SEQRITE

SEQRITE THREAT REPORT

Q1 - 2019

Enterprise Cybersecurity Solutions by Quick Heal

www.seqrite.com

Contributors

Quick Heal Security Labs

Seqrite Marketing Team

Table of contents

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:

Introduction

In this threat report by Seqrite, we look at the latest security threats and trends identified by Quick Heal Security Labs during January 1, 2019 to March 31, 2019 reporting period.

2018 turned out to be a year with some headline-grabbing cyber-attacks, which included the Facebook-Cambridge Analytica data breach, another data breach at Facebook, a hacking at India's Cosmos Bank, a data breach at British Airways and also at UnderArmour with GDPR being a key trend. 2019 has just started and it is likely to shape up to be an eventful year for cybersecurity.

Cryptojacking is a dangerous new threat which threatens to cause havoc in 2019. Our threat report suggests that over 17K cryptojacking malware were detected in Q1 2019 every day indicating the speed at which this new threat is spreading its wings. Considering the widespread popularity of cryptocurrency, this threat is likely to become even more popular among cyber criminals.

The world is still reeling from the many accusations of meddling and interference in elections in the last few years. The New Year of 2019 will see elections in countries from as varied as Nigeria to Israel to the European Union. But closer home, the Indian General Elections which will be held in the summer months will probably be the most significant.

Our threat report suggests that every minute 216 malware were detected on enterprise endpoints. Overall malware detection count in Q1 2019 stands at over 28 million. The month of March clocked the highest detection rate. Our Security Labs also observed that Emotet malware constantly kept changing its payload and infection vectors like spam mail, Malicious Doc and even Malicious JS files. It compromised a very high number of websites on the internet. Quick Heal Security Labs observed continued attack using RDP and SMB brute force. Criminals look for unsecured RDP, SMB services to exploit and access enterprise networks. Ransomware like Dharma, CrySis were distributed through hacked RDP or SMB share by brute forcing.

In Q1, we observed that the Manufacturing industry had the maximum malware detections with over 27% of the total detections followed by Professional Services, Education and Automobile industry respectively.

WINDOWS

Detection Highlights: Q1

Detection Statistics: Month Wise

The below graph represents statistics of the total count of malware detected by Seqrite during the period of January to March in 2019.

Windows Malware Detection Count

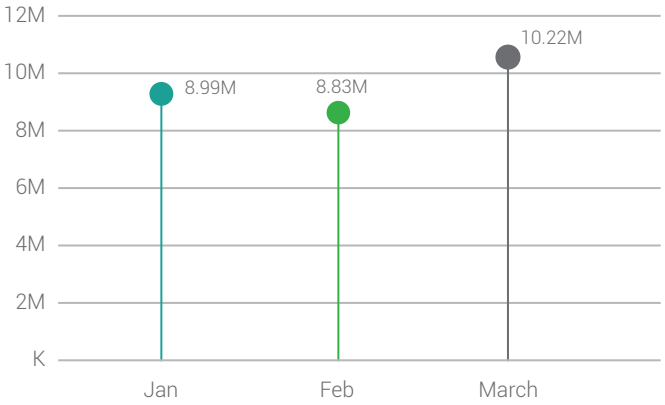


Fig. 1

Observations

- Seqrite detected over 28 million Windows malware in Q1 2019
- March clocked the highest detection of Windows malware

Detection Statistics: Week wise

Windows Malware Detection Count

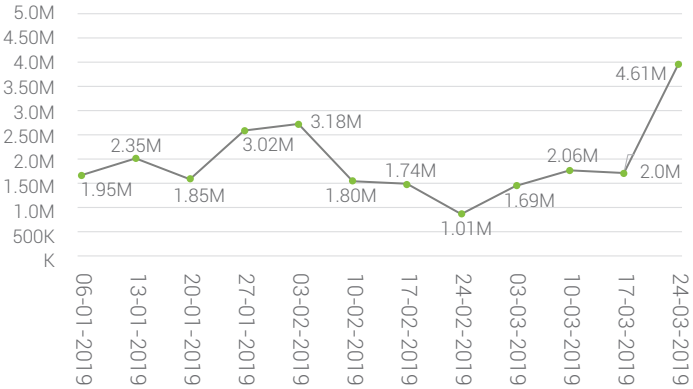


Fig. 2

Observations

- Malware detection count was the highest in the week starting with 24th March.

