SEQRITE

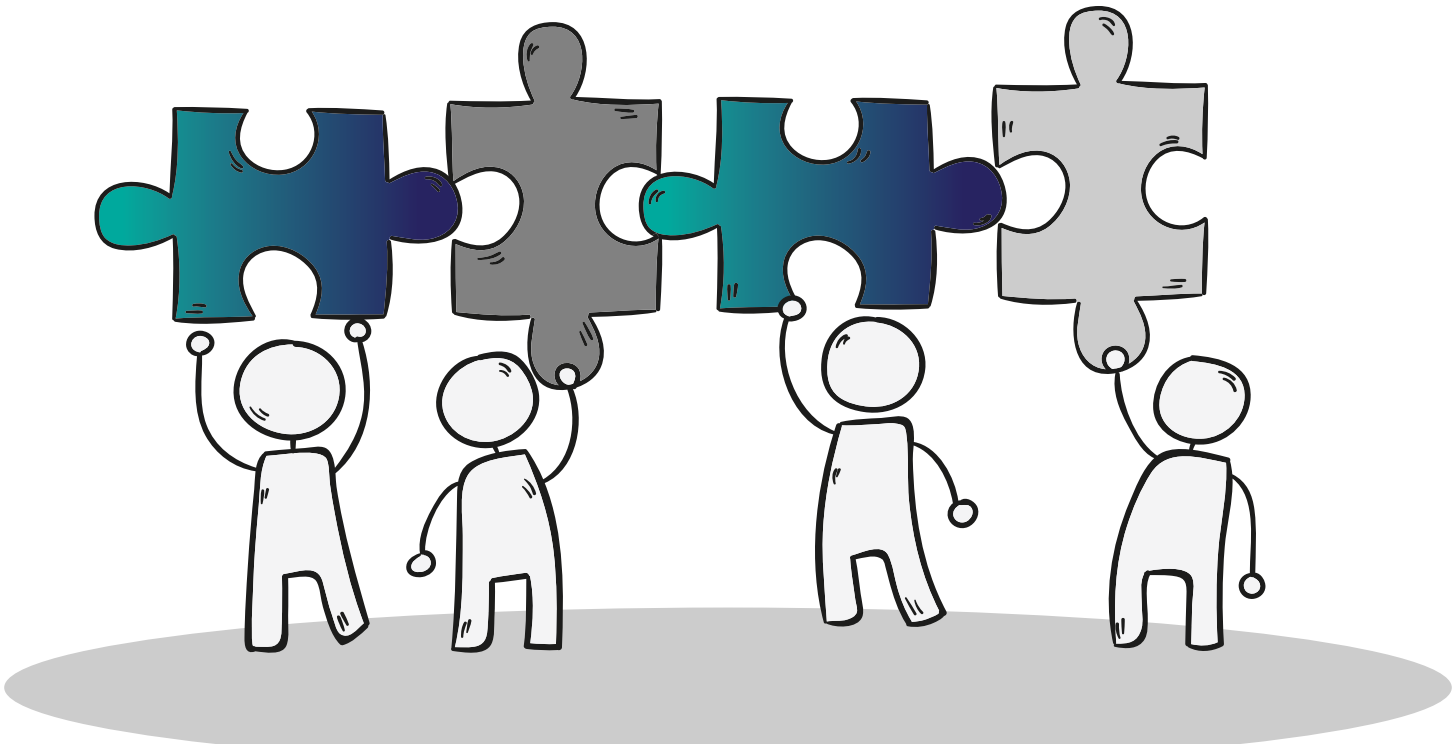
ANNUAL THREAT REPORT 2020

Enterprise Cybersecurity Solutions by Quick Heal

www.seqrite.com

Contributors

Security Labs
Marketing Team



Contents

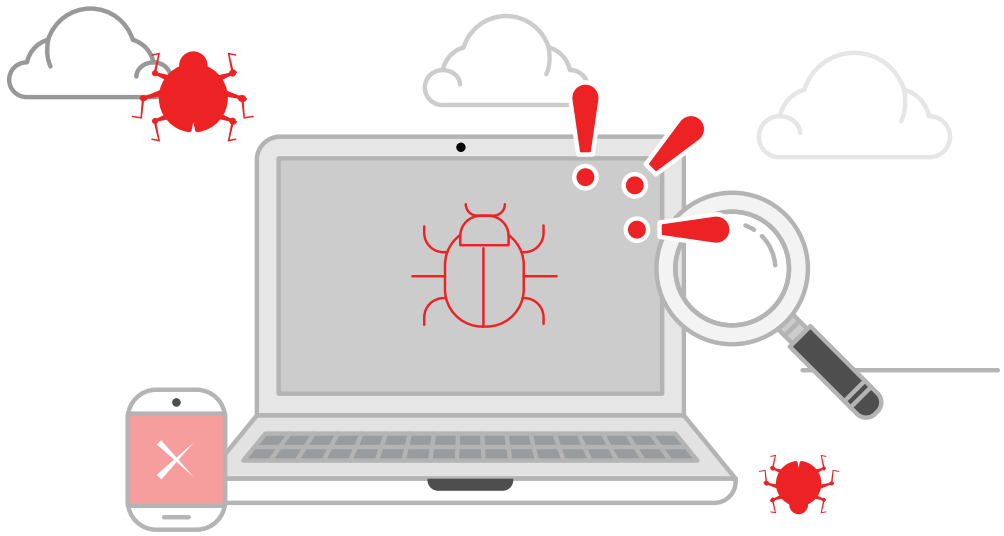
2019 ends with a 48 percent malware spike

2019 is ending with a 48 % malware spike compared to 2018 making it obvious that enterprise cybersecurity, is still in danger. Cybercriminals and threat actors appear to be more aware of vulnerabilities and entry points than enterprises as they relentlessly discover innovative methods to penetrate corporate networks. Our Security Labs have amassed malware data for the sole purpose of bringing forth a realistic picture of the cybersecurity landscape, globally. The report also speaks of two dreadful APT attacks targeted towards governments and critical national infrastructure viz. Operation m_project & Backdoor.DTrack.
At the end of the report, enterprise & government stakeholders will have absolute clarity on building their cyberdefense strategy for 2020.

Summary

Seqrite's Annual Threat Report is sharing information on various facets of malware. One of the biggest revelations it makes is the malware count for 2019, calculated to be 146 million. That's high! Malware attacks will continue to rise and evolve — nothing uncanny about it. The Trojan invasion continued at 8 million counts across the year — the month of December & Q4 2019 in general, seeing the maximum attacks on enterprises. Real-Time Scanning capabilities detected and blocked maximum malware at 51%. Behaviour-based malware detection technology was responsible for 23% signature-less detection in 2019. Seqrite has been raising an alarm for the manufacturing sector to step-up and secure its enterprises from cyberthreats for the entire year, however, more awareness is required for this domain.

The manufacturing sector was the most impacted due to cyberattacks.



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 networks. 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

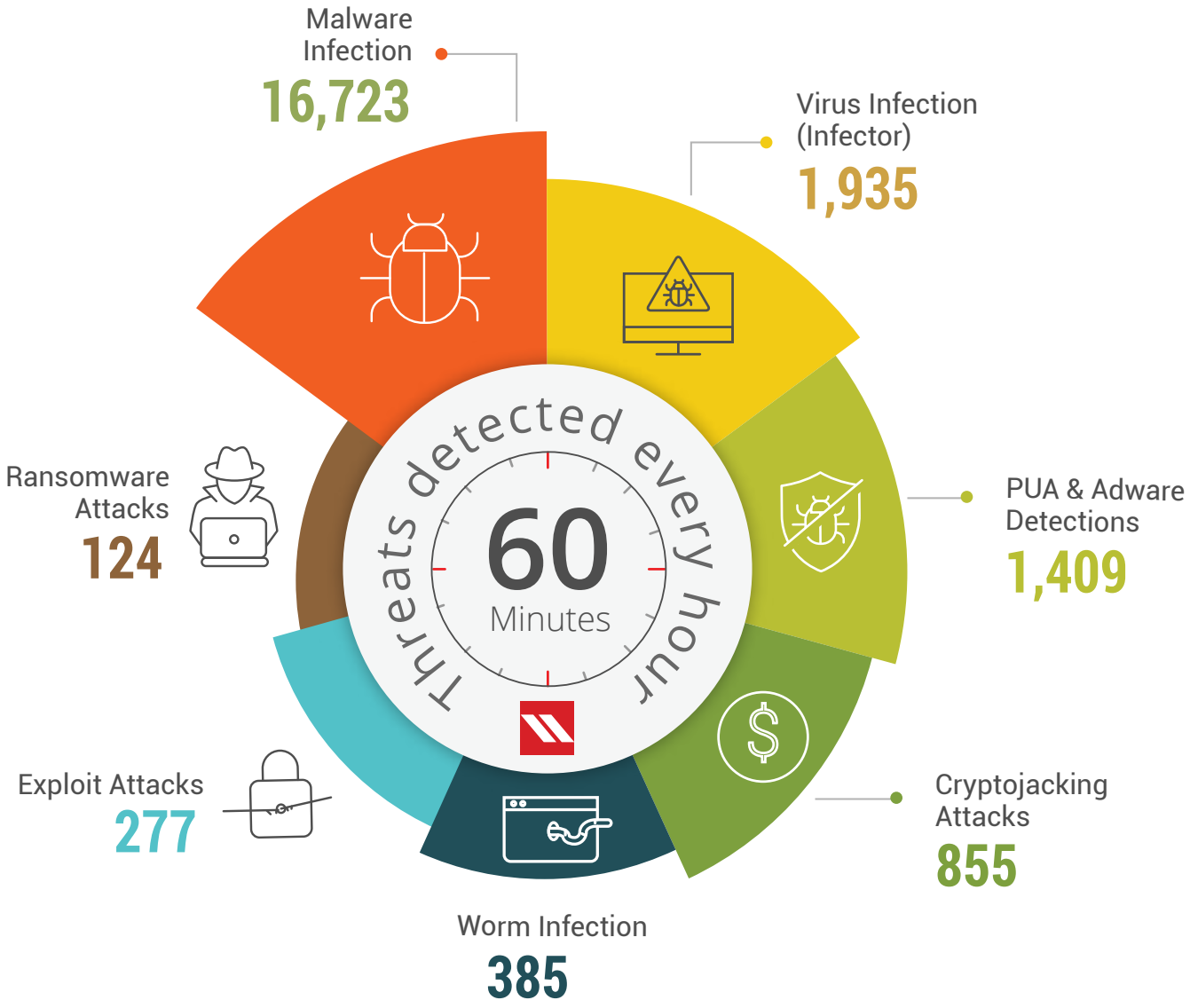
A leading source of threat research, threat intelligence and cybersecurity, Quick Heal Security Labs analyses data fetched from millions of Quick Heal products across the globe to deliver timely and improved protection to its users.

