BCN3233

CYBERCRIME AND FORENSIC COMPUTING

PROJECT FINAL ASSESSMENT TASK 4

SESSION 2020/2021 SEMESTER II

NETWORK FORENSIC INVESTIGATION (LAZARUS GROUP)

SECTION 2

LECTURER'S NAME: DR. SYIFAK IZHAR HISHAM

STUDENT INFORMATION:

Name	Matric ID
NUR ATIQAH BINTI KAMAL	CB20178

Tool to use for the investigation and the reason.

Wireshark Tool

If I were to investigate the Lazarus Group case, I would use Wireshark as a tool to help with my forensic tasks.

Wireshark is a tool that can display data from hundreds of different protocols on all major network types. Data packets can be viewed in real-time or analysed offline. The Wireshark tool can be used for the investigation as it supports dozens of capture/trace file formats. The Wireshark tool can be downloaded online on its website and can run of macOS and Windows.

The Wireshark can capture data packets, view, and analyse packet contents which has three main sections, the packet list pane, the packet details pane, and the packet bytes pane. The packet details present the protocol and protocol field of the selected packet in a collapsible format. The Wireshark also comes with filters to only record packets that meet specified criteria.

Statistic is also featuring inside the Wireshark which include the size, timing information about the capture file and comes with many charts and graphs ranging in topic from the packer conversation breakdowns to load distribution of HTTP request.

LAZARUS GROUP BANGLADESH BANK AND SOUTH-EAST ASIAN INVESTIGATION REPORT

CONDUCTED FOR:

CASE NO. 20211210

Full Name of Investigator:

Nur Atiqah binti Kamal CB20178

Start Date of Investigation:

10/09/2019

Completed on:

17/06/2021

THE CASE

In February 2016, a group of hackers which was unidentified at that time attempted to steal $851 million USD and managed to transfer $81 million USD from the Central Bank of Bangladesh. The theft happened when the Bank was closed for the weekend on 4th to 5th February. The Lazarus Group which is the suspect of the Bangladesh bank incident had managed to compromise Bangladesh Bank's computer network, observe on how the transfers of the money can be done and gain access to the bank's data.

Although several months of silence followed the Bangladesh attack, the Lazarus group was still active. They had been preparing for the operation to steal money from other banks and by the time they were ready, they have already had their foot in a financial institution in South-East Asian.

In August 2016, an incident happened in a South-East Asian country when a new malicious activity from Trojan-Banker. The malware was linked as a tool used by the attackers in Bangladesh. As the attacked organization was a bank, therefore, it is decided to investigate the case in depth. During the months of cooperation with the bank that followed, it was revealed more and more tools hidden deep inside its infrastructure. It is also discovered that the attackers had learned about the upcoming investigation and wiped all the evidence they could, including tools, configuration files and log records. In their rush to disappear they managed to forget some of the tools and components, which remained in the system.

It is claimed that the North Korea-based Lazarus Group was behind the attack. Using that data, the team was able to analyse the methods used by the hackers and linked the Lazarus Group to several attacks through a pattern of code re-usage.

REPORT

Case No.	20211210	**Title**	Lazarus Group Bangladesh Bank and South-East Asian Investigation
Date	10th September 2019	**Incident**	Lazarus network attack
Prepared By	Nur Atiqah Kamal	**Time**	13:05
Incident Detail	In February 2016, a group of hackers which was unidentified at that time attempted to steal $851 million USD and managed to transfer 81 million USD from the Central Bank of Bangladesh. The suspect of the Bangladesh bank incident had managed to compromise Bangladesh Bank's computer network, observe on how the transfers of the money can be done and gain access to the bank's data. This previous incident of Bangladesh bank is being connected to the South-East Asian incident. In August 2016, an incident happened in a South-East Asian country when a new malicious activity from Trojan-Banker. The malware was linked as a tool used by the attackers in Bangladesh. The attacks prompted an alert by payment network SWIFT, after it was found that the attackers had used malware to cover up evidence of fraudulent transfers. The detected malware used by the Lazarus group was Trojan-Banker, Win32.Alreay*. The attackers had already secured their position in the company for seven months. The South-East Asian bank was breached at the time when the Bangladesh heist happened.		
Suspect's	Lazarus Group		
Suspect's Details	Leader of the group (Suspect): Park Jin Hyok Nationality: North Korean Organization: Lazarus Group Criminal Charges: Conspiracy to commit Wire Fraud; Conspiracy to commit Computer Related Fraud		
Items submitted for Investigation	1) Transaction history 2) Security camera 3) Malware code similarity		
Further Investigation	**1) Transaction History** Transaction of $851 million USD were flagged by the banking system. $81 million USD transferred from the Central Bank of Bangladesh to the		

