Deciphering the SWIFT-DRIDEX relationship in Bank

Achint Basoya, Harsh, Monika Arora

(achintbasoya1@gmail.com, hdharsh@protonmail.com, monika.a@lucideustech,com)

Abstract

While newer, and advanced ways are being implemented to secure our cyberspace. There are still flaws and vulnerabilities present in systems that are allowing these Black-Hat Hackers to hack into systems and cause millions worth damage. This study gives an overview about what methodology a hacker uses to hack into a system, this paper discusses about Lockheed Martin kill chain with a real-life example which is the steal of millions of dollars of money from central bank of Bangladesh , this paper covers different aspects of the attack , this paper discusses about the flaws and vulnerabilities which the hackers exploited in order to steal such huge amount of money , this paper also briefs about how the SWIFT system works , which played an important role in the hack , the paper also studies the behavior of malware DRIDEX it's working and all other critical information and then we implement the using cyber kill chain for better understanding of the biggest raid in the world.

1. INTRODUCTION

As long as technology exists, so malicious user's intent on exploiting vulnerabilities. Early computers had self-propagating malicious codes. But with the advance in technology we built anti-viruses to identify these malicious codes, antivirus used hash comparison method to identify the malware. But still, hackers manage to hack their way into the systems and due to these hacks, world's economy has gone through a big financial loss, banks are being hacked, doesn't matter how great our security systems are we still can't rely on them completely with the pace of increase in technology new and new vulnerabilities are detected and so the number of exploits. This paper covers one such hacking case of the central bank of Bangladesh where the hackers robbed almost 81 million USD, which was the highest cyber heist ever. This paper talks about the SWIFT software which was used by hackers to get millions of money. SWIFT is a network used for private communication between worldwide based financial companies.

This paper talks about how SWIFT software works and how hackers used Dridex malware. This paper covers the behavioral study of Dridex malware which helped the hackers to raid 81 million dollars. This paper covers the analysis of the attack with the implementation of Lockheed Martin's cyber kill chain. This chain is a methodology that an attacker uses to hack someone, this kill chain involves steps like reconnaissance where the hacker collects the information then weaponization that is making of malware deliver, exploitation, installation, command, and control and then the last step actions on objective, this paper includes information about each step and what tools can be used to accomplish each step for basic knowledge about each tool.

2. SWIFT

SWIFT software is a network that allows the majority of the world’s banks to view information regarding the financial transactions made. Swift is used for worldwide inter financial telecommunication it’s a Belgium company which provides private communication between the banks around the world.

2.1 Working of SWIFT

So basically a SWIFT message contains 5 parts including three head, message content and a trailer. The SWIFT message is of three types and each type is crucial for the SWIFT message these types are.

-> MT103

-> MT202

-> MT950

So basically a banking system initiates a payment request to the US fed, which means a SWIFT message needs to be sent. The first MT103 message is sent to the SWIFT gateway from there it is sent to the US fed and from there it is sent to the banking information system which checks for details such as the amount in the bank, name, etc.

Now a second message MT202 is sent from the SWIFT messaging bridge to the SWIFT gateway and this MT202 is an actual money transfer order, this message is then sent to the US fed now the MT202 is handled and executed further by the banking information system. At the end of business day, the banking information system from fed sends MT950 which contains the information regarding the transactions being made, these are confirmed by the bank and then these transactions are printed as bank manages these transactions manually.