www.seqrite.com

Follow us on:

WINDOWS MALWARE

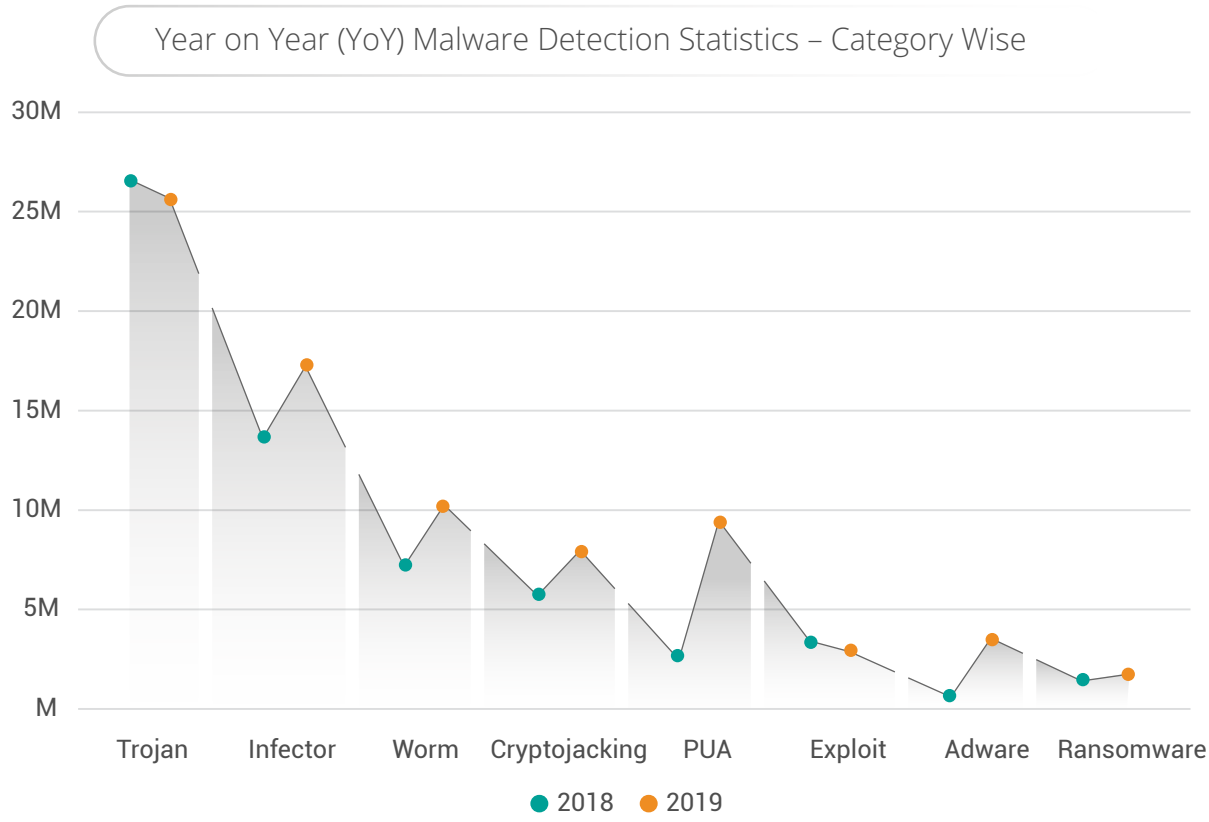
Hourly Malware Detection Highlights* for 2019



*Top six malware categories featured in the chart

Year on Year (YoY) Malware Detection Statistics – Category Wise

The graph below represents year on year (YoY) category-wise malware detection statistics.

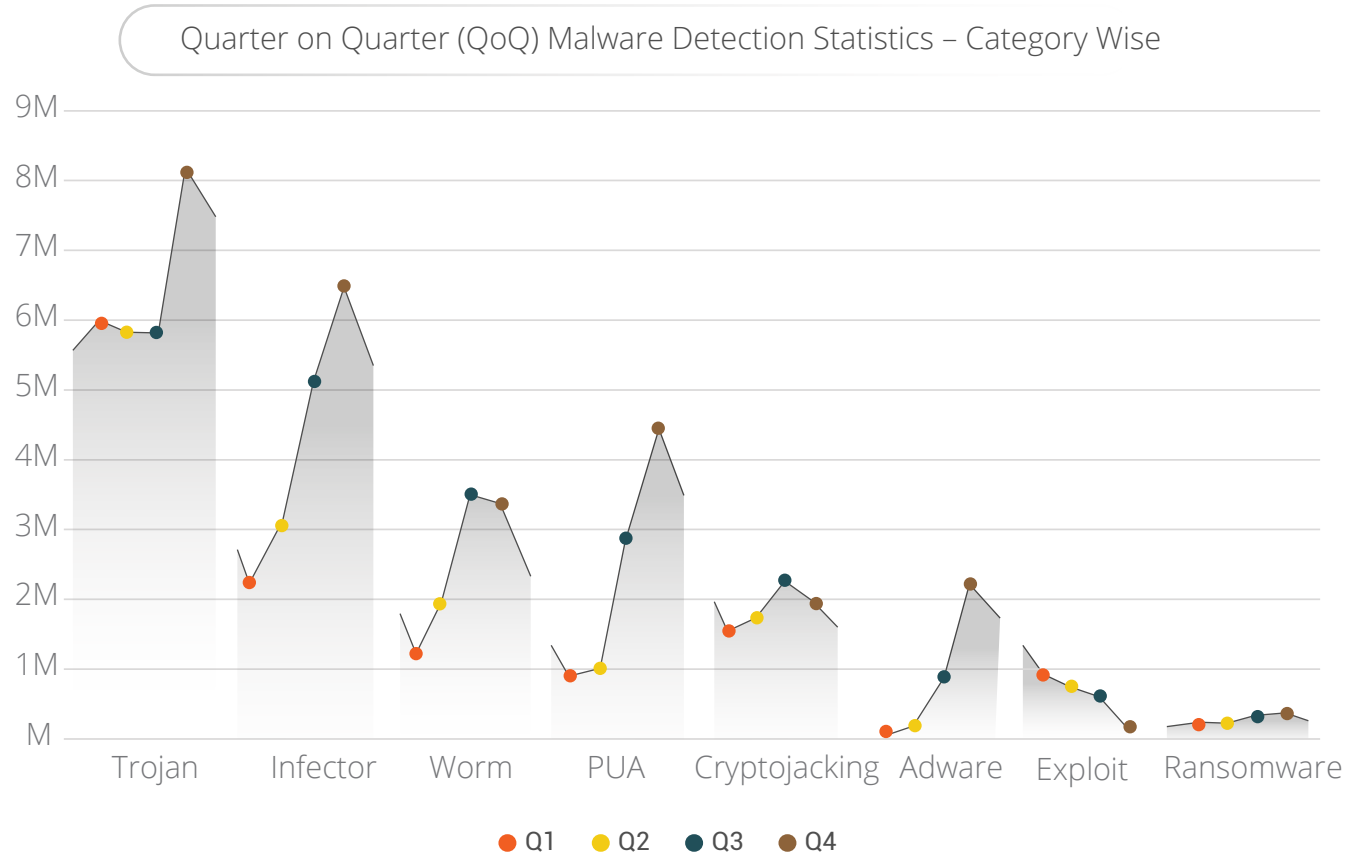


Observation

Trojan was the highest detected malware across 2018 & 2019 indicating its popularity with cyber attackers.

Quarter on Quarter (QoQ) Malware Detection Statistics – Category Wise

The graph below represents quarter on quarter (QoQ) category-wise malware detection statistics for 2019.

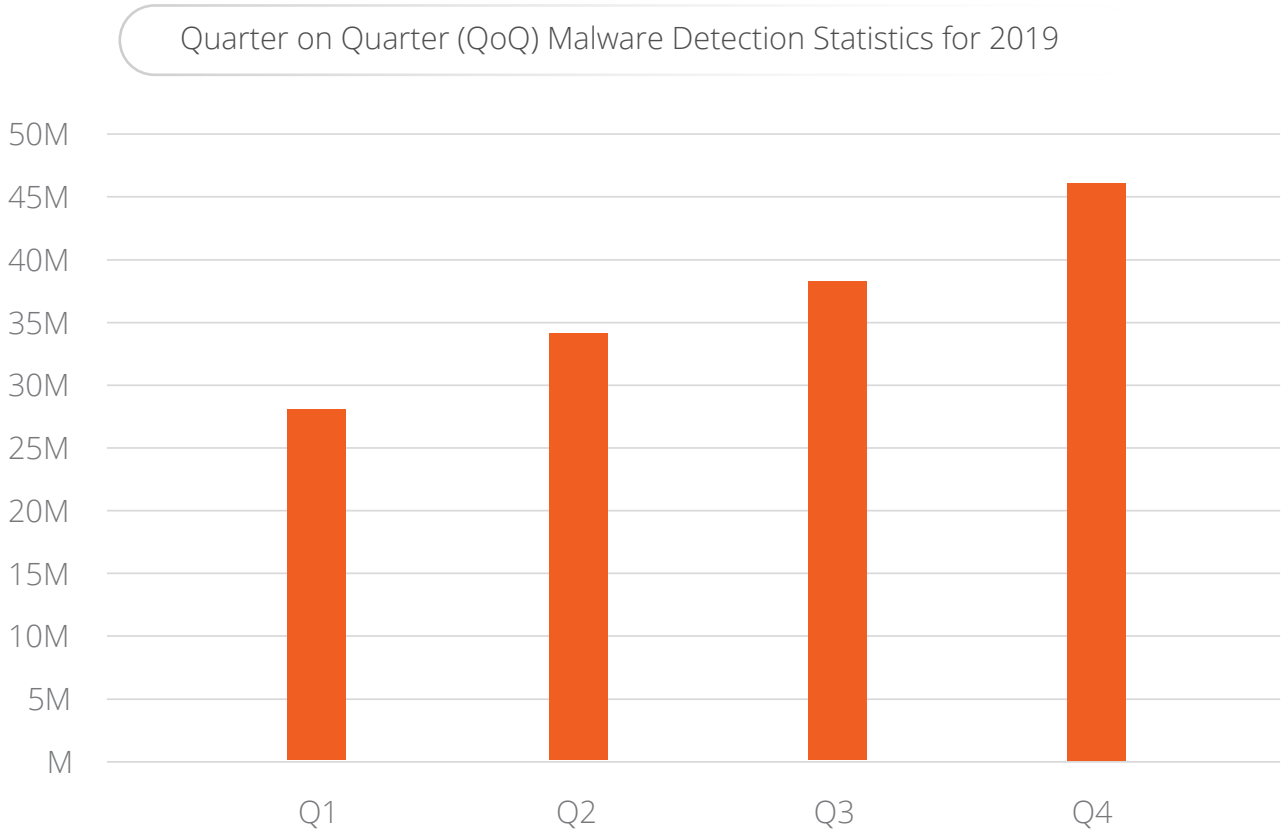


Observation

The Trojan malware dominated throughout 2019 causing maximum damage to enterprises worldwide.

