Ransom and Malware Attacks on Financial Services Institutions

Abstract

This paper is a review of cyber attack incidents, methods, groups, and defenses intended for business decision makers at financial services institutions. It is based on the 2020 Symantec® technical white paper, *Sophisticated Groups and Cyber Criminals Set Sights on Lucrative Financial Sector*, updated to include incidents and trends through July 2021.

Introduction

In its 2021 Data Breach Investigations Report, Verizon names financially motivated external actors as the top threat actors in 2,277 confirmed data breaches across all industries worldwide. Unsurprisingly, the financial sector was a top target. Symantec, a division of Broadcom®, has examined criminal activity directed toward some of its biggest financial customers since the beginning 2019, and has found that both ransomware and malware attacks are on the rise.

Ransomware

Ransomware is emerging as the most dangerous threat on the cyber security landscape. Ransomware attacks are growing more frequent, more effective, and more dangerous. At first, attackers would encrypt the data on a system and then demand a ransom for the decryption key. Organizations with adequate system backups could generally restore their data without paying the ransom, but ransomware gang tactics changed around December 2019. Now, they typically steal the data as well as encrypting it. By threatening to publish the data if the ransom is unpaid, the criminals double their leverage on the victim. Financial institutions are particularly vulnerable to the double threat, since they can't afford downtime and hold vast amounts of their clients' sensitive financial information.

Ransomware Gangs

Behind high-profile attacks on SolarWinds, Ireland's Health Service Executive, and Colonial Pipeline are hundreds of smaller or less widely publicized attacks. Symantec monitors sophisticated cyber criminal groups among more than 100 active ransomware groups targeting financial services companies and their IT service providers across Europe and the US. Many of these operate as "Ransomware as a Service" providers, developing extortion software tools, and selling them in Dark Web marketplaces for themselves or others to use. Prominent actors include:

- Maze, which appeared in May 2019, pioneered the dual tactic of encryption and threatened publication. It often publishes data to encourage ransom payment—as in a 2020 attack on Chubb Insurance—and sells data even after payment. The group claimed to be shutting down in November 2020, although security experts believe they are merely rebranding.
- DarkSide develops ransomware aimed at large financial and other institutions since August 2020. The DarkSide attack on Colonial Pipeline shut down critical infrastructure along the US East Coast and extorted more than $5 million from the company, although $2.3 million was later recovered.
- REvil (a.k.a. Sodinokibi) first appeared in April 2019. The group is reputed to have the largest market share among ransomware actors and was responsible for an attack on up to 1,500 businesses through Kaseya VSA, an IT service provider with system access.

State-sponsored Actors

Nation-state actors, unlike cyber criminals, are generally focused on espionage, not profit, and seldom target financial institutions. An exception is Lazarus, identified by the FBI as backed by the North Korean government and linked to the 2014 attack on Sony Pictures and the 2017 WannaCry ransom attack on Windows computers.

Payment

Experts generally advise businesses not to pay attackers—after all, payment encourages repeat attacks, and there's no assurance attackers like Maze will honor their agreements. But steep data recovery costs—near $20 million when Atlanta and Baltimore did not pay—have led many businesses to pay rather than attempt recovery on their own. Nor does cyber insurance always help, since insurers face the same choice between underwriting the ransom or the recovery costs.

Ransomware (cont.)

Traceable payments can expose cyber criminals, so their demands invariably specify cryptocurrency. Blockchain analyst Chainalysis estimates that ransomware attackers extracted at least $412 million in cryptocurrency from victim organizations in 2020, more than quadrupling their 2019 totals. The pace quickened further in 2021, with payments of more than $127 million in 2021 as of May 28, and a demand of $70 million by REvil from their July 3rd exploit of IT provider Kaseya. After US Federal officials recovered $2.3 million in Bitcoin from DarkSide's Colonial Pipeline attack, hackers will likely turn to newer cryptocurrencies such as Monero or Zcash, which are designed to be less traceable than Bitcoin.