2.2 Visual representation of how SWIFT works (Figure 1)

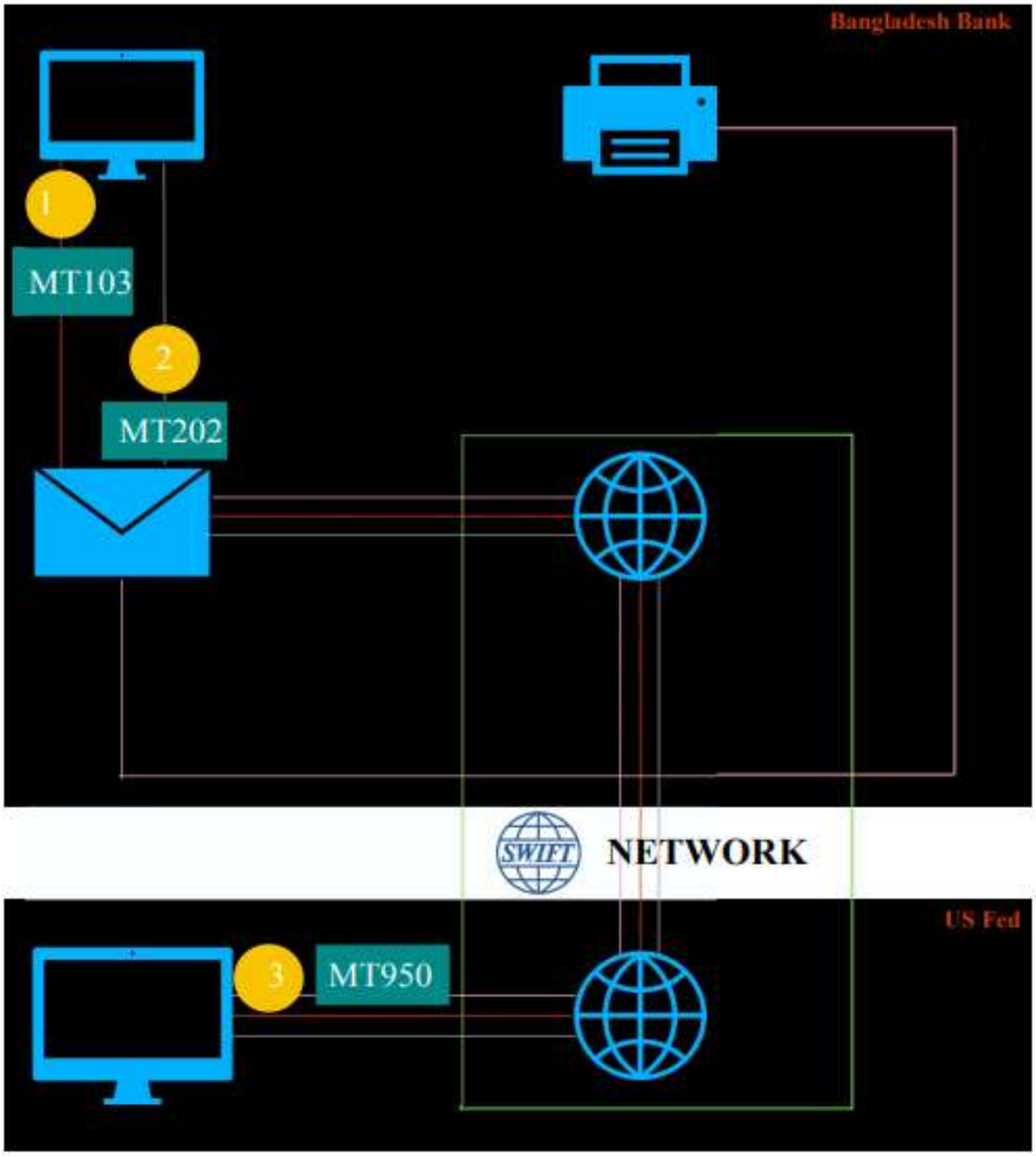


Figure 1: Visual representation of how SWIFT works

2.3 Symbols Meaning (Figure 2)

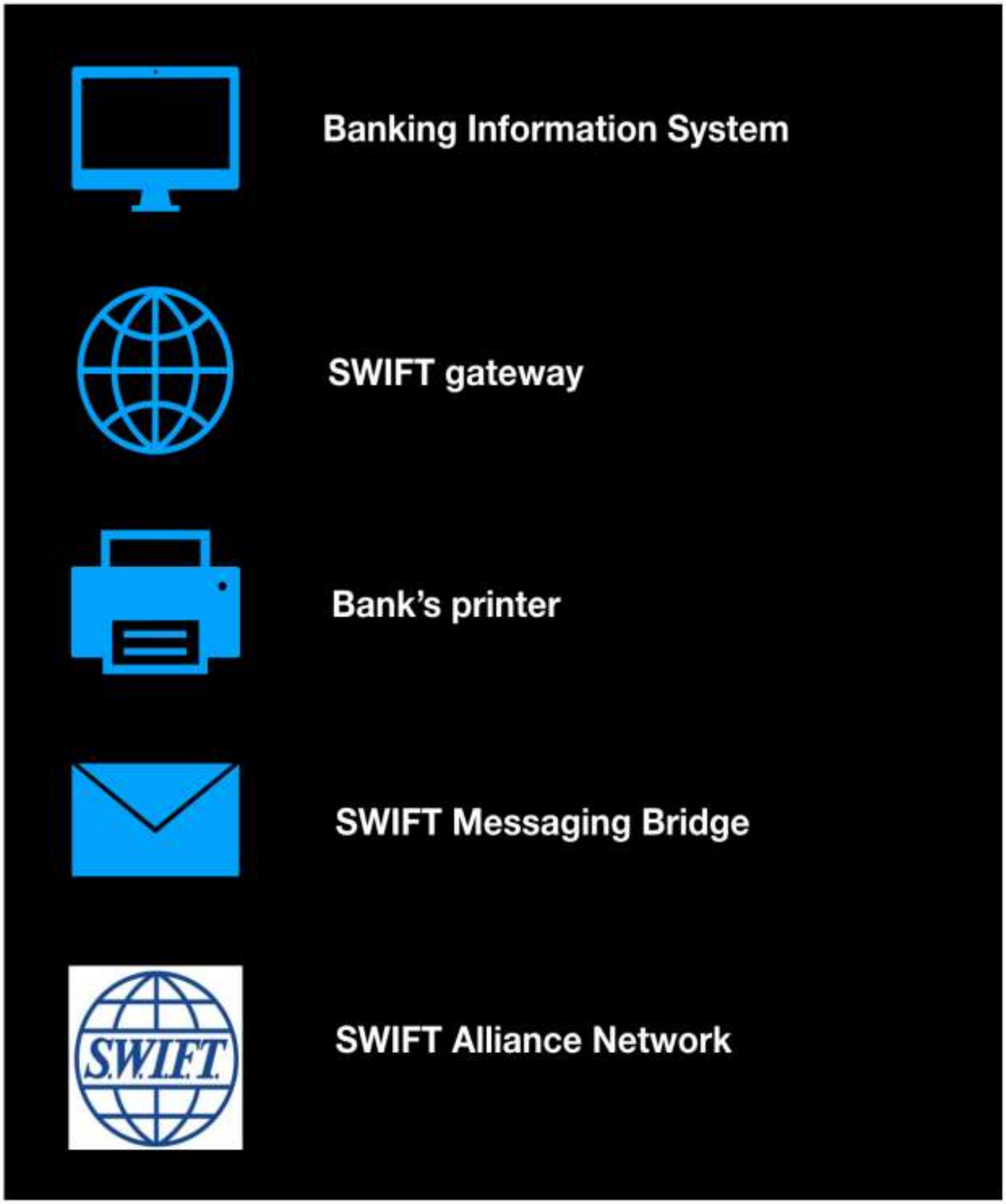


Figure 2: Meaning of symbols used

3. The Bangladesh Bank Heist

The central bank of Bangladesh was hacked in early February 2016, the group who hacked the bank includes high profile professional hackers and IT experts who worked together to hack the bank and heist 81 million US dollars. The bank was informed that 81 million USD was transferred from the Federal Reserve Bank of New-York using SWIFT (an interbank messaging system). The money was moved through the SWIFT transfer request in the bank accounts in the Philippines and SriLanka during the Chinese new year holiday. The hackers managed to hack the SWIFT software and made a total number of 35 transfer requests which sums up to 850 million USD but 30 requests were blocked and the 5 requests which were approved sums up to 81 million USD were transferred.

