The Lazarus Group – Threat scenario

– Report Sheet

Mr. Jonathan Lim

Cyber Threat Intelligence and Incident Response Report

Incident Name	Lazarus Incident
Report Author	Jonathan Lim
Report Date	22 April 2019
Revision Dates and Notes	23 April 2019

This Threat Intelligence and Incident Response Report was created for the community of the With You With Me - Cyber Security Analyst course.

Executive Summary

This report seeks to outline the challenges posed by the state-associated hacking group (The Lazarus Group) and highlights the need for organisations to take pre-emptive measures to boost organisational cyber resilience in constructing a strong defense, challenge one's cyber defences, keep abreast of new technologies, capitalize upon industry threat intelligence, and in appointing a Chief Information Security Officer.

The Lazarus Group has been known to engage in the use of the following cyber-espionage tactics - disruption, misdirection, protectors, and anti-forensics – in incurring the most amount of damage against a target while obfuscating their responsibility. This incorporates the mixed use of APTs, DDoS attacks, and spearphishing tactics – often targeting select high value individuals and organisations.

In responding to the suspected use of a SMB cryptoworm to infiltrate company systems, it is advised that our organisation requests a specialist incidence response team to deal with the attack – adhering to relevant steps along the Intrusion Kill Chain, and utilising the relevant incident response playbook for virus outbreaks which covers all 7 steps defined by the NIST incident response process.

The Adversary's Actions and Tactics

Indications from cybersecurity analysts working at ASX top 100 firms indicates concerns over irregular network activity and the possibility of a pending attack. This is premised upon the belief that malicious code from the cybercrime Lazurus Group has infiltrated through firewalls of a targeted company, and that pre-emptive actions by the CISO focusing on the firewall alone were insufficient.

This CISO of the target company has since taken immediate action to mitigate the attack. Acknowledging the attack vector and tactics utilised by the group, their motive appears premised upon the accessing and theft of sensitive information or private data from the target company – with such information likely forming the basis for future cyber attacks targeting associated ASX companies, identity theft targeting individuals, and data/market manipulation and economic sabotage.

The insights provided hereafter will employ and refer to steps within the Intrusion Kill Chain (IKC), [1] in outlining where the information provided may disrupt the attacker's capacity to mount a successful attack in progressing through the kill chain.

Description of the Adversary

The Lazarus Group is a notorious cybercrime group believed to be a state-funded actor controlled by Bureau 121 – a division of the Reconnaissance General Bureau intelligence agency under the North Korean government responsible for military cyber campaigns. [2] Lazarus is regarded as one of the most prevalent and active APT groups in the world.

The cybercime group has been identified through the use of various Aliases, including: [3]

- Lazarus Group
- HIDDEN COBRA
- Guardians of Peace
- ZINC
- NICKEL ACADEMY

The indications of our Manager, coupled with the alleged threat posed to a large ASX top 100 firm, evidences the intent of the attackers to acquire financial resources from cyber infiltration activities – aligning closely with the outlined profile and behaviours of the Lazarus Group.

Intrusion Kill Chain

The insights provided here include relevant information as to the "Actions on Objectives" stage – as referenced in the Appendix.

[1] Sucuri, 'Intrusion Kill Chain' on Sucuri (12 June 2016) <https://kb.sucuri.net/firewall/Website+Firewall/kill-chain>.
[2] John Leyden, 'NORK spy agency blamed for Bangladesh cyberheist, Sony Pictures hack' on The Register (30 may 2017) <https://www.theregister.co.uk/2017/05/30/nork_spy_agency_lazarus_group_attribution/>.
[3] MITRE, 'Lazarus Group' on MITRE ATT&CK (2019) <https://attack.mitre.org/groups/G0032/>.

