SEQRITE

QUARTERLY **THREAT REPORT** Q1 | 2020

Enterprise Cybersecurity Solutions by Quick Heal

www.seqrite.com

Contributors

Quick Heal Security Labs
Seqrite Marketing Team

About Seqrite

Seqrite is the enterprise security brand of Quick Heal Technologies Ltd., which offers world-class enterprise security solutions. Seqrite develops security management products across endpoints, mobile devices, servers and network. Our solutions are a combination of intelligence, analysis of applications and state-of-the-art technology, and are designed to provide better protection for our customers.

About Quick Heal Security Labs

A leading source of threat research, threat intelligence and cybersecurity, Quick Heal Security Labs analyses data fetched from millions of Quick Heal products across the globe to deliver timely and improved protection to its users.

www.seqrite.com

Follow us on:

Contents

Foreword

Seqrite's threat report reveals that 2020's first quarter saw an increase in malware count when compared with Q1 - 2019 by 8 million+ new threats. Overall, enterprises in January, February & March were intruded by 36 million Windows malware as detected by Seqrite's product inventory spread worldwide. The month of January saw the highest detections at 13 million with Trojans continuing to dominate the quarter's threat chart at 44% of penetration – less by 2% than the first quarter of 2019. While Trojan.KillAv.DR was the worst Trojan for Q1 2020, W32.Brontok.Q, falling under the virus category had most detections throughout enterprises.

Cryptojacking decreased to 10K attacks per day from 17K (Q1 2019) in Q1 2020. The main reason for this decline is predicted to be a drop in the popularity of cryptocurrency itself as hackers look for new revenue channels to capitalize on. Manufacturing has been a sector of choice for cyberattackers for 15 months in a now. Q1 & Q2 of 2019 saw this sector to be most hit by cyberattacks at 27% & 28% respectively. Only in Q3 of the previous year did we see a slight drop with hackers switching to the education sector instead of manufacturing. However, on an aggregate, Seqrite's Annual Threat Report had concluded manufacturing to be the worst-hit industry for the year 2019. Trojan.Shadowbrokers which attacked the manufacturing industry the most was designed to attack SMB, the story for which we have covered in this report.

The first quarter of 2020 saw a localized Coronavirus infection spread throughout the world and become a global pandemic. The mandatory lockdown enforced by governments and health agencies also percolated to enterprises that had no choice other than asking employees to work remotely. Taking advantage of a seemingly unprepared world, cyberattackers launched an offensive against businesses and governments alike by leveraging on the Coronavirus as a theme. Quick Heal's Security Labs observed an entire series of sly attacks through emails, browsers and networks hiding behind the subject of the Coronavirus.

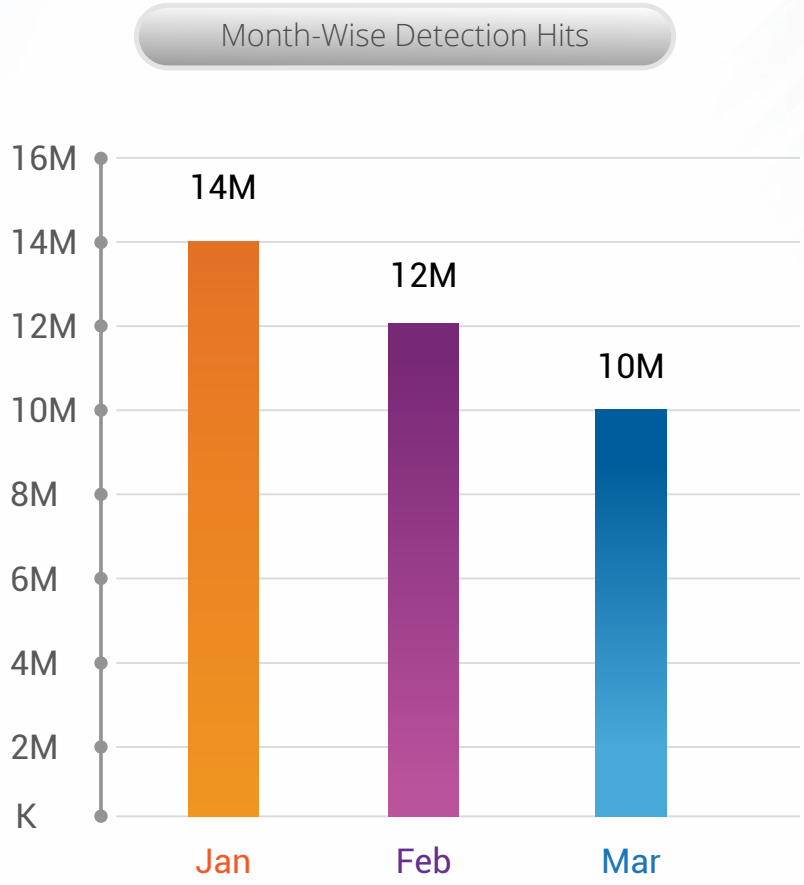
WINDOWS

Detection Highlights – Q1 2020*

*Top six malware categories featured in the chart

Detection Statistics – Month Wise

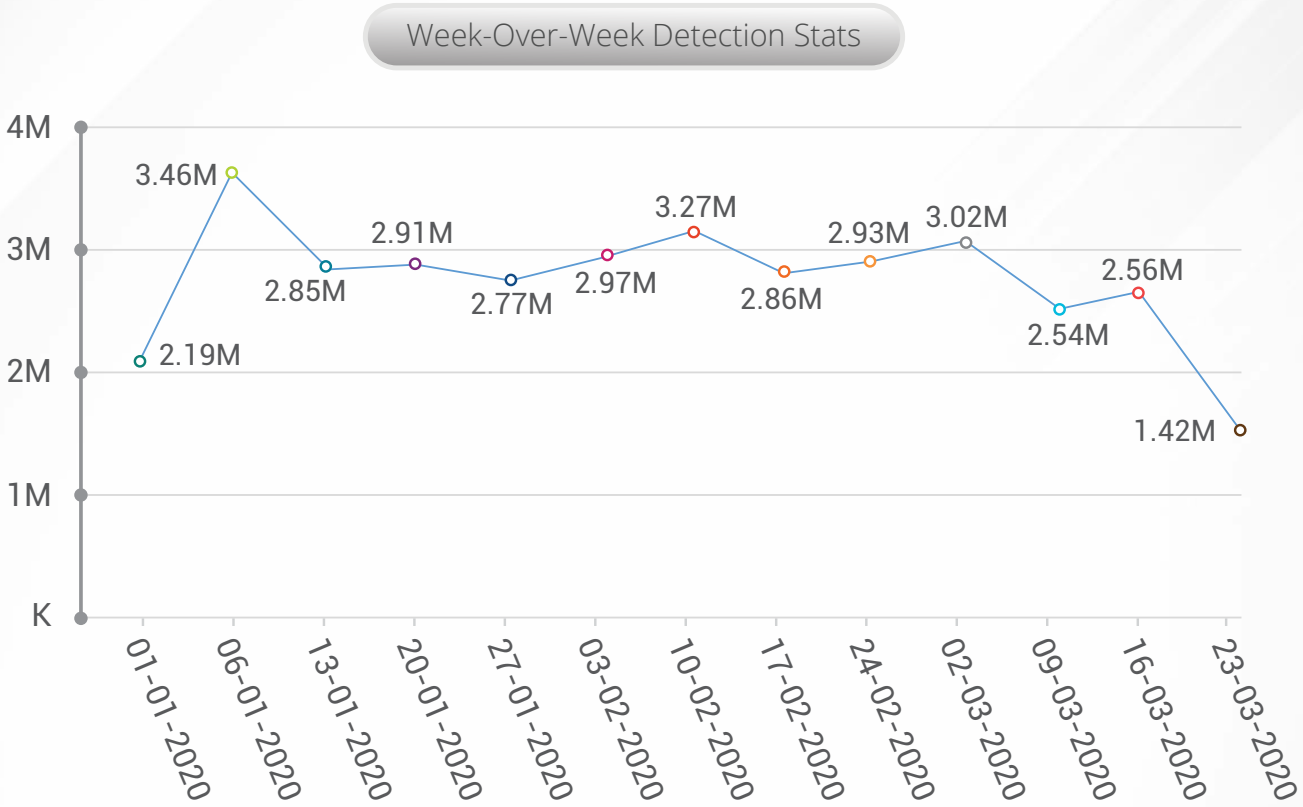
The below graph represents the statistics of the total count of malware detected by Seqrite from Jan to Mar in 2020.