The hackers looted all this money without being in physical touch with the bank, they used technology to get into the bank's system hack their SWIFT software and the approving their request the best part was that 30 requests were blocked and the bank didn't face a loss of 850 million USD. The hackers didn't hack the SWIFT software completely but they hacked the owner of the SWIFT software so the problem wasn't with the SWIFT software but the problem was with the user (the bank) who was using that software at that particular time. The attack was very well planned.

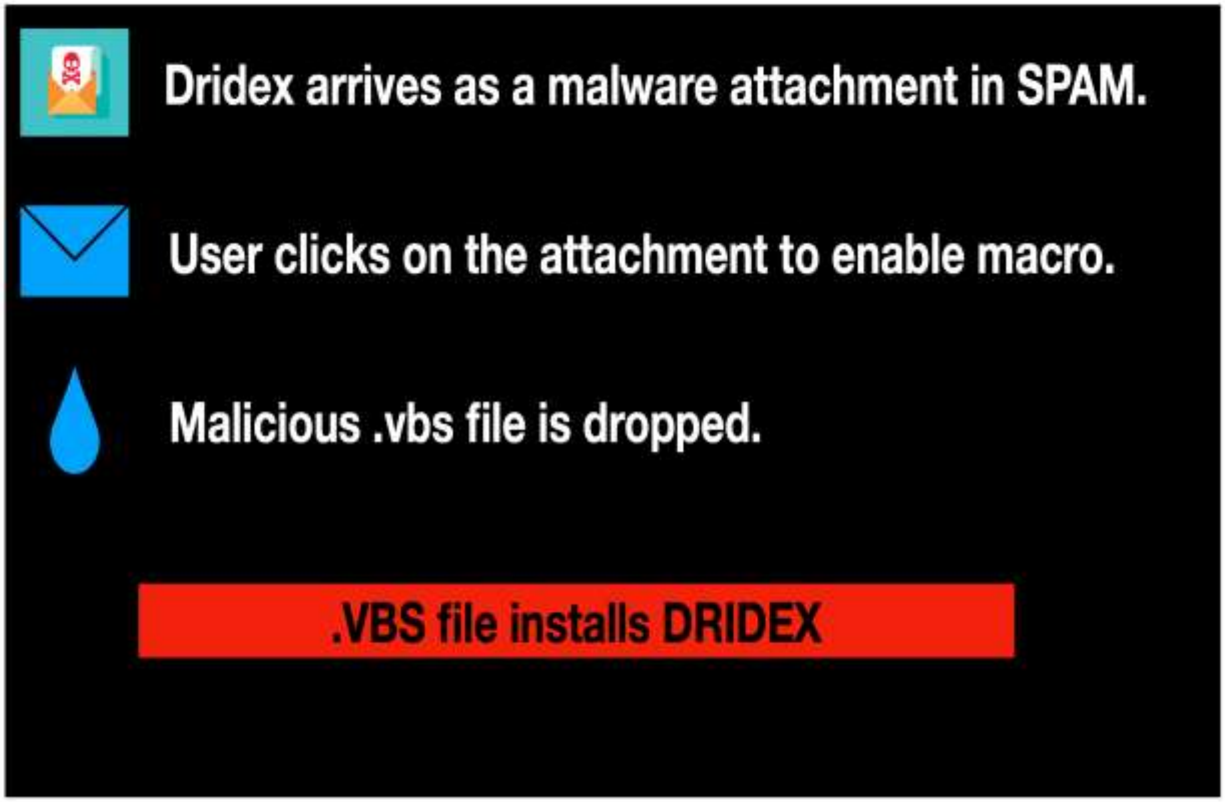
As we can say that the use of Dridex malware to harvest the administrative credentials was a very smart move from technical perspective, the way money was transferred from banks to banks shows that the group had a good knowledge about the financial market and last the SWIFT software not many people have information regarding the SWIFT software, but these hackers had a very in-depth knowledge about the SWIFT software which helped them to harvest millions of money.

4. Dridex Malware

According to the research conducted by CISA, the Dridex malware comes in various forms and is solely used to target financial and business institutions, this malware when gets into the system is capable of impacting sensitive data and information present in the system regarding that institution. The hackers distribute the Dridex malware through emails, the emails contain such a combination of the name of big firms and opportunity that they lured the victim in clicking onto that link and the attached malware was installed onto their systems. Example of links are:

- Link: HTTPS://WWW.GOOGLE[.]COM/URL? Q=HTTPS://WWW.(Cloud Services Provider) [.]COM /S/ (Cloud Account Value) /RECENT%20WIRE%20PAYMENT %######.SCR? (Cloud Provided Sequence).
- Link: HTTPS://WWW.GOOGLE[.]COM/URL? Q=HTTPS://WWW.(Cloud Services Provider) [.]COM/S/ Cloud Account Value/AUTOMATEDCLEARINGHOUSE%20 PAYMENT####.DOC? (Cloud Provided Sequence).

Dridex is an improved variant of Dridex and Bugat Trojan which precedes it. Dridex malware comes with different modules, different modules can be used depending on the action we that we want to execute on our target machine. Dridex works as shown (Figure 3)



Dridex arrives as a malware attachment in SPAM.

User clicks on the attachment to enable macro.

Malicious .vbs file is dropped.