The Adversary's Capabilities

As a state-sponsored actor, the Lazarus Group possess tools which enable it to gain sustained access to an entities IT infrastructure and acquiring data. The preferred Tactics, Techniques, and Procedures (TTP) of the group is the advanced persistent threat (APT) – enabling them to work on multiple attack vectors simultaneously and collecting sensitive data over a sustained period of time. [4] Their common attack tools include: [5]

a) Phishing;
b) Distributed Denial of Service attacks (DDoS); and
c) Software security vulnerability exploits

Tactics

The tactics of the Lazarus group have consisted of the following: [6]

1. Disruption - Involving DDOS attacks and Wipers with time-based triggers. These include
   - KILLMBR with a hard-coded wiping date;
   - QDDOS which has duration date that wipes data ten days after infection; and
   - DESTOVER, a backdoor equipped with wiping capabilities.
2. Misdirection – With their operations attempting disguise as hacktivist activities. This involved:
   - Manufacturing identities through groups such as "GOP," "WhoAmI," and "New Romanic Army" claiming responsibility for alleged hacktivism attacks.
   - Emulating the modus operandi of hacktivists, by defacing web pages and leaking information.
   - Planting of false flags inside their tools as another misdirection technique. One example (i.e. KLIPOD backdoor)
3. Protectors - Use of commercially available protectors for its tools. However, during their actual attacks they deploy both protected and unprotected versions of their tools on the same target:
4. Anti-Forensics – In an effort to obfuscate their identity and activities by:
   a) The separation of components
   b) Command line tools
   c) Disk Wiping
   d) Prefetch, event logs, and MFT record wipers

Tools

In relation to phishing, the Lazarus group's infiltration techniques are characterized by the following infection chain: [7]

1. The use of a ZIP file containing two documents, a benign decoy PDF document and a malicious Word document with macros.
2. The malicious macro downloads a VBS script from a Dropbox URL, followed by the VBS script execution.
3. The VBS script downloads a CAB file from the dropzone sever, extracts the embedded EXE file (backdoor) using Windows' "expand.exe" utility, and finally executes it.

[4] RFSID, 'Proactive Defense: Understanding the 4 Main Threat Actor Types' on Recorded Future (23 August 2016) <https://www.recordedfuture.com/threat-actor-types/>.
[5] Scamwatch, 'Hacking' on Scamwatch (2019) <https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/hacking>.
[6] Trend Micro, 'A Look into the Lazarus Group's Operations' on Trend Micro (24 January 2018) <https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/a-look-into-the-lazarus-groups-operations>.
[7] Check Point Research, 'North Korea Turns Against New Targets?!' on Check Point Research (19 February 2019) <https://research.checkpoint.com/north-korea-turns-against-russian-targets/>.

The Lazarus group has also been known to skip the second stage of the infection chain, with malicious word macros modified to directly download and execute the Lazarus backdoor in stage three. This attack method was noted during the 2014 Sony Pictures Entertainment Hack, the 2016 Bangladesh Bank heist, and numerous cryptocurrency exchange services worldwide. [8] Malware commonly deployed within its attacks include DarkSeoul, Fallchill, Trojan.Fastcash, Bitsran, and assorted backdoors for persistence.

The Lazarus Group has been observed first employing unsophisticated DDoS attacks following its rise to public attention in 2009. This was illustrated through the US Department of Justice's infiltration and mapping of "Joanap" – a claimed botnet of hijacked Microsoft Windows computers operated by botnet masters in North Korea. [9]

The group has also been observed using crypto worms to exploit security vulnerabilities within popular operating systems. This was observed during the 2017 WannaCry ransomware attack, which infected over 200,000 computers across numerous high-profile systems and national critical infrastructure systems in 150 countries. The attack vector lay within the Windows implementation of the Server Message Block (SMB) protocol – a vulnerability noted by the US National Security Agency, whose tools to exploit the vulnerability were stolen and sold onward through the Shadow Brokers. [10]

Location of group

Thorough analysis of prior events proved a strong connection between the Lazarus group and North Korea – with the analysis of command and control (C&C) infrastructure used by the group revealing IP addresses traced to locations in North Korea. [11]

- 210.52.109.22 belongs to an autonomous system China Netcom. However, some sources indicate that the set of IPs 210.52.109.0/24 is assigned to North Korea.

- 175.45.178.222 refers to a North Korean Internet service provider. The Whois service indicates that this address is allocated to the Potonggang District, perhaps coincidentally, where National Defence Commission is located — the highest military body in North Korea.

