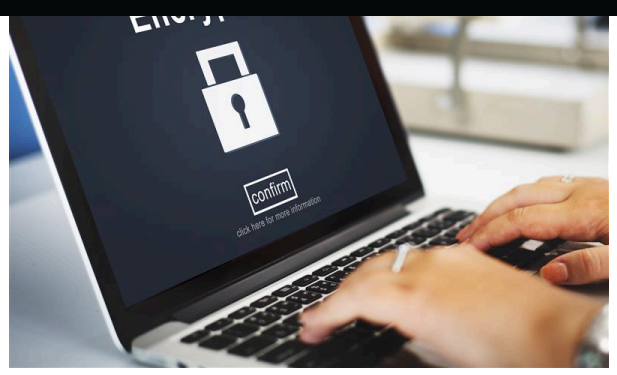
Ransomware Report: Avaddon and New Techniques Emerge, Industrial Sector Targeted

July 08, 2020

Ramos



Updated on July 23, 2020 3 AM EDT with added data on new ransomware families.

This past couple of months, ransomware has remained a formidable threat as new families, techniques, and targets continue emerging at every turn. Recently, we witnessed the rise of new ransomware family Avaddon. We also examined techniques utilized by some ransomware variants and the industries affected by these attacks. Additionally, we included our latest figures about ransomware families with the most detections, new ransomware families, and the most affected industries and segments.

Avaddon ransomware

The new ransomware called Avaddon (detected by Trend Micro as Ransom.Win32.AVADDON.YJAF-A) has been observed at large. A trojan (detected by Trend Micro as Trojan.JS.AVADDON.YJAF-A) downloads the ransomware from malicious sites and runs them on the system. This has been reported in a series of twitter posts by TMMalAnalyst.

The ransomware is propagated through emails with an attachment named IMG{6 random number}.jpg.js.zip that contains a JavaScript file named IMG{6 random number}.jpg.js.