	Philippines by entering the South-East Asian Country banking system. The money was laundered through casinos then transferred to Hong Kong. **2) Evidence from the Transaction History** The money that was stolen had been transferred to the Philippines was deposited into five different separated accounts under the Rizal Commercial Banking Corporation and the account owner are counterfeit. **3) Security Camera** There was security camera which is an evidence for the Bangladesh Bank heist. It was stated that the security camera was turned off when the heist happened. **4) Malware Similarity (Code)** The bank has their own dedicated server to connect to SWIFT just like other banks in the world. The server was running SWIFT Alliance software. Since the Bangladesh bank cyberattack, the SWIFT Alliance software has been updated to include some additional checks which verify software and database integrity. This was an essential and logical measure as attackers had shown attempts to tamper with SWIFT software Alliance on disk and in memory and disabling direct database manipulations. The malware tools found in the incident happened in South-East Asia suggested that the attackers had carefully analysed the patches and implemented a better way to patch new changes. The malware discovered on the server connected to SWIFT strongly linked South-East Asia to the incident in Bangladesh. While certain tools were new and different in the malware code, the similarities left no doubt that the attacker of the incident used the same code base. **5) Evidence from the Malware Similarity** Below are the identical code and encryption key patterns that was found.

```
push    edx             ; lpSystemTime
mov     [ebp+SystemTime.wYear], cx
mov     dword ptr [ebp+SystemTime.wMonth], eax
mov     dword ptr [ebp+SystemTime.wDay], eax
mov     dword ptr [ebp+SystemTime.wMinute], eax
mov     [ebp+SystemTime.wMilliseconds], ax
call    ds:GetLocalTime
push    offset Mode     ; "at+"
push    offset Filename  ; char *
call     fopen
mov     esi, eax
add     esp, 8
test    esi, esi
jz      short loc 10001111
lea     eax, [ebp+var 10004]
push    eax
call    ds:GetCurrentProcessId
movzx   ecx, [ebp+SystemTime.wSecond]
movzx   edx, [ebp+SystemTime.wMinute]
push    eax
movzx   eax, [ebp+SystemTime.wHour]
push    ecx
push    edx
push    eax
push    offset Format   ; "[%02d:%02d:%02d] [%u] %s\r\n"
push    esi             ; FILE *
call     fprintf
push    esi             ; FILE *
call     fclose
add     esp, 20h
```

Figure 1: Evidence discovered in South-East Asia incident to copy SWIFT message files to separate storage. MD5:f5e0f57684e9da7ef96dd459b554fded

```
push    ecx             ; lpSystemTime
mov     dword ptr [esp+1001Ch+SystemTime.wMinute], eax
mov     [esp+1001Ch+SystemTime.wYear], 0
mov     [esp+1001Ch+SystemTime.wMilliseconds], ax
call    ds:GetLocalTime
push    offset Mode     ; "at+"
push    offset Filename ; Filename
call    ds:fopen
mov     esi, eax
add     esp, 8
test    esi, esi
jz      short loc 4010BD
mov     eax, dword ptr [esp+10018h+SystemTime.wSecond]
mov     ecx, dword ptr [esp+10018h+SystemTime.wMinute]
lea     edx, [esp+10018h+DstBuf]
and     eax, 0FFFFh
push    edx
mov     edx, dword ptr [esp+1001Ch+SystemTime.wHour]
and     ecx, 0FFFFh
push    eax
and     edx, 0FFFFh
push    ecx
push    edx
push    offset Format   ; "[%02d:%02d:%02d] %s\r\n"
push    esi             ; File
call    ds:fprintf
push    esi             ; File
call    ds:fclose
add     esp, 1Ch
```

Figure 2: Evidence submitted from Bangladesh. MD5: 1d0e79feb6d7ed23eb1bf7f257ce4fee

The codes above show the disassembly of the logging function implemented in the malware. The code for both incident in South-East Asia and Bangladesh is almost identical.