Detection Statistics: Category-wise

Windows malware detection - Category Wise

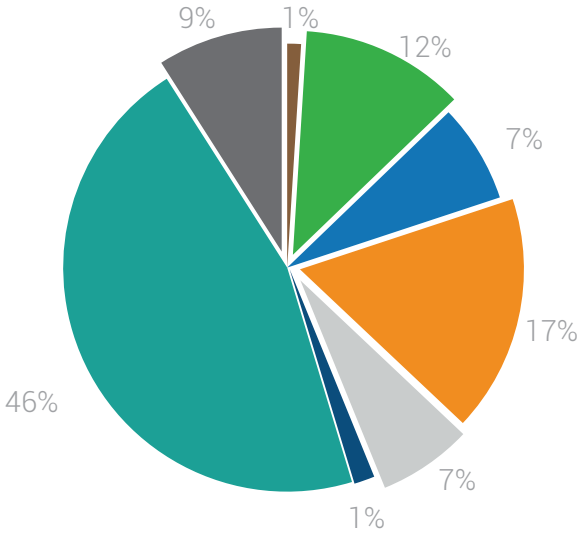


Fig.3

Observations

- Malware detection count was the highest for Trojan followed by Infector and Cryptojacking.

Detection Statistics: Category-wise

Categorywise Detection

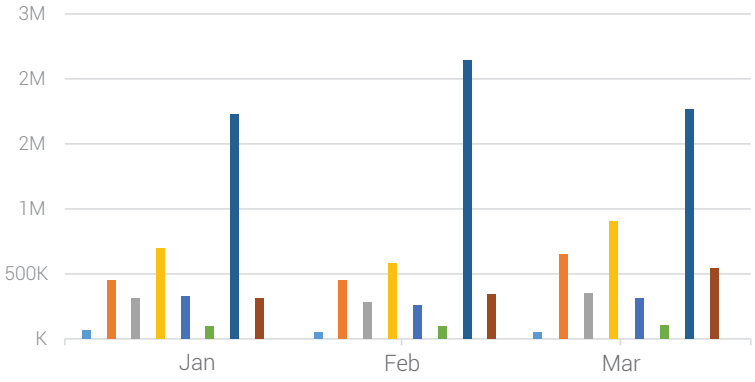


Fig.4

Observations

- Malware detection count was the highest for Trojan in all the three months

Industry Wise Detection Stats

Fig.5 represents the malware detection count for the below mentioned industries.

Industry Wise Detection Stats

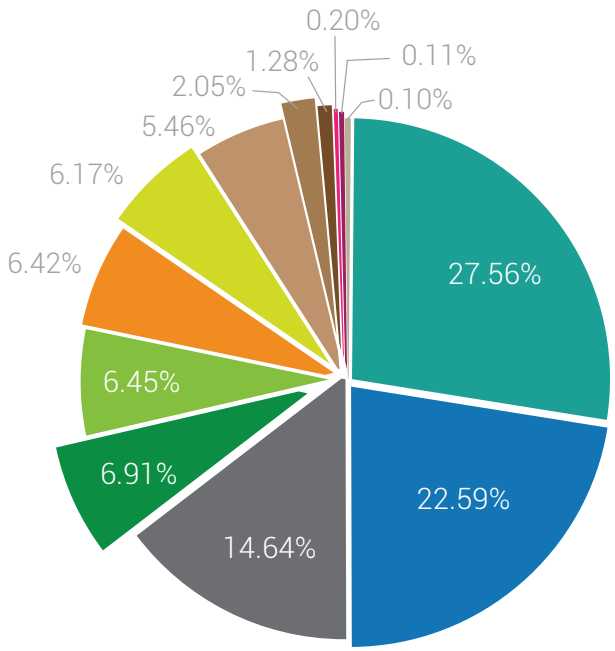


Fig.5

- Manufacturing
- Professional Services
- Education
- Media & Entertainment
- Power & Energy
- Automobiles
- Government
- IT/ITES
- Strategic & Public Enterprises
- Healthcare
- BFSI
- Logistic
- Telecom

Industry Wise Top Detection:

Industry	Detection
Manufacturing	Trojan.KillAv.DR
Professional Services	W32.Pioneer.CZ1
Automobiles	W32.Madang.A
Healthcare	W32.Sality.U
Logistic	Worm.AUTOIT.Tupym.A
Education	Trojan.Starter.YY4
Government	Trojan.KillAv.DR
BFSI	W32.Pioneer.CZ1
IT/ITES	Trojan.KillAv.DR

Observations

- Manufacturing industry had the maximum malware detections with over 27% of the total detections.
- Manufacturing industry was followed by Professional Services, Education and Automobile industry respectively in the highest malware detection count.