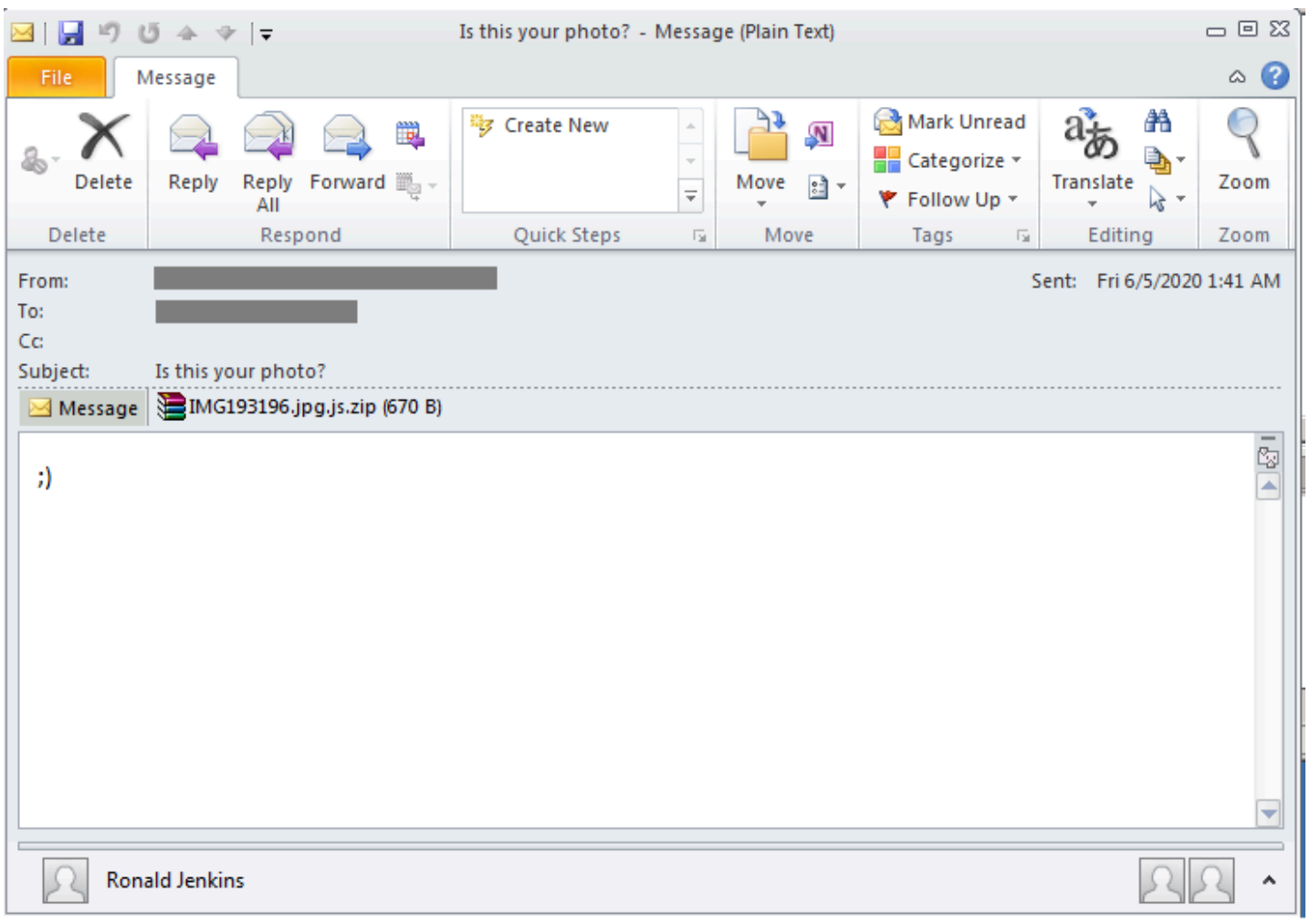


Figure 1. Sample email for Avaddon campaign

As seen in the preceding figure, the email body contains a single smiley. The emails for the Avaddon campaign also follow the footsteps of past malware campaigns that use particular subjects to spark the curiosity of the users, thus prompting them to open the message and download the attachment. Most of these emails have photo-related subjects, which might be particularly enticing for users at a time when

- Unchaining Blockchain Security Part 3: Exploring the Threats Associated with Private Blockchain Adoption
- Generative AI in Elections: Beyond Political Disruption
- Unchaining Blockchain Security Part 2: How Private Blockchains are Used in Enterprises
- From Defense to Offense: The Misuse of Red Teaming Tools by Cybercriminals
- Unchaining Blockchain Security Part 1: The Emerging Risks of Private Blockchains in Enterprises

Recent Posts

- Cellular IoT Vulnerabilities: Another Door to Cellular Networks
- Ransomware Spotlight: INC
- The Realities of Quantum Machine Learning
- Unchaining Blockchain Security Part 3: Exploring the Threats Associated with Private Blockchain Adoption
- Generative AI in Elections: Beyond Political Disruption

- Photo just for you
- You look good here
- I love this photo
- I like this photo
- Is this your photo?
- Is this you?
- My favourite photo
- You like this photo?

After the attachment is downloaded and ran, it uses a PowerShell command and the BITSAdmin command-line tool to download and run the ransomware payload. After this, the affected users will see that the ransomware has encrypted the files and appended them with the .avdn file extension. Users will see that their system desktop's wallpaper has been automatically changed to an image that states that "all your files have been encrypted" and refers to the ransom note: "Instruction 270015-readme.html" (following the {Encrypted Directory}\{random numbers}-readme.html format):