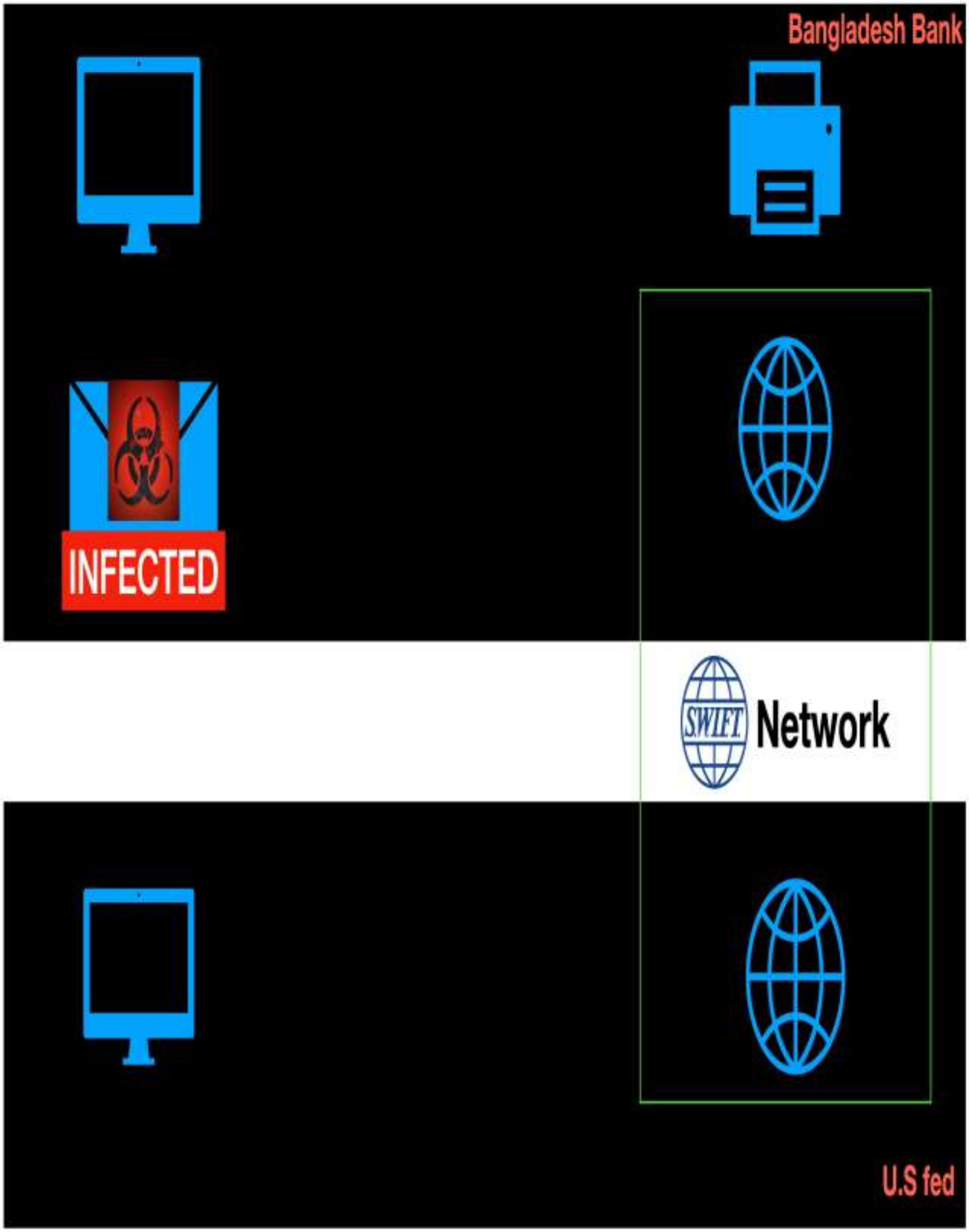
.VBS file installs DRIDEX

Figure 3: Working of DRIDEX

4.1 Dridex in the bank

The hackers used the Dridex malware with a custom module to take over the SWIFT software helping them to grant access to allow the transactions and hide the evidence. The hackers used the module with Dridex which removed the integrity check before any transaction, nowhere hackers were the ones who were doing integrity check. This malware helped the hackers to monitor the transaction through the system, payment order, and conformation for a specific term. These terms and responses were specified to them by the command and control server in Egypt The malware would do different things depending upon the type of message. Confirmation messages from SWIFT were also modified. Confirmations were stored in the database but before they could be printed the malware would alter the conformations and it also deleted the conformations from the alliance database completely. It’s unclear how the malware got into the system but according to an analysis of bank security terms of cybercrime. The bank’s security was very poor, cheap switches were used firewalls present were outdated. So the major weakness was a lack of network security in the company’s infrastructure. (Figure 4)