Quarter on Quarter (QoQ)
Malware Detection Statistics for 2019

The graph below represents quarter on quarter (QoQ) malware detection statistics for 2019.

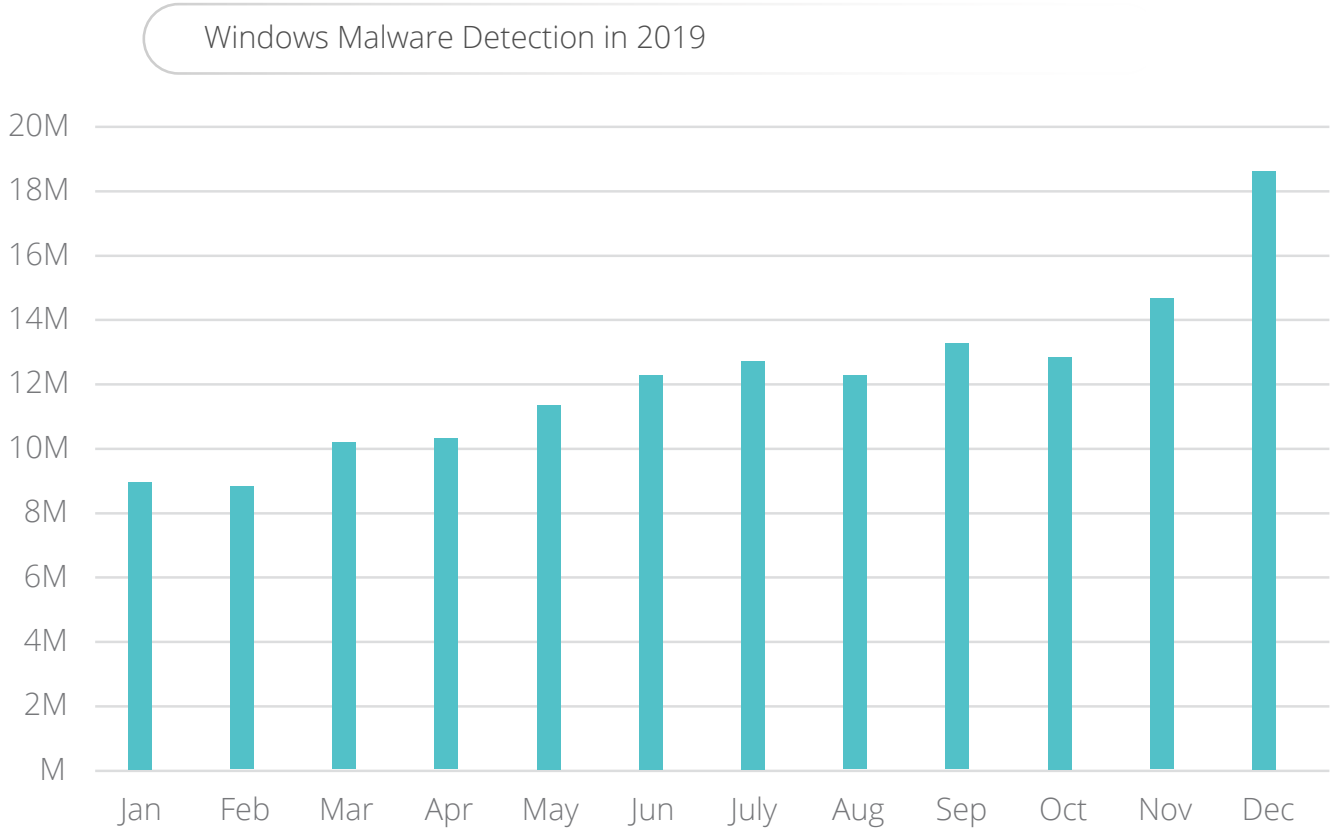


Observation

Seqrite detected over 146 million malware in 2019.
Q4 - 2019 clocked the highest detection of malware at 46 million.

Monthly Malware Detection for 2019

The graph below represents monthly malware detection for 2019.

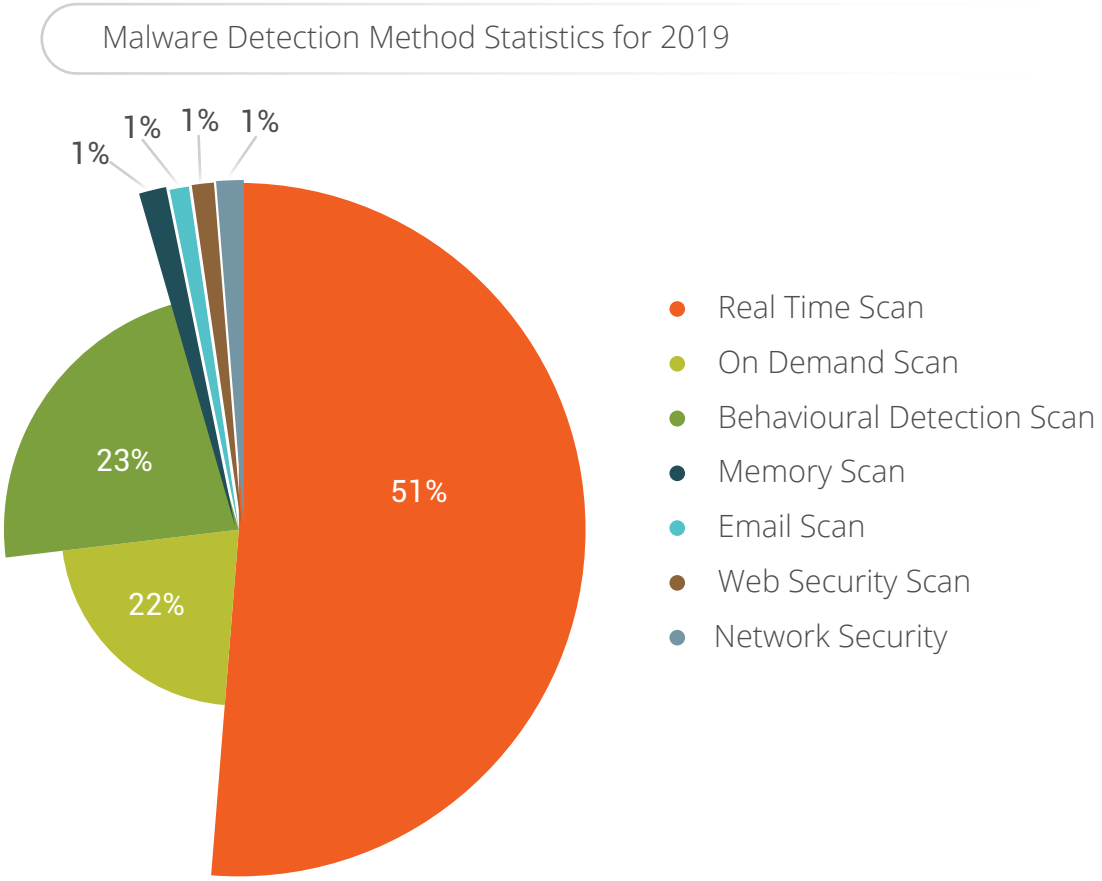


Observation

December 2019 saw maximum malware attacks.

Malware Detection Method Statistics for 2019

The chart below represents the malware detection method statistics for 2019.



Observation

Maximum malware were detected by the Real-Time Protection methodology for 2019. Behaviour-based malware detection technology was responsible for 23% signature-less detection in 2019

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

Real-Time Scan

Real-time scan checks files for malware on every instance.

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.

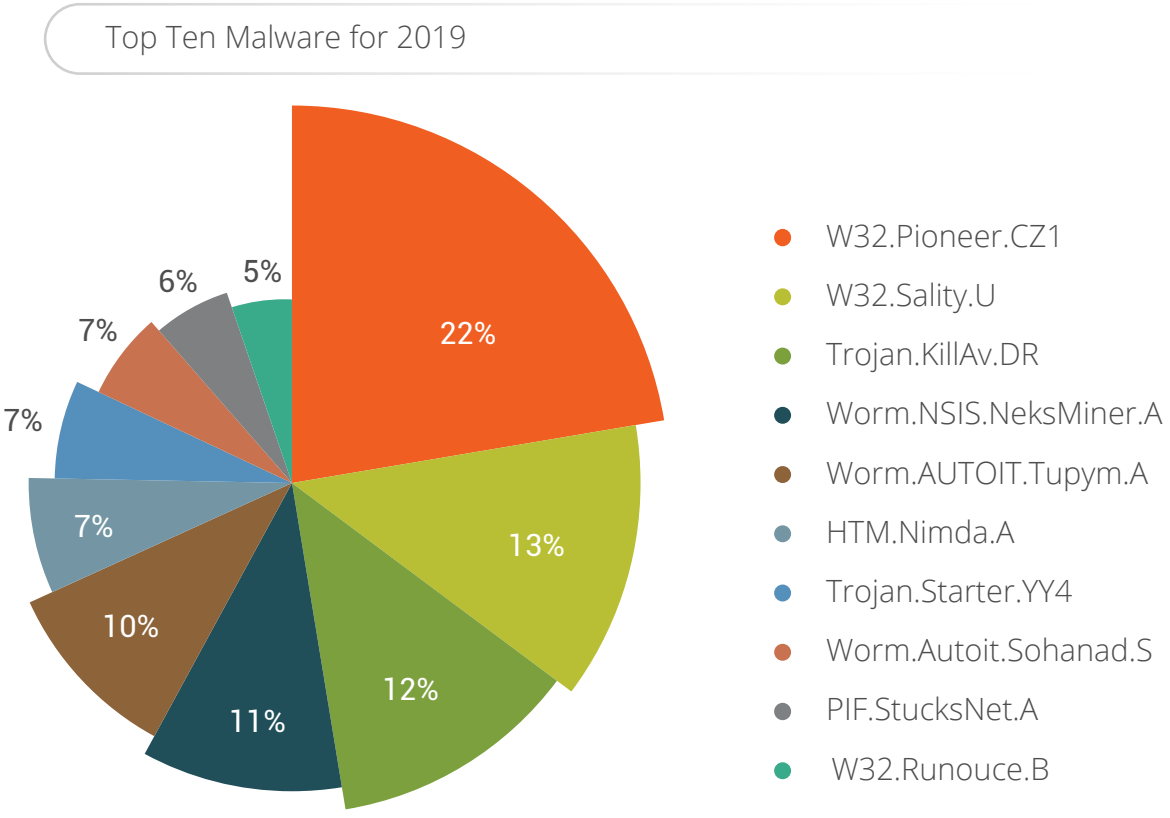
Web Security Scan

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 malware from penetrating enterprise systems.

