SEQRITE

SEQRITE THREAT REPORT

H2 | 2018

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 July 1, 2018 to December 31, 2018 reporting period.

In cybersecurity terms, 2018 could probably be defined as "business as usual". Cybersecurity threats only increased; there were news of even more daring attacks and cyber breaches with more companies waking up to the catastrophic damage the lack of a cybersecurity framework can cause.

Facebook Data Breach in September which exposed the personal information of nearly 50 million users was possibly the biggest data breach of the year, considering the sheer scale, size and reputation of the brand involved. An attack which really illustrated the frightening consequence of a hacking attack to banks in India, Pune's Cosmos Bank was siphoned off Rs 900 million through a malware attack on their servers. Taking cognizance of the growing need for banks to secure themselves against this onslaught of cyber-attacks, the Reserve Bank of India (RBI) issued a circular calling for a robust cybersecurity/resilience framework for Urban Cooperative Banks (UCBs) to ensure proper security. British Airways announced that 380,000 card payments on its website were compromised during a 15-day period between August 21st and September 5th. As we can see, it has been an eventful year for enterprises ranging across all sectors.

Our threat report suggests that every minute 186 malware were detected on enterprise endpoints. Overall malware detection count in H2 2018 stands at over 49 million. The month of August clocked the highest detection rate. We also detected 10 cryptojacking malware every minute in H2 indicating the speed at which this new threat is spreading its wings. We also saw a spike in Emotet activity ("an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans") in November 2018 with the modus operandi being similar: malicious Word and PDFs which are presented as legitimate financial documents like invoices, bank statements, alerts, etc.

In H2, we observed that the IT/ITES industry had the maximum malware detections with over 27% of the total detections followed by Professional Services, Manufacturing and Educational Institutions respectively.

Word of caution from CTO

"Increase in fileless malware is making it very important for other security layers to be rightly deployed and configured."

WINDOWS

Detection Highlights: H2 2018

Malware

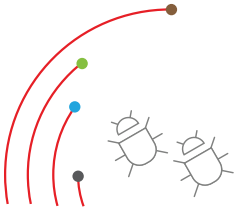
- Per Minute - 186
- Per Hour -11140
- Per Day -267368
- H2 2018 - 49195780

Ransomware

- Per Minute - 02
- Per Hour - 110
- Per Day - 2645
- H2 2018 - 486695

Cryptojacking

- Per Minute - 10
- Per Hour - 627
- Per Day - 15042
- H2 2018 - 2767697

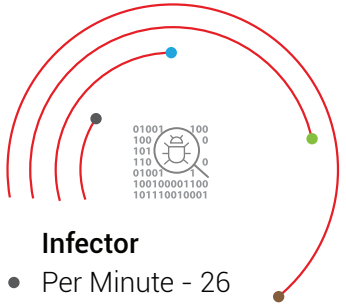


Exploit

- Per Minute - 06
- Per Hour - 344
- Per Day - 8266
- H2 2018 - 1520875

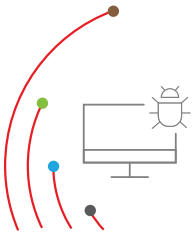
Worm

- Per Minute - 13
- Per Hour - 781
- Per Day - 18753
- H2 2018 - 3450555



Infector

- Per Minute - 26
- Per Hour - 1532
- Per Day - 36774
- H2 2018 - 6766360



PUA & Adware

- Per Minute - 04
- Per Hour - 257
- Per Day - 6178
- H2 2018 - 1136779

Malware Detection Statistics: Month Wise

The below graph represents statistics of the total count of malware detected by Seqrite during the period of July to December in 2018.

Windows Malware Detection Count in H2 2018

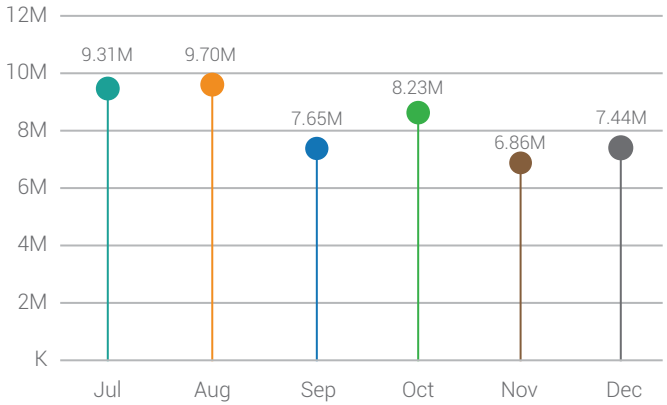


Fig. 1

Observations

- Seqrite detected over 49 million Windows malware in H2 2018
- August clocked the highest detection of Windows malware

