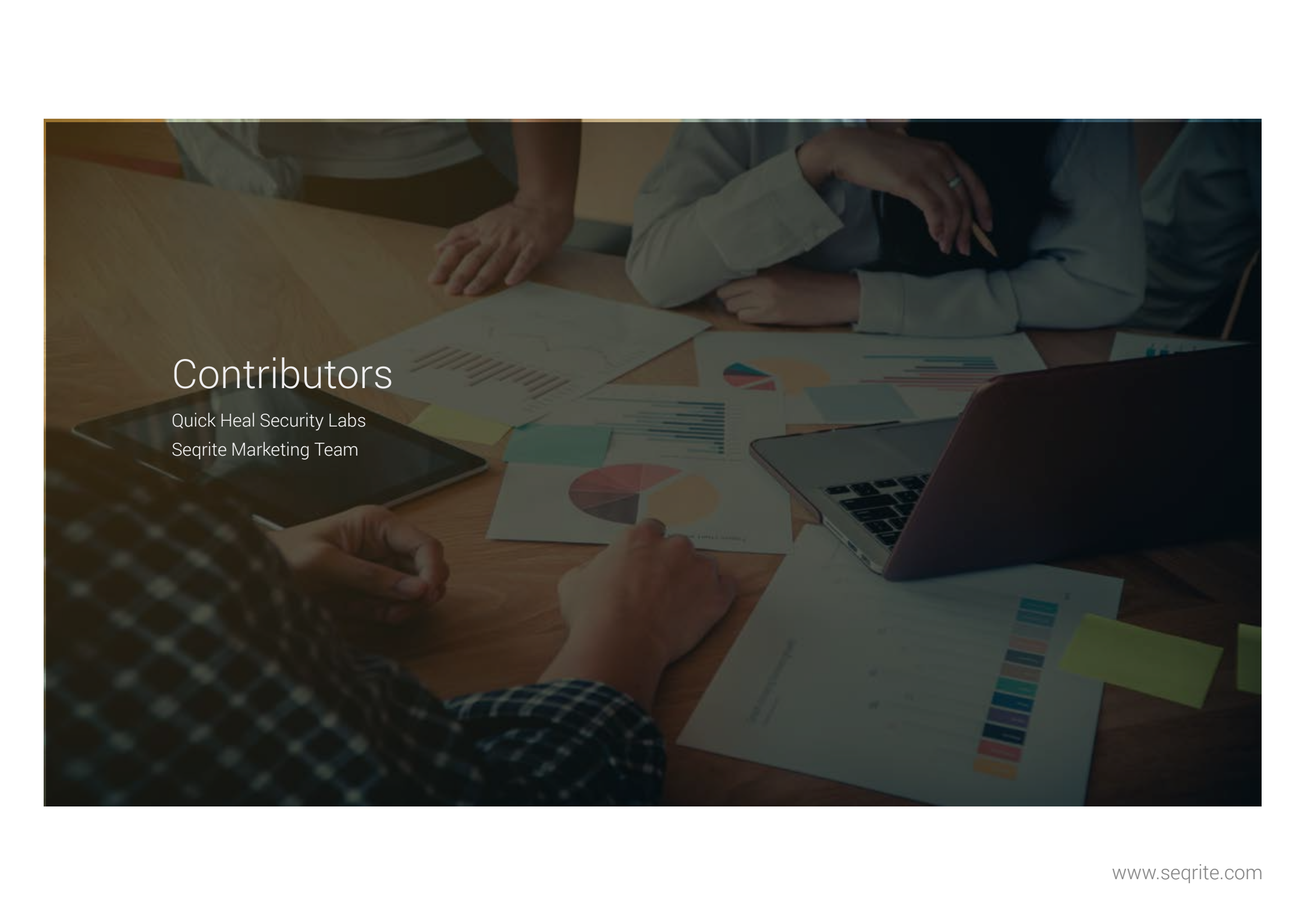




QUARTERLY THREAT REPORT Q3 - 2019

A photograph of a group of people in a meeting, viewed from above. They are gathered around a wooden table covered with various documents, including pie charts, bar graphs, and sticky notes. A laptop is open on the right side of the table. The image is dimly lit and has a dark overlay. The text 'Contributors' is written in white on the left side of the image.

Contributors

Quick Heal Security Labs
Seqrite Marketing Team

Table of Contents

Introduction	1
About Seqrite	2
About Quick Heal Security Labs	2
WINDOWS	3
Detection Highlights – Q3 2019	4
Detection Statistics – Month Wise	5
Detection Statistics – Week Wise	5
Detection Statistics – Category Wise	6
Industry Wise Detection Stats	7
Industry Wise Top Detections	7
Protection Wise Detection Stats	8
Top 10 Windows Malware	9
Top 10 Potentially Unwanted Applications (PUA) and Adware	12
Top 10 Host-Based Exploits	13
Top 10 Network-Based Exploits	14
Trends in Windows Security	15
Conclusion	21

Introduction

Enterprise infrastructure continued to see a threat to itself by a plethora of attacks from a wide range of agents in the third quarter of 2019. While July began with German industrial juggernauts complaining of cyberattacks from state-sponsored agencies, a concerning attack in August this year was hackers breaking into blue-chip corporate networks through IoT devices. The month of September ended the third quarter of 2019 with Huawei complaining that the U.S Government broke into its intranet, a high-risk revelation.

Seqrite's third quarter threat report, a high-value and globally released collation of enterprise cybersecurity statistics sheds more light on the specifics of malware count & trends. Malware numbers have shown growth when compared with the second quarter of this year. With a total count of 38 million, it has increased by 4 million versus Q2, 2019 and by 10 million against Q1, 2019, an alarming fact.

Trojan malware saw a huge surge in Q3-2019 capturing the majority of the malware attack pie – Trojan intrusion was 27%. Almost 19% detections in Windows business endpoints were identified to be Worm.NSIS.NeksMiner.A. Not replicating the pattern for last quarter, the education sector ruled the roost with 30.13% detections. Real-time scanning helped detect 46.5% malware for Q3-2019.