**Disclaimer: Above statistics are based on Seqrite telemetry data.

Protection Wise Detection Stats

This section features the various sources through which we detected the malware infection.

Protection Wise Stats

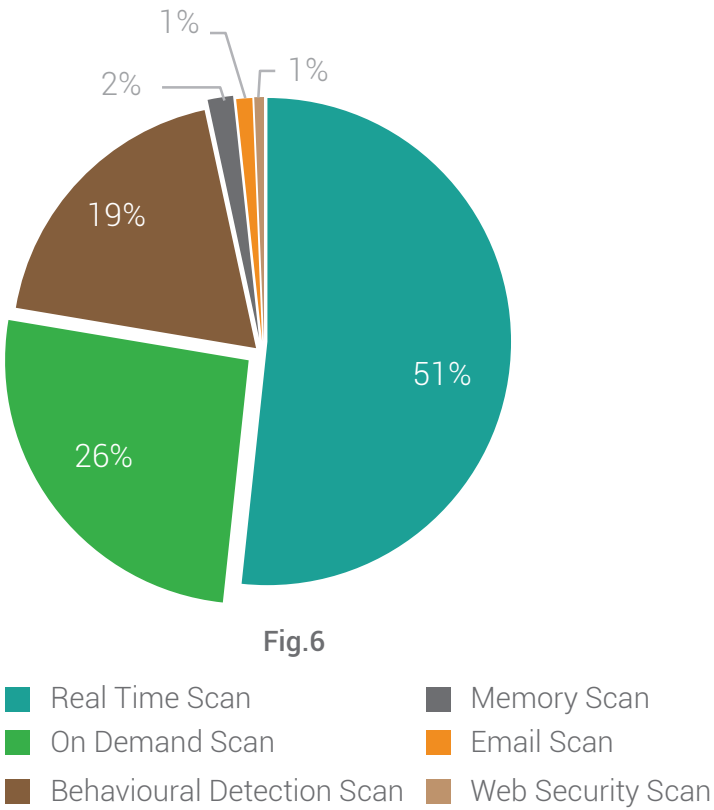


Fig.6

Observations

- Most malware were discovered during Real Time Scanning and On Demand Scanning

- **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**

  It detects and eliminates new and unknown malicious threats based on behaviour.

- **Memory Scan**

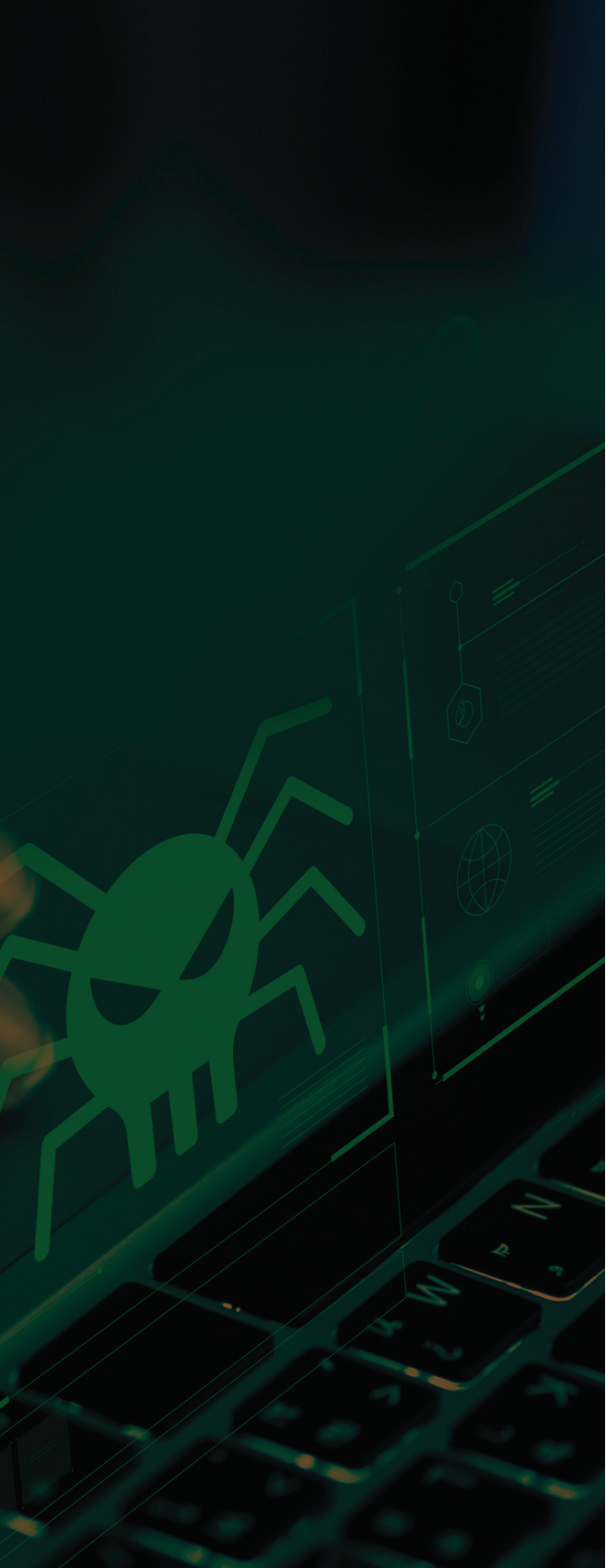
  Scans memory for malicious program running & cleans it.

