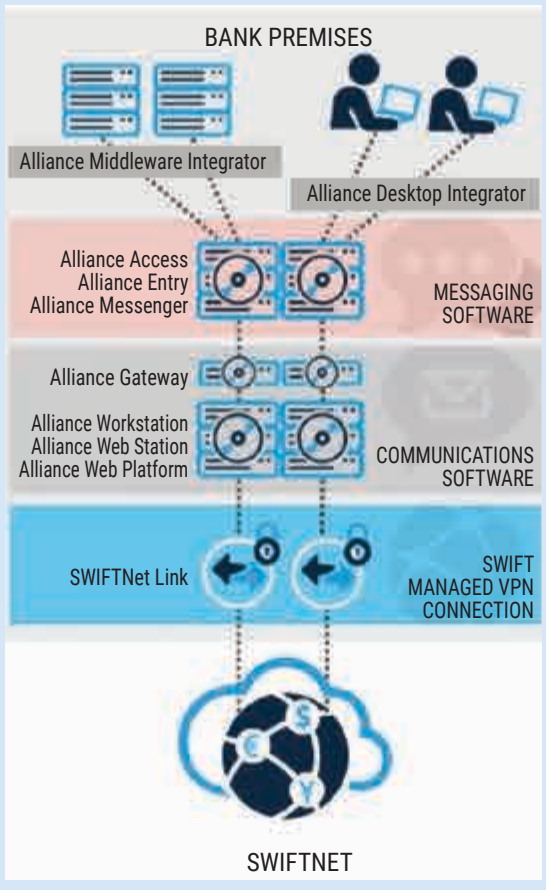
Securing the SWIFT Infrastructure Across the Cyber Kill Chain

Cyberattacks are emerging faster than ever across the world. Banking and financial services have particularly become preferred targets for notorious hacker groups such as Anonymous,[1] Carbanak Group,[2] Metel and GCMAN,[3] who attack the banking and financial services sector on an ongoing basis. After the high-profile Bangladesh Central Bank heist[4] in 2016, SWIFT has become a preferred target for many global hacker groups. Even the famous Shadow Brokers group announced that it offers a monthly information delivery service based on data stolen from SWIFT service providers and central banks across the globe.[5]

Figure 1 depicts the typical SWIFT architecture in a financial organization.

Figure 1—Typical SWIFT Architecture in a Financial Organization



Lack of Understanding of APTs and Cyber Kill Chain of APTs Is the Major Cause

Many may say that poor firewalls and IT infrastructure caused the SWIFT hacking incident that happened at Bangladesh Central Bank. But the fact is, SWIFT attacks can happen in any banking and financial services organization, even those that have state-of-the-art IT infrastructure, security solutions and Security Operations Centers (SOCs) in place. So, what could be the real cause of these targeted attacks on the SWIFT infrastructure?

An analysis of all the latest cyberattacks targeting SWIFT infrastructure revealed the chain of events that happened before the final phase of the attack, in which data exfiltration/illegal SWIFT messaging occurred. These events did not happen in a single day. They were well planned and executed over a period of time. These events were basically driven by well-structured malware called advanced persistent threats (APTs).

In 2011, the US National Institute of Standards and Technology (NIST) defined an APT as follows:

> *An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information; undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.*[6]

APTs can be described as shown in **figure 2**.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

Vimal Mani, CISA, CISM, Six Sigma Black Belt
Is the head of the Cyber Security Program of the Bank of Sharjah. He is responsible for the bank's end-to-end cybersecurity program, coordinating cybersecurity efforts within the banking operations spread across the Middle East. Mani is also responsible for coordinating bankwide cybersecurity strategy and standards, leading periodic security risk assessment efforts, incidents investigation and resolution and coordinating the bank's security awareness and training programs. He is an active member of the ISACA Chennai (India) Chapter. He can be reached at vimal.consultant@gmail.com.