Top Ten Malware for 2019



Observation

The W32.Pioneer.CZ1 malware were detected the most on business endpoints in 2019.

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. 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.

3. 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 or 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 almost always has icons like genuine Windows applications

4. Worm.NSIS.NeksMiner.A

Threat Level: High

Category: Worm

Method of Propagation: Removable or network drives

Behaviour:

- This malware drops multiple copies of self at %APPDATA% location.
- It does coin mining activities and increases CPU usage.
- It modifies the 'Run' registry entry to achieve persistence.
- Drops with filenames like 'images.scr' and 'DOC001.exe'

5. Worm.AUTOIT.Tupym.A

Threat Level: Medium

Category: Worm

Method of Propagation: Malicious links in instant messenger

Behaviour:

- Malware drops file in system32 folder and executes it from the dropped location.
- It connects to a malicious website, also modifies start page of browser to another site through registry entry. It also creates Run entry for same dropped file for persistence.

6. HTM.Nimda.A

Threat Level: Medium

Category: Worm

Method of Propagation: Spreads through emails

Behaviour:

- The worm spreads by sending email attachments with the name 'README.EXE'
- It exploits CVE-2001-0154 by setting unusual MIME header type to HTML email containing the executable attachment.

7. 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.

8. 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 has the ability to 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 due to which it spreads over the network.
- It infects every connected USB drive too.

9. PIF.StucksNet.A

Threat Level: Medium

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.

10. 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'

Top Ten Network-Based Exploits for 2019

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).

The table below represents the top ten network-based exploits for 2019.

Top CVE	Hits
CVE-2017-0144	7,30,107
CVE-2017-0147	1,16,498
CVE-2017-0146	2,367
CVE-2017-0143	1,108
CVE-2017-5638	334

Top CVE	Hits
CVE-2015-8562	79
CVE-2015-1635	61
CVE-2008-4250	26
CVE-2017-9791	15
CVE-2017-9073	5

CVE-2017-0144 is an Integer overflow vulnerability in SrvSMBOS2FEAListSizeToNT function srv.sys. The vulnerability occurs when srv.sys parses the received FEA list to convert it into NtFeaList format, during which wrong typecasting of a WORD into DWORD is done. The Eternalblue exploit uses the vulnerability to perform remote code execution in Windows SMBv1.

CVE-2017-0147 is an information disclosure vulnerability in SrvPeekNamedPipe function of srv.sys. This was used in EternalRomance exploit for leaking memory addresses. Fix of this vulnerability is utilized by vulnerability scanners to identify if the security patch of MS17-010 patch has been applied or not.

CVE-2017-0146 is a race condition vulnerability in how SMBv1 handles transaction requests. EternalChampion exploit triggers this vulnerability twice, once for info leak and later for code execution.

CVE-2017-0143 is a type confusion vulnerability between WriteAndX and Transaction requests. EternalRomance and EternalSynergy used this vulnerability for performing code execution.

CVE-2017-5638 is an Apache Struts remote code execution vulnerability in Jakarta Multipart parser triggered during improper handling of a file upload. Arbitrary commands are sent through a crafted Content-Type HTTP header.

CVE-2015-8562 is a Joomla HTTP Header Unauthenticated Remote Code Execution vulnerability.

CVE-2015-1635 is an Integer Overflow Vulnerability in HTTP.sys, allowing remote attackers to execute arbitrary code via crafted HTTP requests.

CVE-2008-4250 is a Server Service Vulnerability allowing remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization. This vulnerability was used in the famous Conficker worm.

CVE-2017-9791 is an Apache Struts1 vulnerability allowing remote code execution via a malicious field value passed in a raw message to the ActionMessage.

CVE-2017-9073 is a buffer overflow in Smart Card authentication code in gpkcsp.dll. It allows a remote attacker to execute arbitrary code on the target computer which has Remote Desktop Protocol connectivity (or Terminal Services) enabled.

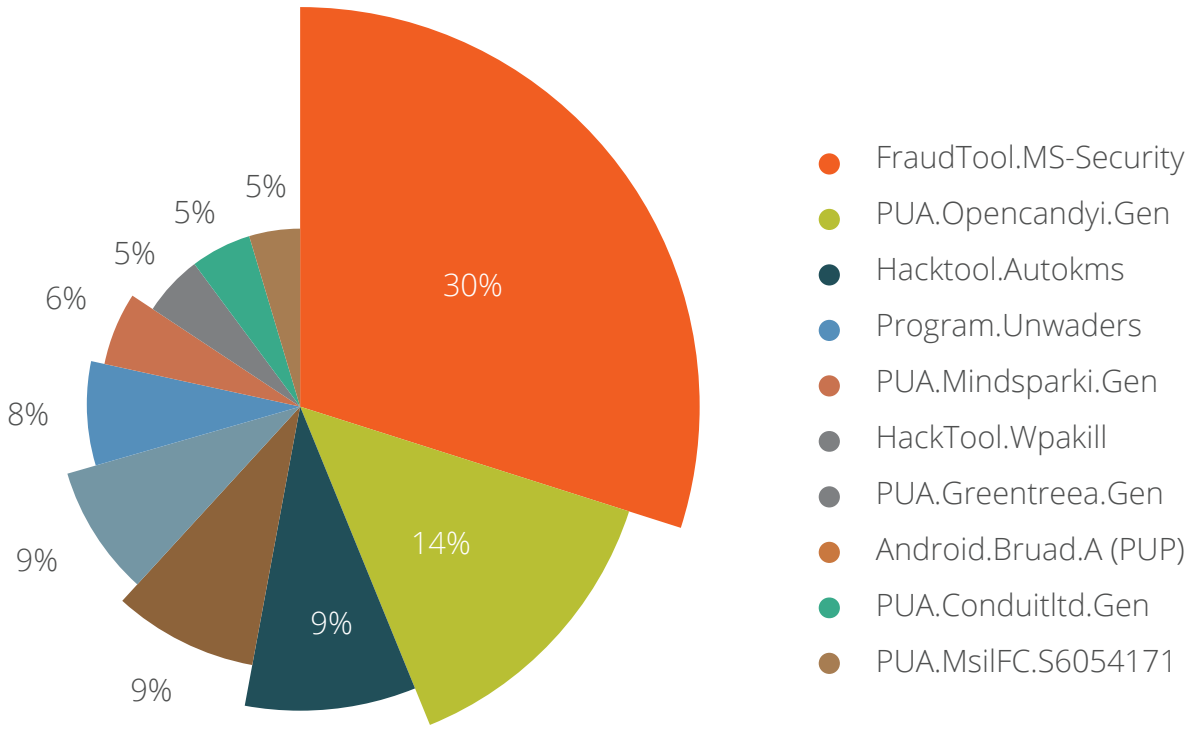
Observation

The CVE-2017-0144 was the most detected network-based exploit for 2019. This is the vulnerability which was used by the most infamous ransomware, WannaCry.

Top Ten Potentially Unwanted Applications (PUAs) and Adware in 2019

Potentially Unwanted Applications (PUAs) are programs that are not necessarily harmful but using them might lead to security risks.
Adware are software are used to display ads to users - some are legitimate while some are used to drop spyware that steals user information.
The chart below represents the top ten PUAs and Adware detected in 2019.