Observation

- Seqrite detected over 36 million Windows malware in Q1 2020.
- January clocked the highest detection of Windows malware.

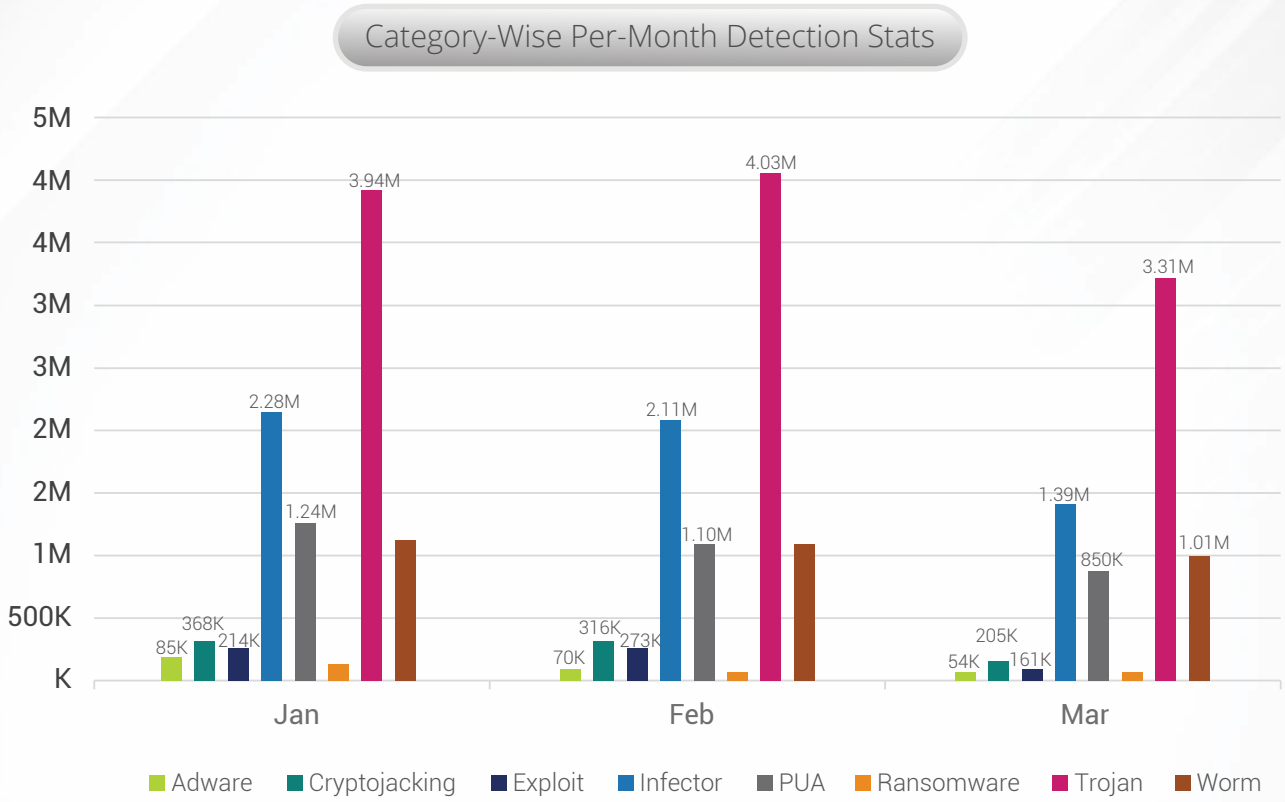
Detection Statistics – Week Wise

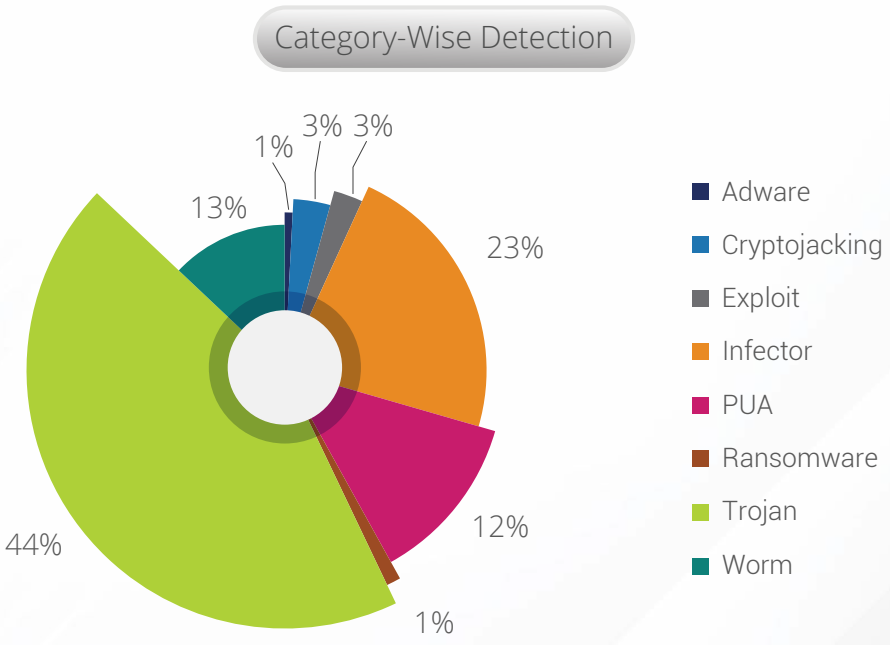


Observation

At 3 million +, there was a major spike in the detection count in January. Post that, malware, in comparison with January, substantially dropped by the end of March.