Figure 2—Description of APTs		
Advanced	**Persistent**	**Threats**
• The cyberattack uses highly advanced techniques to compromise a target. • The cyberattack adapts to defensive countermeasures. • Significant resources to support the cyberattack are available, for example, to allow the attacker to broaden the attack vector and targets.	• The goals of the attacker do not align with a typical criminal mind-set (stealing the information immediately), but rather the surveillance of a target and the extraction of critical information over a period of time. • The attacker is looking for specific information rather than generic information. • The attacker shows a willingness to wait for opportunities.	• Organizations are typically unaware of an attack until the damage has been done. • The attacker can cause a potentially huge impact on the victim organization's bottom line by stealing intellectual property or other critical information and/or disrupting production/service. • The unknown goal of an attack and the awareness level of the victim mean no one knows what was stolen and what the potential future impact might be.

The Stuxnet malware[7] that was used in attacks on the oil and gas sector in the Kingdom of Saudi Arabia and the recently identified Slingshot malware[8] are classic examples of APTs that used highly complex attack techniques.

The chain of activities used by APTs is called the Cyber Kill Chain.

Overview of Cyber Kill Chain

Most of the major cyberattacks observed in recent history were not planned and executed in a single day. They were well thought out, planned and executed in a systematic manner over a period of time. There is a series of activities involved in planning and executing these cyberattacks—the Cyber Kill Chain, a concept invented by Lockheed Martin.[9]

The key phases of the Cyber Kill Chain are:

- Reconnaissance
- Development of a cyberweapon
- Delivery of the cyberweapon
- Exploitation and installation
- Establishment of a command-and-control (C&C) center
- Achievement of the objectives

Reconnaissance

This is the phase in which the hackers gather various kinds of information about the target and the target's SWIFT infrastructure. Initial information gathering can be conducted by studying targets through public websites, social engineering with employees on social media and using other publicly available information from various forums. It may also include techniques such as scanning ports connecting the SWIFT infrastructure for vulnerabilities, and services and applications that are vulnerable and can be exploited. This phase can take place over the course of a few weeks, a few months or even more than a year, depending on the size of the target and its information protection measures.

> "THERE IS A SERIES OF ACTIVITIES INVOLVED IN PLANNING AND EXECUTING THESE CYBERATTACKS—THE CYBER KILL CHAIN, A CONCEPT INVENTED BY LOCKHEED MARTIN."

Development of a Cyberweapon

In this phase, hackers analyze the information gathered in the previous phase to plan the weapon to be used in the cyberattack. This weapon is developed based on analysis of the information gathered about the target and its SWIFT infrastructure. For example, a hacker may embed a deliverable payload into a PDF or

a Word document, or send a malicious URL that could redirect users to a malware-laden site. Attackers may target individuals within the organization through a variety of social-engineering attacks such as phishing and vishing.

Delivery of the Cyberweapon

The attack weapon developed is generally delivered to the target through malvertising—phishing emails having a malicious URL or attachment(s). Attack weapons may be secretly kept in a malware-laden website, enabling drive-by download attacks. The delivery of these weapons can also occur through a vulnerable application (particularly web applications), databases through cross-site scripting and Structured Query Language (SQL) injection attacks. These cyberweapons could even be easily planted on a Universal Serial Bus (USB) stick or other removable media. Endpoint devices remain the major targets for delivery of these attack weapons.

Exploitation and Installation

A cyberattack starts with malware entering into the victim organization's information systems. The malware can be hidden from the scanning of security devices through a variety of methods, including tampering with security processes. An existing vulnerability in the SWIFT infrastructure may be exploited to deliver malware into the SWIFT infrastructure through various kinds of cyberattacks, without much difficulty.

Establishment of a Command-and-Control Center

Attackers set up dedicated command-and-control (C&C) servers to exfiltrate the data from the infected SWIFT infrastructure and to exploit the SWIFT infrastructure to send fraudulent SWIFT messages. These C&C servers use encryption techniques to hide their tracks. Once the malware is successfully

installed in the targeted system, the hacker-controlled C&C servers start communicating with the installed malware. This allows hackers to remotely manipulate the compromised SWIFT infrastructure to manage, maintain and evolve the attack.

Achievement of the Objectives

After compromising a system, a hacker's first job is to find unprotected servers containing sensitive, unprotected data that the hacker will start sending to the C&C servers previously established. As an objective, the hacker could even wipe out any unprotected data found. With this, the hacker has successfully accomplished the set of objectives behind the attack.