Top Ten Potentially Unwanted Applications (PUAs) and Adware in 2019

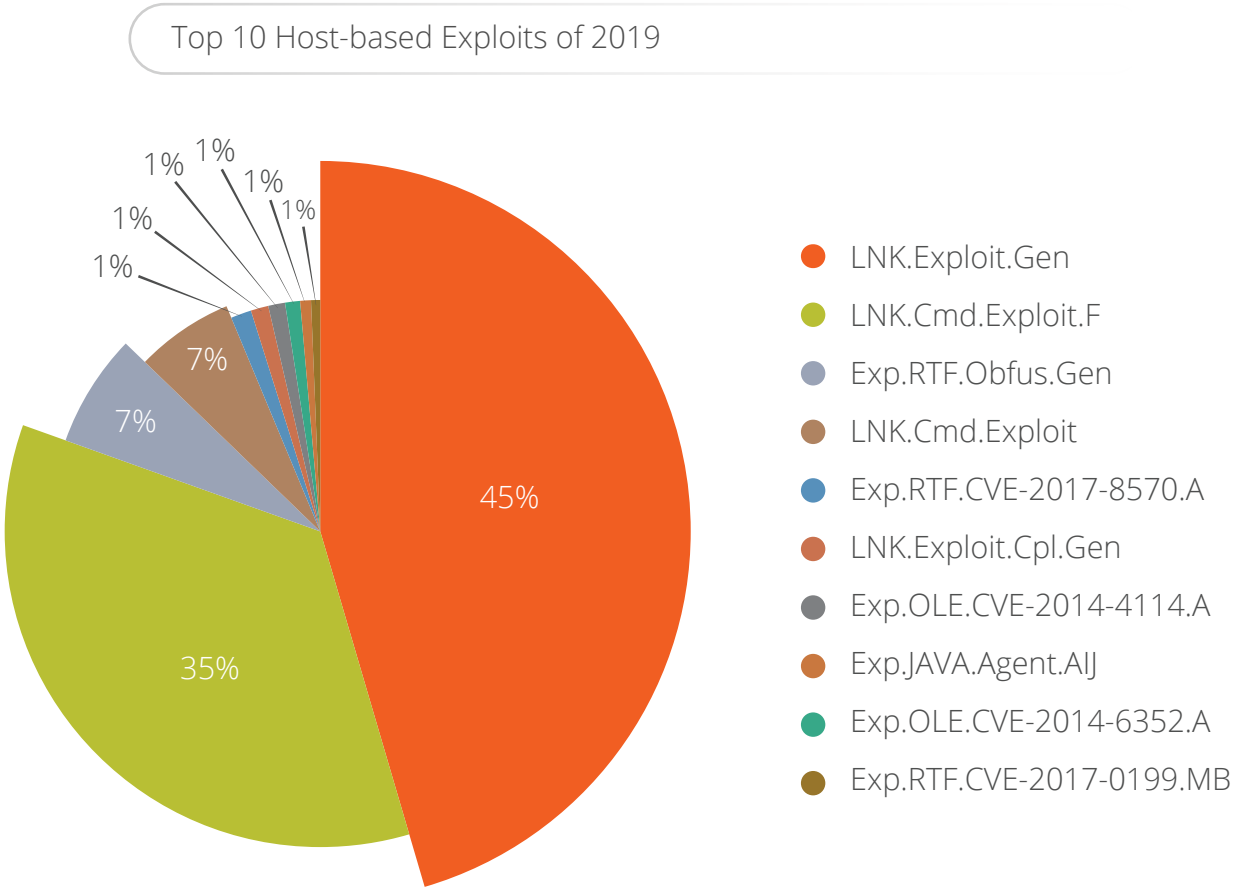


Observation

FraudTool.MS-Security was the most potentially unwanted application for 2019.

Top Ten Host-Based Exploits of 2019

A computer exploit is an attack designed by a hacker to take advantage of a particular security vulnerability the targeted system has. The chart below represents the top ten Host-Based exploits of 2019.

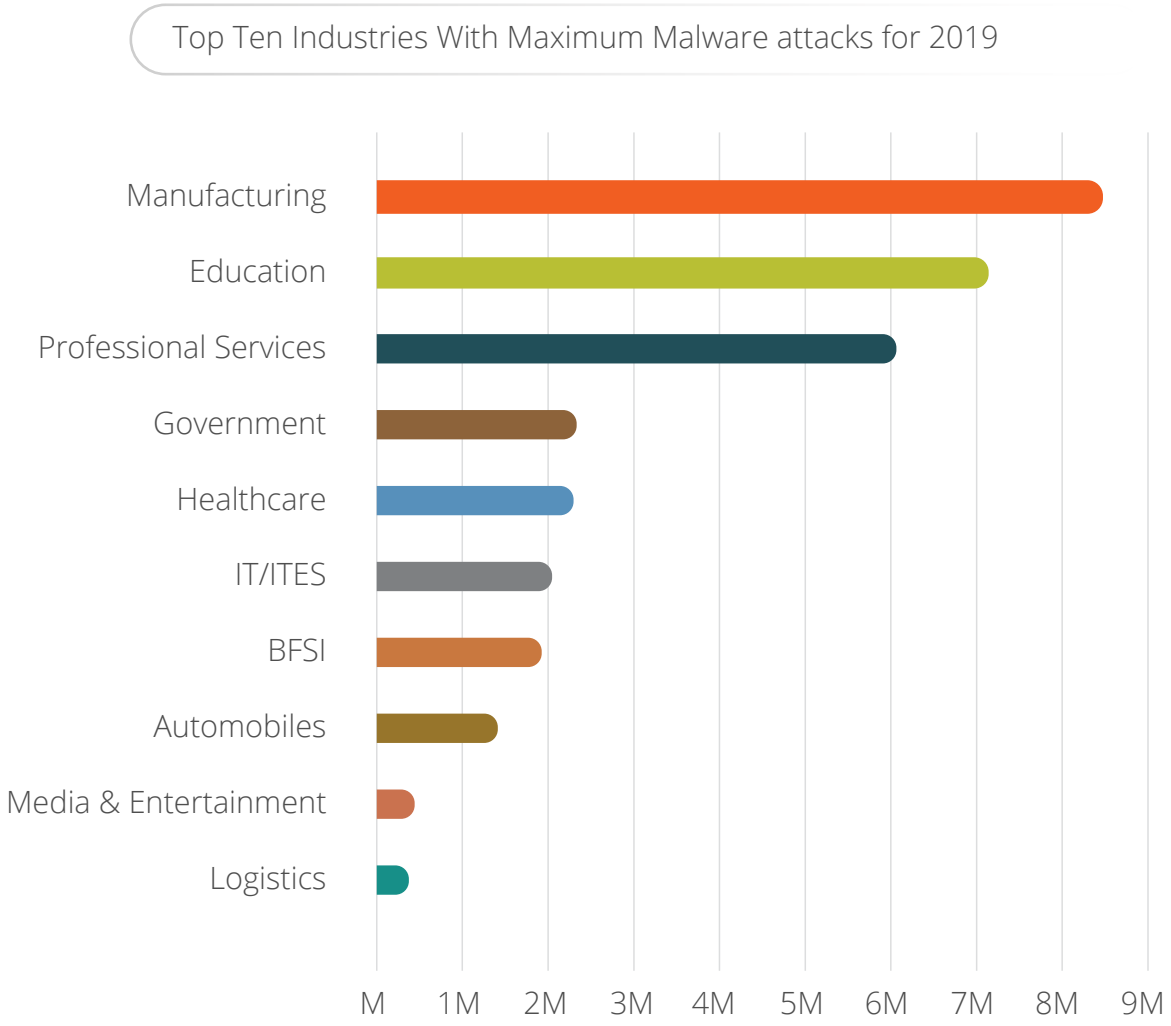


Observation

LNK.Cmd.Exploit.F was the worst host-based exploit for 2019.

Top Ten Industries With Maximum Malware attacks for 2019

The chart below represents the top ten industries with maximum malware attacks for 2019.



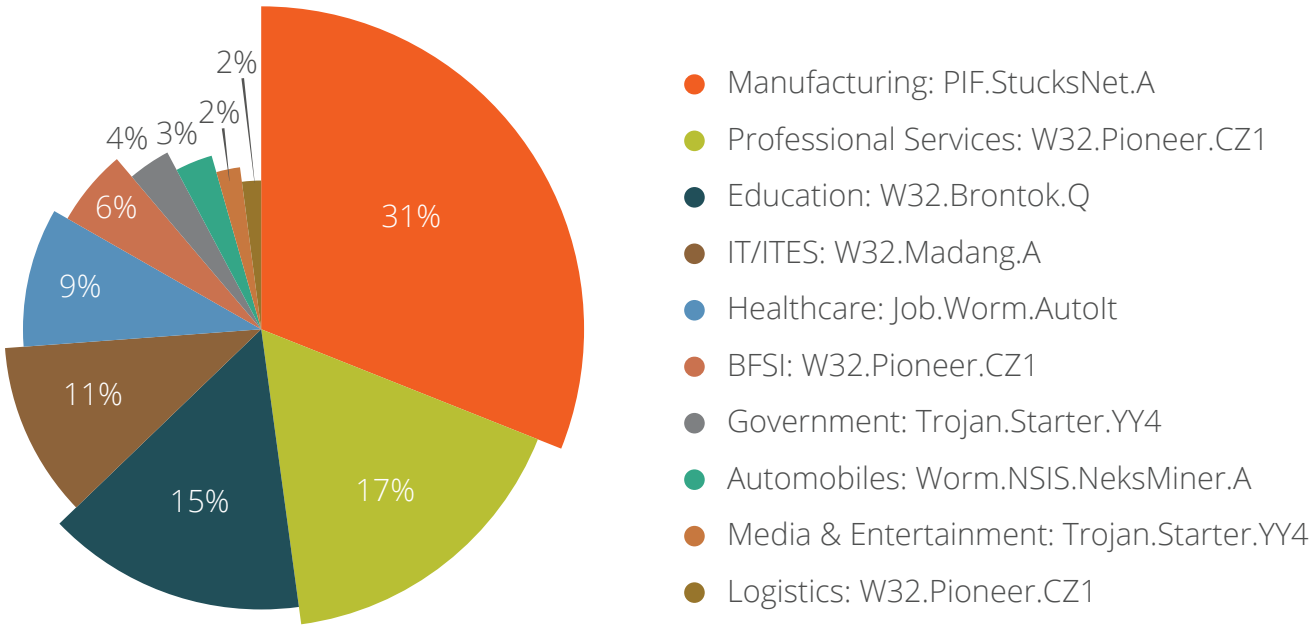
Observation

The manufacturing industry was the worst hit by malware in 2019.

Top Ten Industry-Wise Most Prevalent Malware in 2019

A list of ten industries and the respective malware that attacked these industries the most.

Hits



Observation

The manufacturing industry which was the worst hit by malware in 2019, was most affected PIF.StucksNet.A

Top Ten Commonly Found Malware File Names in 2019

A list of ten industries and the respective malware that attacked these industries the most.

These were the most common file names found in our detections throughout 2019.

1.	KMS-R@1n.exe
2.	clean.exe
3.	autorun.inf
4.	svchost.xml
5.	Service_KMS.exe
6.	SECOH-QAD.dll
7.	autorun.inf
8.	SECOH-QAD.exe
9.	DriverPackNotifier.exe
10.	DOC001.exe

Trends in Windows Security

1 Top Microsoft Office vulnerabilities used by cybercriminals

Malware authors have been using various MS Office exploits in malspam campaigns to deliver malware like key-loggers, info-stealers, banking trojans, RATs, etc. Here is a list of few prominent vulnerabilities affecting different MS Office versions used by cybercriminals.

