theft of $620 million in Ethereum. (FBI, 2022)

October-2017: Successful attack which lead to loss of $100,000 in one night. And another DDoS attack using, perl IRC bot and public IRC chats to Trojans. (Mandaint, 2022)

February-2018: $550,000 via ATM of the bank's counterpart. (Mandaint, 2022)

SILENCE

February-2019–Successfully withdrew money from Omsk IT Bank. According to public sources, the amount of stolen funds was 25 million. (GroupdIB,2019)

January-2019 – Silence attacked financial organizations in the UK. The distributed file was signed with a valid signature of SEVA MEDICAL LTD. (GroupdIB,2019)

July-2019 – Banks in Chile, Bulgaria, Costa Rica and Ghana were successfully attacked. The attackers used the server deployed on 6 June 2019 to control compromised workstations in these banks. (GroupdIB,2019)

Section 4: Frameworks and Conclusion

In this part we will be covering the frameworks, shortcomings with mitigation techniques and final concluding words according to attack vector types used by both attack groups.

Phishing: Either bank customer, employee or other responsible stakeholder would become bait to phishing. Cyber risk awareness training is necessary. It's recommended to use VPN this will cover private network. (BSISP 2019) and the data packets from one segment are encapsulated (commonly also encrypted) at the VPN terminator at then sent through a public network to the peer VPN terminator (BSISP,2020).

Remote desktop connection: If a component supports remote sessions, the component shall provide the capability to terminate a remote session, it is recommended to limit the number of concurrent sessions which can help in many different types of attacks. According to (BSISP ,2019), the ports related to RAT/ RDC shall be auto closed one the process/ user sign off. **Firewalls** in place is a great thing, avoided then it may lead to disaster. This hardening guide is to include both architectural and configuration considerations, such as firewall placement and firewall rules and also considerations when installing new components (BSISP ,2019). Staff to maintain the firewall rules and automating them would protect against general threats to the complete system which means controlling external access and for controlling access between Level 2 and Level 3 (through the use of firewalls/firewall rules) (BSISP,2020).

Safeguarding Credentials and Account Access Authorization: Use of 2FA which makes 90% of the attack fail and enforcing a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. Deny access for a specified period of time or until unlocked by an administrator (BSISP,2019)

Hence this report ends here which says some of the mitigation frameworks, shortcomings of infrastructure applications that needs to be followed by the financial industry so that only legitimate users and process run according how it should be.

Section5: References

FRASE, N (2018) *APT38: North Korean Regime-Backed Threat Group* Available From : https://www.mandiant.com/resources/apt38-details-on-new-north-korean-regime-backed-threat-group [Accessed 01 April 2022].

Anon (2018) *SILENCE Moving into The Darkside* Available From: https://www.group-ib.com/resources/threat-research/silence_moving-into-the-darkside.pdf [Accessed 02 April 2022]

Mandiant (2022) *APT:38 Suspect* Available From: https://www.mandiant.com/sites/default/files/2021-09/rpt-apt38-2018-web_v5-1.pdf [Accessed 02 April 2022]

Winther, P(2020) *Phishing: Spearphishing* Available From: https://attack.mitre.org/techniques/T1566/001/ [Accessed 02 April 2022]

Toux, V(2021) *Mimikatz* Available From: https://attack.mitre.org/software/S0002/ [Accessed 02 April 2022]Team, C(2022) *North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All Time High* Available From : https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/ [Accessed 03 April 2022]

GroupIB(n.d) *Going Global :Silence 2.0* Available From: https://www.group-ib.com/resources/threat-research/silence_2.0.going_global.pdf [Accessed 15 April 2022]

AS, M(2021) *Obtain Capabilities* Available From: https://attack.mitre.org/techniques/T1588/002/ [Accessed 15 April 2022]

Anon (2020) *Scheduled* Task Available From: https://attack.mitre.org/techniques/T1053/005/ [Accessed 16 April 2022]

GE(n.d) *Guide to Cyber security for Operational Technology* Available From : https://www.ge.com/fr/sites/www.ge.com.fr/files/an-executive-guide-to-cyber-security-for-operational-technology-whitepaper.pdf [Accessed 16 April 2022]

Security delta(n.d) *Implications of OT and IT* https://securitydelta.nl/media/com_hsd/report/403/document/HSD-Rapport-OT-mei-2021.pdf [Accessed 16 April 2022]

BSI Standards Publication *(ISA 62443*) BS EN IEC 62443-3-2-2020, BS EN IEC 62443-3-2-2020, BS EN IEC 62443-2-4-2019+A1-2019-BS EN IEC 62443-4-2-2019- BS EN IEC 62443-4-2-2019,BS EN IEC 62443-4-1-2018, BS EN IEC 62443-4-1-2018, BS EN IEC 62443-3-3-2019- BS EN IEC 62443-3-3-2019 ,BS EN IEC 62443-2-1-2019- BS EN IEC 62443-2-1-2019. Blackboard [Accessed 19 April 2022]

Cloudsek(2021) *APT38Threat* Availabel From: https://cloudsek.com/threatintelligence/north-korean-threat-group-apt38-threat-intel-advisory/ [Accessed 18 April 2022]

Positive Technologies(2019) *Hack at all cost* Available from: https://www.ptsecurity.com/ww-en/analytics/advanced-persistent-threat-apt-attack-cost-report/ [Accessed 02 April 2022]