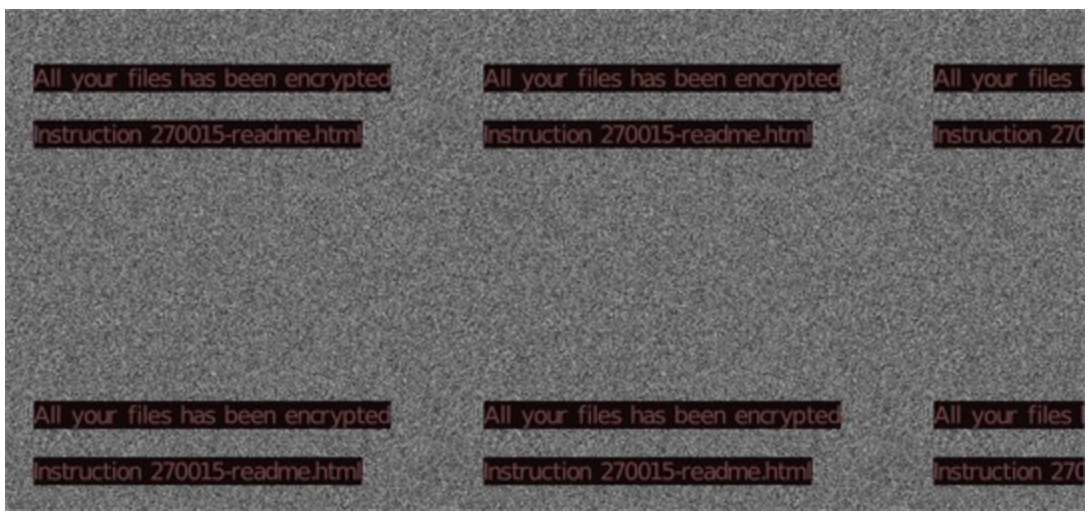


Figure 2. User's wallpaper as modified by the Avaddon attack

The ransom note gives instructions on how the affected user can recover the encrypted files.