The Lazarus Group's changes the code even with not much new functionality to break the Yara recognition and other signature-based detections. One of the Lazarus group malware modules discovered was the used of binary configuration file that was encrypted with RC4 and a hardcoded key.

```
hFile = fopen(a1, "rb");
hFile2 = hFile;
v32 = hFile;
if ( hFile )
{
  fseek(hFile, 0, 2);
  dwSize = ftell(hFile2);
  fseek(hFile2, 0, 0);
  lpData = (char *)GlobalAlloc(0x40u, dwSize);
  lpData2 = lpData;
  hMem = lpData;
  if ( lpData )
  {
    fread(lpData, 1u, dwSize, hFile2);
    rc4_decrypt((int)lpData2, dwSize, "C!@I#%VJSIEOTQWPVz034vuA", 24);
    if ( *( DWORD *)lpData2 == 0xAABBCCDD )
    {
```

Figure 3: Fragmented of the code that loads, decrypt and verifies config file magic.

The new variants of Lazarus malware used since Novetta's publication included a different code, with a new magic number and RC4 key but following the same idea. Below are codes that was found.

```
dwSize = 0;
lpFileData = getfiledata(lpFileName, (int)&dwSize);
if ( !lpFileData )
  return -1;
if ( (unsigned int)dwSize >= 33848 )
{
  dwSize = 33848;
  rc4decrypt((int)&rc4key, 16, (int)lpFileData, 33848);
  if ( *lpFileData == 0xA0B0C0D0 )
  {
    qmemcpy((void *)a2, lpFileData, dwSize);
```

Figure 4: Evidence submitted from Bangladesh. Uses magic value 0xA0B0C0D0
MD5:1d0e79feb6d7ed23eb1bf7f257ce4fee

```
nAttempt = 0;
v17 = -1;
dwSize = 0;
while ( 1 )
{
  lpFileData = getfiledata(lpFileName, (DWORD *)&dwSize);
  lpFileData2 = lpFileData;
  v14 = lpFileData;
  if ( lpFileData )
    break;
  Sleep(100u);
  if ( ++nAttempt >= 5 )
    return -1;
}
v6 = dwSize;
if ( (unsigned int)dwSize >= 35260 )
{
  rc4decrypt(&rc4key, 16, lpFileData, dwSize);
  if ( *( DWORD *)lpFileData2 == 0xA0B0C0D0 )
  {
    v17 = 0;
    memcpy(a2, lpFileData2, 0x89BCu);
```

Figure 5: Evidence discovered in South-East Asia incident. Uses magic value 0xA0B0C0D0
MD5:f5e0f57684e9da7ef96dd459b554fded

From the sample of code from the South-East Asia incident, it has certain differences which can break the regular binary pattern detection with Yara, but we can see that the code is clearly the same but improved.

6) Findings after investigation

It is assumed that the attackers knew about the constraints implied by the responsibility of SWIFT and the bank when it comes to investigating the cyberattack. The Lazarus group's clearly used Malware for the financial benefits in stealing data and money from the Bangladesh and South-East Asian bank.

The attack is initial compromise where once a site in visited by the victims which can be the bank employee, then the computer will get the malware, which brings additional components. After that, the Lazarus group migrates to other bank hosts and deploy persistent backdoors.

One connection was made which was coming from a rare IP address range in North Korea. This shows that could mean that the attackers connected from that IP address in North Korea and someone in North Korea accidently visited the command-and-control URL.

7) Timeline of Attacks

In February 2016, between 4th to 5th February, the Lazarus Group attempt to steal $851 million USD from the Bangladesh Bank which happened during the weekend. The suspect of the Bangladesh bank incident had managed to compromise Bangladesh Bank's computer network, observe on how the transfers of the money can be done and gain access to the bank's data.

In August 2016, researchers prevented an attempted cyber-attack by the Lazarus group against a bank in a South-East Asian country. During the investigation, it was revealed that the Lazarus attackers had spent at least 8 months lurking inside the bank before the failed heist. Since the attacker realized that the behaviour of the system administrators was not normal and soon, they started wiping all traces of their activities.

8) Chain of Custody

Table 1: Table of Description of Evidence

Description of Evidence			
No.	**Item #**	**Evidence**	**Description**
1.	LGN6101	Transaction history	Transaction details of the money being transferred to five account under Rizal Commercial Banking Corporation.
2.	LGN6102	Security camera	The security camera details that the security camera was turned off during the heist.
1.	LGN6103	Disassembly of the logging	The evidence of identical code and encryption key

		function of the Malware	patterns used by the attacker of the incident.
2.	LGN6104	Magic value	The Lazarus Group uses similar magic number and RC4 key for both Bangladesh heist and South-East Asia bank attack.
3.	LGN6105	IP Address	Connection was made which was coming from a rare IP address range in North Korea.