- **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.



Top 10 Windows Malware

Fig.7 represents the top 10 Windows malware of Q1 2019. These malware have made it to this list based upon their rate of detection from January to March.

Top 10 Windows Malware

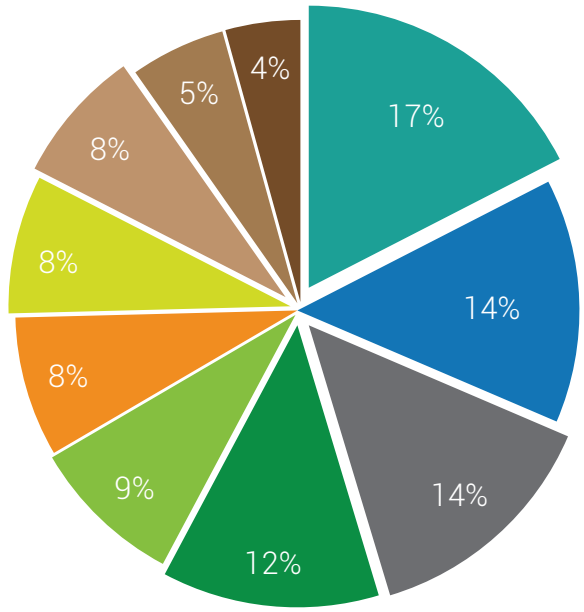


Fig.7

- LNK.Exploit.Gen
- W32.Sality.U
- W32.Pioneer.CZ1
- Trojan.KillAv.DR
- Worm.AUTOIT.Tupym.A
- Trojan.Starter.YY4
- VBS.Dropper.A
- Worm.Autoit.Sohanad.S
- W32.Perite.A
- LNK.Cmd.Exploit.F

1. LNK.Exploit.Gen

Threat Level: High
Category: Trojan
Method of Propagation: Bundled software and freeware
Behavior:

- 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. In order to redirect the user to dubious websites, the virus modifies system hosts file and hijacks the IP address.

2. W32.Sality.U

Threat Level: Medium
Category: Infector
Method of Propagation: Removable or network drives
Behavior:

- 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. W32.Pioneer.CZ1

Threat Level: Medium
Category: Infector
Method of Propagation: Removable or network drives
Behavior:

- Malware injects its code to files present on disk and shared network.
- It decrypts malicious DLL present in the file & drop it.
- This DLL performs malicious activity and collects system information & sends it to CNC server.

4. Trojan.KillAv.DR

Threat Level: High
Category: Trojan
Method of Propagation: Email Attachments and malicious/compromised websites.
Behavior:

- This malware drops a file when executed.
- Popular malwares like skype spy or AV services killer are delivered and executed using this trojan.
- IP address and other related information of victims is also sent to malware authors.
- This malware mostly has icons like genuine windows applications.

5. Worm.AUTOIT.Tupym.A

Threat Level: Medium
Category: Worm
Method of Propagation: malicious links in instant messenger
Behavior:

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

6. Trojan.Starter.YY4

Threat Level: High
Category: Trojan
Method of Propagation: Email attachments and malicious websites
Behavior:

- Creates a process to run the dropped executable file.
- Modifies computer registry settings which may cause the infected system to crash.
- Downloads other malware like keyloggers and file infectors.
- 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.