Malware

Malicious software is typically inserted through phishing emails or by compromised Web applications. Emails include micro-targeted spear-phishing attacks aimed at specific individuals, often after exhaustive mining of their social media accounts for information to make the communications seem credible. Web application attacks gain access to web or email servers, on premises or increasingly in the cloud, through brute-force credential guessing or re-use of credentials stolen elsewhere, a technique called credential stuffing.

Malicious code is inserted in email attachments with plausible names and file types. Web application attacks insert malware into the code of compromised servers, using either hacker tools or legitimate administrative tools. The latter include the Windows PowerShell environment, WMI administration features, installers, and other utilities—a collection of techniques called "living off the land."

Once "backdoor" access is attained, attackers map network topology and spread laterally across networks to locate and collect assets of interest. They often maintain a stealthy presence for days or even weeks to set up exfiltration of data, money, or credentials to use in future attacks.

Malware Gangs

Unlike old-school hackers, today's financially motivated malware users operate in organized, well-equipped gangs, often out of jurisdictions beyond the reach of Western financial authorities. Constant mutations, mergers, and alliances make these groups difficult to track, but Symantec has identified the following:

- Carbanak is a malware-focused gang that appeared in May 2017. Atypically, it targets banks themselves instead of their customers. Its pattern of attack is to deliver malware attached to spear-phishing emails, wait, and then either transfer money to accounts under its control, or hijack ATMs to dispense cash to its confederates. By some estimates, it has stolen more than $1 billion to date.
- FIN7 (a.k.a. Fruitfly) also appeared in May 2017. It shares malware and tactics with Carbanak, but targets a broader range of industries.
- Odinaff appeared in January 2016 and, like Carbanak, targets financial firms. It distributes malware through email attachments, password-protected archives, and botnets. It is believed to be targeting the SWIFT system for interbank payments and using malware to obscure its attacks.
- Jointworm (a.k.a. Evilnum) is discussed in detail below.