Detection Statistics: Quarter Wise

Windows Malware Detection Count in H2 2018

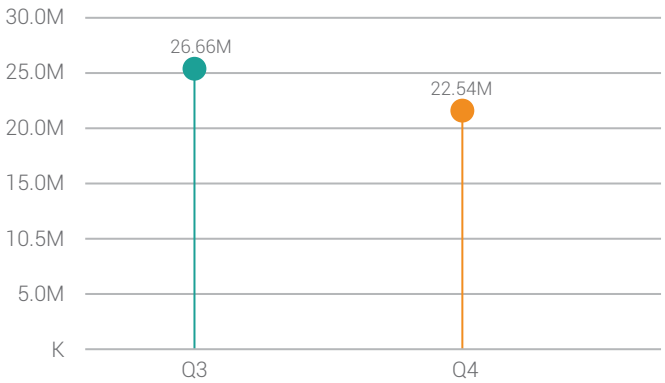


Fig. 2

Observations

- Malware detection count was the highest in Q3

Malware Detection Statistics: Week wise

Windows Malware Detection Count in H2 2018 | Week over Week

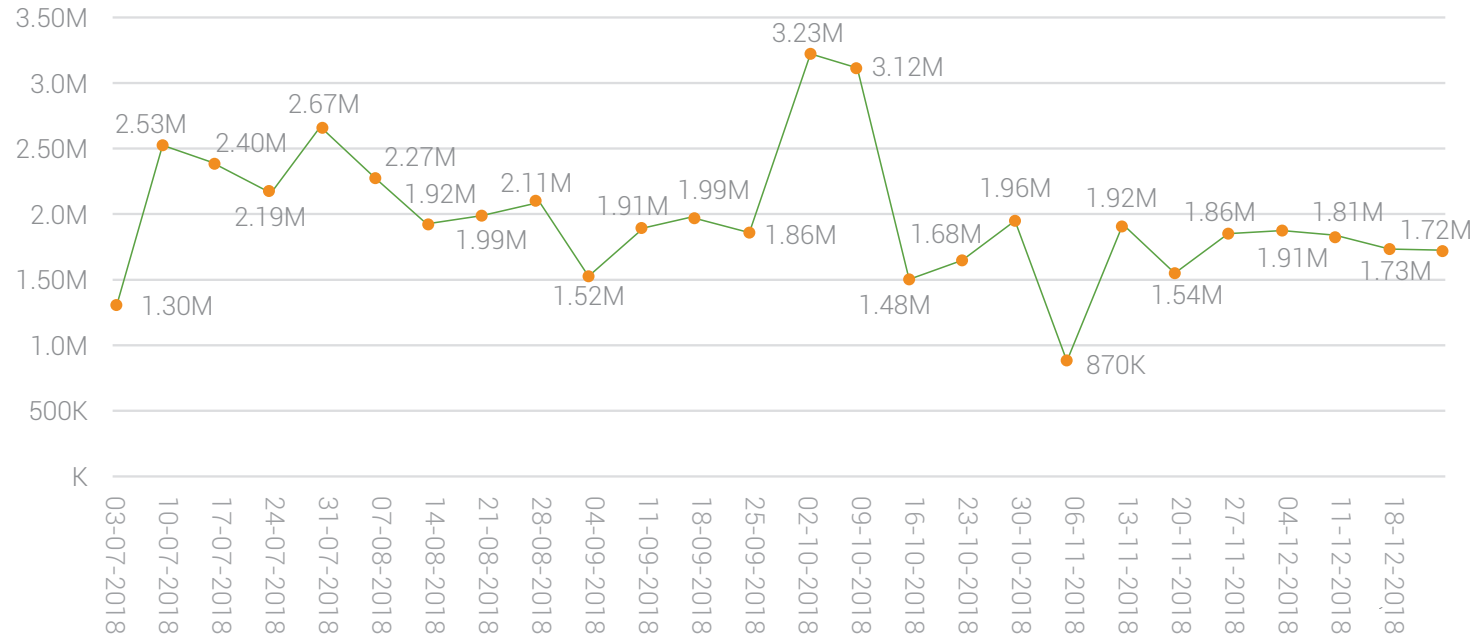


Fig.3

Observations

- Malware detection count was the highest in the week starting with 2nd October.