Detection Statistics – Category Wise



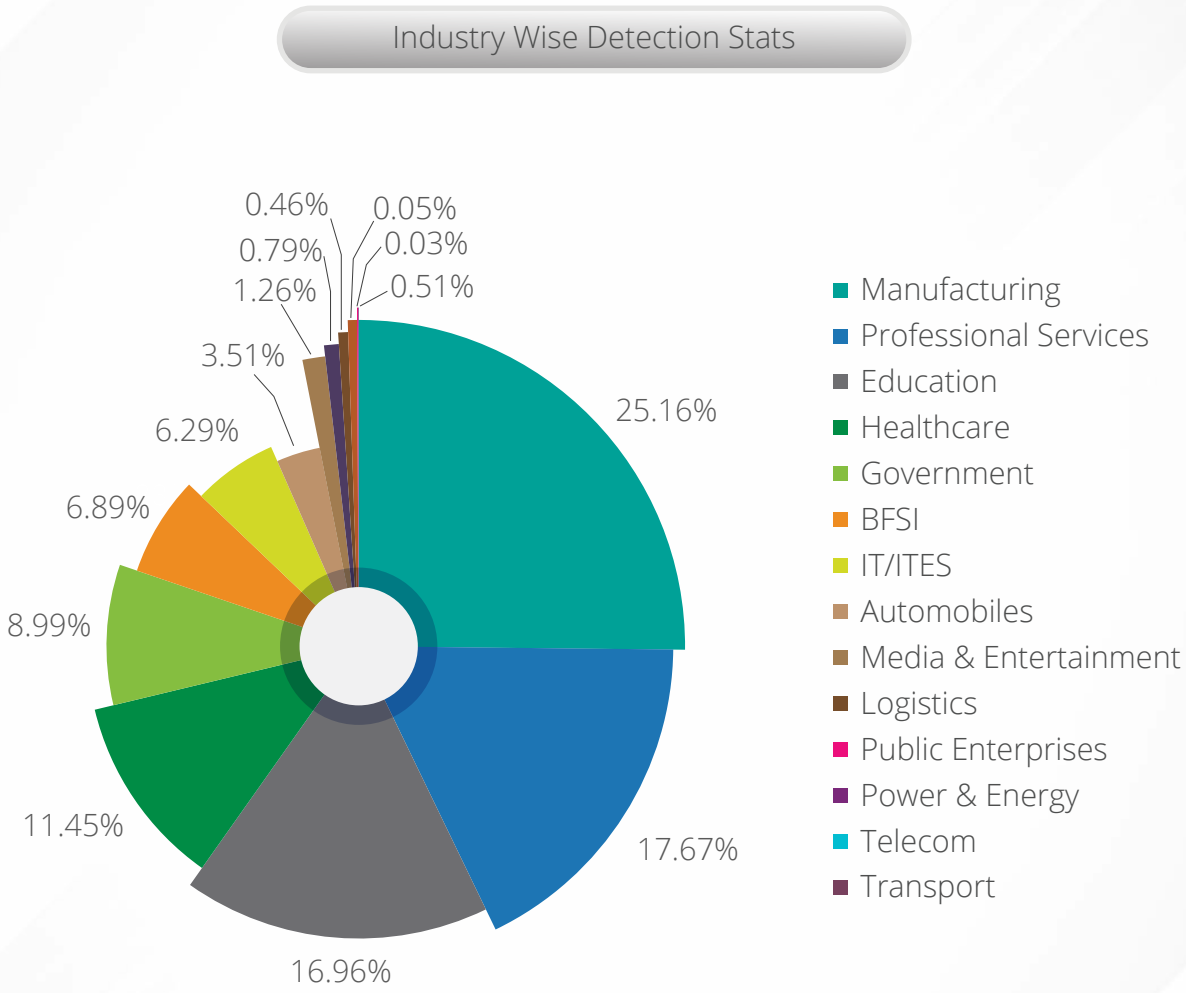


Observation

Malware detection count was the highest for Trojan accounting to 44% of the detections followed by Infector at 23%. The Trojan count was also the highest across all three months of Q1 2020.

Industry Wise Detection Stats

Below figure represents the malware detection count for various industries.



Industry Wise Top Detections

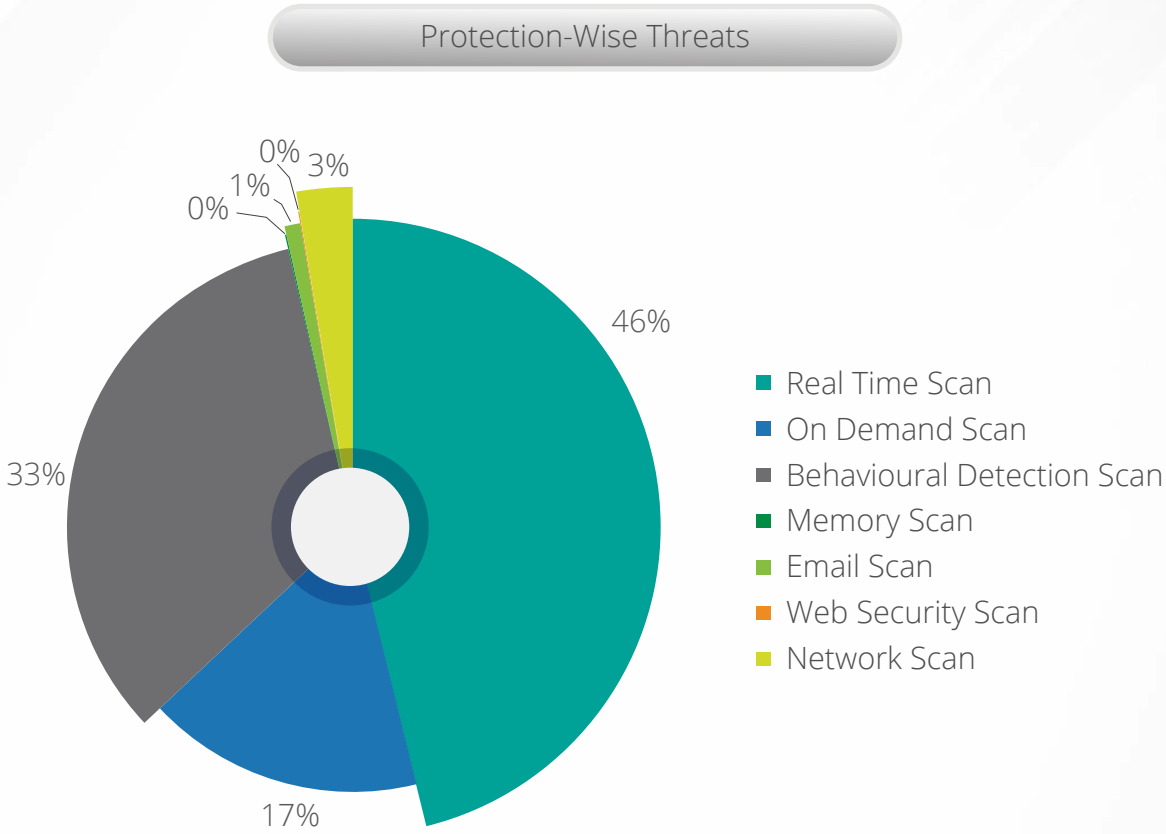
Industry	Detection	Count %
Power & Energy	W32.Brontok.Q	21.30%
BFSI	INF.AutoRun.C	16.71%
Telecom	VBS.Dropper.A	14.48%
Transport	Remoteadmin.Radmin	13.79%
Goverment	Trojan.Starter.YY4	9.51%
Strategic & Public Enterprises	Risktool.Bitcoinminer	7.34%
Automobiles	Worm.Autoit.Sohanad.S	7.31%
Education	Trojan.Agent	4.47%
Hospitality & Healthcare	W32.Sality.U	2.19%
IT/ITES	W32.Pioneer.CZ1	1.37%
Manufacturing	Trojan.Shadowbrokers	0.75%
Media & Entertainment	Worm.Tupym.A5	0.59%
Professional Services	Trojan.IGENERIC	0.08%
Logistics	W32.Neshta.C8	0.05%

Observations

- At 25%, the manufacturing industry had the maximum malware detections in Q1 2020.
- The malware W32.Brontok.Q saw maximum penetrations — the Power & Energy sector was the most sought after target with 21.30% detections.

Protection Module Wise Detection Stats

This section features the various methodologies through which Quick Heal Labs detected malware.



Observation

Most malware were detected by Real-Time Scan at 46% followed by the Behavioural-Detection Scan at 33%.

Here is a brief description of how various detection methods function -

Real-Time Scan

Real-time scanning checks files for viruses or malware each time it is received, opened, downloaded, copied, or modified.

On-Demand Scan

It scans data at rest, or files that are not being actively used.

Behavioural Detection Scan

Detects and eliminates new and unknown malicious threats based on behaviour.

Memory Scan

Scans memory for malicious programs running & cleans it

Email Scan

Blocks emails that carry infected attachments or links to compromised or fake and phishing websites.