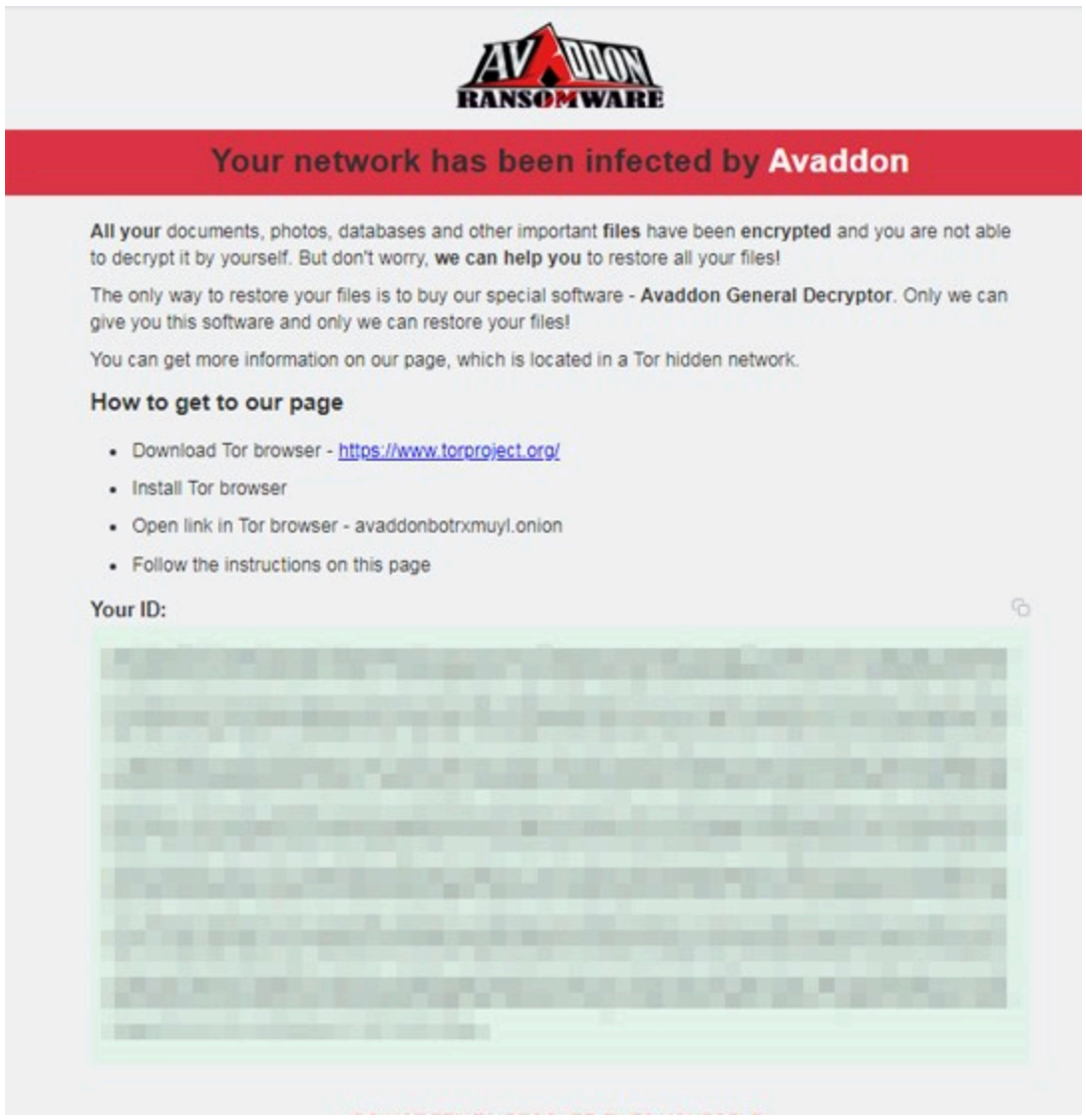


Figure 3. Avaddon ransom note

This ransomware encrypts files found in the following folders:

- Program Files\Microsoft\Exchange Server
- Program Files (x86)\Microsoft\Exchange Server
- Program Files\Microsoft SQL Server
- Program Files (x86)\Microsoft SQL Server

It adds the following processes that deletes backup copies of the system, making it difficult to restore:

- wmic.exe SHADOWCOPY /nointeractive
- wbadmin DELETE SYSTEMSTATEBACKUP
- wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
- bcdedit.exe /set {default} recoveryenabled No
- bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
- vssadmin.exe Delete Shadows /All /Quiet

It terminates services and processes, many of which are related to scanning, storing and retrieving files, and scheduling tasks. Below are some examples:

Terminated services:

- ccEvtMgr
- ccSetMgr
- Culserver
- dbeng8
- dbsrv12
- DefWatch
- Intuit.QuickBooks.FCS
- msmdsrv
- QBCFMonitorService
- QBIDPService

Terminated processes:

- 360doctor.exe
- 360se.exe
- axlbridge.exe
- BCFMonitorService.exe
- Culture.exe
- Defwatch.exe
- fdhost.exe
- fdlauncher.exe
- GDscan.exe
- httpd.exe

It terminates itself if the Windows Locale ID is equal to the following:

- 419 = Russian
- 422 = Ukrainian

It terminates itself if machine is set to the following keyboard layout language:

- 419 = Russian
- 485 = Yakut (Russia)
- 444 = Tatar

countries has similarly been observed in MedusaLocker ransomware campaigns.

For a full list of processes and services and for more details about the ransomware, please refer to our report.

New techniques spotted

In recent months, there have also been updates on the techniques used by some ransomware variants. For example, Netwalker ransomware can now be run filelessly through reflective dynamic-link library (DLL) injection (aka reflective DLL loading). This technique injects the DLL from memory rather than from disk. Although the technique itself is not novel (it has been previously used to deploy ColdLock ransomware), its use by Netwalker is new.

Another notable development is Ragnar Locker's deployment of virtual machines to evade detection by antivirus software. According to Sophos, this attack vector has never been used with any ransomware type before. In the past, Ragnar Locker exploited managed service providers or attacks on Windows Remote Desktop Protocol (RDP) connections.

Manufacturing, logistics, and energy sectors as targets

Ransomware varieties have been used to target several companies under the manufacturing, logistics, and energy sectors in the past months. A variant of Ekans ransomware (detected by Trend Micro as Ransom.Win32.EKANS.D) has been wielded in targeted attacks against manufacturing companies. As observed by Dragos, there is a particular level of intentionality that is evident in the industrial processes terminated in past Ekans attacks, making them a threat that organizations with industrial control systems (ICS) should keep an eye out for.

Nefilim, a ransomware that follows the recent trend of ransomware types that not only encrypt files but also steal data, has been witnessed to attack logistics companies. Investigations into these attacks have led us to uncover more about the recently discovered ransomware's behavior, particularly with regard to its data theft capabilities. We found out that this data theft begins weeks or even months before the ransomware is deployed, and that the attacks use several tools (both malicious and non-malicious) to deploy processes and move through the network.

In related news, operators behind Sodinokibi published, on a Tor webpage, 1,280 files of what they claim to be the passport details and other documents of staff members of an electric service provider. A few weeks before this, the ransomware attack struck the company, thereby interrupting their operations.

On the other hand, another ransomware which we dubbed as ColdLock (detected by Trend Micro as Ransom.MSIL.COLDLOCK.YPAE-A) targeted a region, rather than just a particular industry. Specifically, it launched attacks on Taiwanese organizations, aiming to target databases and email servers for encryption.