Malware Detection Statistics: Category-wise

Categorywise Detection | Quarterwise (Q3-Q4)

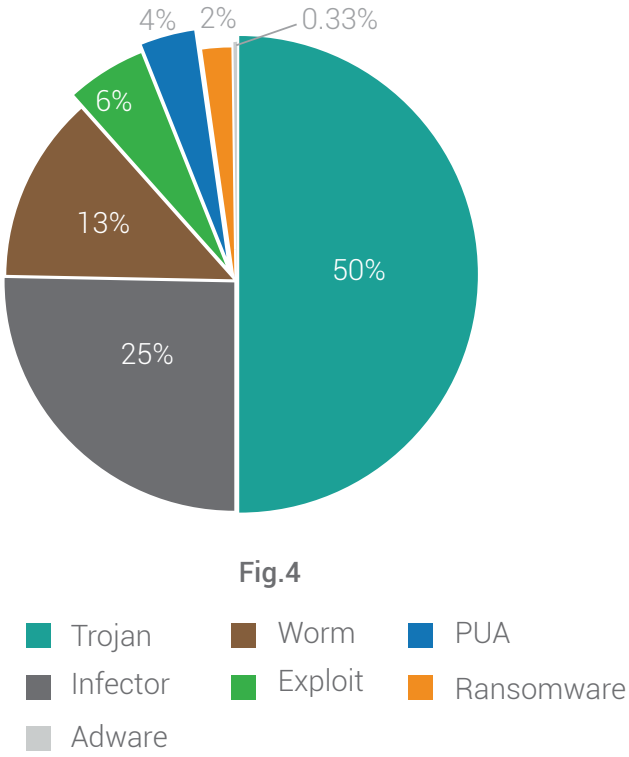


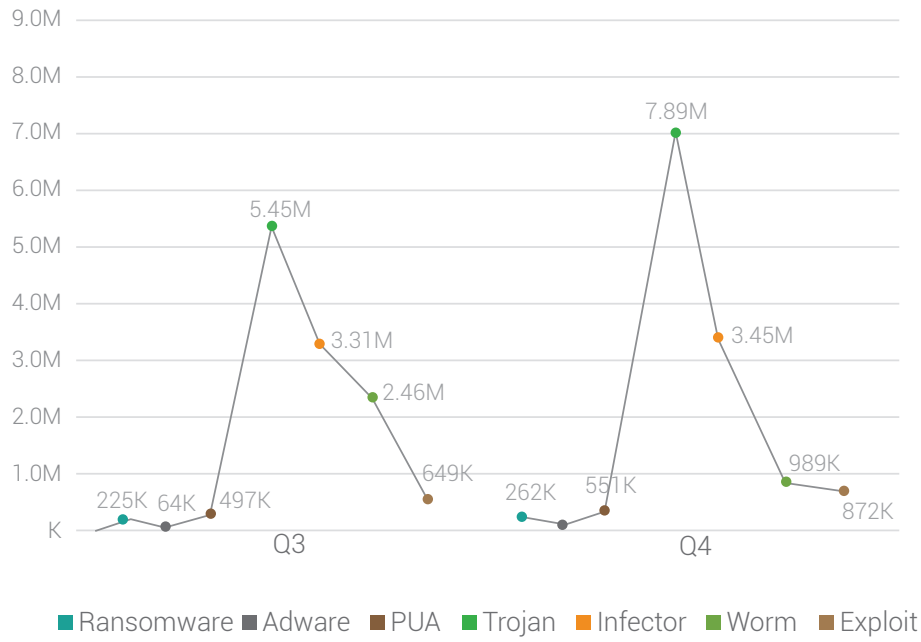
Fig.4

Observations

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

Malware Detection Statistics: Category-Wise by Quarter

Categorywise Detection | Quarterwise (Q3-Q4)



Observations

- Malware detection count was the highest for Trojan in both the quarters

Industry Wise Detection Stats

Fig.6 represents the malware detection count for the below mentioned industries.

Industry	Percentage
IT/ITES	27.83%
Professional Services	24.43%
Manufacturing	17.70%
Education	11.08%
Healthcare	5.17%
Government	4.85%
Logistic	3.20%
Automobiles	2.16%
BFSI	2.16%
Media & Entertainment	0.97%
Strategic & Public Enterprises	0.19%
Transport	0.12%
Telecom	0.10%
Power & Energy	0.04%