7. VBS.Dropper.A

Threat Level: Medium
Category: Dropper
Method of Propagation: Web page

Behavior:

- This malware is spreading via malicious web pages. A web page contains embedded PE file.
- It drops that PE file to specific folder & launches that to perform malicious activity.

8. Worm.Autoit.Sohanad.S

Threat Level: Medium
Category: Worm
Method of Propagation: Spreads through mails, IM apps, infected USB & network drives
Behavior:

- It arrives to 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 typical windows folder icon.
- User mistakenly executes this exe assuming it as a folder and then it spreads over the network.
- It infects every connected USB drive too.

9. W32.Perite.A

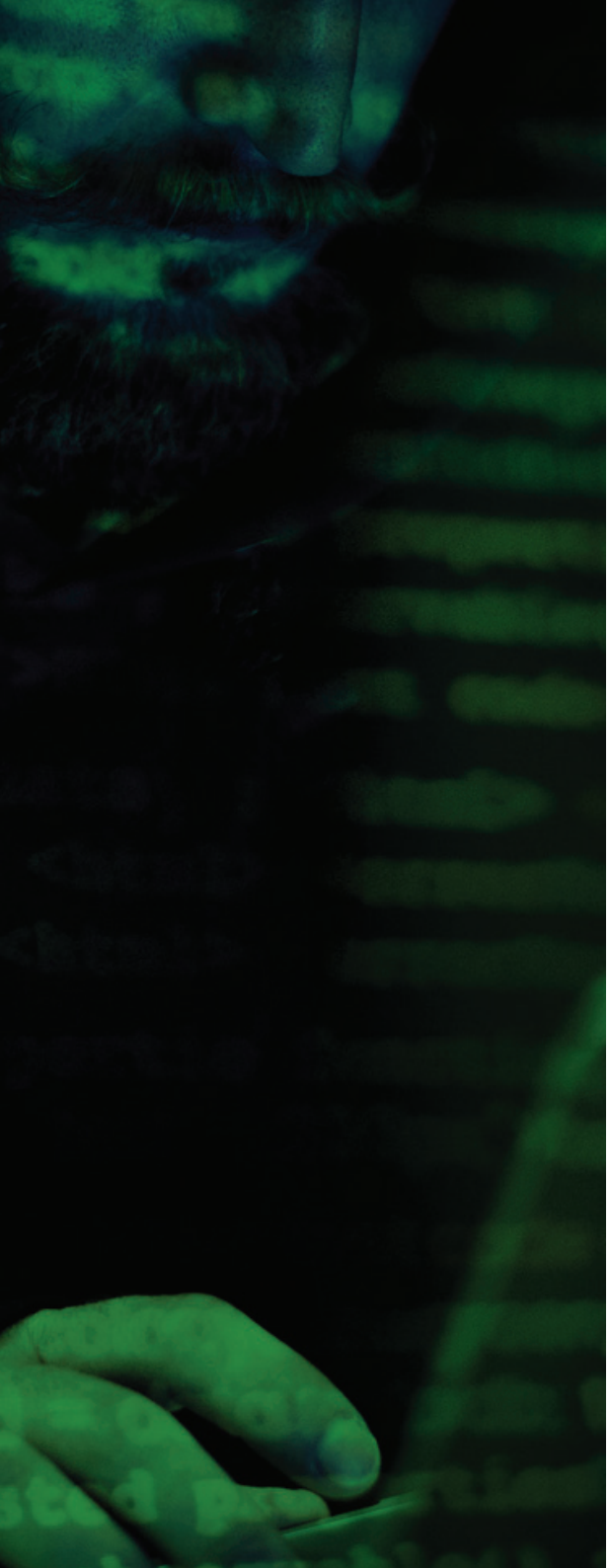
Threat Level: Medium
Category: Infector
Method of Propagation: Removable or network drives
Behavior:

- Drops malware file at %TEMP% folder.
- Infects files with EXE and SCR extensions.
- Also infects files over the shared network.

10. LNK.Cmd.Exploit.F

Threat Level: High
Category: Trojan
Method of Propagation: Email Attachments and malicious websites
Behavior:

- Uses cmd.exe with ""/c"" command line option to execute other malicious files.
- Executes simultaneously a malicious .vbs file with name "help.vbs" along with a malicious exe file.
- The malicious vbs file uses Stratum mining protocol for Monero mining.