The location of the hacking group within North Korea allows them to operate unhindered, while making them virtually invulnerable to international legal prosecution.

Intrusion Kill Chain

The insights provided here include relevant information as to the "Delivery," "Exploitation," "Installation," and "Command and Control" stages of the IKC – referenced in the appendix.

[8] Arun Kharpal, 'North Korea government-backed hackers are trying to steal cryptocurrency from South Korean users' on CNBC (18 January 2018) <https://www.cnbc.com/2018/01/17/north-korea-hackers-linked-to-cryptocurrency-cyberattack-on-south-korea.html>.
[9] Lisa Vaas, 'FBI burrowing into North Korea's big bad botnet' on Naked Security (4 February 2019) <https://nakedsecurity.sophos.com/2019/02/04/fbi-burrowing-into-north-koreas-big-bad-botnet/>.
[10] Josh Fruhlinger, 'What is WannaCry ransomware, how does it infect, and who was responsible?' on CSO (30 August 2018) <https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html>.
[11] Catalin Cimpanu, 'How US authorities tracked down the North Korean hacker behind WannaCry' on ZDNet (6 September 2018) <https://www.zdnet.com/article/how-us-authorities-tracked-down-the-north-korean-hacker-behind-wannacry/>.

The Victims and Affected Assets

The group first rose to public attention in 2009, and has been behind several significant international cyberattack operations against various governments and private entities: [12]

1. Troy Operation (2009 to 2012)
    - ❖ Target – Cyber espionage against armed forces and South Korean government ministries with the intent to sabotage.
    - ❖ Method – DDoS attacks, hacking websites, stealing information.
    - ❖ Affected systems – Utilizing Mydoom and Dozer malware to launch DDoS attacks against front-end public network infrastructure and disrupting public access to said online services

2. DarkSeoul operation (Mar 2013) [13]
    - ❖ Target – Three broadcasting stations (KBS, MBC and YTN) and two banks (Shinhan, Nonghyup), with the intent to sabotage and steal.
    - ❖ Method – Infecting with viruses, stealing and wiping information.
    - ❖ Affected systems – Mal/EncPk-ACE malware designed to overwrite initial sections of an infected computer's hard drive, while attempting to disable South Korean anti-virus products (AhnLab and Hauri AV).

3. Attack on Sony Pictures (Nov 2014)
    - ❖ Target – Sony Pictures Entertainment, premised on the release of the Interview movie.
    - ❖ Method – Infection with malware and stealing and wiping data of the company's employees, correspondence, copies of unreleased films.
    - ❖ Affected systems – Hackers used a Server Message Block (SMB) Worm tool to conduct the attacks and erase the company's computer infrastructure – affecting computers with Microsoft Corp's (MSFT.O) Windows software. The tool included a Listening Implant, Lightweight Backdoor, Proxy Tool, Destructive Hard Drive Tool, and Destructive Target Cleaning Tool.

4. Attack on the Central Bank of Bangladesh (2016)
    - ❖ Target – The Central Bank of Bangladesh with the intent to steal $951 million from the Federal Reserve Bank of New York. The attackers managed to steal $81 million.
    - ❖ Method – Targeted attack on banks connected through SWIFT network, aided by insiders within the targeted banks.
    - ❖ Affected systems – Use of phishing techniques to exploit human element of SWIFT system and pose as the Bank of Bangladesh.

Intrusion Kill Chain

The insights provided here include relevant information as to the "Delivery," "Exploitation," "Installation," "Command and Control," and "Actions on Objectives" stages of the IKC – Referenced in the appendix.

[12] Group-IB, 'Lazarus Arisen' on Group-IB (30 May 2017) <https://www.group-ib.com/blog/lazarus>.
[13] Tania Branigan, 'South Korea on alert for cyber-attacks after major network goes down ' on The Guardian (20 March 2013) <https://www.theguardian.com/world/2013/mar/20/south-korea-under-cyber-attack>.

Course of Action During Incident Response

Since APTs make use of multiple attack vectors, there's no single security solution to address a pending security threat from such an actor. What is require is a strong, consistent, and ongoing security program that includes both the fundamentals (e.g. vulnerability and patch management) and more advanced measures (i.e. threat intelligence).