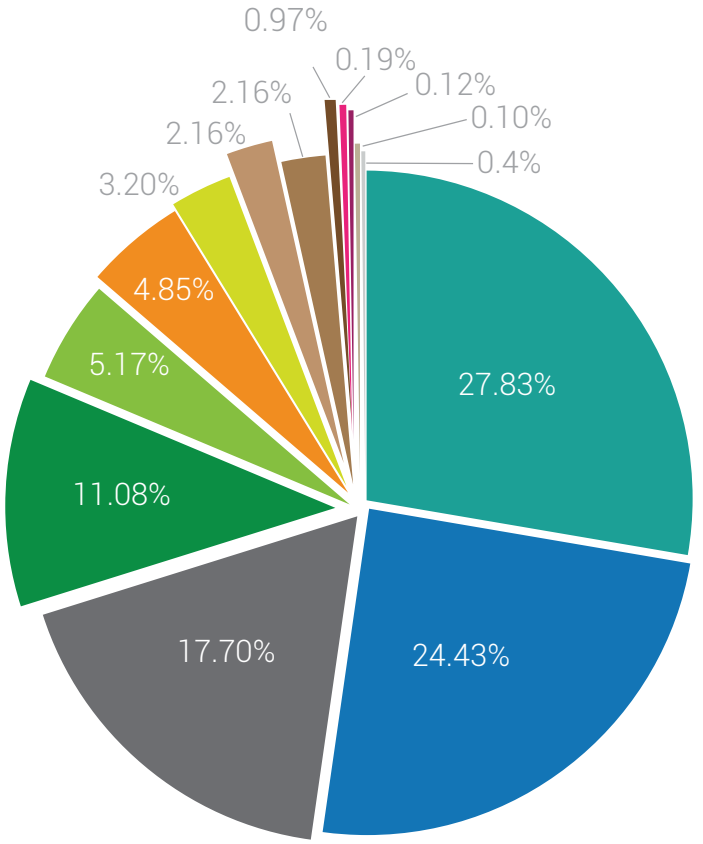


Fig.6

Observations

- IT/ITES industry had the maximum malware detections with over 27% of the total detections.
- The IT/ITES industry was followed by Professional Services, Manufacturing and Educational Institutions respectively in the highest malware detection count.

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

Industry Wise Top Detections

Here are the top detections (malware with the highest count) for each of the below mentioned industries.

Industry	Top Detection
Automobiles	Trojan.Emotet.X4
BFSI	W32.Pioneer.CZ1
Education	W32.Sality.U
Government	Trojan.Shadowbrokers
Healthcare	W32.Sality.U

Industry	Top Detection
IT/ITES	W32.Pioneer.CZ1
Manufacturing	Trojan.KillAv.DR
Media & Entertainment	W32.Ramnit.A
Professional Services	W32.Pioneer.CZ1

Observations

- Trojan.Shadowbrokers, Worm.NSIS.NeksMiner.A, and W32.Sality.U have shown their presence in most of the industries.
- Trojan.Shadowbrokers malware is mostly observed in ransomware attacks. It has the capability to delete shadow copies on the system.
- Worm.NSIS.NeksMiner.A is a malware observed in Cryptojacking attacks
- W32.Sality.U injects its code into all running system processes & then spreads further by infecting the executable files on local, removable, and remote shared drives.