Web Security Scan

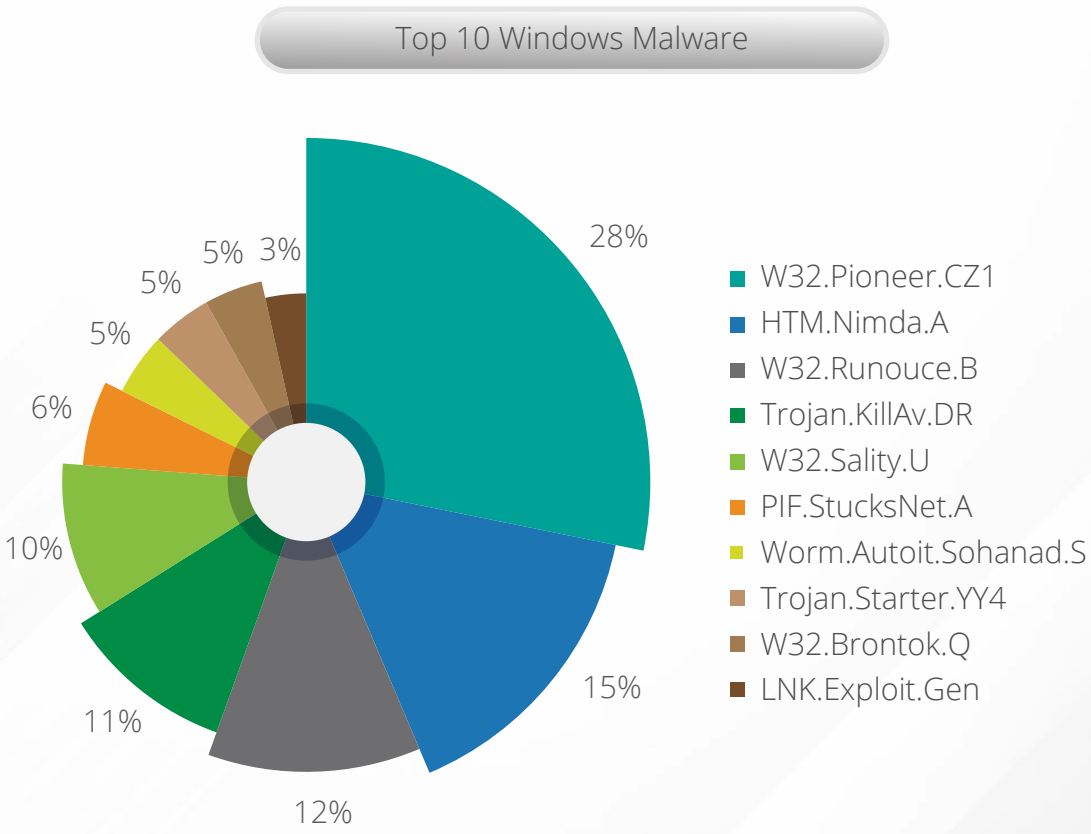
Automatically detects unsafe and potentially dangerous websites and prevents visiting them.

Network Scan

Network scan (IDS/IPS) analyzes network traffic to identify known cyberattacks & stops the malware from destroying the system.

Top 10 Windows Malware

The below figure represents the Top 10 Windows malware of Q1 2020. These malware have made it to this list based upon their rate of detection from Jan to Mar.



1. W32.Pioneer.CZ1

Threat Level: Medium

Category: File Infector

Method of Propagation: Removable or network drives

Behaviour:

- The malware injects its code to files present on the disk and shared network.
- It decrypts malicious dll present in the file & drops it.
- This dll performs malicious activities and collects system information & sends it to a CNC server.

2. HTM.Nimda.A

Threat Level: Medium

Category: Worm

Method of Propagation: Spreads through emails

Behaviour:

- The worm spreads by sending email attachments with name 'README.EXE'
- It exploits CVE-2001-0154 by setting unusual MIME header type to HTML email containing the executable attachment.
- The worm infects files on victim machines and network drives

3. W32.Runouce.B

Threat Level: Medium

Category: Virus

Method of Propagation: Spreads through emails

Behaviour:

- It sends a copy of self as an email attachment to email ids present on victim contact lists.
- Drops copy of itself at %system% folder as 'runouce.exe' with hidden attributes.
- Creates mutex with name 'ChineseHacker-2'

4. Trojan.KillAv.DR

Threat Level: High

Category: Trojan

Method of Propagation: Email Attachments and malicious/compromised websites.

Behaviour:

- This malware drops a file when executed.
- Popular malware like 'skype spy' and AV services killer are delivered and executed using this Trojan.
- The IP address and other related information of victims are also sent to malware authors.
- This malware mostly has icons resembling genuine Windows applications

5. W32.Sality.U

Threat Level: Medium

Category: File Infector

Method of Propagation: Removable or network drives

Behaviour:

- Injects its code into all running system processes. It then spreads further by infecting the executable files on local, removable, and remote shared drives.
- Tries to terminate security applications and deletes all files related to any security software installed on the system.
- Steals confidential information from the infected system

6. PIF.StucksNet.A

Threat Level: High

Category: Trojan

Method of Propagation: Removable Drives

Behaviour:

- The Trojan drops a .LNK file, which is a shortcut to the main Trojan file.

- It exploits CVE-2010-2568 which allows the attacker to execute arbitrary code on victim machines.
- The exploit CVE-2010-2568 was used in Stuxnet

7. Worm.Autoit.Sohanad.S

Threat Level: Medium

Category: Worm

Method of Propagation: Spreads through mails, IM apps, infected USB & network drives

Behaviour:

- It arrives at your computer through Messaging apps, infected USB or network.
- It can spread quickly.
- After arrival, it creates a copy of itself as exe with a typical Windows folder icon.
- A user mistakenly executes this exe assuming it as a folder and then it spreads over the network.
- It infects every connected USB drive too.

8. Trojan.Starter.YY4

Threat Level: High

Category: Trojan

Method of Propagation: Email attachments and malicious websites

Behaviour:

- Creates a process to run the dropped executable file.
- Modifies computer registry settings which may cause a system crash.
- Downloads other malware like keyloggers.
- Slows down the booting and shutting down process of the infected computer.
- Allows hackers to steal confidential data like credit card details and personal information from the infected system

9. W32.Brontok.Q

Threat Level: Medium

Category: Worm

Method of Propagation: Spreads through emails or infected USB & network drives

Behaviour:

- This worm spreads through emails or infected USB drives.
- It stores several copies of itself on different places on the hard disk, including system directories.
- It gains persistence by modifying registry keys and creating an entry in the Startup directory.
- It modifies several system configuration parameters to disable the registry editor and command prompt.
- It also modifies the safe boot shell to prevent the user from cleaning the machine.