Top 10 PUA

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.

Fig. 8 represents the top 10 PUAs and Adware detected in Q1 2019

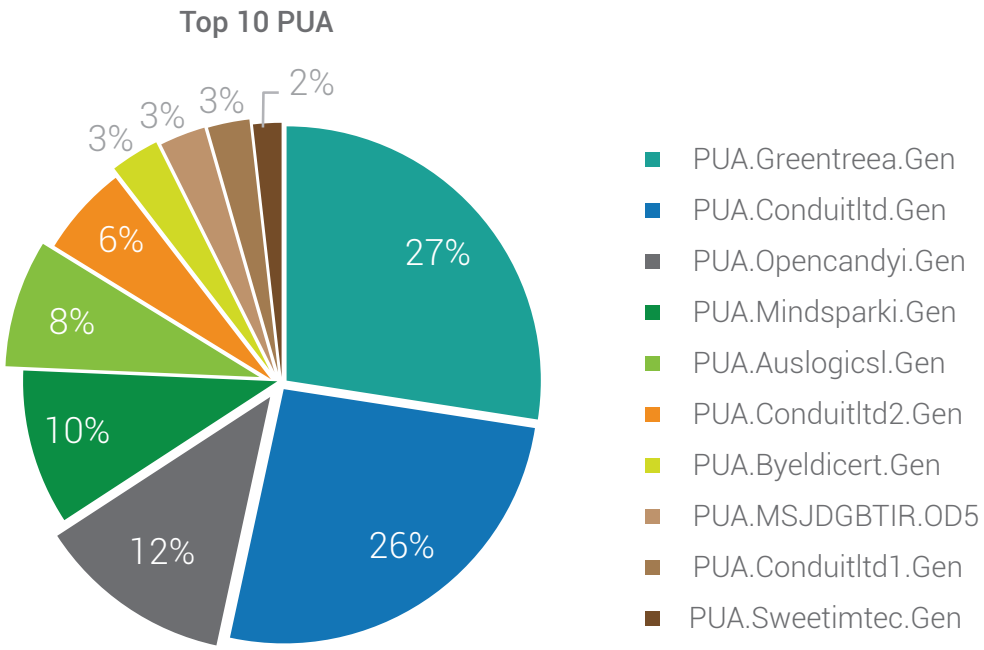


Fig.8

Observations

- With 27% detection, PUA.Greentreea.Gen is the top PUA in Q1 2019

Top 10 host-based exploits

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.