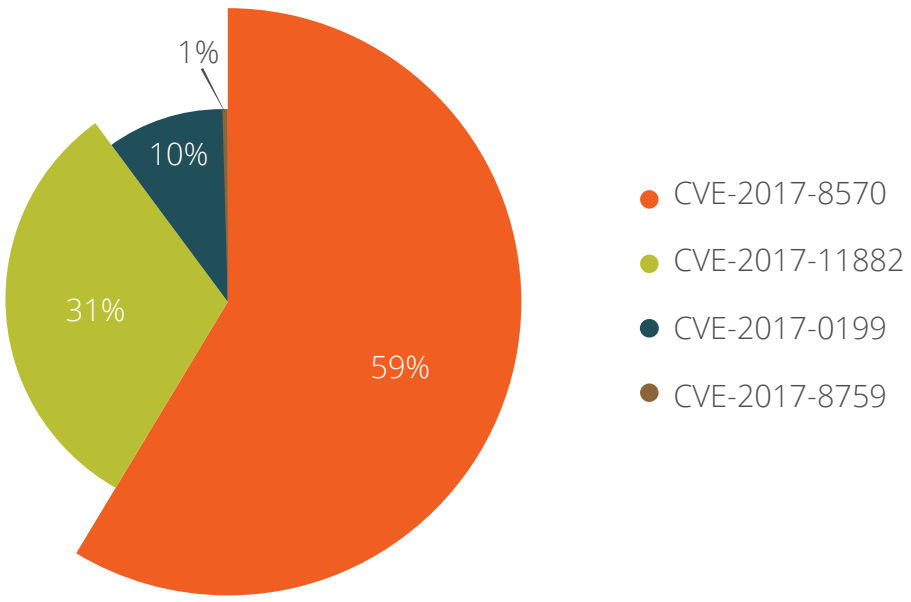
CVE-2017-8750 is a remote code execution vulnerability present in Microsoft Office due to improper handling of objects in memory. By tricking a victim to open a crafted document, the attacker can execute arbitrary code on the system with high privileges.

CVE-2017-0199 is a vulnerability that triggers due to the improper handling of an HTA file while parsing a crafted RTF file having an embedded OLE2 link object. Attackers use crafted RTF files with doc extension to exploit this vulnerability.

CVE-2017-11882 is a stack-based buffer overflow vulnerability present in Equation Editor component of MS Office. An attacker can successfully exploit this vulnerability which allows remote code execution on a victim's machine.

CVE-2017-8759 is a remote code execution vulnerability in the SOAP WSDL parser of .NET framework. Malspam campaigns make use of malicious RTF file as an attachment for exploiting CVE-2017-8759 to deliver info-stealer malware.

Below chart shows percentage-wise detection stats of MS Office exploits blocked by Seqrite:



This shows the lax attitude of users towards applying security patches considering that Microsoft has provided these for all vulnerabilities. There are many users who still haven't applied the security patches leaving the systems vulnerable to attacks.

2. Open-source tools assist in the success of popular malware campaigns in 2019

Emotet, an advanced banking trojan, that primarily functions as a downloader or dropper for other banking trojans, was one of the most successful malware campaigns of this year. We tracked it throughout the year to validate our detections - we also have been tracking Phobos ransomware, the implementation of which was very similar to that of Dharma ransomware. One common thing which we noticed across these campaigns is the use of open-source tools to carry out certain tasks.

Nirsoft has a unique collection of Freeware desktop utilities, command-line utilities, network monitoring tools and password recovery tools. All these tools are freeware and used for genuine purposes, but malware authors use them for malicious purposes.

Emotet used few modularized components utilizing the following Nirsoft tools:

MailPassView is a small password-recovery tool that reveals the passwords and other account details for various email clients like Outlook Express, Microsoft Outlook, Gmail, Yahoo! Mail, etc.

WebBrowserPassView is a password recovery tool that reveals the passwords stored by Web browsers like Internet Explorer, Mozilla Firefox, Google Chrome, etc.

A recent analysis of Phobos ransomware reveals that it has used 12 Hack Tools out of which 7 are from Nirsoft, and few are from opensource tools available in GitHub to dump credentials from memory, like Mimikatz.

These supporting tools are created with good purpose, but their association with malware campaigns have posed a challenge for the cybersecurity industry pertaining to classifying them as riskware.

3. Ransomware Attacks on Government Bodies

Ransomware attacks can turn out to be a nightmare for an individual or an organization storing crucial data. This year, the security industry saw a sudden rise in cases of targeted ransomware attacks on municipal corporations and government bodies across the globe demanding huge ransoms in the form of bitcoins.

In the second quarter of 2019, the Baltimore city government was attacked, infecting multiple systems. According to the ransom note retrieved, it was the 'RobinHood' ransomware which demanded around $75,000 in ransom. Subsequently, the Municipal Corporation of Lake City

(Florida) was infected which unfortunately locked down the city's email and servers. The hackers demanded 42 Bitcoins which approximately sum up to $300,000.

The City of New Bedford also faced one of the highest ransom demands at more than $5 Million. The infamous Ryuk ransomware which has been infecting various large organizations this year was said to cause this mess. Additionally, in November, the state government of Louisiana was also hit by ransomware which adversely impacted multiple services like websites of the Office of Motor Vehicles, the Department of Transportation and Development and many more. Fortunately, the government had maintained backups through which they could restore their data back. In another case in the same month, the systems connected to 'LiveScan fingerprint-tracking' system of NYPD were infected by the 'Thwart' ransomware. This was caused due to a human error of connecting an external device to the internal network while installing new hardware.

Most of these organizations refused to pay ransom to hackers even though the cost of recovery was more than the ransom amount itself. However, Lake City officials voted in favour of paying 42 Bitcoin to hackers. But paying to ransomware authors and hackers will only promote these kinds of attacks, which is not ethical. In the attacks above, infection vectors varied from external devices and spam emails to simple human errors. The organizations which had backups faced less downtime and were back to their operations within a few days.

This empathizes the need of following security best practices, maintaining data hygiene, using proper security solutions and data backups.

4. BlueKeep Attacks seen in the wild!

RDP is Remote Desktop Protocol, typically used for taking remote control of a Windows machine. For most of the home users, RDP functionality is not required. It's typically used in offices for accessing remote hosts.

CVE-2019-0708, popularly known as BlueKeep, is an RDP pre-authentication vulnerability which allows an attacker to compromise a vulnerable system without user's interaction. This exploit is also wormable, meaning that it can spread to other vulnerable systems in a similar way as the WannaCry malware spread across the globe in 2017. Interestingly, healthcare products like radiography, X-ray and other imaging software of various healthcare vendors running on Windows OS are also affected by the BlueKeep exploit. Since the time this vulnerability was patched by Microsoft, multiple PoCs exploiting it have emerged in public. In September, exploit code for this vulnerability was added in the popular exploitation framework, Metasploit for triggering DoS. Chances are that script kiddies would jump on this Metasploit module to carry out large scale attacks on vulnerable hosts with RDP port open to the Internet. Recently, attackers exploited this vulnerability for dropping cryptocurrency miner on the unpatched vulnerable machines.

5 Insecure Remote Desktop & SMB

Quick Heal Security Labs observed continuous attack using RDP and SMB brute force. Criminals look for unsecured RDP, SMB services to exploit and access enterprise networks. Ransomware like Dharma, CrySis distributed through hacked RDP or SMB share by brute-forcing. Remote Desktop Protocol (RDP) is widely used for remotely were connecting to Windows systems, whereas, Server Message Block (SMB) Protocol is a client-server communication protocol used for sharing access to files, printers, serial ports and other resources on a network.

Brute Force Attack: A brute force attack is a trial-and-error method used to retrieve critical information such as usernames and passwords. A brute force attack is generally carried out through automated scripts.

RDP Brute Force Attack: The Remote Desktop Protocol (RDP) running on default port 3389 - by brute-forcing the user credentials to access the RDP on a victim's machine, attackers can uncover usernames and passwords. Once credentials are obtained, the attacker gets the ability to carry out any type of attack.

SMB Brute Force Attack: The Server Message Block (SMB) Protocol running on port 445, is targeted with a typical brute force attack using Metasploit. As a result of the brute force, the attacker gets a reverse Meterpreter shell. Then the attacker can create a new user with administrative rights on the victim's machine. Once the attacker creates a user, he gets the ability to carry out any type of attack.

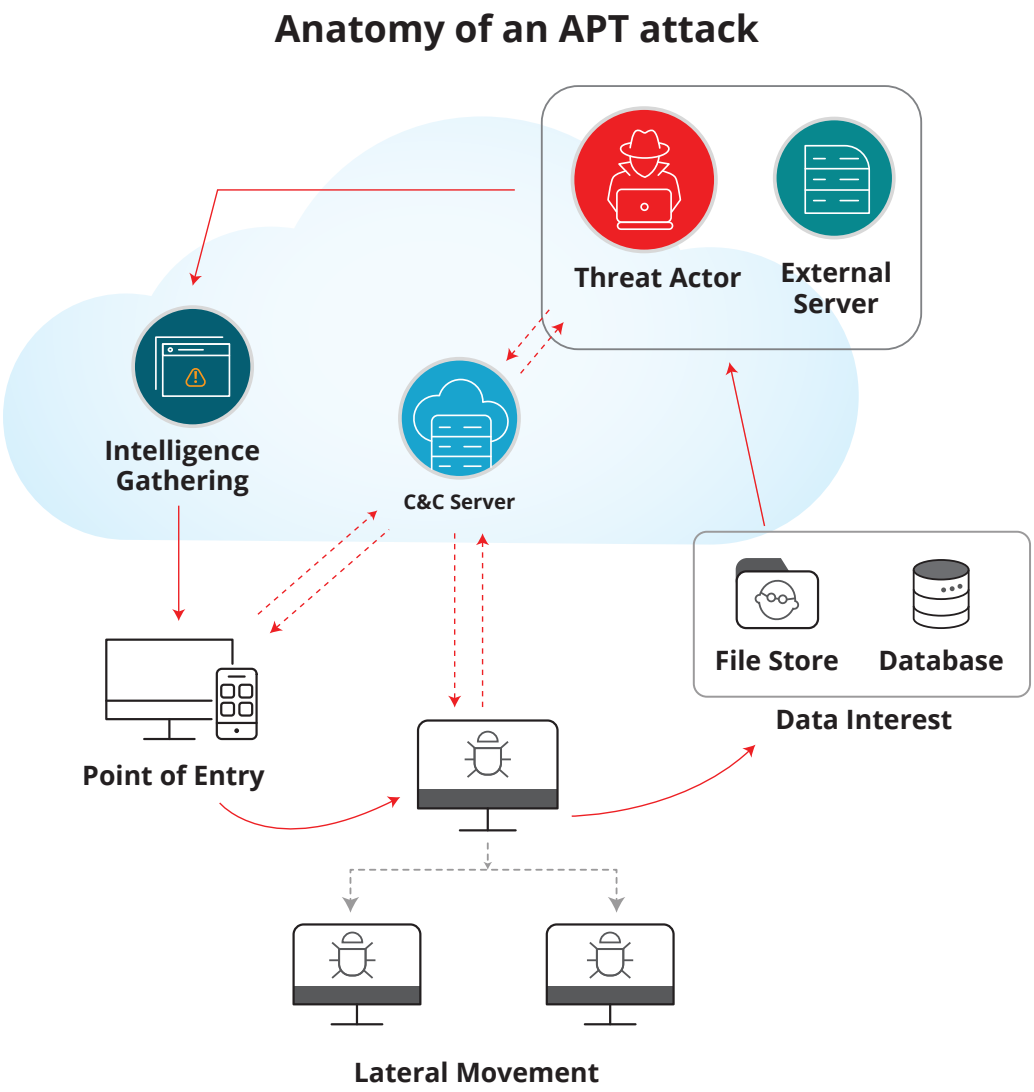
Many organizations fail to secure RDP services against unauthorized access. It is strongly advised to protect it by setting up appropriate configuration (For Eg. Firewall, Do not keep RDP over Public Network). Keep Operating System up to date, along with setting up a complex password - password expiration & account lockout policies should also be implemented.