Figure 4: Dridex in the bank



4.2 Working of DRIDEX in Bank

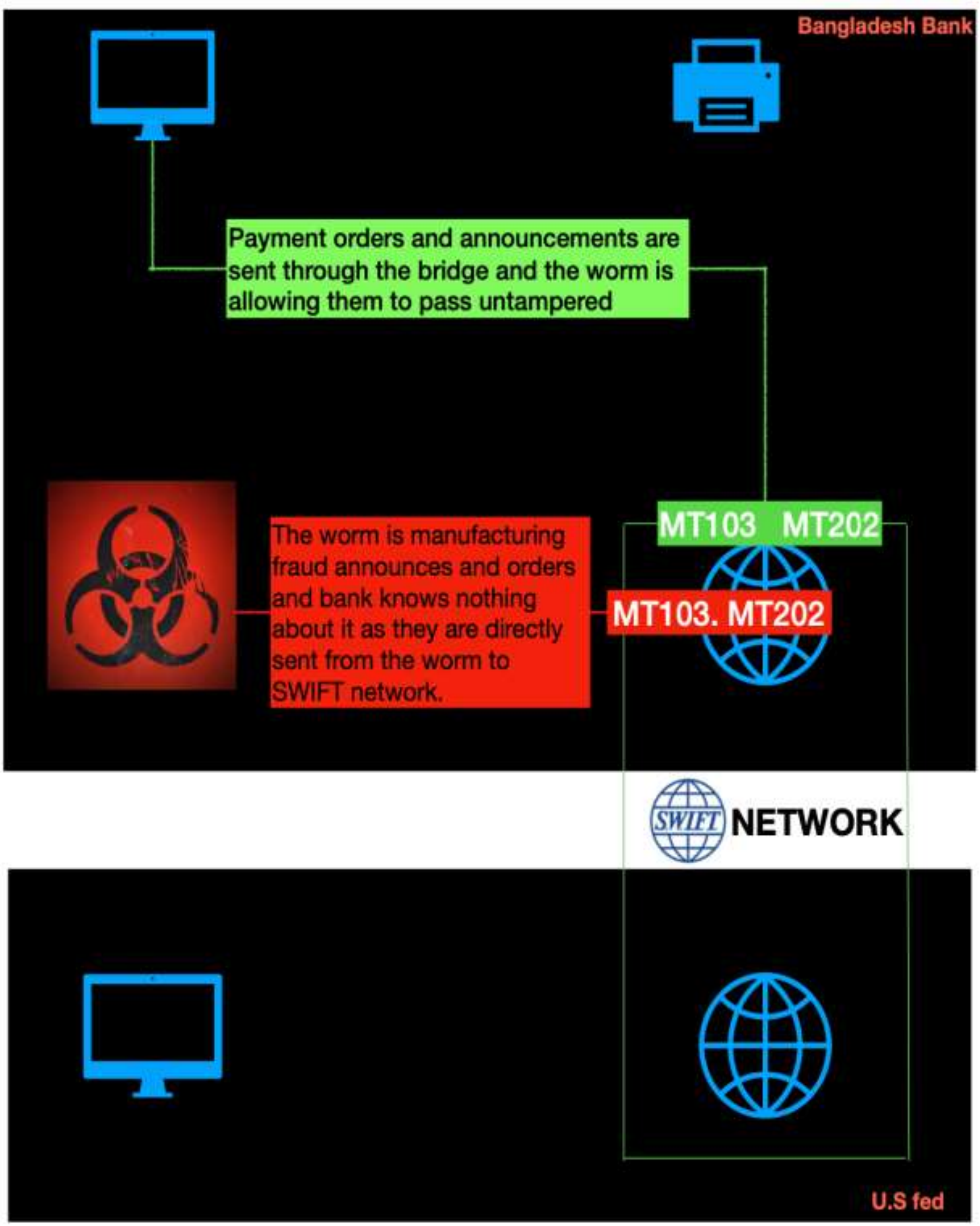

Bangladesh Bank
Payment orders and announcements are sent through the bridge and the worm is allowing them to pass untampered
MT103 MT202
The worm is manufacturing fraud announces and orders and bank knows nothing about it as they are directly sent from the worm to SWIFT network.
MT103. MT202
SWIFT NETWORK
U.S fed

Figure 5: Working of Dridex in the bank

The worm wasn't generating MT103 and MT202 as it was quite difficult for it, the worm was tampering the authentic messages sent directly from the bank to the SWIFT network.