Top 10 host-based exploits of H2 2018

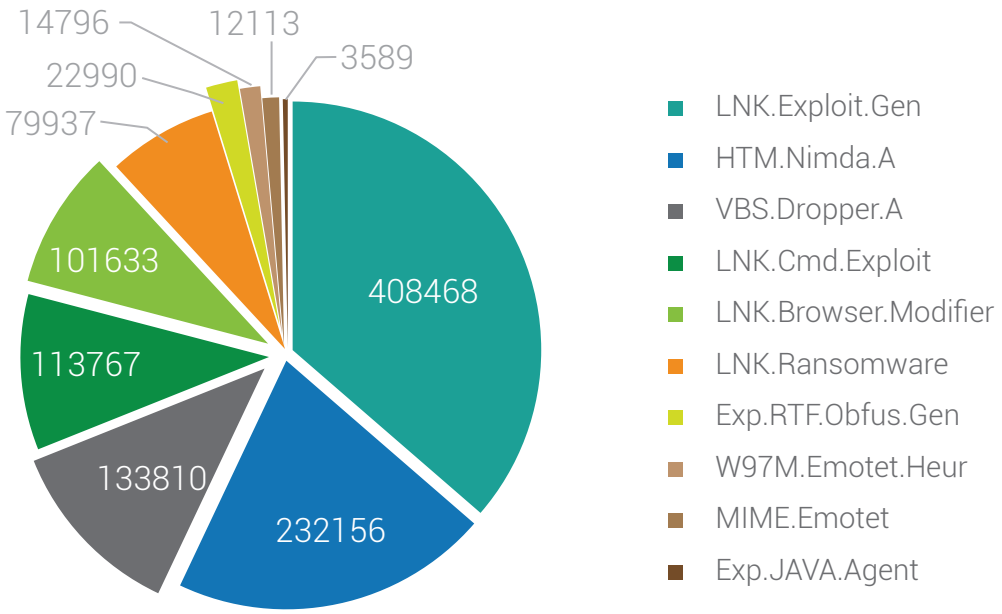
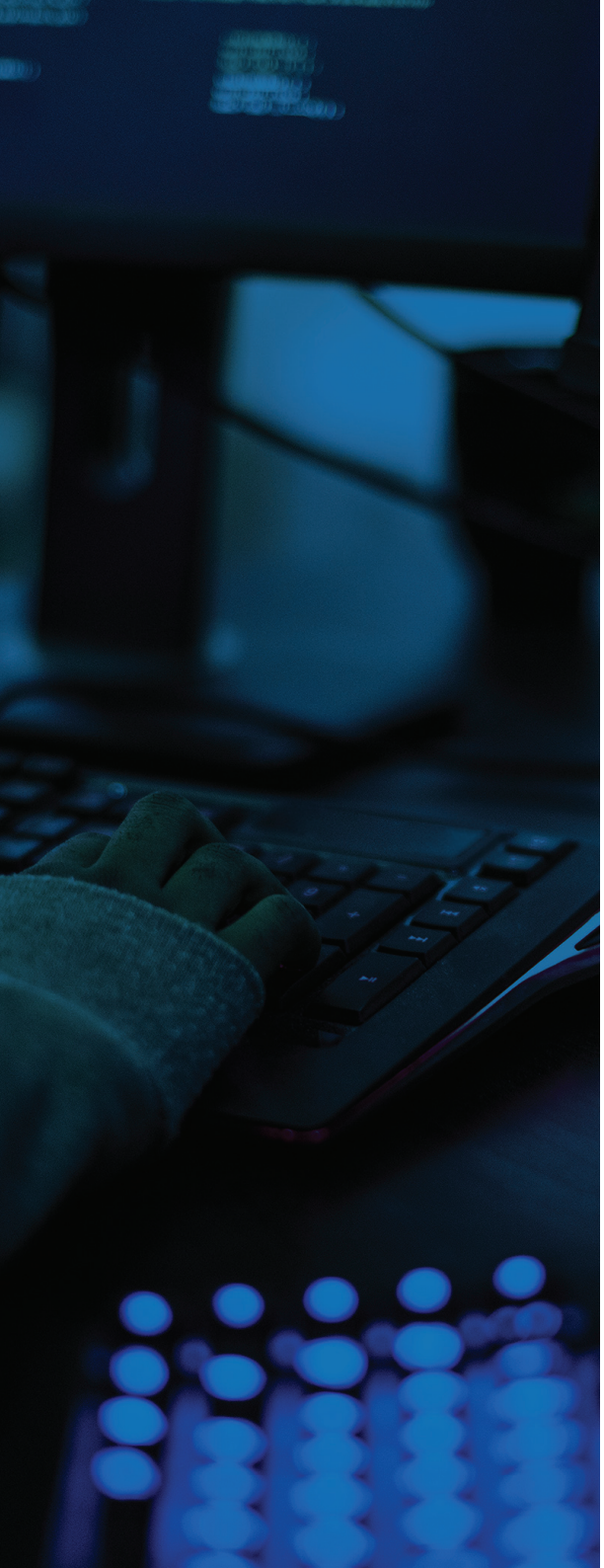


Fig.9

Top 10 Commonly found malware file names

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

1. autorun.inf	3. Service_KMS.exe	5. Public.exe	7. images.scr	9. AutoPico.exe
2. KMS-R@1n.exe	4. DOC001.exe	6. movies.exe	8. mssecsvc.exe	10. Key.exe



Trends in Windows Security

Insecure Remote Desktop & SMB

Quick Heal Security lab observed continues 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. RemoteDesktop Protocol (RDP) widely used for remotely connecting to Windows systems. Where as

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, 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 Metaspolite. As a result of the brute force, the attacker gets reverse meterpreter shell. Then attacker can create new user with administrative rights on victim's machine. Once attacker creates 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 complex password, password expiration & account lockout policies should be implemented. Most important - **Keep backup of all important data**.

Open source tools being misused

Quick Heal Security Labs observed a rising trend of abusing open source tools for building new malware.

These tools help extensively for finding new methods of attack. Incorporating such utilities make attacker's life easy and reduce their development time drastically. Also, these abusers do not need to be sapient for crafting hostile payloads. They just need to choose and integrate tools with their main component and new malware variant is ready to deliver.