Seqrite recently received a patent for Signatureless Behaviour-Based Malware Detection Technology further strengthening its inventory by leveraging Go.Deep.AI, our AI-enabled deep predictive malware hunting technology. Acknowledged by the U.S. Patent and Trademark Office (USPTO), the capability proactively detects and blocks zero-day malware attacks bolstering the enterprise.

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

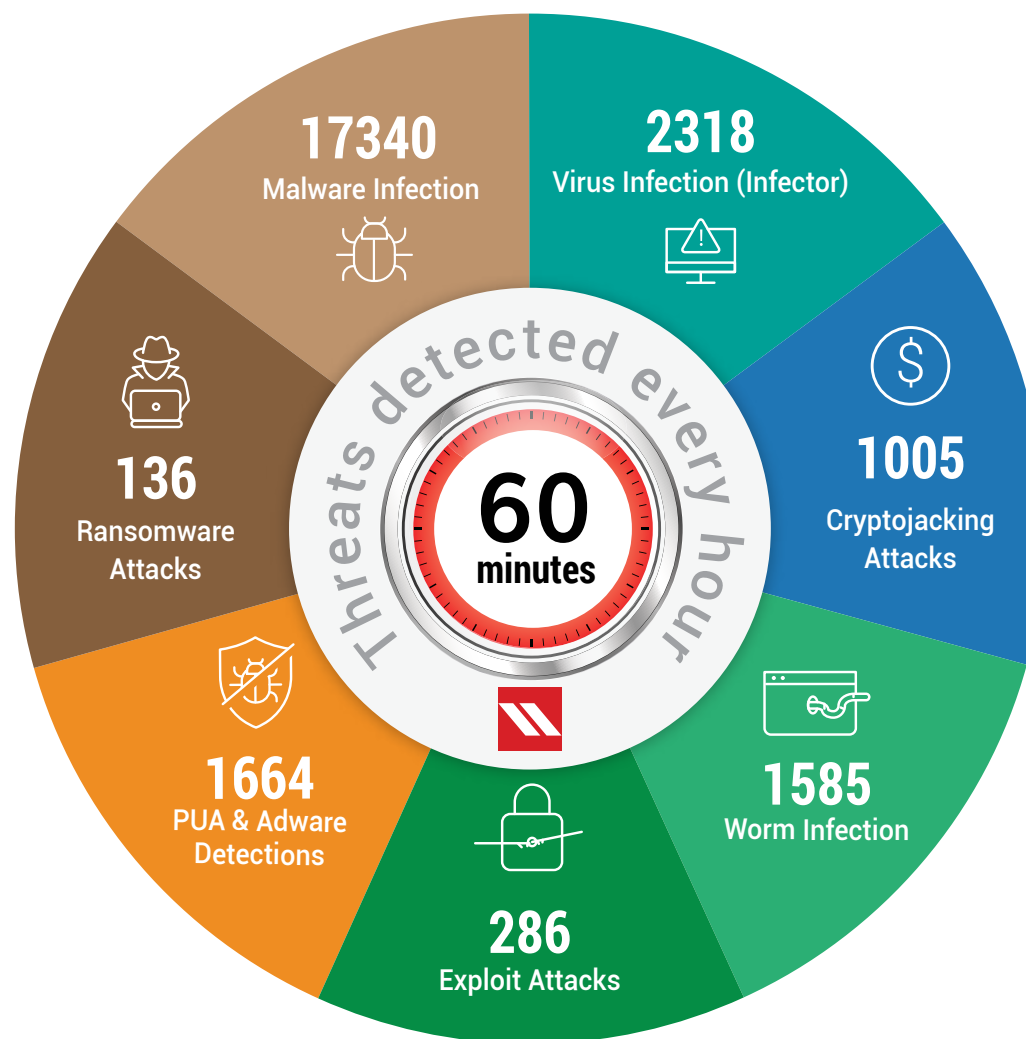
Follow us on:



WINDOWS



Detection Highlights: Q3*



*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 during the period of Jul to Sep in 2019.

Windows Malware Detection Count

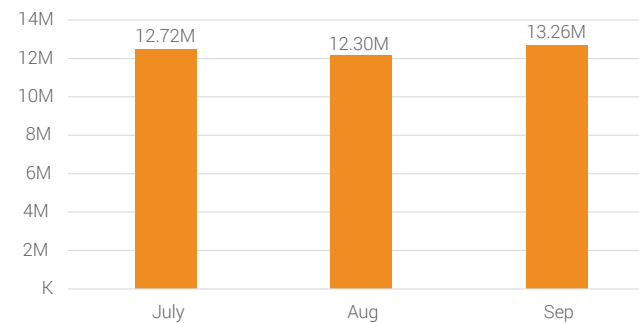


Fig. 1



Observations

- Seqrite detected over 38 million Windows malware in Q3 2019.
- September clocked the highest detection of Windows malware.