Figure 3 illustrates a Cyber Kill Chain of activities involved in a cyberattack

Multiple potential areas of security risk need to be addressed in each phase of the Cyber Kill Chain, as related to cyberattacks launched on the SWIFT infrastructure of an organization. **Figure 4** summarizes the various phases of the Cyber Kill Chain, security risk involved and some risk mitigation measures.

Figure 3—Cyber Kill Chain Activities

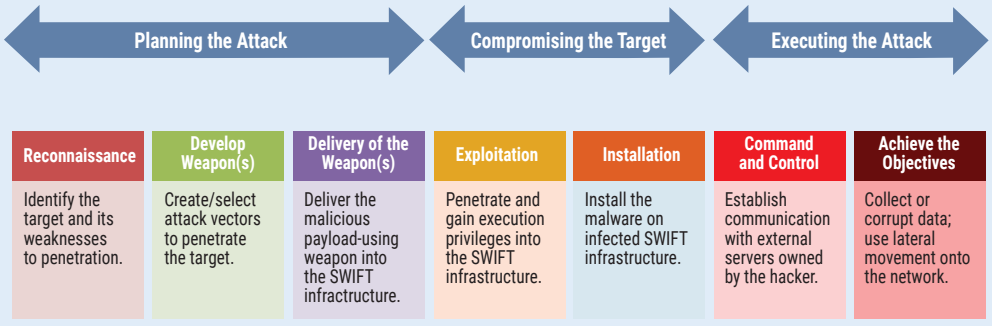


Figure 4—Security Risk and Mitigation Controls for the Cyber Kill Chain Phases

Attack Phase	Risk Scenarios Identified	Mitigation Controls
Reconnaissance This is the phase in which the hackers gather various kinds of information about the target and the target's SWIFT infrastructure. Initial information gathering can be conducted by studying targets through public websites, social engineering with employees on social media and using other publicly available information from various forums. It may also include techniques such as scanning ports connecting the SWIFT infrastructure for vulnerabilities, and services and applications that are vulnerable and can be exploited.	• Social-engineering attacks such as phishing, vishing and hackers visiting in person aimed at stealing critical information about the information systems owned by the targeted organization • Port scanning • OS scanning • Website scanning • Domain Name System (DNS) lookup • Stealing data posted by the staff of the targeted organization on social media sites • Stealing hard copies of documents stored physically	• Apply cyberhygiene to Internet websites (e.g., limiting the number of email addresses displayed on publicly accessible websites). • Close unnecessary services (SWIFT hardening). • Employ Transmission Control Protocol (TCP) wrappers, where applicable. TCP wrappers give the administrator the flexibility to permit or deny access to services based upon Internet Protocol (IP) addresses or domain names. • Anonymize information on IP ranges owned by the targeted organization. • Implement well-defined firewall rules to prevent port scan efforts and block the concerned IPs/domains. • Run information security awareness programs to limit sensitive information posted on social media by the staff of the targeted organization. • Obfuscate banner information of externally reachable servers and services so that attackers receive no or false information when probing. • Implement robust physical and environmental security controls. • Use vulnerability scanning and take subsequent actions to close the gaps found in scans. • Implement robust password management and access control policies. • Implement exclusive controls such as multifactor authentication solutions. • Implement network segmentation. • Implement encryption. • Implement honeypots. • Limit user and administrator privileges. • Implement segregation of duties. • Block the use of USB drives on user systems (physical, logical or both). • Implement a data loss prevention (DLP) solution.

Enjoying this article?