10. LNK.Exploit.Gen

Threat Level: High

Category: Trojan

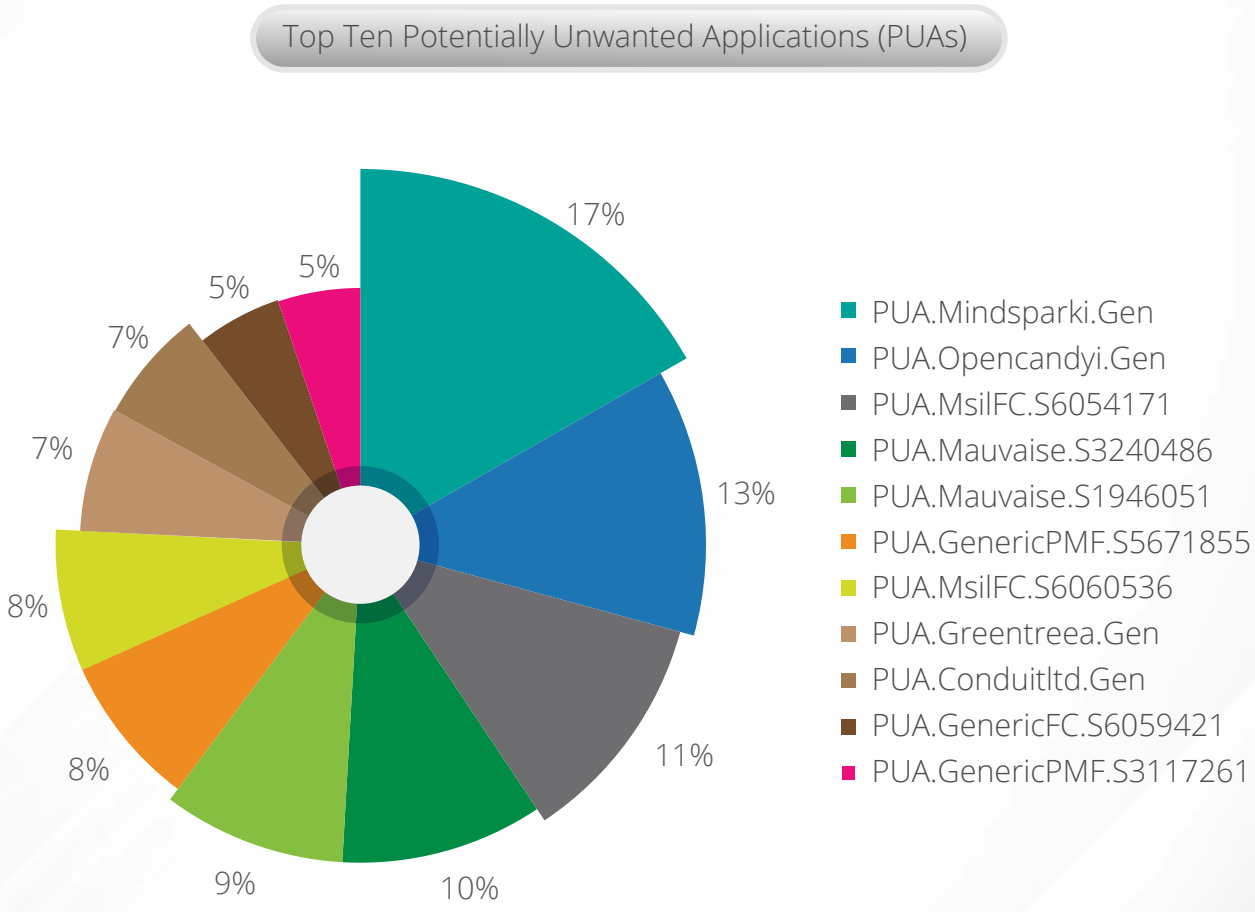
Method of Propagation: Bundled software and freeware

Behaviour:

- It is a destructive Trojan virus that could hide in spam email attachments, malicious websites and suspicious pop-ups.
- This kind of virus can be installed on Windows systems by using illegal browser extensions.
- It changes some of the system files without the user knowing about it. Next time the user launches the Windows system, this virus will run in the system background and spy on their activities. To redirect the user to dubious websites, the virus modifies system hosts file and hijacks the IP address.

Top 10 Potentially Unwanted Applications (PUA) and Adware

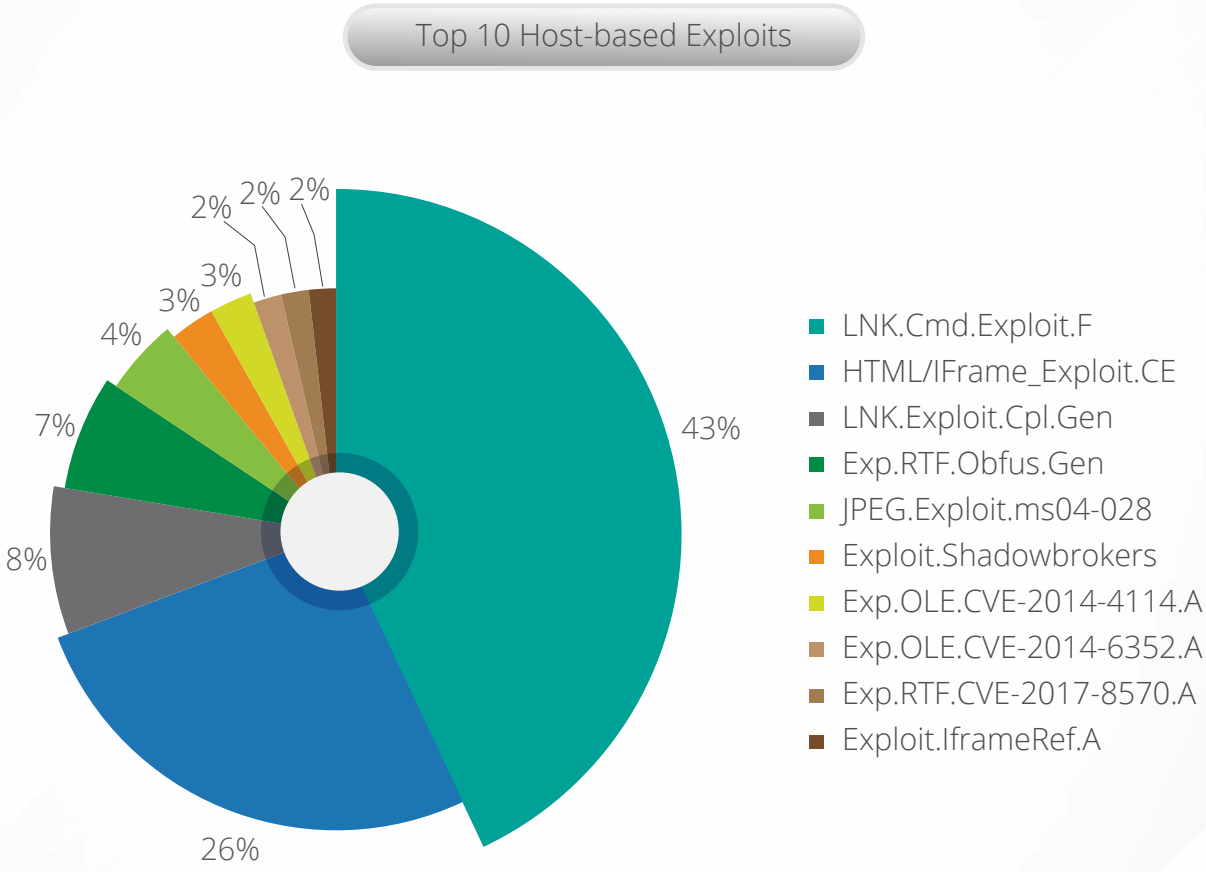
Potentially Unwanted Applications (PUAs) are programs that are not necessarily harmful but using them might lead to security risks.
Adware are software used to display ads to users - some are legitimate while some are used to drop spyware that steals user information.
Below figure represents the top 10 PUAs and Adware detected in Q1 2020.



Observation
With 17% detection, PUA.Mindsparki.Gen was the top PUA in Q1 2020

Top 10 Host-Based Exploits

A computer exploit is an attack designed by a hacker to take advantage of a particular security vulnerability the targeted system has. Below figure represents the top 10 Host-Based exploits for Q1 2020.



What are host-based exploits?