Week Wise

Windows Malware Detection Count

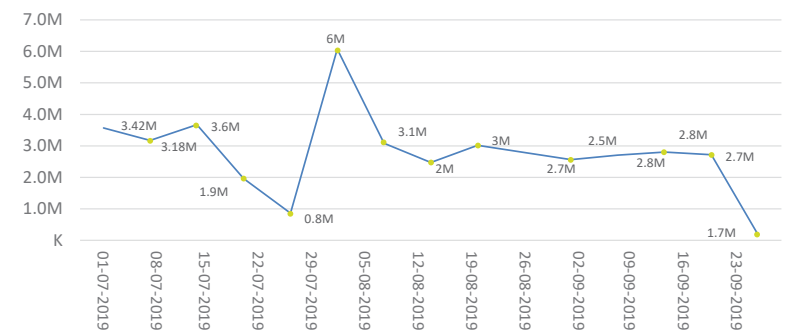


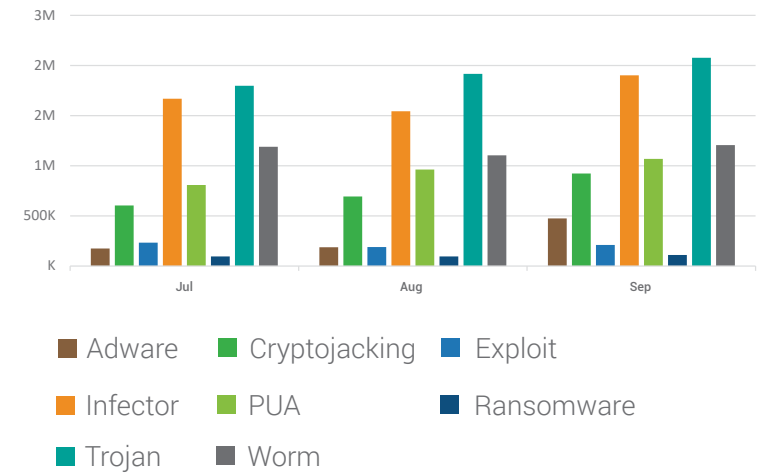
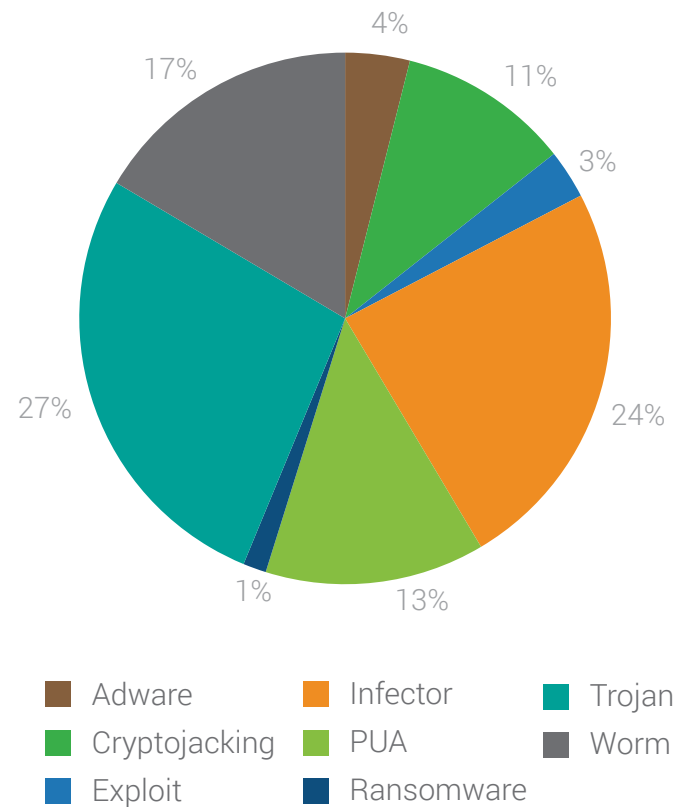
Fig. 2



Observations

- Malware detection was the highest at 6.07 million in the month of August receding substantially by the end of the quarter.

Detection Statistics Malware Category Wise



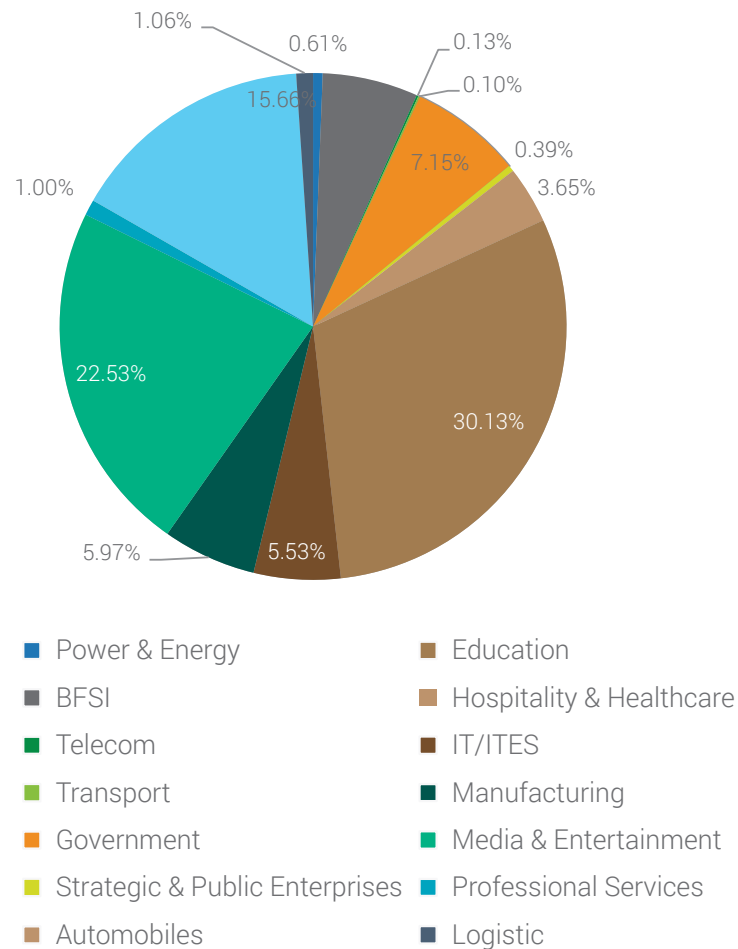
Observations

- Malware detection was the highest at 6.07 million in the month of August receding substantially by the end of the quarter.

Industry Wise Detection Stats

Below figure represents the malware detection count for various industries.

