COLORTOKENS

THREAT RESEARCH

Defending Against Advanced Persistent Threats

Introduction

As the name "Advanced" suggests, APT (advanced persistent threat) is one of the most sophisticated and organized forms of network attacks that keep cybersecurity professionals up at night. Unlike many hit & run traditional cyberattacks, an APT is carried out over a prolonged period of time by skilled threat actors who strategize multi-staged campaigns against their targets, employing clandestine tools & techniques such as Remote Administration Tools (RAT), Toolkits, Backdoor Trojans, Social Engineering, DNS Tunneling etc. These experienced cybercriminals are mostly backed & well-funded by nation states and corporation-backed organizations to specifically target high value organizations with the following objectives in mind:

- Theft of Intellectual Property & classified data i.e. Cyber Espionage
- Access to critical & sensitive communications
- Access to credentials of critical systems
- Sabotage or exfiltration of databases
- Theft of Personal Identifiable Information (PII)
- Access to critical infrastructure to perform internal reconnaissance

To achieve the above goals, APT Groups use novel techniques to obfuscate their actions and easily bypass traditional security barriers that are not advancing at the same rate as the sophisticated attack patterns of cybercriminals. To understand the evolved behavioral pattern of APT Groups in the year 2020, a review of their latest activities revealed interesting developments and a few groundbreaking events[1]:

- Southeast Asia continues to remain an active region for APT activities in the year 2020 with Chinese Threat Adversaries, including ShadowPad, HoneyMyte, CactusPete and SixLittleMonkeys being the biggest contributors
- Recent activities of various APT Groups such as Rancor and Holy Water indicate that geo-politics remains an important motive behind APT activities
- Financial gains remain a motive behind many APT activities as evidenced by the latest attack pattern followed by APT Group Lazarus and Roaming Mantis
- APT threat actors such as Kimsuky, Hades and DarkHotel, as well as opportunistic criminals, are exploiting the COVID-19 pandemic.

Study of a recent attack by Lazarus Group (APT38)

Although most of the APT Groups follow the same basic attack pattern to fulfill the main goal of an attack, a deep dive into the most recent APT attack by a prominent APT Group would show how the activities and motives have evolved. To understand the same, let's take into consideration the most recent attacks on cryptocurrency firms by the infamous Lazarus Group.

Known for carrying out hacking campaigns all over the world, Lazarus Group has broadened its spectrum by bringing cryptocurrency firms under its ambit and conducting campaigns that are more money-driven than information-driven. This has increased the necessity to become more aware and informed about social engineering attack vectors, especially for organizations that operate within the targeted verticals and financial sectors.

What is Lazarus Group?
North Korean Threat Adversary (Cryptonym APT38)

Target Sectors: South Korea, Japan, Vietnam, Financial Institutions world wide

Attack Vectors: Backdoors, Tunnelers, Dataminers, Social Engineering Tactics

Lifecycle of the attack on a cryptocurrency firm

Researchers and security professionals who keenly observed the attack by Lazarus Group on a cryptocurrency firm found these phases in the attack lifecycle[2]:

1. Reconnaissance & Weaponization Cyber attackers from the Lazarus Group targeted the system administrators of the cryptocurrency firm. They made use of a phishing document that was incorporated within a message they had sent to the administrators' personal LinkedIn accounts.

2. Delivery - This phishing document carried an authentic advertisement for a job role in the blockchain technology company. The victim whose profile and skill sets perfectly matched with the requirements of the job was successfully lured to click on the phishing document.

3. Exploitation – Upon clicking, a tab opened, informing the target that the document is secure via GDPR (General Data Protection Regulation) and hence the access to it is blocked. It further informed them that to gain access to the document, they had to enable macros in MS Word. As soon as the target enabled the macros, the embedded macro code included in the document by the hackers started functioning.

4. Installation - The malicious macro code generated an LNK file that further enabled the execution of mshta.exe. This regenerated or enabled the functioning of a "bit.ly" link created back in May 2019.

5. Control & Command - The "bit.ly" link that was generated redirected the victims to a particular platform that implemented a VBScript to execute detailed follow-ups on them and collected valuable information.