- Read Threat Pattern Life Cycle Development. *www.isaca.org/Threat-Pattern-Life-Cycle-Development*
- Learn more about, discuss and collaborate on cybersecurity in the Knowledge Center. *www.isaca.org/cybersecurity-topic*

Figure 4—Security Risk and Mitigation Controls for the Cyber Kill Chain Phases *(cont.)*		
Attack Phase	**Risk Scenarios Identified**	**Mitigation Controls**
Development of a Cyberweapon In this phase, hackers analyze the information gathered in the previous phase to plan the weapon to be used in the cyberattack. This weapon is developed based on analysis of the information gathered about the target and its SWIFT infrastructure. For example, a hacker may embed a deliverable payload into a PDF or a Word document, or send a malicious URL coupled with a backdoor or remote access tool. Attackers may target specific operating systems, firewalls and applications. They may also target individuals within the organization through phishing and drive-by download attacks on the endpoints possessed by the individuals.	NA	NA
Delivery of the Cyberweapon The attack weapon developed is generally delivered to the target through a phishing email with a URL or attachment, or it could be posted on a vulnerable website for enabling a watering hole attack, could be posted as malvertising, could be planted on a USB stick or other removable media, or as a reply to social media posts in LinkedIn, Facebook, Twitter, etc. The delivery of these weapons can also occur through a vulnerable application (particularly web applications), databases through cross-site scripting and SQL injection attacks. Endpoint devices remain the major targets for delivery of these attack weapons.	There are a variety of cyberattacks aimed at delivering malware into the SWIFT infrastructure.	• Filter and scan emails using email gateways. • Filter using firewalls/proxies/ routers. • Disable macros. • Implement an intrusion detection system (IDS)/intrusion prevention system (IPS). • Implement network monitoring mechanisms. • Implement an endpoint suite. • Implement a file integrity monitoring mechanism. • Implement access control lists (ACLs). • Implement demilitarized zones (DMZs) in the network. • Implement mobile security solutions. • Use application whitelisting. • Implement a bring your own device (BYOD) policy. • Proactively block user access to identified malicious URLs, IPs, domains. • Implement sandbox-driven APT solutions. • Collect threat Intelligence and take appropriate preventive actions.

Figure 4—Security Risk and Mitigation Controls for the Cyber Kill Chain Phases *(cont.)*		
Attack Phase	**Risk Scenarios Identified**	**Mitigation Controls**
Delivery of the Cyberweapon (cont.)		• Run general information security awareness training. • Perform log monitoring (SWIFT and security information and event management [SIEM] integration). • Limit user privileges. • Implement robust backups.
Exploitation and Installation A cyberattack starts with a malware infection with an exploitation that can be hidden from security devices through a variety of methods, including tampering with security processes. An existing vulnerability in the infrastructure may be exploited to deliver a payload onto the systems, such as by clicking on a link or opening a malicious attachment. Then, a malicious payload such as a Trojan, malware or spyware can be installed into the network infrastructure of the targeted organization.	• Malware infection of the SWIFT infrastructure of the targeted organization through a well-defined attack vector • Hacker's successful access of the infected SWIFT infrastructure of the targeted organization	• Implement removal of local administrator privileges given to users into the SWIFT infrastructure. • Implement proactive patch management. • Implement proactive vulnerability management. • Implement system hardening for the SWIFT infrastructure. • Implement next-generation malware protection appliances (APT solution). • Implement endpoint suite, antibot, next-generation antivirus or malware suites. • Implement incident response. • Conduct breach assessments. • Implement network forensics tools.

Figure 4—Security Risk and Mitigation Controls for the Cyber Kill Chain Phases *(cont.)*		
Attack Phase	**Risk Scenarios Identified**	**Mitigation Controls**
Establishment of a C&C Center To communicate, attackers set up C&C servers to operate between the infected SWIFT infrastructure and themselves. These servers use encryption to hide their tracks. An external C&C server controlled by the hacker will start communicating with the installed malware to allow remote manipulation of the compromised SWIFT infrastructure to manage, maintain and evolve the attack.	• Full compromise of the SWIFT infrastructure by the hackers • Hacker's elevation of his rights, accesses into the SWIFT infrastructure • Lateral movements of the hackers inside the targeted organization's network from SWIFT to other critical information systems of the targeted organization	• Implement internal network monitoring having anomaly detection capabilities. • Implement network segmentation. • Implement network access control (preferably based on certificates) on all systems. • Implement an endpoint security suite. • Implement end-to-end encryption between all systems to prevent network sniffing (based on feasibility). • Implement firewall ACLs. • Implement DNS redirect. • Implement DNS sinkholes.
Achievement of the Objectives After penetrating and compromising a system, the hacker will find unprotected servers in which to park sensitive data and, from there, send the data out of the organization to another compromised server operating as a "bot" (remotely controlled computer). The hacker then achieves the ultimate objectives behind the hacking, such as exfiltration of data, destruction of data or further intrusion into the network to infect further systems.	• SWIFT data exfiltration by the hackers • Permanent deletion of SWIFT data elements by the hackers • Outage of SWIFT and other critical information systems of the targeted organization	• Scan outbound network traffic to detect data exfiltration happening from the SWIFT infrastructure. • Implement identity and access management tools with approval flows for the SWIFT infrastructure. • Implement encryption for data at rest. • Block the use of USB drives in the entire SWIFT infrastructure (physical, logical or both). • Implement a DLP solution for the SWIFT infrastructure. • Implement egress filtering. • Implement data vaults for storing critical data related to SWIFT operations. • Implement firewall ACLs. • Implement IPS. • Improve document security controls in place.