Industry Wise Detection Stats



Top Detections

Industry	Detection	Count
Manufacturing	Worm.NSIS.NeksMiner.A	4,03,789
Education	W32.Brontok.Q	1,29,926
Professional Services	W32.Pioneer.CZ1	1,12,985
Automobiles	LNK.Browser.Modifier	27,769
BFSI	INF.AutoRun.C	62,470
Media & Entertainment	HTML.IframeRedirect.SK	30,258
Hospitality & Healthcare	W32.Sality.U	40,883
Government	Trojan.KillAv.DR	40,323
IT/ITES	W32.Brontok.Q	39,679
Logistic	W32.Pioneer.CZ1	26,673



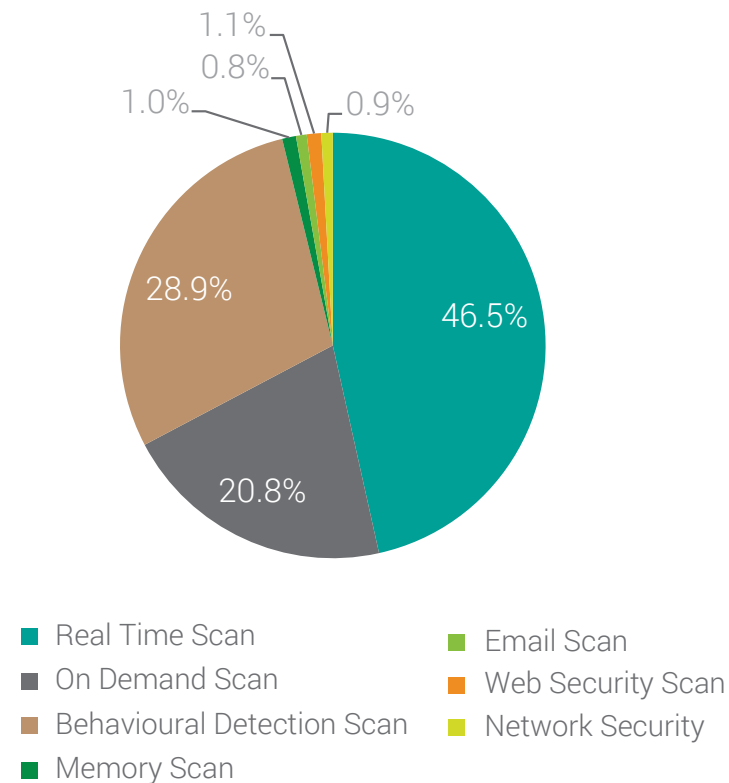
Observations

- The education industry had the maximum malware detections with over 30% of the total detections.
- The Education industry saw the maximum attacks of the malware W32.Brontok.Q at 0.12 million hits.

Protection Wise Detection Stats

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

Protection Wise Stats



Observations

- Most malware was discovered during Real-Time Scans.

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 you from visiting them.

- **Network Scan**

Network scan (IDS/IPS) analyzes network traffic to identify known cyberattacks & stops packets being delivered to the system.

Top 10 Windows Malware

The below figure represents the Top 10 Windows malware of Q3 2019. These malware have made it to this list based upon their rate of detection from July to Sep.

Top 10 Windows Malware

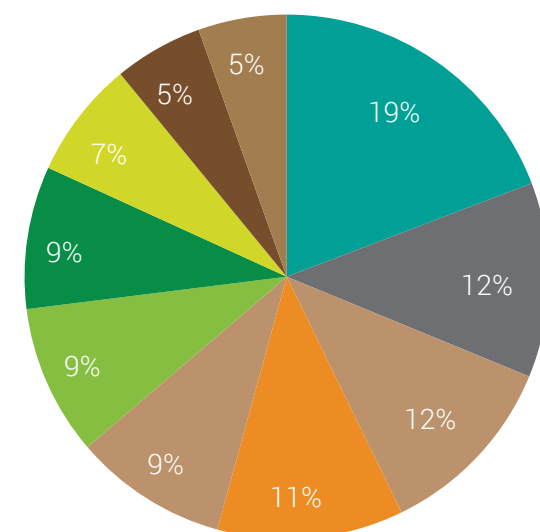


Fig.7

Worm.NSIS.NeksMiner.A	HTM.Nimda.A
Trojan.KillAv.DR	PIF.StucksNet.A
Worm.AUTOIT.Tupym.A	W32.Runouce.B
W32.Pioneer.CZ1	Trojan.Starter.YY4
W32.Sality.U	Worm.Autoit.Sohanad.S

1. 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'

2. 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.

3. 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 execute it from the dropped location.
- It connects to a malicious website and modifies the start page of the browser to another site through registry entry – it also creates a 'Run' entry for the same dropped file for the sake of persistence.

4. 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.

5. W32.Sality.U

Threat Level: Medium

Category: Polymorphic file infector

Method of Propagation: Removable or network drives

Behaviour:

- It starts with Injecting 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. 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

7. 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.

8. 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'

9. Trojan.Starter.YY4

Threat Level: High

Category: Trojan

Method of Propagation: Email attachments and malicious websites

Behaviour:

- Creates a process to run a 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.

10. 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 computers through messaging apps, infected USB or network.
- It has the ability to spread quickly.
- After arrival, it creates a copy of itself as a .exe with a typical Windows folder icon.
- Users mistakenly execute this .exe assuming it as a folder ensuring it spreads across the network.
- It infects every connected USB drive too.

Top 10 Commonly found malware file names

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

1. clean.exe	3. SECOH-QAD.dll	5. SECOH-QAD.exe	7. DriverPackNotifier.exe	9. SppExtComObjHook.dll
2. KMS-R@1n.exe	4. DOC001.exe	6. Service_KMS.exe	8. mssecsvc.exe	10. utopico.exe

