Menlo Security

SECURING SWIFT DEPLOYMENTS WITH ISOLATION

Menlo Security Isolation Platform

WHITEPAPER

SECURING SWIFT DEPLOYMENTS WITH ISOLATION

Introduction

In the past few years, cybercriminals have stolen millions of dollars by using stolen credentials to access SWIFT, the secure messaging system used in more than 200 countries by tens of thousands of banks, financial services companies (FSIs), and their corporate clients. Originally set up by 15 large financial institutions in 1973, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) provides the most commonly used messaging platform for completing cross-border payment messaging and transactions in a secure manner compliant with local and national regulations. Using a variety of techniques, cybercriminals have been able to issue bogus payment requests that appeared to be valid SWIFT communications, or to simply use stolen SWIFT credentials to abscond with stolen funds. In this paper, we look at how Menlo Security's Isolation Platform provides an effective defense against this class of attack.

SWIFT Security Incidents

While the SWIFT platform does not hold funds, manage accounts, or provide clearance or settlement, it is the means by which many banks and FSIs communicate the details of payments made with each other. This makes SWIFT a prime target for cyberattacks.

1.2015

In January 2015, Wells Fargo transferred $12 million to accounts with Banco de Austro in Ecuador[1], per instructions received over SWIFT that turned out to be bogus. The messages were either legitimate SWIFT instructions, using secure SWIFT credentials stolen from a Banco de Austro employee, or were a nearly identical likeness of actual SWIFT transfer requests.

2.2016

In February 2016, attackers used SWIFT to send a series of payment instructions to the Bangladesh Bank, the central bank of Bangladesh[2], requesting the transfer of $951 million to various accounts around the world. Five of the transactions were executed, causing the withdrawal of $101 million from a Bangladesh Bank account at the Federal Reserve Bank of New York.

10.2017

In October 2017, attackers planted credentials-stealing software in computers at the Far Eastern International Bank in Taiwan[3], possibly via a phishing or spear-phishing attack. Using the stolen user credentials, the attackers stole $60 million by using the bank's SWIFT terminals to request the transfer of funds.

[1]https://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD [2]www.nytimes.com/2016/05/01/business/dealbook/hackers-81-million-sneak-attack-on-world-banking.html
[3]https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/

Methods of Attack

Phishing and its more targeted cousin, spear-phishing, are two of the most prevalent attack vectors. By getting an employee, a contractor, a vendor, or other authorized user to click on a bogus link in an email that downloads malware, or completes a fake web form, attackers can steal their credentials. Once on the corporate network, attackers can easily harvest the credentials of other users until they find one with the authority to access SWIFT, at which point they can surreptitiously abscond with electronic funds. Attackers have also obtained credentials through watering-hole attacks, where they spread malware via legitimate websites commonly used by an organization's employees, or through drive-by downloads, in which employees unknowingly agree to download software off the web that conceals the malware.

Despite deploying myriad legacy security solutions, banks and financial organizations continue to be victimized by these and other types of attacks. Too many of these solutions rely on "good" versus "bad" determinations by third-party data feeds or by analysis of the company's past traffic. While this approach can help stop known threats, it cannot protect against new attacks that have not yet been identified. These services will never also be able to flag unique links, such as a spear-phishing attack based on a web link designed to entice a particular individual. In addition, legacy systems struggle with attacks that have been deliberately built to avoid detection by traditional security measures. For example, many companies use secure web gateways that assign websites to categories. These gateways allow access to supposedly "safe" categories such as Government or Finance and Technology, and restrict access to "bad" ones such as Gambling or Porn. Trouble is, attackers have a multitude of ways to embed malware into safe sites—say, by dropping a line of malicious code in an ad that appears on the page, or by hijacking the entire web page domain.

Clearly, it's time for a new, holistic approach to keep SWIFT secure that doesn't require being able to detect every attack. That new approach is isolation.

Isolation and Securing SWIFT

Isolation, also known as browser isolation or remote browsing, is a technology that makes it impossible for web-based attacks to infect an organization's computers. All of an employee's web-based activity is executed in a secure, trusted environment in a private or public cloud. What the employee sees onscreen are safe renderings of the content they seek. Since none of the web pages are opened on the device, the employee cannot inadvertently unleash malware on that device or any other devices it is connected to through the corporate network.

This strategy is akin to putting an invisible, protective force field around your employees as they access the Internet—making them invulnerable to attackers without degrading the web experience they have come to expect. Users can continue to access links on web pages, play videos, print documents, and cut and paste content, just as they do when executing commands within the browser on their PC or smart device.

Isolation also provides future-proofing. Companies that have isolation platforms in place do not have to worry about whatever as-yet-uncreated cyberattack will sweep the web, or about even the most cleverly weaponized spear-phishing attack. That's because with isolation, all traffic is presumed to be potentially dangerous. Better safe than sorry.

Isolation Checks Many of the Boxes in the SWIFT Framework

As a result of the increasing number of attacks leveraging its platform, SWIFT introduced new security best practices to strengthen their bank, FSI, and corporate clients' network defenses. This SWIFT Security Controls Framework has three main objectives, with eight supporting principles and 27 specific controls. SWIFT mandates that clients implement 16 of these 27 security controls. The other 11 are considered "advisory." An isolation platform addresses several of the principles. Here's how:

SOURCE: Society for Worldwide Interbank Financial Telecommunication (SWIFT)

OBJECTIVE 01

Secure Your Environment

RESTRICT INTERNET ACCESS

An isolation platform allows security teams to set and enforce policies regarding which sites employees can access, whether for particular URLs, categories of websites, file types, or any other criteria.