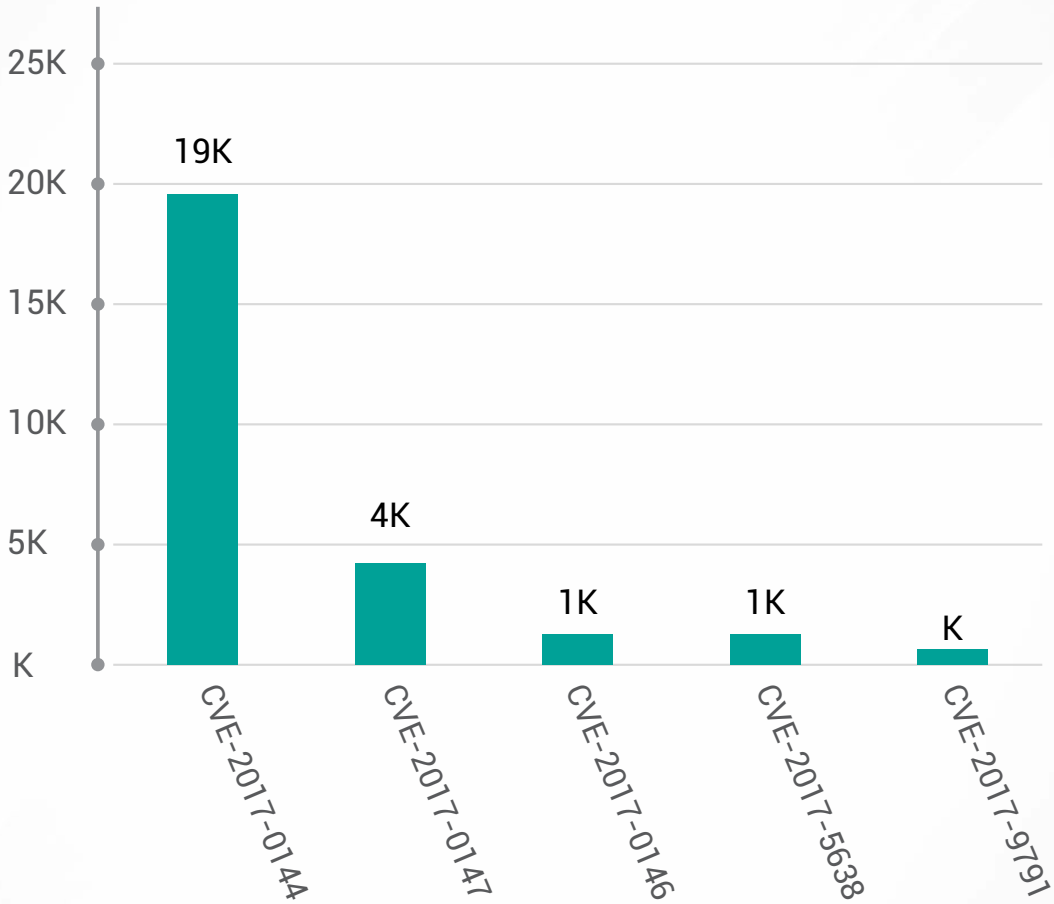
Host-based exploits are those that target security vulnerabilities found in host-based applications (host is a computer or other device connected to a computer network). These exploits are detected by endpoint detection modules such as Virus Protection, Email Protection, and Scanner.

Observation

With 43% attempts, the LNK.Cmd.Exploit.F was the top detected host-based exploit

Top 5 Network-Based Exploits

Below figure represents the top 5 Network-Based exploits for Q1 2020.



What are network-based exploits?

Network-based exploits are those that target security vulnerabilities found in network-based applications. Such exploits are detected by IDS/IPS (Intrusion Detection and Prevention System).

Observation

With 74% attempts, the CVE-2017-0144 was the top detected network-based exploit in Q1 2020.

Top 10 commonly found Malware file names

Beware of these file names as they are most likely to contain malicious code.

1.	KKPTA-POS-104.eml
2.	Default64.SFX
3.	DOC001.exe
4.	images.scr
5.	zibe.dll
6.	crli-0.dll
7.	riar-2.dll
8.	posh-0.dll
9.	Doublepulsar-1.3.1.exe
10.	tucl-1.dll

Trends in Windows Security

1. Coronavirus-themed Threats

With Q1 2020 seeing the Coronavirus spreading, mal-actors took full advantage of this global issue for delivering different RATs, ransomware and info stealers. New malware sites and domains with the substring 'corona' and 'COVID' were being registered in huge amounts to deceiving users into believing that they are accessing a site showing useful information about the dreadful disease. Some of these domains were using fully functional and real working maps of Coronavirus infected areas and other data from WHO, along with a payload.

Decoy documents and executable files were used having names like "AWARENESS NOTICE ON CORONAVIRUS COVID-19 DOCUMENT_pdf", "COVID-19 Supplier Notice", "UNICEF COVID-19 APP", "WHO-COVID-19 Letter", "Corona", "LetterCovid-19Mesures" and "Solution_to_coronavirus" to trick users into opening it.

Such attacks are still active and very much in use!

Many of such files have a spoofed file extension like pdf, doc or rtf, however, their original extensions are exe, scr or lnk. Malspam campaigns use attachments containing compressed .zip, .rar or .arj files which carry malicious exe, lnk or vbs files.

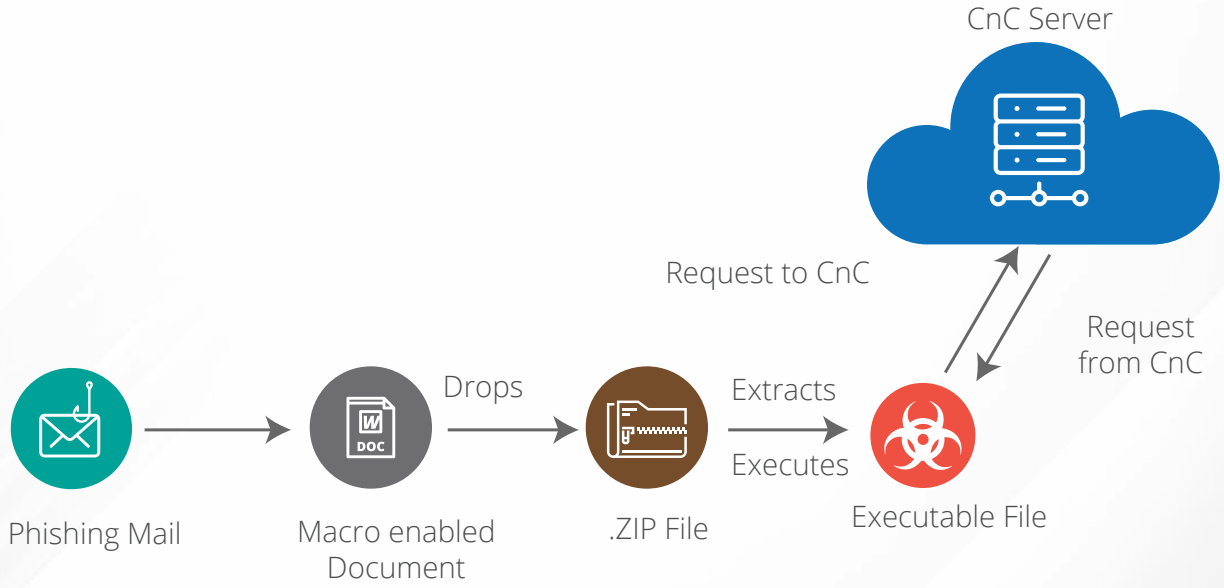


Fig1. Attack Chain

Loki-Bot, Agent Tesla and Netwire RAT are some of the popular threats which use the above-mentioned techniques to infect users. In the current pandemic situation, the healthcare industry needs to stay more careful against cyber threats since thousands of Coronavirus infected patients' health relies on their medical facilities. DoppelPaymer and Maze ransomware operators have posted a 'Press Release' stating that they will stop all activity

against all kinds of medical organizations until the end of the pandemic. However, only the test of time would prove if they adhere to their own words (or not).

Quick-Heal detects these malware and malicious domains however, to be on the safer side following preventive measures can be followed.

- Turn on the email protection of your antivirus product.
- Do not open any link in the email body sent by an unknown source.
- Do not download and open any attachments from an unknown source.

2. Ransomware exploring new technique for process code injection!

Process code injection is a very popular technique among malware authors to evade from security products. Process hollowing is an injection technique where the legitimate process is created in suspended mode, its memory is overwritten with malicious code and process is resumed. It seems like all the malicious activities are performed by a legitimate process, so it is untouched by security products. The new ransomware Mailto or Netwalker is using this old trick in a new way. Instead of creating a process in suspended mode, 'Debug Mode' is used. It gets the process and thread details using debug API WaitForDebugEvent. Then a section is created with a size that of the sample and whole file data is copied. It then manually resolves the relocation.