Ransomware figures for May

For May, WannaCry emerged as the top ransomware family with 15,496 detections. WannaCry's retention of the highest number of detections can be attributed to its

detections until either a new, massive ransomware comes into being, or the sources for WannaCry are found and removed.

Trailing behind are Locky with 1,532 detections and Cerber with 392 detections. Indeed, these ransomware families have consistently been on the top three since January of this year. They were also on the top three for last year's total ransomware detections.

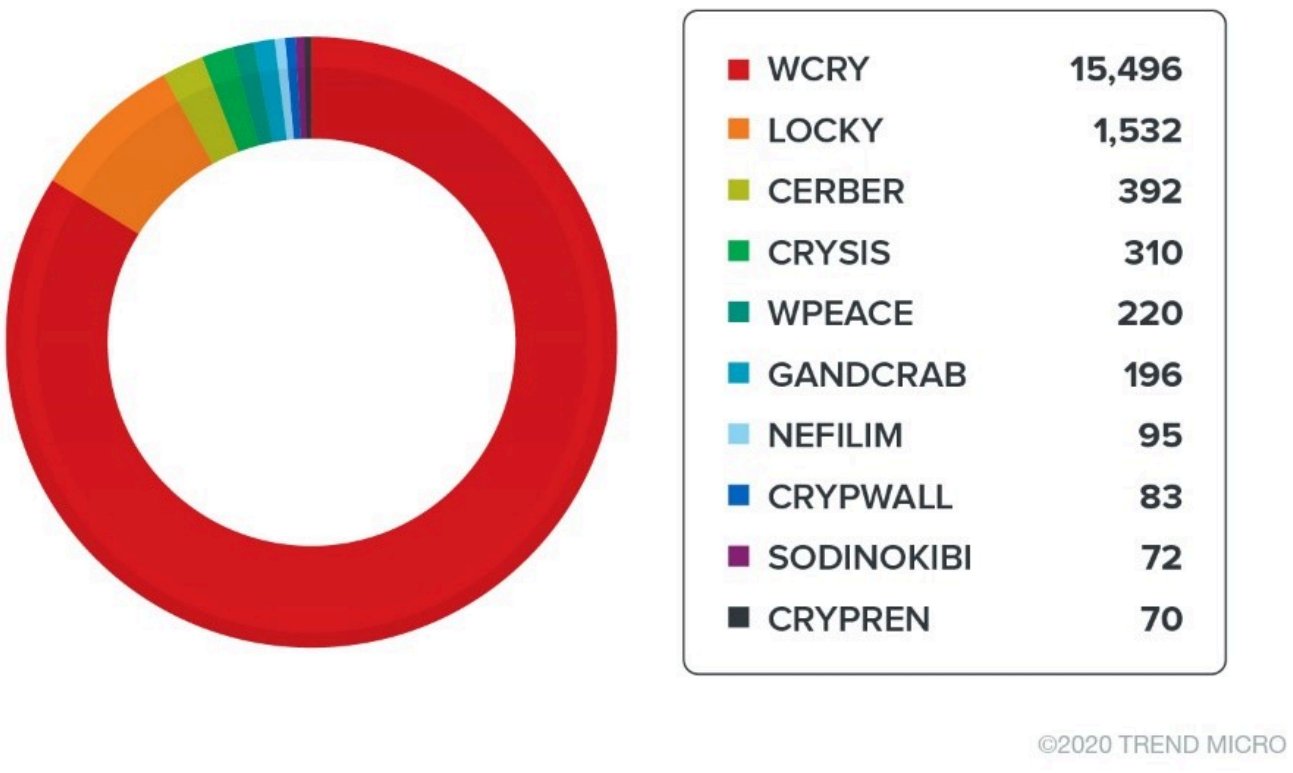


Figure 4. Ransomware families with the most detections (May 2020)

In the same month, the industries with the most detections were government (1,870), manufacturing (1,599), and healthcare (1,217).