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 Q3 2019

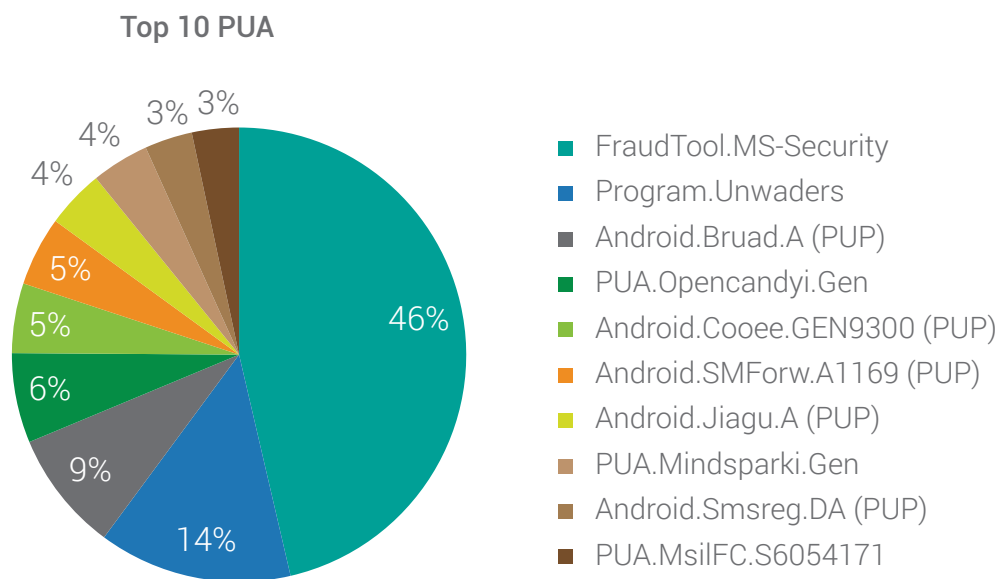


Fig.8



Observations

- With 46% detection, FraudTool.MS-Security was the top PUA in Q3 2019

Top 10 Host-Based Exploits

An exploit is a piece of code or crafted data that takes advantage of a bug or vulnerability in the targeted system or an application running on it.

Top 10 host-based exploits of Q3 2019

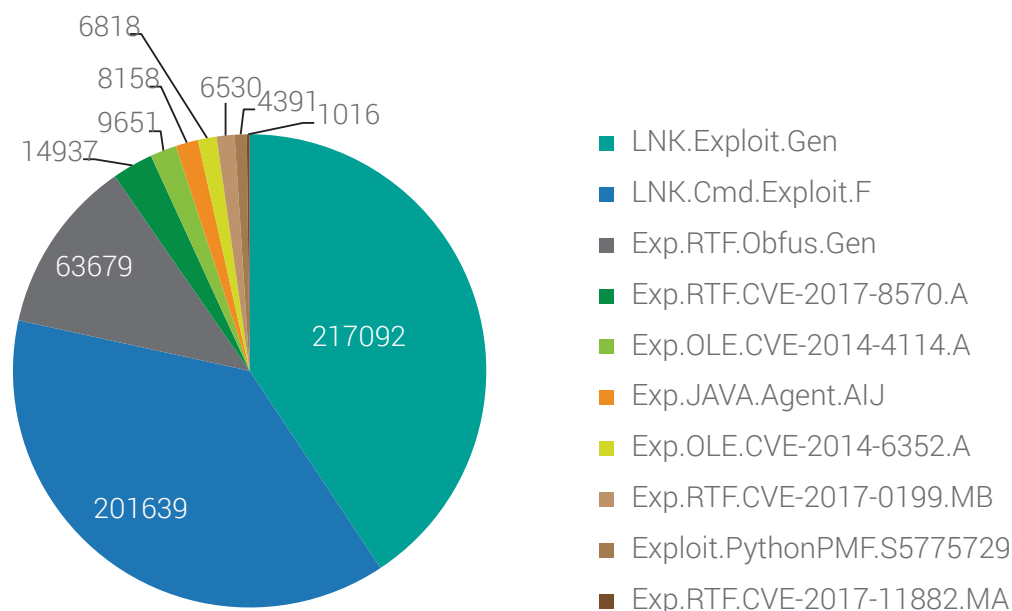


Fig.9

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.



Observations

- With 217092 instances, the LNK.Exploit.Gen was the top detected host-based exploit

Top 10 Network-Based Exploits

Below figure represents the top 10 Network-Based exploits for Q3 2019.

Top 10 network-based exploits of Q3 2019

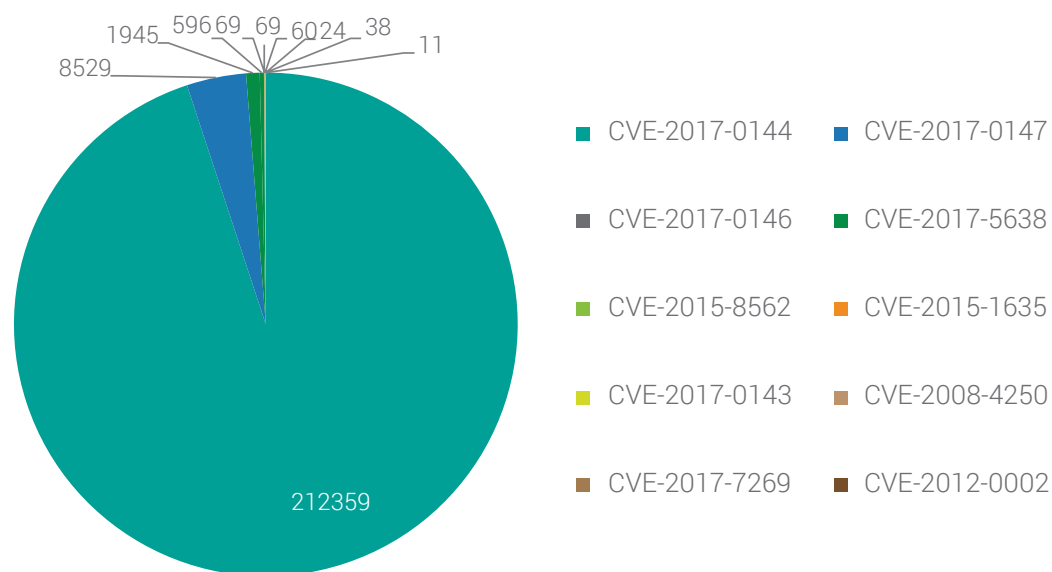


Fig.9

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).



Observations

- The CVE-2017-0144, with 21235 intrusions, was the most detected network-based exploit.