Where prior details concerning the ASX top 100 firm allegedly involved the infiltration of malicious code through a firewall, where the pre-emptive efforts focused upon the firewall were ineffectual – this Incident Response Playbook (IRP) proceeds upon the assumed nature of the pending threat as involving a malware outbreak within internal systems.

Discover

Monitoring of the system logs may be implemented via:

A. SEIMs
B. Log viewer
C. Text editor viewer

SEIMS help translate the bulk of data from logs into identifiable information and can be tied in with machine learning to auto examine event logs, determine the level of the event, and auto-escalate the matter. In overcoming the issue of log processing, the following options may be used:

1) Purchase SIEM that has EPS specification to handle high-loads;
2) Segment the network to allow multiple SIEM servers to handle a given segment and report to a master SIEM; or
3) Configure the logs by priorities to only report important events.

The log viewer displays data from the logs in real-time. Filters can be applied to refine the number of visible events. This process is useful in checking on the latency of ping times to determine a pattern, or if a device is impacting network functionality. The objective in interpreting the logs is to clarify the cybersecurity incident by establishing and considering:

1) The timestamp
2) Event ID
3) The event type
4) The event description
5) The source IP
6) The destination IP

Where the threat actor engages in the research, identification and selection of targets

Intrusion Kill Chain

The insights provided here include relevant information as to the "reconnaissance"" stage of the IKC – referenced in the appendix.

Detect

Defining the threat indicator standards of a SMB cryptoworm attack by:

1) Identifying unknown or unexpected services and applications configured to launch automatically on system boot
2) Recognizing unknown or unexpected internet traffic
3) Highlighting unknown or unexpected network traffic from your organisations offices
4) Noting that anti-virus programs are malfunctioning or becoming disabled for unknown reasons
5) Acknowledging degraded processing capabilities, owing to increased CPU utilisation by unknown applications.

This should encompass measures to restrict activities to core security information, train staff on recognizing commonly used attacks by the Lazarus Group, restricting administrative privileges, and conducting routine scans of incoming files which progress through the firewall.

Intrusion Kill Chain

The insights provided here include relevant information as to the "delivery" stage of the IKC – referenced in the appendix.

Deny

Pre-emptive action through upgrading firewall and antivirus software, and updating all Windows OS devices should be considered as a high-priority.

We may also consider purchasing the following products and services to effect continuous protection against cryptoworms and APTs:

- Stealthwatch can detect connections to SMB shares, correlating this activity to alert administrators.
- AMP's continuous monitoring and patented retrospective security capabilities are ideally suited to keep you safe against attacks such as WannaCry and Nyetya.
- Network Security appliances like NGFW, NGIPS, and Meraki MX can detect malicious activity associated with SMB attacks.
- Threat Grid helps identify malicious file behaviour and automatically informs all Cisco Security products.

Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised. Regularly install latest updates for Windows OS to close vulnerabilities

Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task. When prompted for a root or UAC password, ensure that the program asking for administration-level access is a legitimate application.

Intrusion Kill Chain

The insights provided here include relevant information as to the "delivery" and "exploitation" stages of the IKC – referenced in the appendix.

Disrupt

A firewall should be employed to terminate active network connections - blocking all incoming connections from the internet to services that should not be publicly available. By default, we should deny all incoming connections and only allow services we explicitly want on offer to the outside world.

Analysts should seek to identify, isolate, and eliminate suspicious and affected files to disrupt the growth of the attack across key systems – aided by the distribution of updated antivirus signatures. Where a threat exploits one or more network services, disable, or block access to, those services until a patch is applied.

In disrupting the adversary's attack, we should:

1. Identify the systems which have been affected
2. Identify compromised data across network connected devices
3. Identify the IT services being impacted
4. Identify the attack route and vulnerability being exploited (SMB worm)
5. Identify the scope of the attack
6. Identify tools used to detect the incident

Intrusion Kill Chain

The insights provided here include relevant information as to the "delivery" and "exploitation" stages of the IKC – referenced in the appendix.