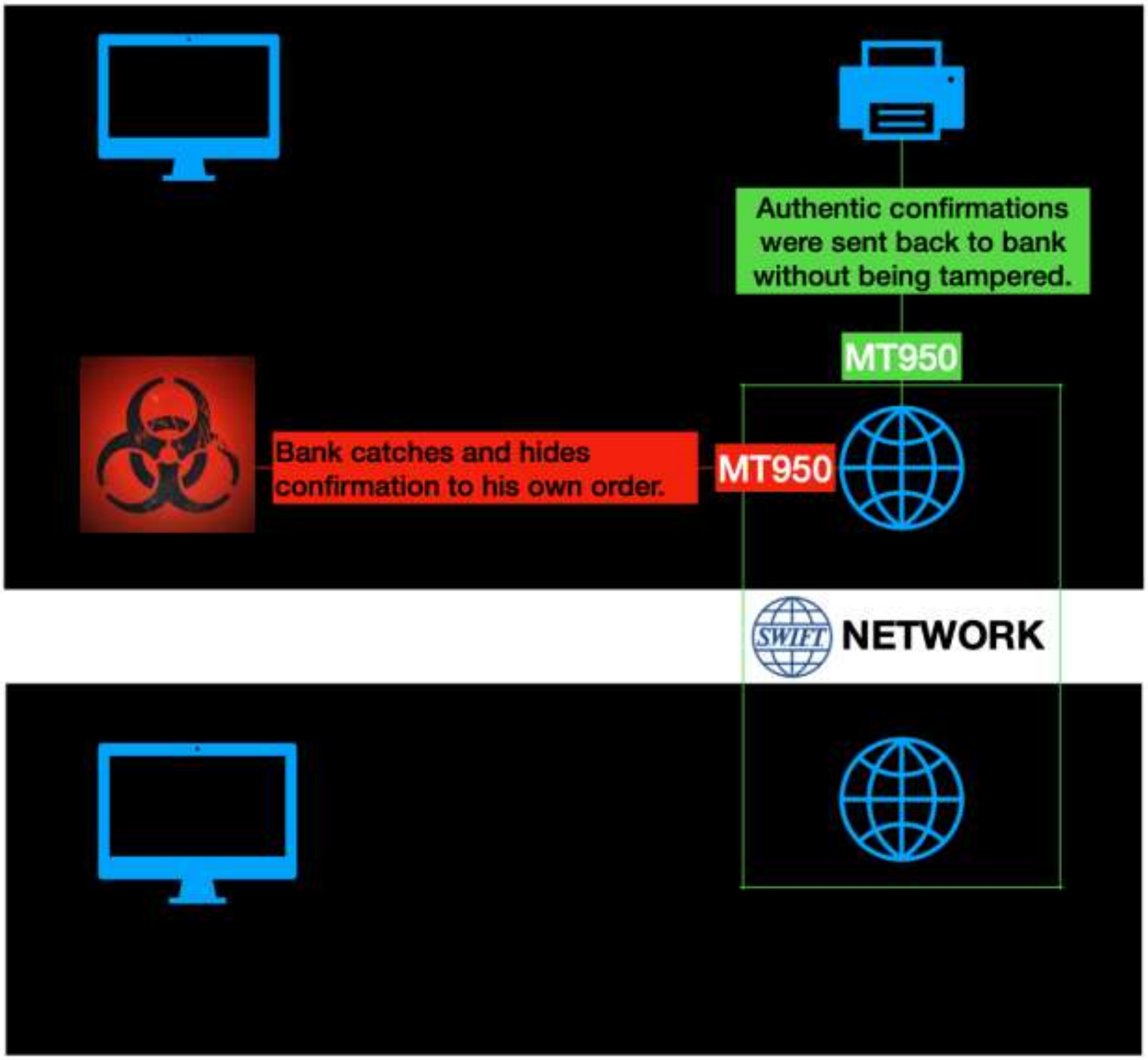

Authentic confirmations were sent back to bank without being tampered.
MT950
Bank catches and hides confirmation to his own order.
MT950
SWIFT
NETWORK

Figure 6: Tampering of messages by worm

The worm was made in such a way that it was intercepting genuine messages from the fed. The conformation of authentic orders was allowed to pass through untampered while the fraudulent messages were hidden. Hence, the bank knew nothing about these fraudulent requests and conformations. (Figure 6)

5. What is Cyber Kill chain?

The cyber kill chain is a series of steps or a framework which was given by Lockheed Martin which lets us understand stages of a Cyberattack. Cyber Kill Chain is based on the kill chain tactic of the US military's F2T2EA (find, fix, track, target, engage and assess). The Cyber Kill Chain (CKC) is one

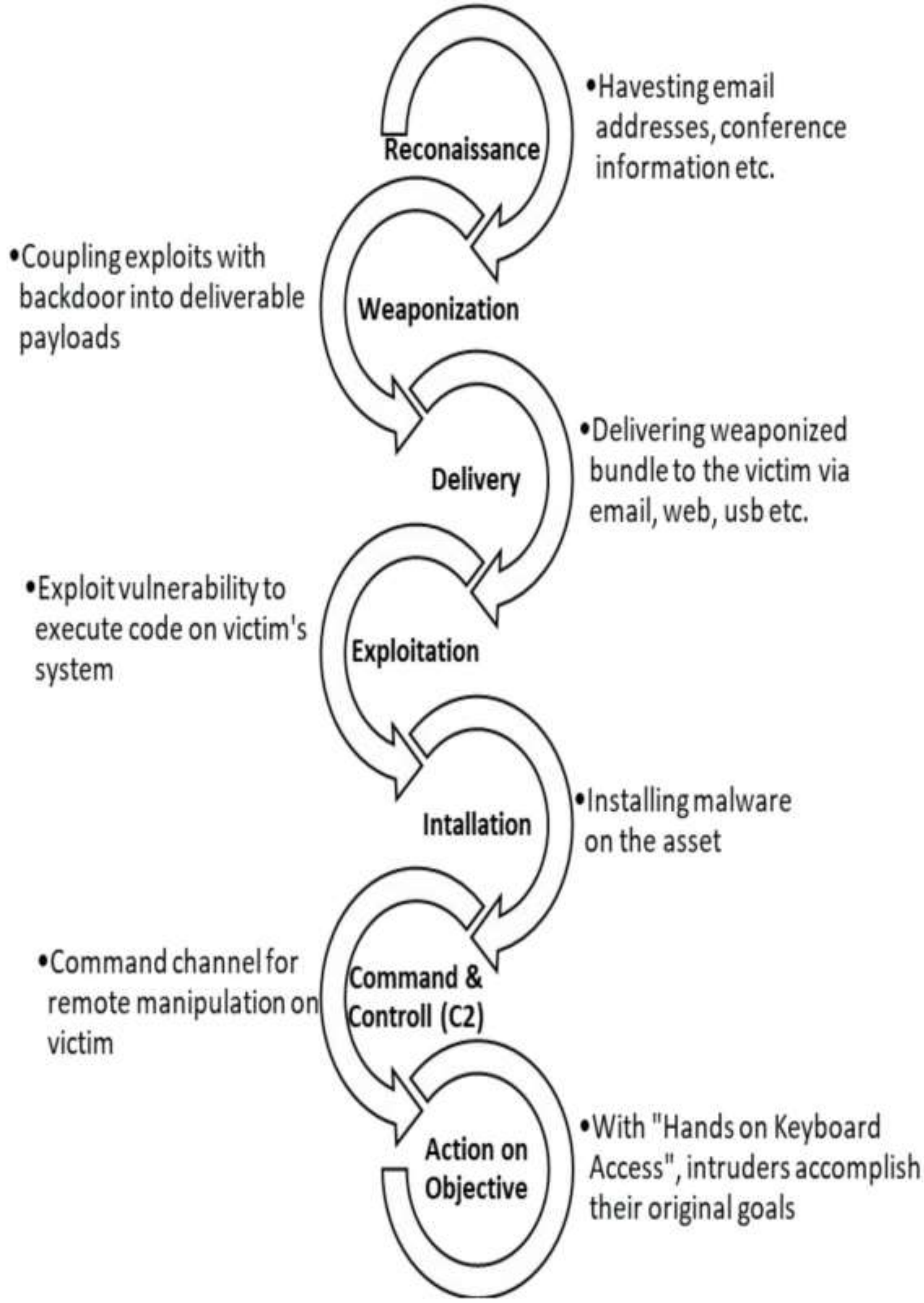

Reconaissance
•Havesting email addresses, conference information etc.
•Coupling exploits with backdoor into deliverable payloads
Weaponization
Delivery
•Delivering weaponized bundle to the victim via email, web, usb etc.
•Exploit vulnerability to execute code on victim's system
Exploitation
Intallation
•Installing malware on the asset
•Command channel for remote manipulation on victim
Command & Controll (C2)
Action on Objective
•With "Hands on Keyboard Access", intruders accomplish their original goals