Most importantly critical data has to be backed up.

Advanced Persistent Threats

Advanced Persistent Threats (APTs) are an elite breed of cyberattacks designed to infiltrate high-value targets important to national governments such as the military, power grids, nuclear plants etc. The motive of these attacks is to stay undetected for a long period of time in order to monitor and steal extremely sensitive information, the leak of which may completely ruin its stakeholders. These threats become all the more dangerous as, in almost all cases, they are custom-made by highly skilled individuals using tools usually not available commonly in the cybersecurity sphere. Typically, Nation-States design APTs in order to wage cyber warfare against enemy nations in order to either outsmart them or extract Government secrets.

To further explain how APTs typically work, here is a quick infographic –



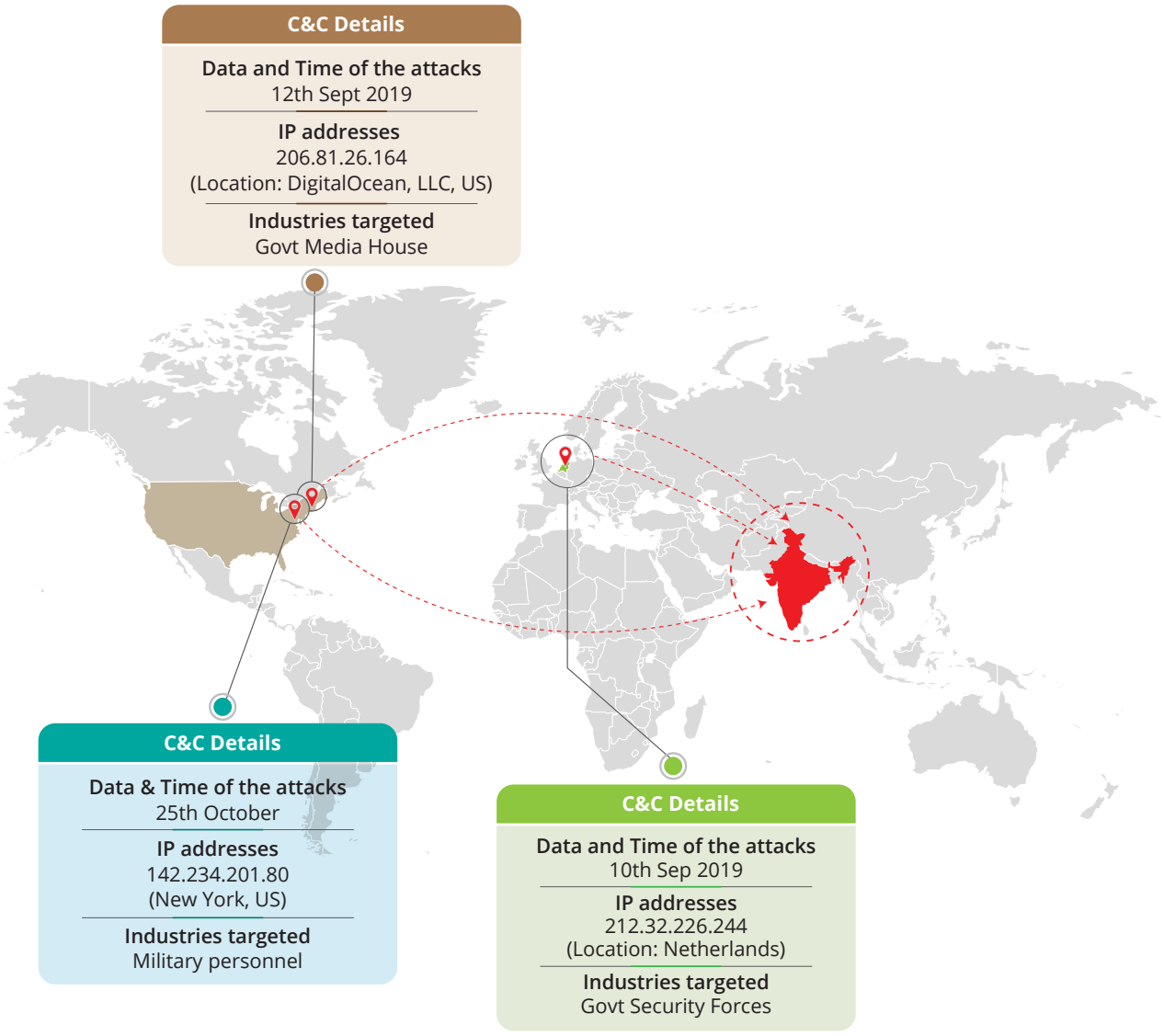
The Indian subcontinent has been a victim of such attacks. During the current year, Quick Heal Security Labs has been monitoring APT campaigns against some important Indian government organizations known as Operation m_project. We are covering two stories, the first targeting vital Indian Government organizations & the second, an attack on a Nuclear Power Plant. The stories present interesting insights into how dangerous APTs are.

1. Operation m_project:

Operation m_project is a long-running cyber-espionage campaign against the Indian Government organizations since 2015 and is very similar to ***Operation Transparent*** Tribe. We suspect that attackers are based in Pakistan as per Threat Intelligence and ***Security Blogs***.

We have published our research related to this campaign in March 2016.

From the past few months, this campaign has become widely active, targeting critical government organizations in India.



*These were the CnC Server locations at the time of attacks. However, we are not validating that the attackers were from the aforementioned countries.

Attack on Government organizations

In this attack, the victim receives a spear-phishing email with a malicious link/attachment, which further downloads a macro-enabled malicious XLS file. When the victim opens the file and clicks on the 'enable macros' button, a VBA code gets executed and drops a .zip file which further extracts and launches a .NET PE file. This executable has several functions like capturing screenshots, gathering running process information, OS and system information -this data is sent to a C2 server.

We have noticed a huge difference in the usage of exploits by cyberattackers. Glance at the graphic real quick for an idea about the same.

Exploits in use previously	Exploits in use currently
CVE-2012-0158	**VBA Macro**
CVE-2010-3333	

These exploits have most often been projected via spear-phishing attacks.

The ultimate motive of this operation is information and data gathering from important Indian entities.

Mentioned below are a few common file names -

1. Fauji India September 19.xls
2. PMAYCLSSMIGSeptember201920.xls
3. PradhanMantriAwasYojana76487.xls
4. Program.xls
5. NHQ Notice File.xls

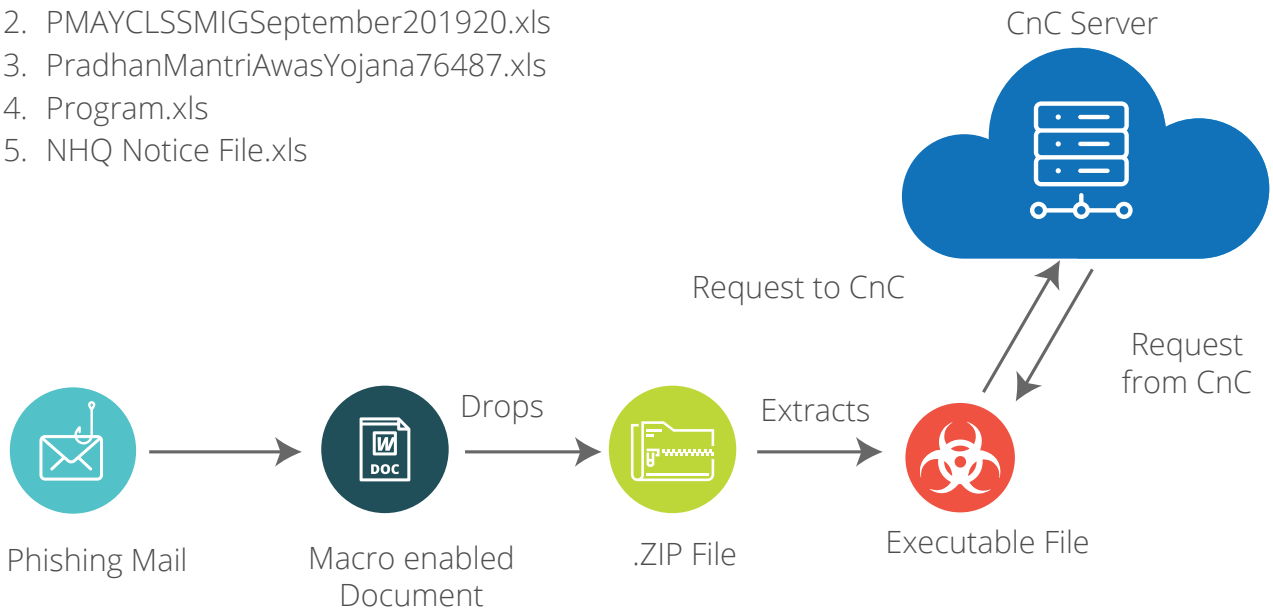


Fig.1: Attack chain

Targeted Sectors:

1. Defence Organizations
2. Government Media Houses
3. Protection and Security Organizations

2. Deciphering the targeted attack on a Nuclear Power Plant and other critical sectors in India

The alleged cyber-attack on a Nuclear Power Plant in India this year was widely discussed in the researcher community as well as online media, making cybersecurity of critical infrastructure the talk of the town.