Trends in Windows Security

1. Ransomware as a Tool - LockerGoga

Ransomware authors keep experimenting with the development of payload in various dimensions. In the timeline of ransomware operations, we have seen its evolution from a simple screen locker to multi-component model for file encryption, and from a novice approach to a sophisticated one.

Quick Heal Security Labs detected one such ransomware named LockerGoga which was unique as it acts as a tool giving various options for performing encryption such as '-e' option - it also allows launching multiple threads to initiate encryption. The '-p' option allows selecting any specific process in which malicious code needs to be injected. If the process name is not provided, then by default it will inject code into 'winlogon.exe.'

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Admin>C:\Users\Admin\Desktop\1e8a6aabf4adf3ae1890a4c8a2cff276.exe -h
Allowed options:
-h [ --help ]           produce help message
-v [ --version ]        print version
-k [ --key ] arg        public key
-m [ --e-mail ] arg     e-mail
-e [ --encrypt ] arg (<=2) encrypt using n threads
-p [ --process ] arg (<=winlogon.exe) inject into process matching name

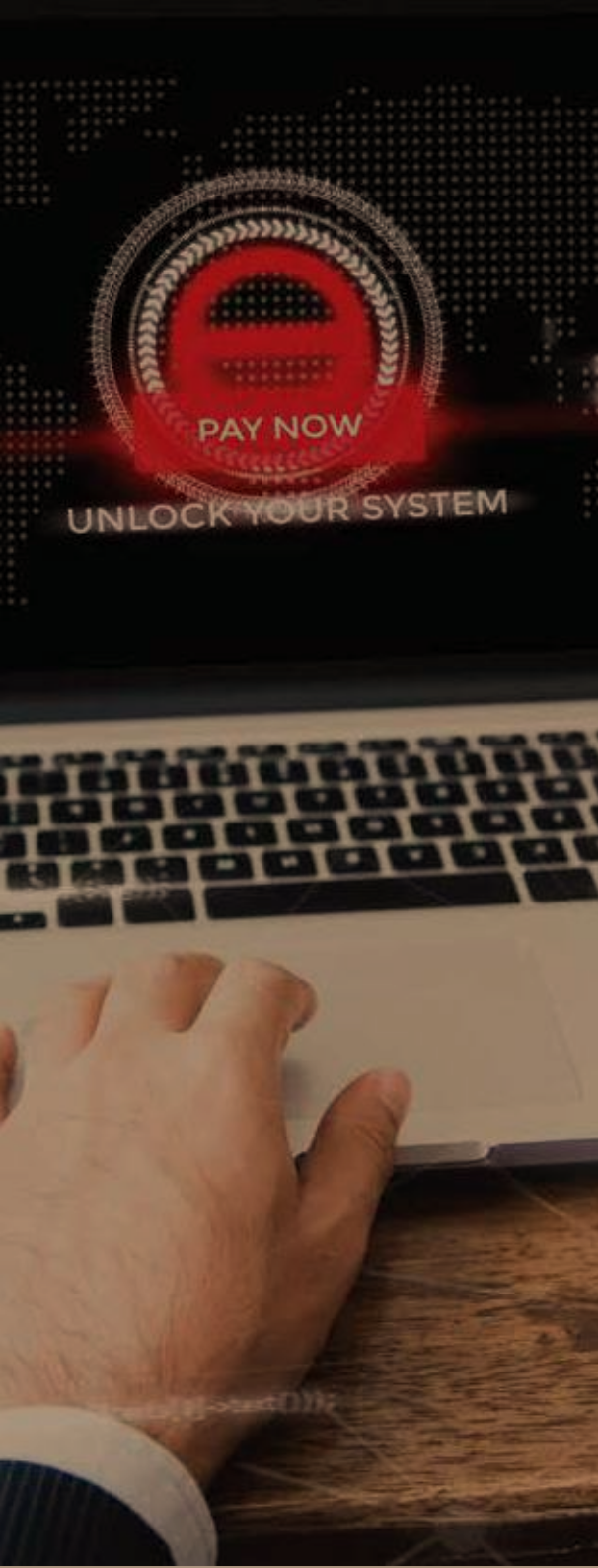
C:\Users\Admin>
```

The infection vector of LockerGoga is not yet verified, but in many scenarios, it is likely to be coming from spear-phishing emails.

The threat actors behind LockerGoga use different digital certificates (Alisa Ltd., Kitty Ltd.) to sign the malicious payloads which help bypass a few of the traditional security procedures. Some variants of the malware have been equipped with 'taskkill' capabilities.

LockerGoga focuses on encrypting files with popular extensions including .doc, .xml, .ppt, and .pdf using AES-256 keys. The extension *.LOCKED is used and instead of using Microsoft Crypto API for encryption, it uses the Crypto++ library (Boost Software License).

Ref: <https://blogs.seqrite.com/ransomware-as-a-tool-lockergoga/>



2. Tflower Ransomware

A new ransomware named 'TFlower' was discovered in July 2019 which continues to target corporate and government agencies. The path to the main attack leads through hacking insecure or exposed remote desktop services and the attack ends with infecting the local machine and traversing through the entire network using PowerShell, PSEXec, etc.

It takes help of a known malicious file named as 'chilli.exe' which after execution shows the infection activity which is being carried out by ransomware. It also tries to modify the Windows automatic backups and repairs functionality and looks to stop the repair mechanism.

The ransomware adds *tflower marker in each file. After the encryption gets over, It drops a .TXT file on various locations and asks users for an amount to be paid if they want their encrypted files back. In order for the user to believe whatever the authors are saying in the .TXT file to be really true, they suggest users try their decrypting mechanism once, for a single file. In all likelihood, user decryption methods do not work at which point they have no other option other than paying hackers to reclaim their files.

Seqrite successfully detects this threat via its multilayered detection and award-winning anti-ransomware technology.

3. APT Attacks

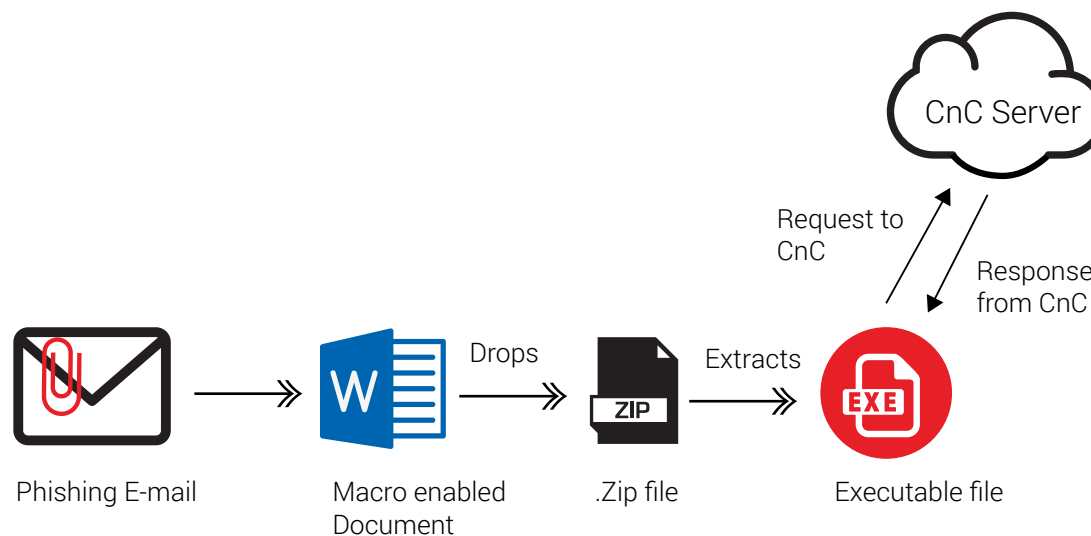
In the last quarter, Quick Heal Security Labs monitored APT campaigns that happened against some important Indian Government organizations. These campaigns have close similarity with Operation Transparent Tribe. It is a long-term operation against India.

In this attack, the victim receives a spear-phishing email with intriguing content and also has a malicious link or an attachment. To read further, the receiver clicks on the link/attachment which instead downloads a macro-enabled malicious XLS file. When the victim opens the XLS file and clicks on 'enable macro' button, the malicious VBA code gets executed. The script drops an embedded zip file, extracts it and launches the unzipped .NET PE file. The executable has several functions like capturing screenshots, gathering running process information, OS and system information and sending data to 'C2' server.

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

Below are some filenames which were observed to be affected while analyzing campaign:

- a. Fauji India September 19.xls
- b. PMAYCLSSMIGSeptember201920.xls
- c. PradhanMantriAwasYojana76487.xls
- d. Program.xls



4. Top 10 MITRE's ATT&CK techniques