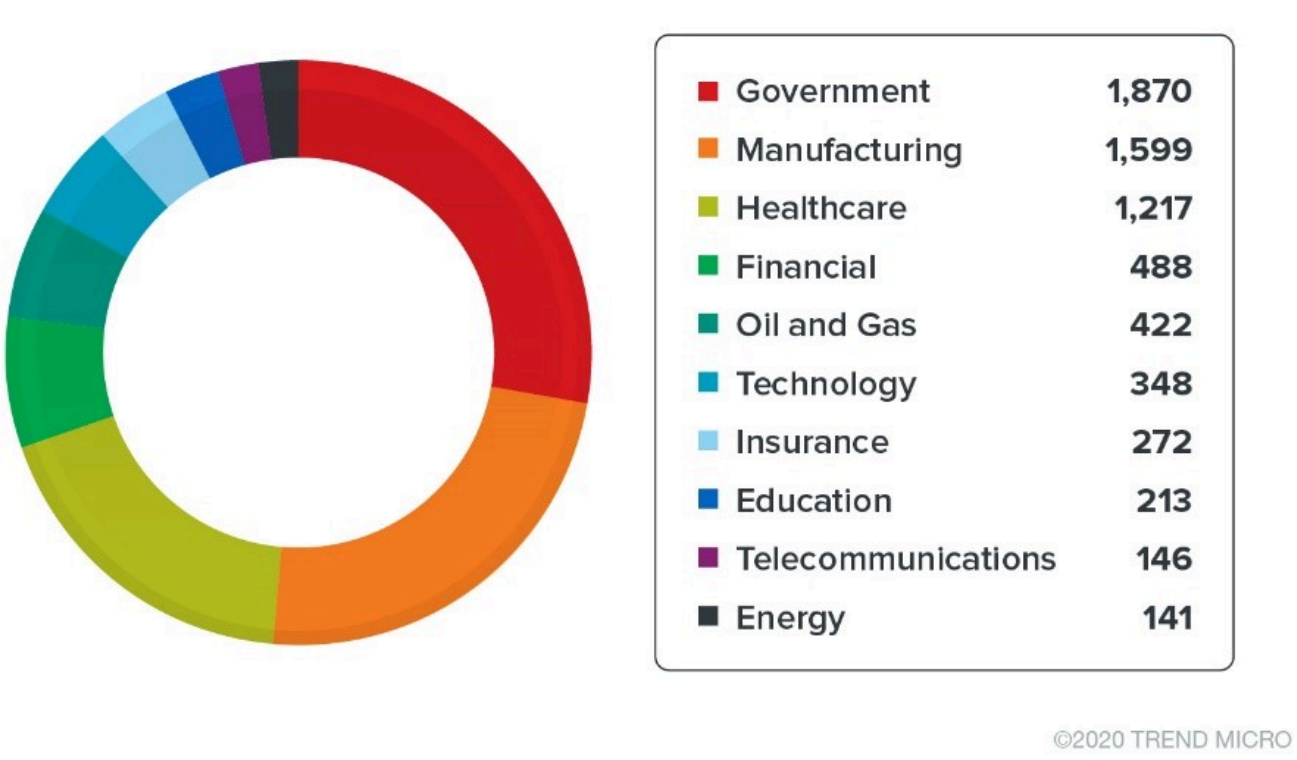


Figure 5. Top industries for ransomware detections (May 2020)

For segments, enterprise had the highest number of detections with over 18,000. Meanwhile, detections in the consumer segment numbered over 4,000, compared with over 1,000 detections in small and medium-sized businesses (SMB).