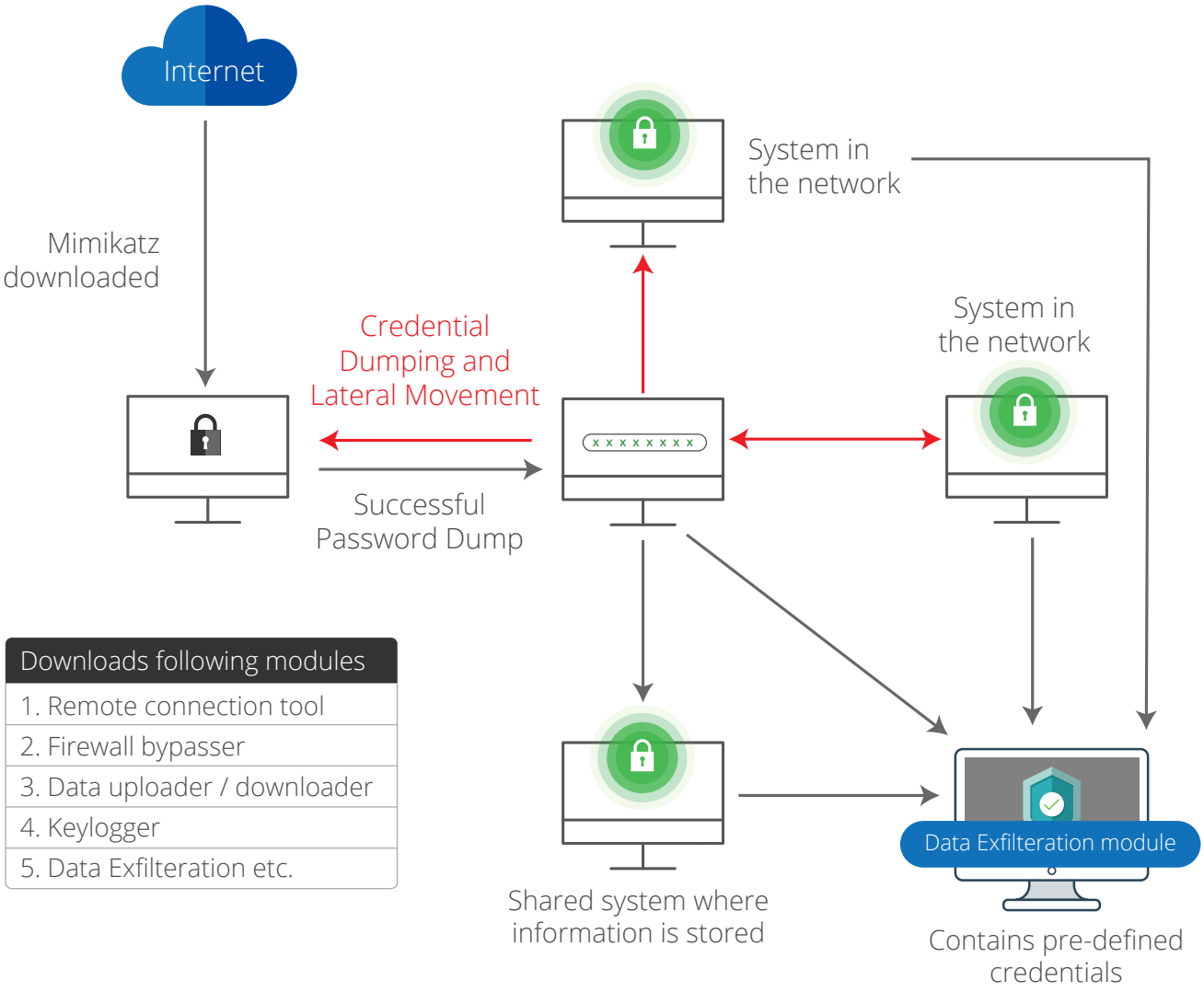
The officials mentioned in their statement that there was no damage to control systems of the plant. However, the incidence raises huge questions on the security aspect of critical national infrastructure. Quick Heal Security Labs also observed some attacks on employees of some reputed research centers in India.

Security Labs analyzed the samples claimed to be related to this targeted attack and tried to build a modus-operandi of it, by co-relating different samples and their usage. The malware sample widely reported online and available on VirusTotal, seems to be a variant of Backdoor.DTrack family, which is known for carrying out cyber-attacks on financial and research institutes in India.

It is alleged that infamous Lazarus group from North Korea is behind this attack and North Korea has been interested in the thorium-based nuclear power to replace the uranium nuclear power. India is a leader in thorium nuclear power technology. It has also been observed that other critical sectors In India are also being targeted through individual users.

However, the important question is, how did this sample penetrate such a well-guarded network? One possible theory is of spear-phishing emails with a malicious office document as an attachment, which is a very common technique used in targeted attacks. Our analysis of all the Dtrack related samples leads to the following modus operandi of this cyber-attack. A system with access to the public network (Internet), may have been compromised, possibly through a spear-phishing attack that downloaded a password theft program, used in stealing credentials required for doing a lateral movement. Once it extracted the credentials for one computer in that network, it tried to gain access to other computers and possibly of the domain controller in that network. This claim is based on the hardcoded login credentials found in one of the samples available on VirusTotal.

Here is a flow-chart detailing possible modus operandi of this cyber-attack.



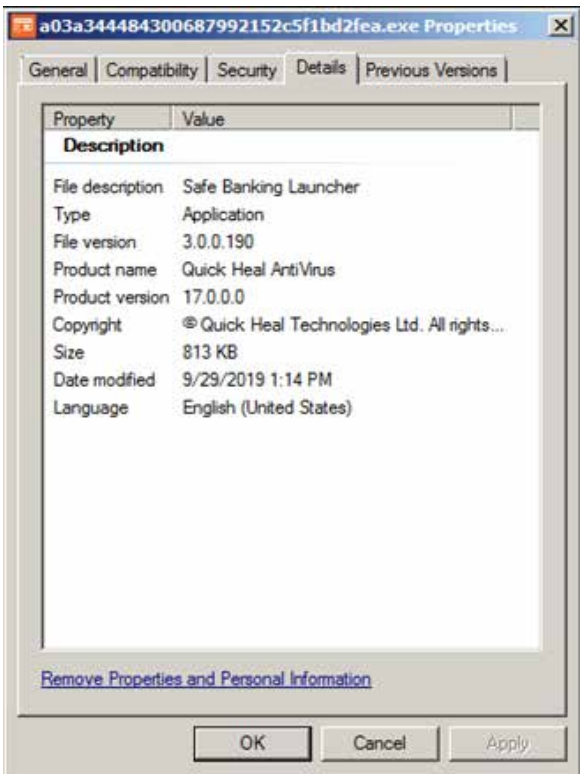
Once the malware has landed in the target system and gained the domain controller credentials, it could have further downloaded a few other components used in this attack for information stealing, keeping a persistent backdoor for remote administration and downloading other modules that are required to accomplish the attack. The main payload of the attacks seems to be an information collector. The information was gathered using different windows commands and APIs. The information consists of running processes, network information, system installation data, browser history, etc. All this information is stored in an archive format at a shared location in the network. There were different versions of the payload observed in the lab.

Another component in the attack uploads the data collected from different systems in the network to CnC servers. The server information was present in the module either in bare or encrypted form.

Following URLs were found in the memory where malware was trying to send the data.

hxxp://heromessi.com/wp-public/career/car_add.php	**[IP: 51.91.7.156, Roubaix, France]**
hxxp://hawai-tour.com/wp/wp-imgs/luxury/scenes/view.php	**[It redirects to above URL]**
hxxp://210.16.102.78:53/dns/query.php	**[Mumbai, India]**

Currently, the domains are not responding as they might have been taken down. Few antivirus vendors have categorized these URLs as malicious. The module also has the capability to receive some commands and download new payloads. The modules are extremely sophisticated to generate the logs for this activity. These logs would be very important in case it failed to perform some task. An interesting finding was that we observed a couple of variants to mislead users by imitating Quick Heal's Safe Banking Application's icon and version information. This file was not having digital certificate. This is a general tactic used by the attacker to lure the user to execute malware. Seqrite as well as Quick Heal successfully detect these files as Backdoor.Dtrack.



One of the important payloads of the campaign may be a keylogger. An MFC application inspired by a keylogging code shared on Github repo, grabs the key-strokes and clipboard data using multiple threads. All this data is then shared with the attacker using the data uploader/downloader component mentioned earlier. We have also found some samples that we suspect to be part of the campaign. Samples seem to be a patched variant of plink.exe file, which is a part of PuTTY utility. Plink is a command-line connection tool similar to UNIX `ssh'. It is mostly used for automated operations, such as making CVS access a repository on a remote server. Also, PuTTY is an SSH and Telnet client. This module is used to connect to the servers from current machine. A backdoor, which is generally known as part of Dtrack family, has the capability to stay hidden in the systems as a daemon and provide the bind shell to the remote attacker.

This attack has once again highlighted the importance of security of the Nuclear Power Plants and other critical infrastructures of India. The imitation of reputed software to gain trust, continues to be one of the favorite tricks used by attackers. Modular approach makes such campaign undetectable for several days. Though the research section is kept isolated, the attacks on administration can help attackers devise an intrusion plan in research centers as well.

Conclusion

The annual report encapsulates our previous three quarterly reports and builds on to it to project a larger picture about the modus operandi of cyberattacks for 2019. While Trojans represent a superset, ransomware, specifically, is still a large threat for organizations worldwide. This is likely to go down in 2020 as cybersecurity vendors emphasize the criticality of data-back ups. Ransomware attacks on data stored on the cloud may increase. Anti-Ransomware solutions cannot ensure 100 percent data recovery, hence enterprises should invest in a data-backup solution provider.

Attackers will be leveraging on Artificial Intelligence (AI) and its versatility to harness new attack vectors in 2020. Businesses and cyber thieves will continue outwitting each other with no clear winner in sight. Our Security Labs continues to observe the fact that enterprises are not taking steps to educate employees on the importance of cybersecurity.

Simple and often ignored attack surfaces like removable devices and RDP, SMB ports open to the public network, etc. will continue to get abused by attackers in coming days as well. Such avenues are go-to attack channels for hackers so businesses should revisit their security posture and work on reducing attack surfaces from time to time.

We hope that this report does ready you for 2020 - read our ***Predictions Report*** to know more about emerging cyberattacks in 2020. For deeper insights, do get in touch for a complete assessment of your business' cybersecurity preparedness for the future.