The sample contains an encrypted JSON file in resource section having required information like a key for generating ID i.e. extension to be added to encrypted files, base64 encoded ransom note, whitelisted paths and email-ids which are part of the extension. The ID is generated using the key kept under the tag 'mpk' in decrypted JSON, the retrieved computer name and the hardware profile information about the machine being infected. SHA-256 of these components is calculated and the first five characters of the output are used as the ID i.e. extension of the files. The name of the ransom note file is also kept the same as ID generated. Changing the extension on each device makes cybersecurity difficult to detect ransomware based on the software's pre-defined extensions.

Ref.: https://blogs.quickheal.com/mailto-ransomware-hiding-under-explorer-exe/

3. Wake up On LAN Implementation By Ryuk

Wake up on Lan (WoL) is a hardware feature that allows a computer to be turned ON or awakened by a network packet. The packet is usually sent to the target computer by a program executed on a device connected to the same LAN. This feature is used for administrative functions that want to push system updates or to execute some scheduled tasks when the system is awakened.

For sending WoL Packets, Ryuk collects system ARP (Address Resolution Protocol) table and enumerate each entry in the ARP table. This packet is sent over the User Datagram Protocol (UDP) socket with socket option SO_BROADCAST using destination port 7. The WoL magic packet starts with FF FF FF FF FF FF followed by target's computer MAC address. For the sent WoL packet, if a successful response is received, Ryuk tries to mount the remote device administrative share. If it can mount the share, it will then encrypt the share drive.

This WoL feature could be seen adapted by other ransomware groups in future to infect more machines through a single system infection. It can be prevented by an administrator by setting WoL packets to be allowed from administrative devices and workstations.

Reference: https://blogs.quickheal.com/deep-dive-wakeup-lan-wol-implementation-ryuk/

4. Now Ransomware at Its Next Stage: Publish the Stolen Data Before Encryption

Most ransomware which we see are only encrypting the victim's files and then proceeding to encrypt network shared drives. Recently, we came across few ransomware samples which are taking it to another level by stealing all the victim data from the system to their C&C before encrypting the files.

There are a lot of ransomware which do this currently, one of them being BitPyLoc. The recent variant of BitPyLock is now stealing data before encrypting it. It claims that the data shall be released/published online if the ransom payment is not paid.

The Nemty ransomware has also announced that it will create a blog to publish stolen data from ransomware victims who refuse to pay the ransom. Also, both Sodinokibi and Maze ransomware are adopting this new tactic.

If this ransom method is successful in getting higher ransom payments then we can expect more and more malware authors to switch to this new approach, adversely impacting the privacy policies of organizations and their consumers.

Reference :

https://gdpr.report/news/2020/01/21/privacy-new-ransomware-threatens-to-publish-stolen-data/

https://gdpr.report/news/2020/01/14/privacy-nemty-ransomware-still-start-leaking-stolen-data/

5. HorseDeal Riding on The Curveball!

It's surprising to see how quickly attackers make use of new vulnerabilities in malware campaigns. In this quarter, Microsoft patched a very interesting vulnerability in their monthly Patch Update for January 2020. It's a spoofing vulnerability in Windows CryptoAPI (Crypt32.dll) validation mechanism for Elliptic Curve Cryptography (ECC) certificates. An attacker could exploit the vulnerability by using a spoofed certificate to sign a malicious executable, making it appear as if the file was from a trusted, legitimate source. This vulnerability is being referred to as a 'Curveball' and 'Chain of Fools'. In our lab we came across ransomware —HorseDeal leveraging this vulnerability. While HorseDeal pretends to be signed by Microsoft ECC TS Root Certificate Authority 2018, it has the publisher name of a genuine AV-vendor.

Once executed, the UPX-3.94 packed HorseDeal payload deletes shadow copies from the system. Using bcdedit, the payload disables the automatic repair feature and sets the boot status policy to ignore errors if there is any failure in the boot process. Along with that, it turns off the firewall using netsh advfirewall. The files are encrypted using the Salsa algorithm for faster encryption. The Salsa key is different for each encrypted file. 0x24 Bytes are generated using CryptGenRandom(). The first 0x20 bytes are used as a Salsa key. Only initial 0x2800 bytes of file data are encrypted with Salsa. After data encryption, a dword encryption marker 'DEC0ADD3' is inserted. The randomly generated 0x24 bytes are then encrypted with local RSA public key and are appended to encrypted files after the encryption marker. Unlike other ransomware, HorseDeal uses jabber and ICQ for communication. The instructions to use jabber are also included in the ransom note.

Though it was yet another ransomware with no extravagant behaviour, the use of this critical vulnerability, 'CurveBall' has made it special.

Ref: https://blogs.quickheal.com/horsedeal-riding-curveball/

6. Ouroboros: Following A New Trend in Ransomware League

Ouroboros has been around from a year now and it spreads through RDP Bruteforce attacks, deceptive downloads, and through Server Message Block (SMB). During analysis, we found that initially, it stops SQL process (SQLWriter, SQLBrowser, MSSQLSERVER, MSSQL$CONTOSO1, MSDTC, SQLSERVERAGENT, MySQL, etc.) to encrypt those files which are open in a database by creating process cmd.exe with 'net stop' command and few other SQL processes by using Windows APIs.

ENCRYPTION:

It forms 0x40 bytes key stack consisting of 0x20 key bytes generated from CryptGenKey Crypto API and combines it with 0x20 bytes which are already present in the file. It forms 0x40 bytes

key stack consisting of 0x20 key bytes generated from CryptGenKey Crypto API and combines it with 0x20 bytes which are already present in the file. It builds initial block cypher using the instruction set shown in (fig.3) by using expanded key and IV. This ransomware keeps 0x100 bytes PEM encoded RSA public key in a file. It encrypts AES key with this RSA public key and appends it at the end of the file. If CNC is present, it generates the RSA public key through the implemented algorithm and sends the private key through CnC. Ransomware are now not only using packers but are also using Crypto++ libraries as well as different instruction sets to make the analysis difficult — and noticing that other ransomware (LockerGoga) have also used similar techniques, we can say that this trend will be followed in the future.

7. CVE-2020-0796 – A 'wormable' Remote Code Execution vulnerability in SMBv3

This quarter was very special (and worrisome) for Microsoft and all the users of Windows Operating system. January started with an unpatched IE Zero-day getting actively exploited with February seeing a critical vulnerability in the Crypto API used in Windows for validating ECC Certificates. March witnessed another wormable Remote Code Execution vulnerability -CVE-2020-0796, also known as SMBGhost. It is a vulnerability in the way Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain compression requests.

An attacker who successfully exploits the vulnerability could gain the ability to execute code on the target server or client. To exploit the vulnerability against a server, **an unauthenticated attacker could send a specially crafted SMB2 'Compression Transform Header' packet to a targeted SMBv3 server service supporting data compression.**

We advise customers to disable SMB access to their Windows hosts from unknown/public IP addresses unless it's necessary. The facts that remote code execution is possible, and authentication is not required makes this vulnerability very critical. We can expect malware authors adding this exploit in their arsenal for lateral movement, in a similar way as 'Eternal Exploits' were used in the past.

8. The new variant as seen in the Transparent Tribe APT campaign

In this quarter, Quick Heal Security Labs has come across a new variant of Transparent Tribe APT. In the previous variant, the victim used to receive an email containing a decoy document as an attachment. The macro code inside the document would drop a zip file, extract it and execute the malicious file present inside it. The payload executed would connect to the CnC server to receive commands from the master and ultimately perform the data-stealing activity.