Figure 7: Cyber Kill chain stages

of the most widely used operational threat intelligence models to explain intrusion campaigns activities. This contains seven stages/steps as shown in Figure 7

Reconnaissance includes the identification, selection, and profiling of potential targets. In **Weaponization,** a custom malware (cyber weapon), say a Trojan with an exploit code with some evasion techniques and Anti-Forensic techniques to reduce the risk of detection and investigation by the victim. In **Delivery**, the cyber weapon is sent to the victim's space. **Exploitation** is the triggering / activating of the malicious payload in the target environment. During **Installation**, the cyber weapon allows making a persistent connection to deliver more payloads to the victim space. In **Command and Control (C2),** commands given by the attacker to trigger special actions. Finally, in **actions on objectives**, planned activities are executed (i.e. exfiltration of data) to achieve the intended goals.

For expanded CKC model

https://www.blackhat.com/docs/us-16/materials/us-16-Malone-Using-An-Expanded-Cyber-Kill-Chain- Model-To-Increase-Attack-Resiliency.pdf

5.1 Reconnaissance

The first phase of CKC is Reconnaissance or information gathering, both are the same terms. It aims at collecting as much information as possible about the target, much of which does not require explicit interaction with the organization's IT infrastructure

Reconnaissance can be divided into two phases:

1. Active reconnaissance

2. Passive reconnaissance

Active reconnaissance

Active reconnaissance includes the use of tools and techniques that can aid you in gathering more information about your target. This involves tasks that may be logged by the target's system. Tools like – Nmap, Recon-ng, Zenmap, Advance IP Scanner, OpenVAS, Nikto, Nessus, Masscan, Amass, etc. are used.

Passive reconnaissance

Passive reconnaissance is collecting host information about the target company without communicating with any of their systems.

Tools and Methods:

WHOIS lookup, GHDB (Google hacking database), Search Engines {Shodan, Censys}, Google Dorks, Social Media, Company Websites, Netcraft, DNS Tools {DNS recon, dnscan, dmitry}, etc. As in Bangladesh bank heist, recon played very well because attackers had all the information about Central Bank of Bangladesh and about its employee details and emails that's why they were able to do spear-phishing attack attached with their custom FUD malware embedded with “zero-day” exploit

5.2 Weaponization

Weaponization is an important step to increase the success of not getting detected and reduce forensics investigator's abilities to analyze detected threats. Various types of techniques to defeat the host level and network level detection and defeat cyber investigators.

Host-based Evasion Host-based cyber defense is mainly based on Anti-Virus and end-point security solutions installed on host machine, that scans for known virus signatures or detect and limit malicious behaviors.

Embedding Malicious Code within application: It uses techniques such as process hollowing that would allow a malicious program to run within a known good process spec and evade antivirus detection even if malware signature exists in Antivirus database.

Heap Spraying: In this technique malicious code are divided into several pieces that are loaded in different locations on the heap memory so there is no single chunk of data mapped to any antivirus signatures. This technique decreases the detection of malicious code and also increase the success rate of attack.

Network-based Evasion: In network protection firewalls and Intrusion Detection/Prevention System (IDS/IPS) are very common but these also have their limitations i.e. a malicious document is attacked to an email can bypass IDS. There are several techniques to avoid or bypass network-based detection.

Use of Common Protocols and Ports: In this technique Trojan uses only very common protocols and ports to proceed its malicious intents. Most Trojans uses protocols like HTTP, DNS and HTTPS of ports such as 443, 80, 53. This technique reduce the chance of port being restricted and connection detection as malicious. By this technique Trojans can communicate with their C2s, download payloads, and upload exfiltrated data.

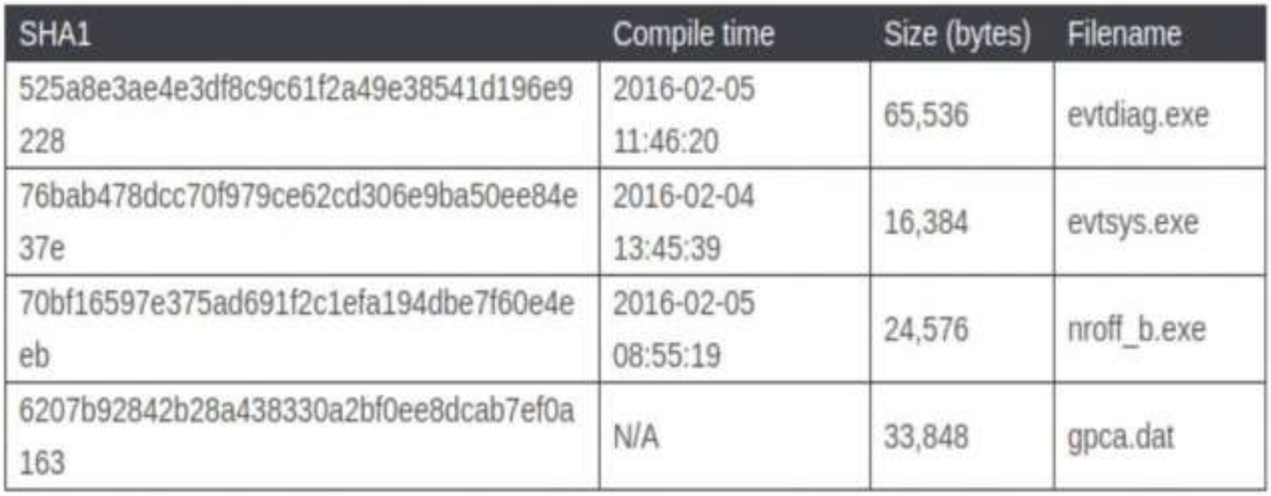
Network Spoofing: By this technique attacker spoof the origin of malicious content as if it is coming from a known good source. Most Trojans obfuscate their origin to well-known company’s domains which are local to victim to avoid being blacklisted.

