This product was created as part of a joint effort between the Financial Services – Information Sharing and Analysis Center (FS-ISAC), the American Bankers Association (ABA), BITS Division of the Financial Services Roundtable (FSR) and NACHA — The Electronic Payments Association.

Security of Payment Network Access Points

Risk Mitigation Recommendations Related to Recent Payment Account Takeover Attacks Against Banks Leveraging the SWIFT Network

July 1, 2016

Ensuring the safety and soundness of the global payment infrastructure is a key priority for all participants in the global financial system. The ability to efficiently move funds safely and securely enables the global economy to function at the most basic level. Any disruption or threat to this capability represents a “top-line” threat that requires a broad industry response.

There have been a number of recent cyber incidents involving the Society for Worldwide Interbank Financial Telecommunication (SWIFT) payment messaging network and, according to media reports, incidents involving the Bangladesh Central Bank and banks in the Philippines and Vietnam. Based on current intelligence, perpetrators of these incidents did not attack or breach the SWIFT payment messaging network.

- The attacks targeted specific financial firms by stealing legitimate credentials of bank employees.
- The associated thefts are the result of sub-optimal infrastructure management (e.g., lack of firewalls, inexpensive routers, default passwords not being changed).
- Phishing attacks at the affected banks are reported to have played a key role in the events.

Given the reported information, the attacks appear to follows traditional Account Take Over (ATO) tactics with malicious insiders and/or external attackers managing to submit SWIFT messages from financial institutions’ back-offices, PCs or workstations connected to through the affected banks’ local interface to the SWIFT network. In one instance, the target amount was US$1 billion. Based on publicly available information, the estimated losses from several attacks exceed US$81 million thus far this year.

Insight and Analysis

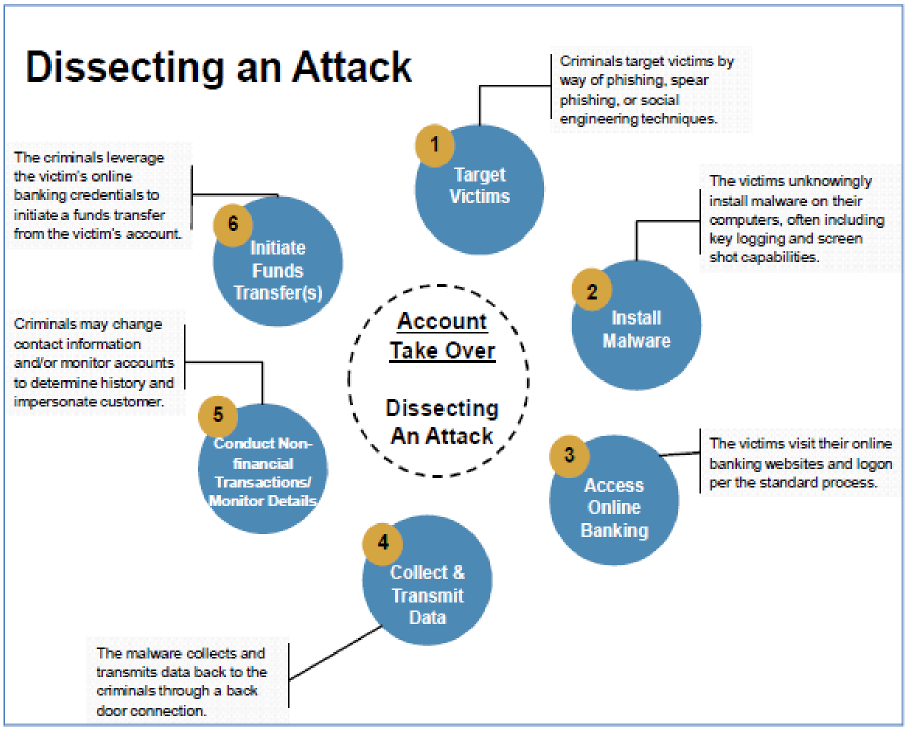
Many cyber events with significant impact start off as an ATO event. As noted, ATO is not a direct attack against core payment systems or networks but is an exploit against inadequate security practices and human weaknesses.