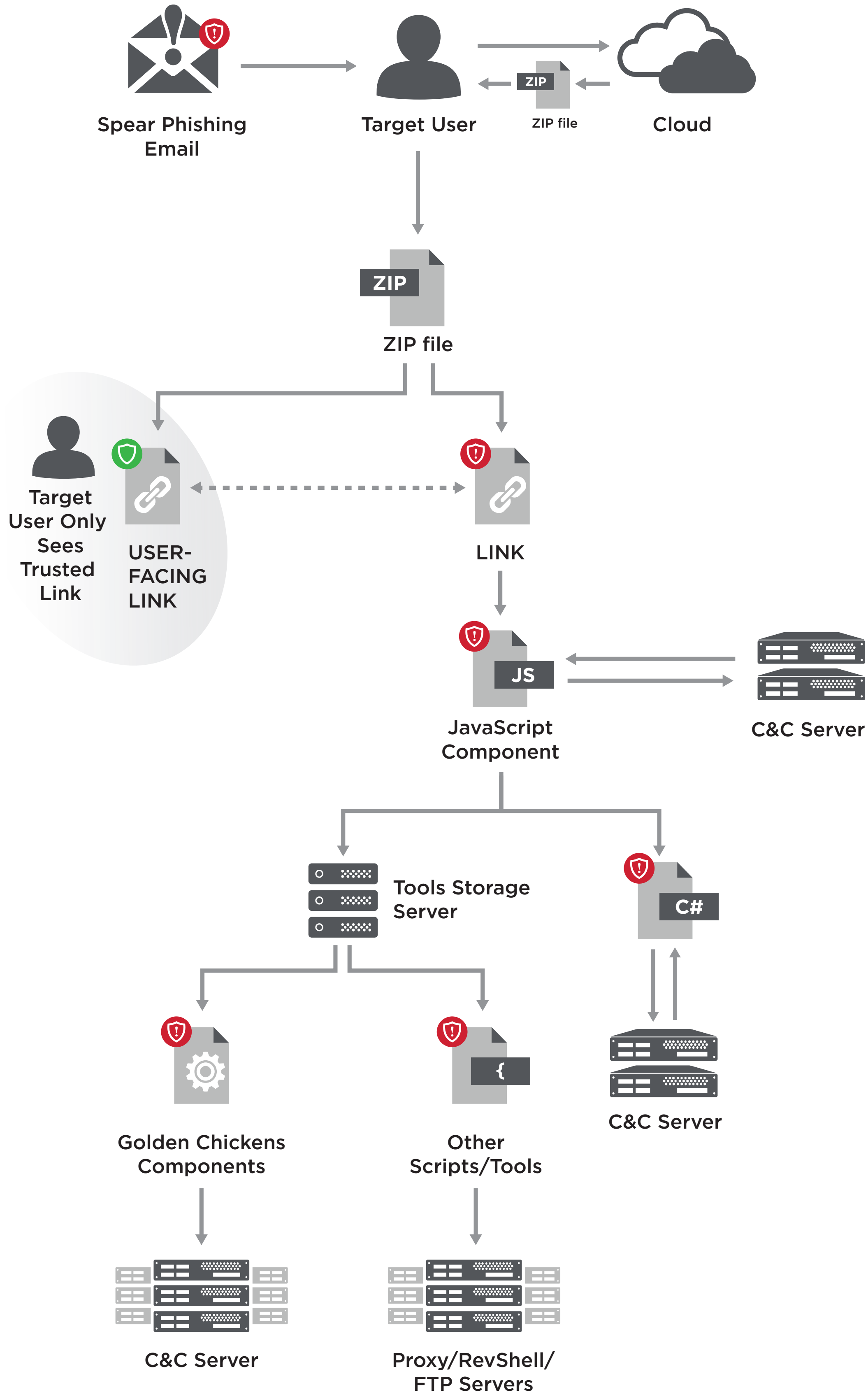
State-sponsored Actors

North Korea-backed Lazarus, source of the WannaCry ransomware attack discussed above, has also been linked to a series of attacks on banks by exploiting the SWIFT system. The most infamous example was the Bangladesh bank heist, in which the group attempted to steal $81 million, but made off with a lot less due to the quick actions of bank staff.

Anatomy of a Malware Attack: Jointworm/Evilnum

Symantec researchers have identified a cyber attack group focused on financial services companies and the IT companies that serve them in Cyprus, Ukraine, the US, and Czech Republic. The group, called Jointworm (also known as Evilnum), has been active since at least August 2017; its latest campaign against the financial sector appears to have started in December 2019. It is a highly disciplined and well-equipped organization.

Anatomy of a Malware Attack



Anatomy of a Malware Attack—Jointworm/Evilnum (cont.)

Symantec observed Jointworm's activity on multiple machines in a leading European finance company that offers online trading of shares, contracts, and international foreign exchange. The group's activities there provide an excellent example of a high-end malware attack, and an illustration of what financial firms are up against.

Targets

Jointworm steals financial information from targeted companies and their customers, including the following:

- Customer lists, trading records, financial spreadsheets, and other documents
- Internal presentations
- Software licenses and credentials
- Cookies and session information
- Email credentials
- Customer credit card information and proof of address/identity documents

Initial Access

Malware was first implanted by a multi-step process beginning with an email spear-phishing attack narrowly targeting account management staff responsible for compliance with Know Your Customer regulations:

1. Emails sent to administrators were made to look innocent using generic financial-related language, requests, and attachment names. The emails also included links to a ZIP archive on Google Drive controlled by Jointworm.
2. When opened, the archive displayed what appeared to be images or Office documents, but were actually LNK shortcuts.
3. When the reader clicked to open one of the decoys, the link displayed a plausible-looking document, but also executed a custom JavaScript to install a backdoor, giving attackers access to the reader's machine.

Downloading Tools and Malware

The backdoor gave attackers network access and the ability to both download additional malware from outside and "live off the land" by exploiting legitimate tools available on network endpoints and servers.

1. About two hours after the first machine was compromised, Jointworm ran a successful test of its network connectivity.
2. A short time later, the attackers launched an interactive interpreter on the machine, and used it to download scripts and loaders for later use. Over the course of two weeks, they installed their backdoor on a second machine and used it to download an archive of additional tools.
3. They also used installers, utilities, and applications available on the compromised machines to download additional tools.