Degrade [14]

- Configure network equipment to rate-limit the connections attributed to the adversary.
- Turn off file sharing if not needed. If file sharing is required, use ACLs and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.
- Turn off and remove unnecessary services. By default, many operating systems install auxiliary services that are not critical. These services are avenues of attack. If they are removed, threats have less avenues of attack.
- Isolate compromised computers quickly to prevent threats from spreading further. Perform a forensic analysis and restore the computers using trusted media.

Intrusion Kill Chain

The insights provided here include relevant information as to the "Command and Control" stage of the IKC – referenced in the appendix.

[14] Symantec, 'W32.Brambul' on Symantec (11 May 2015) < https://www.symantec.com/security-center/writeup/2015-051114-3802-99>.

Destroy

We should document the details of the virus, its infection path, and its objectives and share the relevant information to anti-virus companies. Cyber security analysts should seek to determine and block originating IP of the suspicious/affected files, while keeping a continuous stream of records – in line with the Notifiable Data Breaches scheme, and to follow up with the alert the Australian Information Commissioner post-incident.

The IPs traced within the attack should be blacklisted, while affected physical systems should remain isolated until wiped. Where visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched, immediate steps taken to close OS vulnerabilities and keep all operating software updated to the latest version.

Employees are recommended to undergo continuous cyber security awareness training - educating them not to open email attachments unless they are expecting them, and not to execute software that is downloaded from the Internet unless it has been scanned for viruses.

Intrusion Kill Chain

The insights provided here include relevant information as to the “Command and Control” and “Actions on Objectives” stages of the IKC – referenced in the appendix.

Intrusion Campaign Analysis

Other Intrusions in the Campaign

There have been no other publicly reported intrusions to date by Lazarus Group, nor detection of their SMB cryptoworm tools affecting other ASX top 100 entities.

However the anticipated threat may be interpreted as an extension of the 2014 Attack on Sony Pictures involving malware infection and data wiping of leading financial and business companies. Premised upon the ease of the exploit through the use of a Server Message Block Worm tools to affect computers with Microsoft Corp's (MSFT.O) Windows software, there appears to be a high likelihood of further incidents appearing in the near future.

Shared Intrusion Attributes [15]

The following table specifies the relevance of key indicators and behavioural characteristics consistent across intrusions – categorizing the attributes according to the IKC phase when they were exhibited, and their relevance to the adversary description, attack infrastructure, capabilities, and affected victims

	Adversary	**Infrastructure**	**Capabilities**	**Victim**
Reconnaissance Crawling internet websites, mailing lists for email addresses	Medium	Low	Low	Medium
Weaponization Coupling a crypto worm tool with an exploit into a deliverable payload	High	Low	Low	Low
Delivery Transmission of the weapon to the targeted environment	Low	High	Low	Medium
Exploitation Exploitation triggers the intruders' code	Low	High	High	High
Installation Installation of a remote access trojan or backdoor	Low	High	High	High
Command and Control Active access inside the target environment	High	High	High	High
Actions on objectives Achievement of original objectives	High	High	High	Low

[15] Tripwire, 'Intrusion detection and the "kill chain"' on Tripwire (31 July 2012) <https://www.tripwire.com/state-of-security/security-data-protection/intrusion-detection-and-the-kill-chain/>.