Often such open source tools are easily available on GitHub and other similar platforms. We can classify them as an exploit framework, vulnerability scanners, password stealer, privilege elevators, evaders, etc. Generally, these tools contain the framework for exploiting existing vulnerabilities in the system and often target unpatched systems.

In our lab, we observed increasing trends in the last quarter. Many cryptojacking and ransomware cases have been reported in the lab which were bundled with open source components using Squiblydoo, download cradle techniques, tools like Mimikatz and eternal blue vulnerable scanners.

GandCrab Riding Emotet's Bus!

Emotet known for constantly changing its payload and infection vectors like spam mail, malicious doc and even malicious JS files. It compromised a very high number of websites on the internet. Emotet malware campaign has existed since 2014. Most of the websites are genuine but somehow tricked into delivering Emotet. But this time, some of these websites were seen delivering the infamous GandCrab Ransomware V 5.1 for some time. The payload was downloaded through a malicious doc on the victim's computer using VBA macro. The PowerShell script from macro connected to the compromised website and downloaded GandCrab Ransomware from the URL. The GandCrab v5 ransomware has started using task scheduler ALPC vulnerability to gain System privileges on an infected computer. After encryption, it asks for $700 in dash/bitcoin cryptocurrency; also 10% charges are applicable for miner fees/commission.

Ref - https://blogs.seqrite.com/gandcrab-riding-emotets-bus/

A new ransomware campaign in the wild, LockerGoga!!

Quick Heal Security Lab observed new destructive ransomware - "LockerGoga." Source of infection of this ransomware includes Spam Mails, RDP (Remote Desktop Protocol). Upon arrival on the target machine, LockerGoga ransomware changes password of targeted machine. Further, it tries to log off users who are currently logged into the system. Further it drops self-copy at %temp% with random name. Then it starts encryption activity. It appends ". locked" extension to the encrypted files. After completion of encryption activity, it drops ransom note as "README_LOCKED.txt" on a desktop.

A 19-year-old vulnerability in WinRAR (CVE-2018-20250)

Few days back, researchers at Israel based cybersecurity vendor reported a 19 year old code execution vulnerability in the WinRAR tool. WinRAR is widely used tool for compression and decompression of multiple archives. This vulnerability affected over 500 million users of this program. This vulnerability is absolute path traversal bug while extracting ACE archives. Attackers can craft and embed malware payload in ACE archive with rar extension. When a vulnerable version of WinRAR is used to extract such crafted ACE archive, the malicious payload by attacker is extracted in startup folder and executed by system on next time when system restarts.

Past discloser of this vulnerability attackers have started using exploiting this vulnerability to distribute ransomware. According to security forums many APT campaigns have started exploiting this vulnerability to distribute their payload.

Conclusion

Enterprises continue to remain at significant risk of malware infections, data breaches and other cyber-security related breaches, as evidenced by Seqrite's Threat Report Q1 2019. Malware continues to present a significant threat, as per the statistics, 216 malware are detected every minute on enterprise endpoints.

Enterprises hence cannot afford to drop their guard against the continued threats. Cyber criminals keep discovering new ways to create havoc, as evidenced by the threat of cryptojacking, a dangerous threat which silently uses a victim's computer to generate cryptocurrency. Over 17K cryptojacking malware were detected in Q1 2019 every day.

The year is also likely to see increased awareness about privacy laws, the right to be forgotten and data security in this day and age. Governments across the world are slowly expanding their horizons to cybersecurity legislation and the year could well see more legislation like the wide-ranging GDPR from the European Union. Behemoths like Facebook and Google, which deal with huge amounts of personal data, will continue to come under added pressure from countries around the world trying to make sense of the entire furore around election meddling and the loss of privacy.

Enterprises must then stay nimble and agile to keep up with these changes. Often, enterprises do not invest in back-ups as much as they should, in the often misplaced belief that they are not at risk. Modern businesses depend heavily on the continuous availability of data be it of the customer, product, employee or financial. Data backups, in such cases, are the life savers of enterprises. There are many instances where businesses have suffered the loss of data but were able to get back on their feet very quickly because they were wise enough to backup their data. Backups restore the data quickly and enable the business to continue its operations. While fortifying their cybersecurity defences by securing endpoints and maintaining resilient network infrastructure, it is also incumbent to stay abreast with changing laws and regulations. Penalties for non-compliance will continue to be staggeringly high and enterprises must ensure they do not put themselves at risk, either through a cyber attack or a fine due to non-compliance with cybersecurity regulations.