Reconnaissance and Credential Stealing

With access established and a full set of tools, Jointworm began mapping the network, identifying assets of interest, and acquiring credentials to upgrade their permissions.

1. The Jointworm team browsed and mapped the network, collecting information on assets, including storage on a growing number of compromised machines.
2. A search for files containing the string "cpassword," led the group to old Active Directory Group Policy files they could unlock using an obsolete password published by Microsoft over a decade ago.
3. The Active Directory files contained passwords and other credentials that allowed Jointworm to move laterally across networks and escalate their privileges to the Network Administrator level.

The process of mapping networks and escalating privileges took Jointworm more than 100 days to complete, on par with their attacks on other financial institutions. With Network Administrator-level privileges, Jointworm now had virtually complete access to information on the company's network.

Jointworm maintains its strong focus on financial organizations and other companies with links to the financial sector, including fintech companies and organizations that provide IT services to companies in the financial sector. Companies in this sector should be aware that they are targets of sophisticated and professional groups like Jointworm.

Conclusion

The financial sector is a tempting target for both individual cyber criminals looking for quick profit, and organized gangs and nation-state actors with both financial and intelligence motivations.

Conclusion (cont.)

The most common attacks on financial institutions are increasing in frequency and impact:

- Ransomware and data theft targeting companies in the financial sector are trending upwards, and ransom demands are growing.
- Ransomware campaigns in general are becoming a significant public policy, law enforcement, and national strategic issue.
- Malware incidents directed at companies in the financial sector are trending upwards.

There may have been some anticipation that the COVID-19 pandemic would lead to a slowdown in cyber-criminal activity, but that doesn't seem to have occurred, at least among cyber actors targeting the financial sector.

The threats facing these companies are significant, ongoing, and unlikely to diminish. Financial firms need to be aware of them and protect their networks, data, and customers using a comprehensive security approach like the one outlined below.

Best Practices

Protection against ransomware and malware requires defense in depth, including the following provisions:

- A cyber defense platform that comprises the following:
  - Integrated, sharing threat data across endpoint, email, web, applications, and infrastructure.
  - Comprehensive, across cloud and on-premises environments.
  - Up to date, including the latest protection capabilities such as machine learning and AI.
  - Real-time, with threat information, analytics, content classification, and threat blocking data based on the latest threat intelligence.
  - Consistent in its enforcement of security rules and access policies across platforms, devices, and environments.
  - Agile, with fast, tested detection and resolution to reduce the impact of data breaches.
- Specific defenses against ransomware and malware, such as the following:
  - Identity and access management solutions to prevent theft of executive credentials.
  - Strong passwords and two-factor authentication enabled and enforced for critical information stores.
  - Backups that are off-site and unconnected company networks to avoid being encrypted by ransomware.
  - Restore capabilities that are regularly tested and fast enough to meet business requirements in case of wholesale encryption.
- Addressing known vulnerabilities with the following:
  - The latest patches installed on all devices, ideally by an automated patch management solution.
  - The latest PowerShell version, installed with logging enabled.
  - Restricting Remote Desktop Services (RDS) and other administrative tools with access only from specific, known IP addresses and protected by multi-factor authentication.
- Personnel practices that include the following:
  - Staff training in cyber security principles to prevent behaviors that risk company or customers data.
  - Behavioral analytics to identify and prevent anomalous behavior by privileged users or devices.

About Symantec, A Division of Broadcom Software

A division of Broadcom Software, Symantec is the global leader in cyber security and helps financial services organizations secure identities and information wherever they live. Symantec Integrated Cyber Defense approach simplifies cyber security with comprehensive solutions to secure critical business assets across on-premises and cloud infrastructures.

Symantec Endpoint Security, Network Security, Information Security, and Identity Security solutions are uniquely integrated and infused with rich threat intelligence from the Symantec Global Intelligence Network, as well as advanced AI and machine-learning engines to protect data, connect authorized users with trusted applications, and detect and respond to the most advanced targeted attacks.

Symantec™
A Division of Broadcom

For more product information: broadcom.com

Ransom-Malware-Fin-Ser-WP100 October 22, 2021