Campaign Motivations

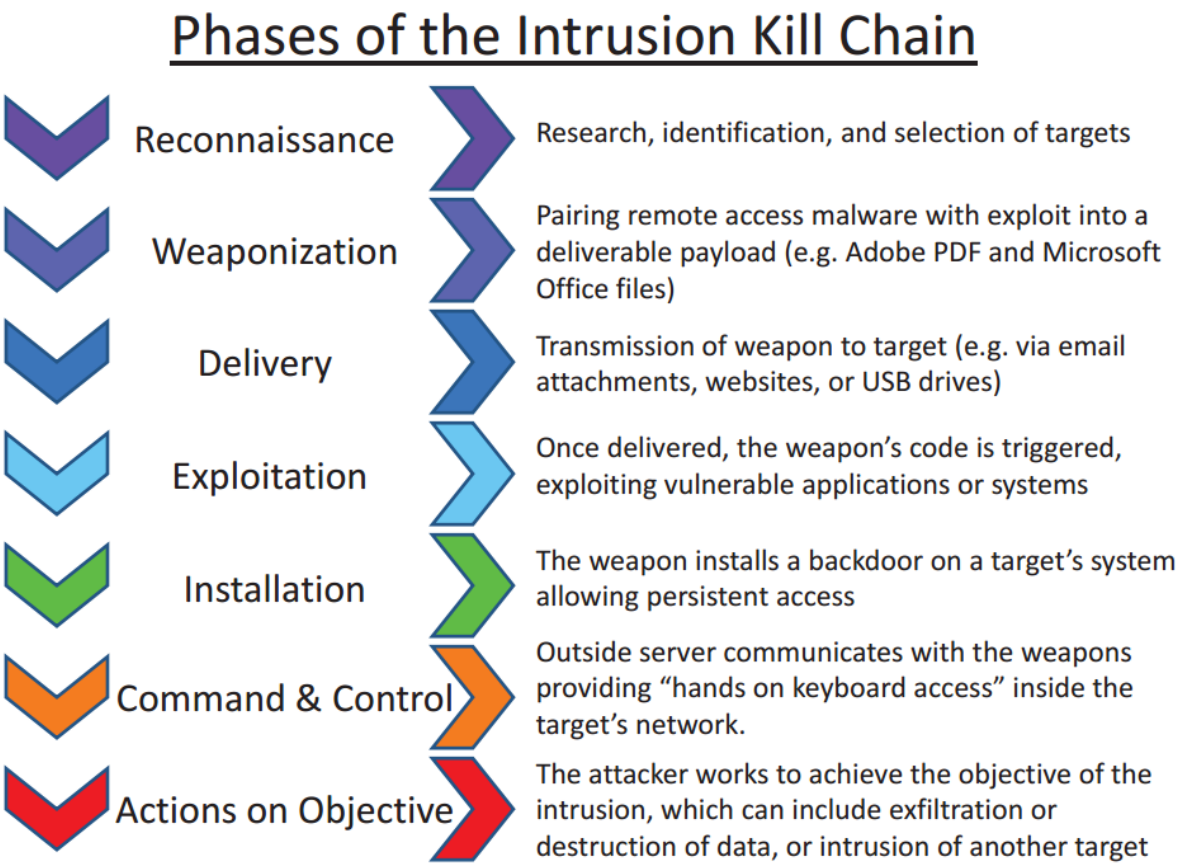
Being a state actor involved in criminal activities, the group can be described as backed or employed by the central government with a political motive and significant resources, while also being motivated by financial gain. [16] Accordingly, the Lazarus Group may be interpreted as seeking:

a) Financial gain in the furtherance of Pyongyang's attempts to circumvent longstanding United Nations sanctions against the regime; or
b) Furtherance of the regime's political goals and national security objectives.

The anticipated cyber threat represents a high-risk to other ASX 100 entities and leading Australian business institutions. The intent of the Lazarus Group may be to obtain intellectual property to further its industrial base, to siphon off funds to benefit the regime, to humiliate Australian companies over their lack cybersecurity frameworks and privacy vulnerabilities, or to gather information for possible blackmail operations.

[16] Daniel Miller, 'The cyber attack on Parliament was done by a 'state actor' — here's how experts figure that out' on ABC News (20 February 2019) <https://www.abc.net.au/news/2019-02-20/cyber-activists-or-state-actor-attack-how-experts-tell/10825466>.

Appendix



Source: US Navy

Third Party References

CISCO, 'Server Message Block Worm Tool Used in Targeted Attacks' on CISCO (1 May 2015) <https://tools.cisco.com/security/center/viewAlert.x?alertId=38606>

Islam, Ali et al., 'SMB Exploited: WannaCry Use of "EternalBlue"' on Fireeye (26 may 2017) <https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html>

Nahorney, Ben, 'SMB and the return of the worm' on CISCO (14 January 2019) <https://blogs.cisco.com/security/smb-and-the-return-of-the-worm>

Symantec, 'What is a computer worm, and how does it work?' on Symantec (2019) <https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html>

Copyright Disclaimer