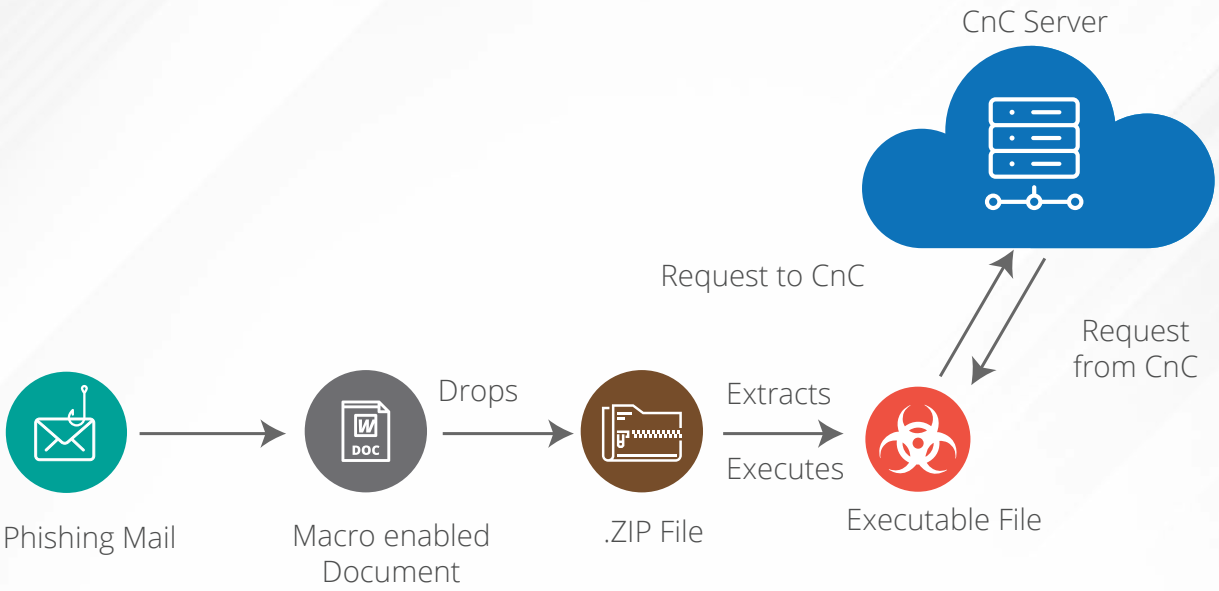


Fig 2. Old Attack Chain method

Now, in a new variant, the initial attack vector is the same as the decoy document, but the use of macro code is different here. Macro code drops a .zip file, .cs file and a .vbs file. This dropped VBS file is responsible for extracting the zip file. Unlike the previous variant, the zip file here contains 4 embedded files in it.

Two of them are open-source silent MD files which execute csc.exe and cvtres.exe for runtime compilation of .cs file. The compiled file is used to download a new payload from the CnC server and execute that payload to perform further activity. The payload again drops another file at %programdata% location and execute it to perform actual malicious activity. The malware is used to steal the data from the host machine and send it to the CnC server. After the running processes' information is sent to the CnC server, it responds with a command to perform further tasks.

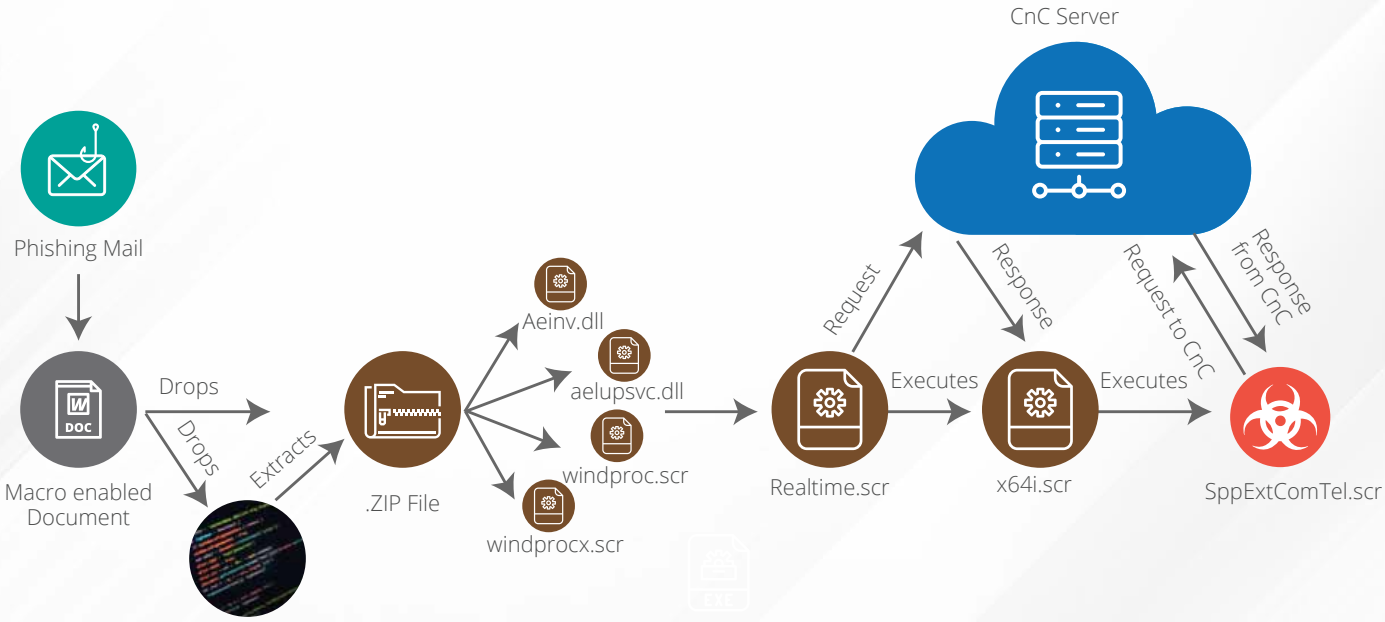


Fig 3. New Attack Chain method

Inference

The biggest vulnerability for enterprises today is the fear of a data breach happening due to its employees working out of office networks. Home networks are vulnerable to cyberattacks far more when compared with office networks. The earth is now literally closed and amidst the ambiguity of an economic recession, businesses being hit with a severe cyberattack is strictly unwanted.

Hence businesses should ask their employees to adhere to –

- Working from a VPN or other similar networking solution
- Reporting of suspicious activities to respective IT teams
- Leveraging on Seqrite's product range to protect end-to-end enterprise data

With the Coronavirus theme as a point of origination of a new wave of cyberattacks, we are likely to see multiple offsprings of the same transforming into lateral attacks. Enterprises cannot afford to drop their guard whatsoever — prevention is always better than a cure. The worst part is, it is not just the virus theme that is worrisome—attackers are trying to proliferate from all dimensions where they are seeing security loopholes, as comprehensively described in this quarter's top threat stories.

APTs are being novel in their approach whilst attacking and with sensitive sectors such as manufacturing already vulnerable to cyberattacks, such threats can be quite menacing. Ransomware continues to be a problem, shifting strategies to now launch attacks on data stored on the cloud as well. We found Ouroboros, new process code injections & pre-encryption disbursing of data as the latest ransomware trends. Microsoft's products too, are being targeted by attackers but the software behemoth has been pro-active in releasing patches quickly towards newly discovered flaws in 'different Windows Operating Systems'.

Quick Heal Security Labs is acting on its pledge of being pro-active in the testing times of the Novel Coronavirus. All our staff is fully equipped to tackle new and existing cyber threats even when working remotely. We are constantly adding detections and have instructed our technical support staff to be on-guard round-the-clock to handle any emergencies that may arise in these traumatic times. We are on a constant endeavour to publish our actions on multiple platforms that we are active on with our contingency teams ensuring the best of cyberdefense in all possible avenues.