6. Exfiltration – The collected data was subsequently forwarded to a second Command and Control (C&C) domain. This eventually resulted in the download and execution of a PowerShell script that retrieved a malicious payload from a third C&C domain.

The payload, as an attack vector, instigated the auto-installation of several malicious software or implants into the victim's system. These implants further paved the way for the installation of more malicious files, initiated C&C communication, performed random commands, and stole personal credentials and corporate information from their operating systems. The hackers disabled the Windows Defender monitoring protocol in all of the victims' operating systems to evade detection and identification.

APT Detection & Protection Measures

As is evident from the above attack, signature-based detection tools and daily monitoring of logs can no longer suffice to protect against APT, and today's security professionals must perform the following to recognize symptoms of an APT in real time:

- Filtering emails & blocking malicious attachments from getting downloaded would stop an APT in its very first stage and stop APT Groups from penetrating
- Regularly assessing vulnerabilities associated with endpoints and detecting a possible sign of compromise could prevent takeover of endpoints by APT attackers
- Real time monitoring & scanning of the network can detect anomalies associated with user behavior, unusual data bundles and information flows, thereby stopping lateral movements and stalling data exfiltration.

ColorTokens Zero Trust Security Prevents APT

Reconnaissance, Weaponization and Delivery – Xshield detects 'Drive by Compromise' and prevents the downloading of data from social sites

Exploitation – Xprotect prevents the functioning of malicious macro-enabled documents

Installation – Xprotect prevents the downloaded document from creating unusual/malicious files (LNK file) and calling legitimate applications to run scripts

Command & Control – Xshield detects processes connecting to C&C (bit.ly – URL shortener) and Xprotect prevents processes connecting to C&C (bit.ly)

Exfiltration – Xshield detects malicious site or IP address connections (Exploitkit sites) and data infiltration (Payload downloads) from a bad domain or IP. Xprotect prevents malicious payload executions.

Watch this video to learn more about our solutions

Overview of Techniques used by Lazarus vs ColorTokens coverage

Phase	Technique	Sub-Technique	Explanation	ColorTokens
Initial Access	Drive-by Compromise	-	APT38 has conducted watering holes schemes to gain initial access to victims.	Xshield
Execution	Command and Scripting Interpreter	Windows Command Shell	APT38 has used a command-line tunneller, NACHOCHEESE, to give them shell access to a victim's machine.	Xprotect
Defense Evasion	Indicator Removal on Host	Clear Windows Event Logs	APT38 clears Window Event logs and Sysmon logs from the system.	Xprotect
		File Deletion	APT38 has used a utility called CLOSESHAVE that can securely delete a file from the system.	Xprotect
Discovery	Process Discovery	-	APT38 leveraged Sysmon to understand the processes, services in the organization.	Xprotect

Phase	Technique	Sub-Technique	Explanation	ColorTokens
Discovery	System Network Connections Discovery	-	APT38 installed a port monitoring tool, MAPMAKER, to print the active TCP connections on the local system.	Xprotect
Command and Control	Application Layer Protocol	Web Protocols	APT38 used a backdoor, QUICKRIDE, to communicate to the C2 server over HTTP and HTTPS.	Xshield
	Ingress Tool Transfer		APT38 used a backdoor, NESTEGG, that has the capability to download and upload files to and from a victim's machine.	Xprotect
Data Exfiltration	Exfiltration Over Alternative Protocol	-	Exfiltration over Alternative Protocol can be done using various common operating system utilities such as Net/SMB or FTP.	Xshield
	Exfiltration Over C&C Channel	-	Stolen data is encoded into the normal communications channel using the same protocol as command and control (C&C) communications.	Xshield
Impact	System Shutdown/ Reboot	-	APT38 has used a custom MBR wiper named BOOTWRECK, which will initiate a system reboot after wiping the victim's MBR.	Xprotect

References

https://securelist.com/apt-trends-report-q2-2020/97937/
https://securityboulevard.com/2020/08/infamous-lazarus-group-targets-cryptocurrency-firms/