To effectively address the gamut of security risk factors involving the SWIFT infrastructure, the global SWIFT Corp. has issued a robust set of controls called the SWIFT Customer Security Controls Framework,[10] which the corporation has mandated for use by the global banking and financial services community through regional central banks that are the regulators for specific regions.

Conclusion

Recent cyberattacks have shaken faith in the traditional security measures implemented at global organizations in and around the SWIFT infrastructure in place. So, it is an unavoidable obligation for chief information security officers (CISOs) and chief information officers (CIOs) to take a much deeper look into the Cyber Kill Chain of attacks targeted on SWIFT in their respective organizations and implement multilayered security controls in a defense-in-depth approach. This will help prevent cyberattacks in subsequent phases of the Cyber Kill Chain even if the previous phase has been successfully executed by the hacker. It is very important to mention that the business should provide all the support required to IT and information security teams in implementing and maintaining an effective security posture around the SWIFT infrastructure in the organization. It should never be seen as the responsibilities of only the IT and security teams. It is clear that securing the SWIFT infrastructure of an organization is the responsibility of the business, enabled by the IT and information security functions.

Endnotes

1 PYMNTS, "Anonymous Is Increasing Hacks of Central Banks," PYMNTS.com, 20 March 2017, *https://www.pymnts.com/news/security-and-risk/2017/anonymous-is-increasing-hacks-of-central-banks/*

2 Osborne, C.; "Carbanak Hackers Pivot Plan of Attack to Target Banks, the Enterprise," *ZDNet*, 10 October 2017, *www.zdnet.com/article/carbanak-threat-group-change-plan-of-attack/*

3 Kaspersky Lab, "Financial Cyberthreats in 2017," *SecureList*, 28 February 2018, *https://securelist.com/financial-cyberthreats-in-2017/84107*

4 Paul, R.; "Bangladesh to Sue Manila Bank Over $81-Million Heist," *Reuters*, 7 February 2018, *https://www.reuters.com/article/us-cyber-heist-bangladesh/bangladesh-to-sue-manila-bank-over-81-million-heist-idUSKBN1FR1QV*

5 Seals, T.; "Shadow Brokers Offer Monthly Service of SWIFT Info, Exploits and Nuke Data," *InfoSecurity Magazine*, 31 May 2017, *https://www.infosecurity-magazine.com/news/shadow-brokers-offer-monthly*

6 Ross, R.; R. Graubart; D. Bodeau; R. McQuaid; *Systems Security Engineering*, SP 800-160 volume 2, National Institute of Standards and Technology, USA, March 2018, *https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf*

7 Fruhlinger, J.; "What Is Stuxnet, Who Created It and How Does It Work?" *CSO*, 22 August 2017, *https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html*

8 Kaspersky Lab Daily, "Slingshot APT: Riding on a Hardware Trojan Horse," 9 March 2018, *https://www.kaspersky.com/blog/web-sas-2018-apt-announcement-2/21514/*

9 Lockheed Martin, "The Cyber Kill Chain," *https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html*

10 SWIFT, SWIFT Customer Security Controls Framework, *https://www.swift.com/myswift/customer-security-programme-csp/security-controls*