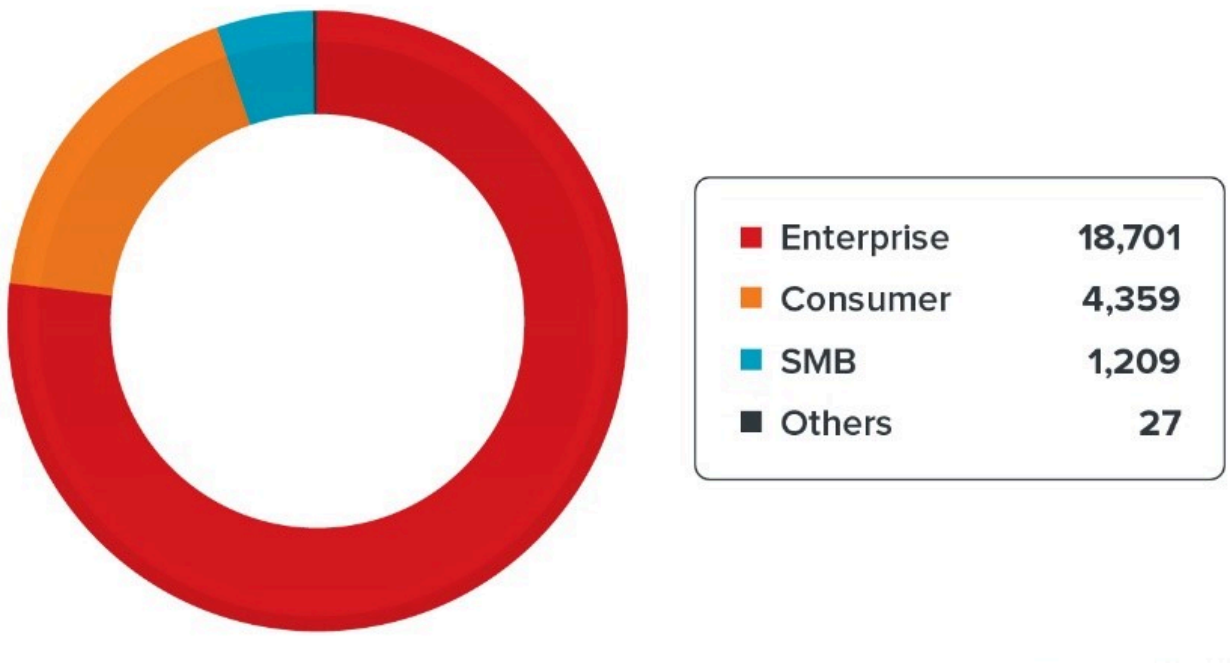


Figure 6. Top segments for ransomware detections (May 2020)

As for ransomware families, five new ones were detected in May, including the aforementioned ransomware ColdLock. One of these new families is BlueCheeser (detected by Trend Micro as Ransom.MSIL.BLUECHEESER.A), a ransomware family that appends encrypted files with the .himr extension and instructs affected users to pay US$400 to decrypt files.

Another is CoronaLock (detected by Trend Micro as Ransom.Win32.CORONALOCK.A), also known as CovidWorldCry. This ransomware, propagated through coronavirus-themed spam, renames encrypted files with .corona.lock extension. A different ransomware family named PonyFinal (detected by Trend Micro as Ransom.Java.PONYFINAL.A) is a Java-based, human-operated ransomware that targets Microsoft systems. Lastly, GonnaCry (detected by Trend Micro as Ransom.Linux.GONNACRY.A) is a ransomware that targets Linux systems. Compared with detections in April, the number of new ransomware families detected has decreased.