MITRE's ATT&CK Framework has gained the attention of the security community over the past few years. MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a globally accessible knowledge base for cyber adversary behaviour that is used in various phases of an adversary's lifecycle. ATT&CK is useful for defenders to develop analytics that detects the techniques used by an adversary.

At Quick Heal Labs, we have applied the MITRE ATT&CK framework in our Advanced Behavioural Detections and Telemetry. This report includes the most widely used ATT&CK techniques observed with our clients. We have observed that PowerShell is one of the most used techniques by adversaries.

Following are the top 10 techniques and their details.

a. PowerShell:

PowerShell is a command-line interface utility which can be used by an attacker to perform several actions such as code execution, the discovery of network, information, etc. PowerShell can also be used to download and execute a file from the internet. It also has the capability to load an executable in a system's memory. Using PowerShell, it is possible to connect with remote systems and execute a command on these systems.

b. Process Hollowing:

In the Process Hollowing method, a new process is created in suspended mode, followed by unmapping of a portion of the code, replacing it with malicious code. This technique is similar to Process Injection in which malicious code is masked under a legitimate process to bypass a security product.

c. Deobfuscate/Decode Files or Information:

Attackers used Obfuscation techniques to hide code from analysis. There are different techniques to deobfuscate information. Certutil tool is used to decode a remote access tool file hidden in a certificate file.

d. Mshta:

Mshta.exe is a utility responsible for executing HTA (Microsoft HTML Application) files. Attackers execute malicious HTA files like JavaScript or VBScript files through legitimate applications. Mshta.exe can be used to bypass application whitelisting solutions. For e.g., by exploiting Office application, mshta.exe gets executed which further downloads and executes next stage malware.

e. Process Injection:

Process Injection is a method which is used to execute arbitrary code in

context to another process which allows access to a process' memory. To evade detection from security products, execution via process injection technique is used.

f. Regsvr32:

Regsvr32.exe is a Windows command-line utility used to register and unregister object linking and embedding of controls including dynamic link libraries (DLLs). Attackers use this utility to bypass process whitelisting functionality to load COM scriptlets for executing malicious DLLs. This utility is also responsible to download external components from the internet.

g. Command-Line Interface:

Command-Line interface is used to perform several tasks on operating systems. Executing scripts for software deployment on systems or interacting with remote systems are a few avenues where the command-line interface can be used.

h. BITS Jobs:

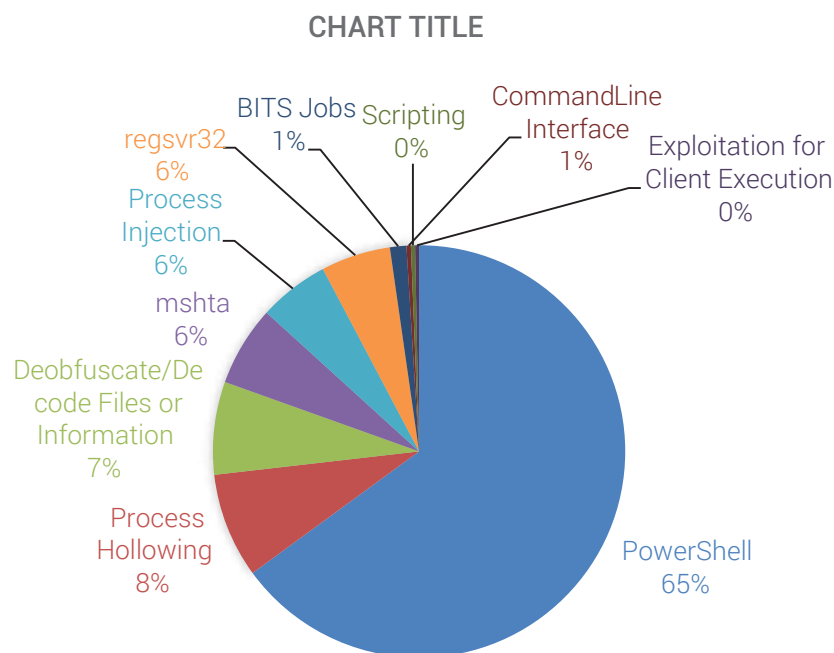
BITS Jobs is a Windows Background Intelligent Transfer Service, which is used to download and execute code. To bypass the behaviour-based detection, BITS jobs are used allowing persistence by creating long-lasting jobs.

i. Scripting:

Scripting is basically used to reduce manual efforts and speeding up operational tasks. Some of the scriptings can also directly interact with Operating Systems by calling system APIs instead of other programs which can help bypass process monitoring mechanisms. The commonly used scripting languages are VBScript, PowerShell and most of the times these scripts can be embedded inside Office applications as macros.

J. Exploitation for Client Execution:

Vulnerabilities are present in most software and applications that we use in our systems. To exploit one's system, the attacker takes advantage of such vulnerabilities present in OS or installed applications.



the same. So again, it is emphasizing that the choice of an advanced layer of protection is critical over the conventional signature-based approach to stop such complex malware campaigns. Emotet is continuing its faith in 'malspams' for spreading.

We have seen the journey of Emotet from a banking Trojan to a complex threat distributor. Emotet malware campaign has existed since 2014. Initially, Emotet campaign used to spread through 'malspams' with 'PDF' and 'JS' file attachments. Later on, it started exploiting MS Office Word documents with a heavily obfuscated macro inside it. It mostly targeted the websites based on 'PHP' using vulnerabilities like Arbitrary File Upload, Direct access to XMLRPC.php for brute-force attacks, remote privilege escalation, cross-site scripting and Information disclosure vulnerabilities to get root access of a server.