PROTECT CRITICAL SYSTEMS FROM GENERAL IT ENVIRONMENT

An isolation platform logically separates critical systems—such as a bank's or a FSI's SWIFT network—from the wilds of the Internet. It can also segregate critical systems from the rest of a bank's or a FSI's business network.

REDUCE ATTACK SURFACE AND VULNERABILITIES

Web links: Since web links are executed in the isolation platform, those containing malicious code are neutralized. Even if an employee clicks on a phony but genuine-looking site, no malware will be downloaded to their computer or other device.

Web Documents: Attackers often distribute malware by embedding it in innocent-looking documents, offered for download off the web. With an isolation platform, documents are downloaded to the cloud, allowing users to view the document safely or to download a safe PDF version of the document, and policies can be set to prevent the user from downloading the original document to their own machine.

Email Attachments: As with web documents, users can view attachments safely via their web browser. Policies allowing users to view the document safely, or to download a safe PDF version of the document, can be set to give some users the ability to download a safe PDF version of the attachment, or let others download the original attachment—but not before it has been scanned and sandboxed. By checking original email attachments for embedded malware before allowing users to access the content, an isolation platform ensures that users receive only clean, threat-free attachments.

Category-based Attacks: By treating all content as potentially malicious, isolation platforms defuse attacks designed to hide malicious code within websites in supposedly "safe" categories of URLs.

OBJECTIVE 02

Know and Limit Access

PREVENT COMPROMISE OF CREDENTIALS

If the isolation platform includes a "read-only mode," the organization's security team can set a policy preventing specific users from entering their credentials or other sensitive information into a web page. General website content may also be put into read-only mode.

OBJECTIVE 03

Detect and Respond

PLAN FOR INCIDENT RESPONSE AND INFORMATION SHARING

An isolation platform should be able to provide logging and threat information to enable a better understanding of incoming web-based threats to banks and FSIs, as well as the ability to share collected threat data with internal and external partners, including security information and event management (SIEM) products.

Not All Isolation Platforms Are Created Equal

Isolation platforms are not new. Over the years, various attempts have been made to inoculate companies against web-based attacks by executing all web content on remote computers. Technologies such as Virtual Desktop Infrastructure (VDI) invariably resulted in a slow, glitchy browsing experience. The reason is that the content executed on this separate computing infrastructure was rendered pixel for pixel on the employees' screen—sans any of the so-called "active content" that allows native browsers to treat videos as videos rather than as a series of snapshots. Generations of users have complained that VDI and similar isolation platforms resulted in slowed web page loading, reduced responsiveness, and sorely missed capabilities of all modern browsers, such as the ability to print and copy and paste content.

The Menlo Security Isolation Platform uses a different approach to isolation, called Document Object Model (DOM) mirroring, which maintains the complete user experience that people have come to expect. DOM mirroring maintains an understanding of the type of content that is being rendered, actively monitors the currently loaded web page tab for any changes, such as a video, and isolates active content, which is often how attackers inject their malware.

In this manner, a web page is rendered on the user's device and is automatically updated in sync with the original web page. Instead of sending an Adobe Flash video to a user's device, the same video is sent as HTML5, with nonactive elements transmitted as they are. All natively available fonts are reproduced on the device, so the entire web page looks, feels, and behaves as it should, maintaining the true look and feel and user experience. The DOM mirroring approach also allows a document to be printed locally, and all commands, such as cut and paste and other right-click commands, remain

active and under user control. The user's web experience remains the same, but is now safe, without the threat of malware or credentials theft. And the bank, FSI, or corporation can't be compromised, nor can the SWIFT platform be used to funnel stolen funds.

Conclusion

The successful theft of hundreds of millions of dollars through attacks leveraging the SWIFT network will almost certainly lead to similar attempts in the future. As such, it's time for SWIFT's client banks, financial services companies, and corporate finance departments to look for new ways to protect their financial assets. SWIFT was created precisely as a means to derisk payment transactions between institutions in more than 200 countries. There's already sufficient evidence that hackers have instead found ways to use the network as a means to funnel funds stolen by cybertheft to their accounts.

A new methodology is necessary—one that provides restricted, safe web access for employees with SWIFT network access.

This new approach needs to protect employees from falling prey to phishing and spear-phishing campaigns, as well as other schemes to spread malware. It should neutralize the distribution of web-borne malware, including through watering-hole attacks and targeted drive-by attacks. But it should not rely on easily circumvented reputation services. In a world with so many increasingly sophisticated cyberattacks, systems that define web traffic as simply "good" or "bad" are fast becoming irrelevant or, worse, misleading.

This new approach should also maintain the native browsing experience users expect, without the burden and overhead of client software or insecure web browser plug-ins. It should reduce the administrative burden on security staffs to create, maintain, and manage web security policy exceptions, and it should be device, operating system, and web browser agnostic.

Web isolation, and in particular Menlo Security's Isolation Platform, checks all these boxes. It is the technology that delivers a new, holistic approach to addressing SWIFT network security for banks, financial organizations, and corporations worldwide.

Menlo Security

About Menlo Security

Menlo Security protects organizations from cyber-attacks by seeking to eliminate the threat of malware from the web, documents, and email. Menlo Security's cloud-based Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and financial services institutions, and backed by General Catalyst, Sutter Hill Ventures, Engineering Capital, Osage University Partners, American Express Ventures, Ericsson Ventures, HSBC, and JP Morgan Chase. Menlo Security is headquartered in Palo Alto, California.

2300 Geng Rd., Ste. 200

Palo Alto, CA 94303

Tel: 650 614 1705

info@menlosecurity.com

menlosecurity.com