Anti-Forensic Techniques: Attackers not only evading detection mechanism but also they try to make it difficult for forensic investigators to understand their intentions.

Dead-Code Insertion: In this technique attacker’s inserts hundreds of codes lines which are never executed or serve no purpose which make the malware quite time consuming on the time of investigation.

Utilizing Packers: In this technique malware encrypts its main body and only include a decrypting module which decode encrypted instructions at run time. This makes hard in static code analysis and code reversing. Parkers change malwares signature that's makes Trojan invisible to signature-based detection technique.

As per reports and talks with investigators of Bangladesh bank heist case a custom malware with a "zero-day" exploit and utilizing advance anti-VM/Sandbox technique (most high-end packers) was used with advance features of C2 including key logger and software that monitors strokes on a keyboard, to steal creds of SWIFT and other accounts from Bangladesh bank (Figure 8)



SHA1	Compile time	Size (bytes)	Filename
525a8e3ae4e3df8c9c61f2a49e38541d196e9228	2016-02-05 11:46:20	65,536	evtdiag.exe
76bab478dcc70f979ce62cd306e9ba50ee84e37e	2016-02-04 13:45:39	16,384	evtsys.exe
70bf16597e375ad691f2c1efa194dbe7f60e4eeb	2016-02-05 08:55:19	24,576	nroff_b.exe
6207b92842b28a438330a2bf0ee8dcab7ef0a163	N/A	33,848	gpca.dat

Figure 8: Malware samples that were collected during forensic investigation

Source: https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html
525a8e3ae4e3df8c9c61f2a49e38541d196e9228 is the main component that contains logic for interacting with the SWIFT software

For detail malware analysis see https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html 3.

5.2 Delivery

In this phase or stage attacker uses various techniques to deliver its cyber weapon in victim's network. The most common methods of malicious payload delivery of cyber weapon are email attachments, social engineering and drive by download. As in Bangladesh bank heist way of delivery was spear phishing or by email attachments which bypass the Network based detection in which they attacked their cyber weapon and sent that to employee of central bank of Bangladesh

5.3 Exploitation

After the delivery of the malware, attackers code should be triggered on the target machine by running the malicious application or their cyber weapon. A successful exploitation lead to exfiltration of private information, injection of code into web applications, log keystrokes, steal password, steal cookies or download other module that may perform intended malicious activities.

Web inject: Cyber weapons are equipped with a functionality called web-inject, that can silently modify webpages on victim's machine to intercept private credentials such as usernames, passwords and even 2FA

Form Grabber: In this technique Trojan manipulate and inject arbitrary contents into data transmitted between an HTTPS server and a client browser. The module is placed between the browser rendering engine and the HTTPS API function, so that the Trojan has access to decrypt data even if an encryption is in use (i.e. SSL).

User land Rootkits: In this technique Trojan uses communication API hooking to inject malicious code during initialization of victim's browser and intercepts and manipulates web traffic.

Keystroke Logging: In this technique malicious code records user's keyboard as they are being types either through a software program or a hardware device or even monitoring electromagnetic emissions. Software based keylogging can be implemented in and kernel, hypervisor or in memory

Kernel-based Keystroke Logging: In this technique malware should run as root or system administrator. This is done by kernel-mode rootkits; the rootkits modify the kernel code (example system calls) or kernel data to change the kernel behavior in order to have stealthy capabilities to hide malicious activities.

Hypervisor-based Keystroke Logging: In this type of technique Trojan resides on hypervisor level which is "Ring-1" lower than kernel "Ring-0". As these Trojans are much stealthier giving more control.

API Hooking: In this technique flow of application can be modified through inserting memory break point and JMP (jump) instructions. API functions manipulation on system libraries such as Kernel32.dll, advapi32.dll and ntdll.dll (dynamic link loader) can provide a privileged access to attackers.

5.4 Installation

In this stage attackers try to extend the attack scope or try to access to more systems of victim's network, technique used by DLL side loading and Heap spray

DLL Side-Loading: Windows allows application to load DLL by specifying full path or of the DLLs or using DLL redirection, or utilizing manifest. If none of these locate the DLL, then Windows will perform a search through predefined directories. Attackers abuse this feature by putting their malicious DLLs in higher priority locations than original location of benign DLLs, hence the application would load the malicious DLLs instead.

Heap Spray: This technique increases the chance of successful attack because attacker do not need to know the exact location of their malicious code in heap. The heap spraying attack insert as many malicious code as possible into the heap.

5.5 Command and Control (C2)

When the attacker has to put in place their management and communication APT (advance persistence code) onto to the target network. This C2 allows the attacker to move deeper into the network and make a persistent connection. By this attacker can also download additional software if network access is available.

5.6 Actions on Objectives

After the attack has completed all the other steps in the kill chain what is left is to accomplish its objectives which could be data exfiltration or system disruption. In Bangladesh bank heist attackers tried to steal $951M in which they were able to steal only $81M as described in above pages

Reference

[1] https://www.us-cert.gov/ncas/alerts/aa19-339a

[2] https://www.niceideas.ch/roller2/badtrash/entry/deciphering-the-bangladesh-bank-heis