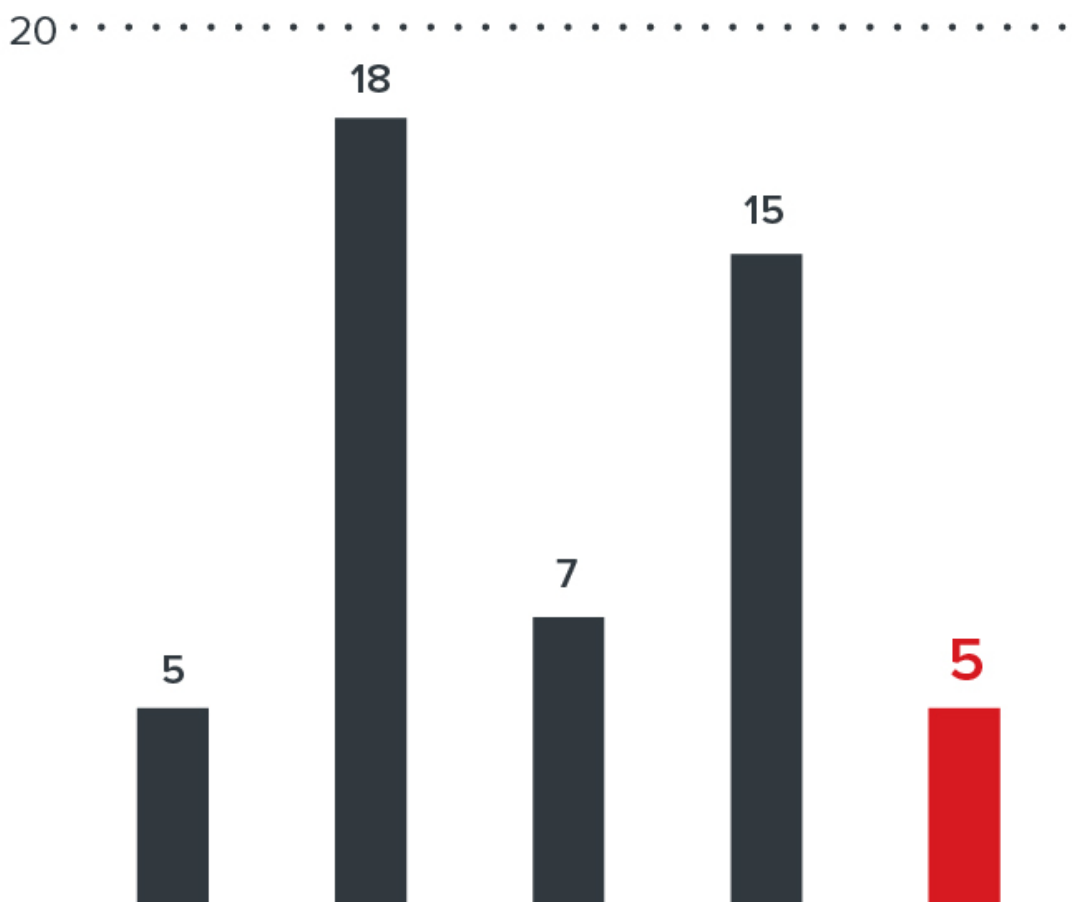


Figure 7. Number of new ransomware families (January to May 2020)

Robust defense against ransomware

Interrupted operations, lost data, and the publication of confidential company data are some of the ways that a ransomware attack can put a company at risk. However, companies can still find ways to protect their organizations from these attacks.

Here are some of the best practices for users to protect systems from ransomware:

- Back up files using the 3-2-1 rule. This rule involves regularly creating three backups in two different formats while storing one copy off-site.
- Periodically patch and update applications and software. This ensures that vulnerabilities are addressed. For zero-day vulnerabilities, deploy virtual patching.
- Enable sandbox analysis. Through this, malicious files can be run in an isolated environment. Therefore, these files can be monitored without putting the system at risk.
- Enable advanced detection capabilities for new ransomware families like machine learning or behavior monitoring technologies within your solutions.

Here are some security solutions that are recommended against ransomware:

- Trend Micro™ XDR for Users – for earlier detection of threats before they can compromise endpoints and other layers of the system
- Trend Micro Apex One™ – for actionable insights and centralized visibility across the network
- Trend Micro Deep Discovery™ Email Inspector – for blocking and analyzing malicious email attachments

Indicators of compromise

Avaddon Ransomware

SHA-256	Trend Micro pattern detection	Trend Micro mac detect
f3f4d4e4c6704788bc8954ca6f6ddc61b006aba89d5d384794f19424a3d24132	Ransom.Win32.AVADDON.YJAF-A	Troj.Win32.TRX.X
6616abb725c24307f4f062996edc5150079bc477acd4236a4f450e5835a20c62	Ransom.Win32.AVADDON.YJAF-A	Troj.Win32.TRX.X
4f198228806c897797647eecce0f92d4082476b82781183062a55c417c0bb197	Ransom.Win32.AVADDON.YJAF-A	Troj.Win32.TRX.X
05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2	Ransom.Win32.AVADDON.YJAF-A	Troj.Win32.TRX.X
b8d6fd333973adb640649cab8c9e7575a17b5a8bc382e3335400d43a606a6253	Trojan.JS.AVADDON.YJAF-A	Not Appl
a481d2b64c546f68d55e1fd23e57ada80b6b4e2c3dd7b0466380dba465f3d318	Trojan.JS.AVADDON.YJAF-A	Not Appl
5a47a89a870d7db244c76da43887e33c9ee4b26f9972878b1a6616be0302439f	Trojan.JS.AVADDON.YJAF-A	Not Appl
12bc439445f10a04b574d49ed8ccc405e2dfaa493747585439643e8a2129e5e5	Trojan.JS.AVADDON.YJAF-A	Not Appl

URLs

- hxxp://217.8.117.63/jpr.exe
- hxxp://217.8.117.63/sava.exe
- hxxp://myphotoload.com/photo.php

Posted in Cybercrime & Digital Threats