Table 2:Table of Chain of Custody

Chain of Custody				
Item #	**Date/Time**	**Released by**	**Received by**	**Comment/Location**
LGN6101	11/09/2019	Nur	Atiqah	Transaction History
LGN6102	11/09/2019	Nur	Atiqah	Security Camera
LGN6103	11/09/2019	Nur	Atiqah	Malware Code
LGN6104	11/09/2019	Nur	Atiqah	Malware Code
LGN6105	11/09/2019	Nur	Atiqah	Connection

Tools used by the attacker

- TCP Tunnel Tool: Aggregates and transfer packets sent between end hosts as a single TCP connection.
- Session Hijacker: A method of taking over a web user session by obtaining the session ID and impersonate as the authorized user.
- WiperTool: A wiper that deletes the file of the infected system.

Tools used for the investigation

Wireshark is a network forensic tool that is used for the investigation. Wireshark is a packet sniffer and analysis tool. It captures the network traffics on local network and stores the data for offline analysis.

Step-by Step to begin capturing the packets with Wireshark:

- First is to run the Wireshark as administrator.
- Next, forensic analyst selects one or more of networks, go to menu bar, the select **Capture**.
- Then, in the Wireshark Capture Interface window, select **Start**.
- After that, select **File** > **Save As** or choose an Export option to record the capture.
- Lastly, to stop capturing, press C**trl+E**. Or go to the Wireshark toolbar and select the red **Stop** button that is located next to the shark fin.

	The Wireshark has capture filters to only record packets that meet specified criteria such as TCP packets. This tool can help the forensic analyst to filters the packets that is being captures in the network traffics.
Findings/ Overall Result	The attack of the Bangladesh bank was a success heist as Lazarus group's managed to transfer 81 million USD from the Central Bank of Bangladesh in 2016. The attacker of the Lazarus Group prompt a malware to delete and hide evidence of their crime. The Bangladesh bank had shut down their server and the malware failed to be executed. The Lazarus Group had initiated a series of transactions into different accounts. In this South-East Asian attack, it is infections on both server connecting to SWIFT and several systems that belong to the IT department of the company. From the analysis of the incident, there are cross-victim event correlations which the attackers worked in multiple compromised banks at the same time. From the forensic analysis: 1. The attackers had a foothold in the company for almost seven months as the South-East Asian bank was breached at the same time as the Bangladesh bank incident happened. 2. The malware was compiled before being deployed. 3. Most modules are designed to run as a service or have administrative rights. 4. Backdoor was found in the attack on the server connecting to SWIFT which linked the incident to the Lazarus. 5. The Lazarus used a keylogger which was stored in an encrypted container and decrypted and loaded by a loader that fetched the encrypted information from a different machine (disguised as one of the files in C:\Windows\Web\Wallpaper\Windows\). The Lazarus group attempted the same malware attack from the Bangladesh bank incident on the South-East Asian bank, but the heist failed as the server were being investigated. The Lazarus group wiped all the evidence they could, including tools, configuration files and log records.
References	1. Kaspersky, (April 05, 2017), *Chasing Lazarus*, Retrieved from https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies 2. Kaspersky, (n,d), *A hunt for the infamous Lazarus group hackers to prevent cybercrime*, Retrieved from https://www.kaspersky.com/cyber-crime-lazarus-swift

	3. SecureList, (February 24, 2016), *Operation Blockbuster revealed*, Retrieved from https://securelist.com/operation-blockbuster-revealed/73914/ 4. Scott Orgera, (July 08, 2020), *How to Use Wireshark: A complete Tutorial*, Retrieved from https://www.lifewire.com/wireshark-tutorial-4143298

Conclusion Case No. 20211210	
Conclusion of the investigation	The Lazarus Group from North Korea are trying to have access to many banks around the world to steal the data and transfer the money from the bank. Similar techniques and codes are being used for the attack which can confirmed that the same group of attackers are involve with the attack.

Status	**Completed**
Date	17th June 2021
Full Name	Nur Atiqah binti Kamal
Signature	*AtiqahKamal*

Reflection

The link below is my reflection video for task 4. The video discussed about how I present the case and defend the analysis in court.

https://youtu.be/eAthEITwAco

The link below is my video task 4. The video discussed about steps on how to present the case and defend the analysis in court with evidence.

https://youtu.be/020Gq_4OtvI