Security measures to follow:

- Don't open any link in the mail body sent by an unknown source.
- Don't download attachments received by an untrusted source.
- Always turn on email protection of your antivirus software.
- Don't enable 'macros' or 'editing mode' upon execution of the document.

5. Emotet: A new mask on the dark face

Emotet is now a familiar name in the cybersecurity world. It was the most severe threat last year. It never deviated from its nature of coming frequently in intervals with different techniques and variants to deliver malware on victim machines. After a prolonged break, a new variant has been observed with a new wrapper blending and some complex obfuscation techniques. But the interesting thing we noticed is that the main payload inside the file remains

6. Stop: The Rampant appending of extensions!

With 150+ extensions in the wild, STOP (.djvu) can be considered today's most widespread Ransomware with its share of around 35%. Although it's been more than a year, we have seen upgraded versions with more infections in the recent quarter.

The infection vector for this ransomware particularly is cracked software from the internet. The main advantage is, the user usually tends to allow these cracked software even when antivirus does not allow it. Over the period 'STOP' has been observed to use a complete framework to mitigate current detection techniques, whether it may be a newer extension, newer obfuscation techniques or even anti-emulation techniques. According to our observations, crack files or activators for different software like Tally, Minecraft, Nero 7, Autocad, Adobe Photoshop, Internet Download Manager, Cyberlink Media Suite, Microsoft Office, VMware Workstation, DreamWeaver, Corel Draw Graphic Suite, Quick Heal Total Security, Ant Download Manager, IBESOFTE Data Recovery, Any Video Converter Ultimate were seen spreading this Ransomware.

The encryption is carried out with the 'Salsa20' algorithm.

There are 2 types of encryption:

1. Online Key Encryption
2. Offline Key Encryption.

In the first case, the encryption key is calculated at the server's end and then used to encrypt files on the victim's system. Here, it is mandatory for the system to have an internet connection. On the other hand, in the second case, if the system is not connected to the internet, it uses the predefined encryption key. So, it says that in second case decryption is possible where the key is predefined. The encryption is carried out with the 'Salsa20' algorithm.

With the continuous introduction of newer extensions, STOP authors keep on adding different software cracks to their infection list. For every new extension, their online 'CnC' servers stay active for a specific period only. After that, it switches to another extension. The usual ransom amount is \$980 for which they offer a concession of 50% if paid within 48 hours of encryption.

To stay protected our advice to users will be:

1. Do not use/download crack applications.
2. Do not install software from untrusted sources.
3. Always update your antivirus.
4. Do not allow suspicious/malicious applications to run.
5. Backup your data.

Conclusion

MITRE's extremely popular knowledge base to cope up with ATT&CK, a menacing cyberattack methodology has been helpful so far for cybersecurity companies to detect threats for enterprises. However, is it enough? Adversaries are now developing what we call as micro streaming for system penetration in which attackers keep screening systems till they find a vulnerability and penetrate.

Behavioural Detection Scan (BDS) is one of the best ways currently, to counter hacks – however, there is a lot of development that needs to occur in this technology for it to encapsulate the entire paradigm of advanced cyberthreats. Ransomware remains a problem with new variants of Emotet and LockerGoga surfacing.

But the real problem with enterprises today is the inability to train its employees in practising caution for the sake of cybersecurity. Exactly like last quarter, this quarter is also seeing maximum malware penetration through simple channels such as office messengers, emails, detachable drives et al. Overlooking the securing of such a simple element is increasingly becoming a pain area for enterprises all around the world.

Seqrite's award-winning anti-ransomware and endpoint security products can be excellent in blocking malware that poses a threat due to employee ignorance or otherwise. Unlike last quarter where we saw the manufacturing sector to be the apple of the eye for cyber attackers, this quarter, maximum attacks were directed towards the Education sector.