- ATO victims typically do not follow basic security practices to include patching, network segmentation and least-privileged access.
- Cyber criminals will always seek the weakest link in any system, even those with redundancies and safeguards, and will exploit human errors and use social engineering as they perpetrate their crimes. Financial firms are strongly advised to take proactive measures to defend against these types of attacks including taking steps to reduce the online footprint of information about employee access to core payment systems (e.g., role descriptions on LinkedIn).

It is important to note that while these attacks were targeted and sophisticated, they reportedly combined known attack tactics, including phishing attacks, to steal legitimate credentials. This gave attackers access and enabled them to initiate fraudulent transfers and commit the alleged thefts. Many financial institutions around the world have already implemented security practices and controls that defend against these types of attack tactics. Those that have not should implement security controls based on best practices immediately.

While recent events targeted national financial institutions with access to a global payment network, financial institutions should assess the risk of all critical systems to ensure appropriate controls are in place.

The following figure from *Recommended Practices for Financial Institutions to Prevent, Detect and Respond to Corporate Account Take Over Fraud* (FS-ISAC September 2012) shows the six steps attackers use to execute ATO attacks.



Dissecting an Attack

Criminals target victims by way of phishing, spear phishing, or social engineering techniques.

The victims unknowingly install malware on their computers, often including key logging and screen shot capabilities.

The victims visit their online banking websites and logon per the standard process.

The malware collects and transmits data back to the criminals through a back door connection.

Criminals may change contact information and/or monitor accounts to determine history and impersonate customer.

The criminals leverage the victim's online banking credentials to initiate a funds transfer from the victim's account.

Risk Mitigation Recommendations

1. Update financial institution cyber risk assessments.
2. Maintain strong situational awareness of cyber threats via information sharing.
3. Adopt and maintain best practices associated with good cyber hygiene to protect against the types of threats associated with the recent attacks on (and thefts from) financial institutions utilizing SWIFT. Best practices dictate locking down one's IT environment using layered defenses, redundant controls and evaluating the efficacy of primary and secondary controls in case one control is defeated.
4. Focus on specific tactics associated with securing access to payment networks and systems including the following:
    a. Deploy and maintain strong:
        i. Access Controls
            1. Ensure employees with access to core payment systems, particularly those with elevated access, are closely monitored for the potential of direct phishing attacks and are on watch lists for logins from new or unexpected end-points. Limit information on social media about employees with payment processing roles to reduce their exposure to targeted attacks. Consider targeted anti-phishing exercises to employees with payment processing roles;
            2. Use dedicated workstations where web browsing, email access and USB ports are disabled. (Whenever practical, the workstation should not be connected to the rest of the network);
            3. Review access lists, processes, and policies associated with access to payment networks to make sure that only authorized individuals or entities have access and that credentials are properly utilized, updated, and secured. Follow the principle of least privilege as appropriate; and
            4. Ensure all default passwords for equipment related to core payment systems are replaced with a strong password policy. Consider using the most secure form of authentication provided in the products that connect to the payment networks, especially multi-factor authentication and/or one-time passwords, if available.

        ii. Operating Procedures
            1. Ensure that cancelled transactions are removed from the system;
            2. Consider processes for additional appropriate verification of activity (e.g., transfers and withdrawals) via SWIFT and other payment messaging systems;
            3. Leverage internal fraud resources to monitor for suspect payments; and
            4. Review internal control process and procedures around payment initiation and reconcile Line of Defense 1 (LOD1) and Line of Defense 2 (LOD2) review of procedures.

        iii. Hygiene and Maintenance
            1. Validate network security posture of critical payment processing and money movement systems, limit or separate exposure to external networks, and ensure the timely patching of security vulnerabilities, especially for systems that initiate payments;

   2. As appropriate, apply the system update recommended by SWIFT and provided to SWIFT users; and
   3. Identify new control processes that networks, operators and participants may implement to align with internal control processes such as transaction size, destination, time, volume and other indicators of anomalous behavior.

5. Coordinate with financial regulators on any supervisory review of payment system controls.

Technical Indications

- SWIFT Technical bulletin (https://www2.swift.com/go/tip/5020872)
- FFIEC Link (http://www.ffiec.gov/press/PDF/Cybersecurity_of_IMWPN.pdf)