Protection Wise Detection Stats

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

Protection Wise Stats | H2 2018

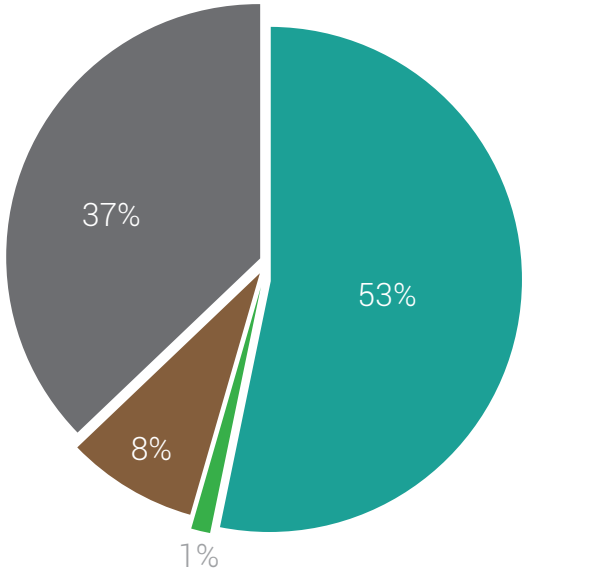


Fig.7

- **Real Time Scan**

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

- **Email Scan**

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

- **Memory Scan**

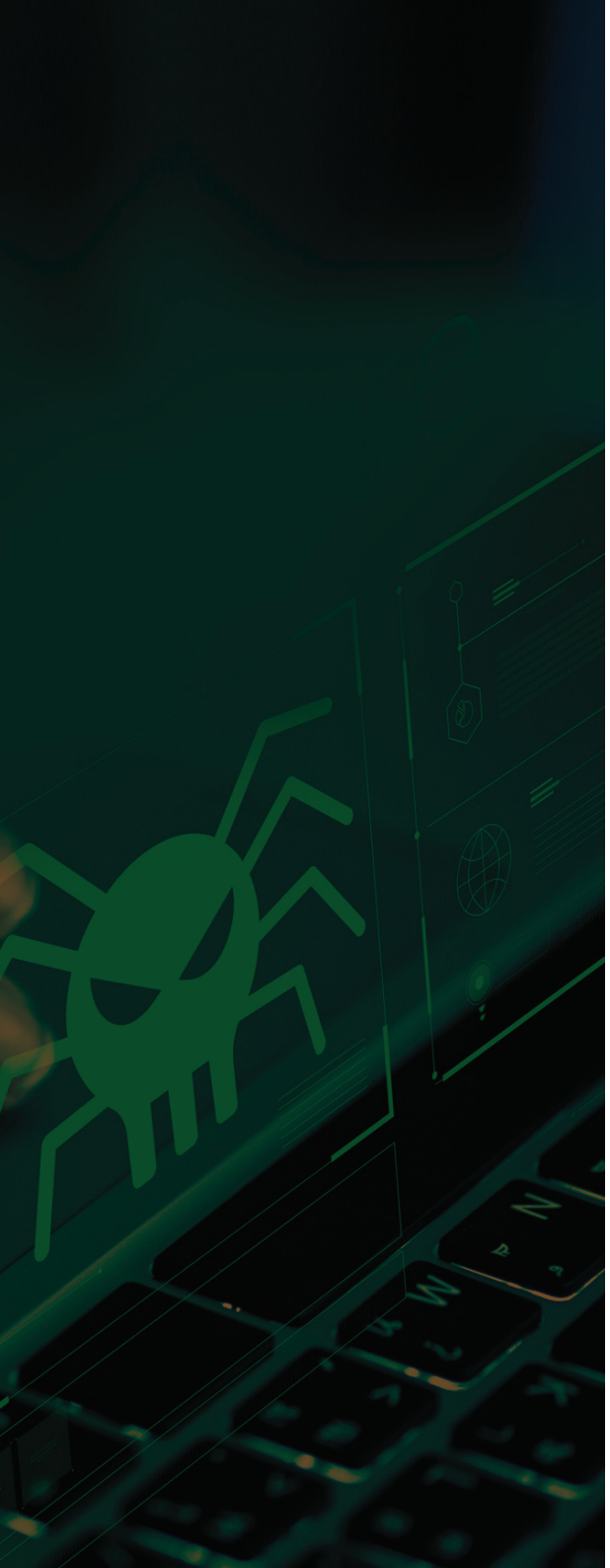
  Scan which controls and oversees the operations necessary to optimize the use of RAM.

- **On Demand Scan**

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

Observations

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



Top 10 Windows Malware

Fig.8 represents the top 10 Windows malware of H2 2018. These malware have made it to this list based upon their rate of detection from July to December.

Top 10 Windows

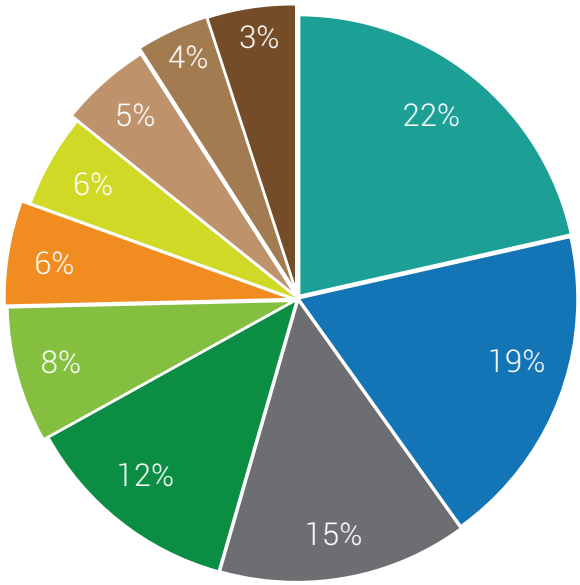


Fig.8

- Trojan.KillAv.DR
- W32.Sality.U
- W32.Pioneer.CZ1
- W32.Brontok.Q
- LNK.Browser.Modifier
- LNK.Exploit.Gen
- Trojan.Emotet.X4
- Trojan.Starter.YY4
- W32.Virut.G
- LNK.Cmd.Exploit.F

1. 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 malware 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 has icons similar to genuine windows applications.

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 the disk and shared network.
- It decrypts malicious DLL present in the file & drops it.
- This DLL performs malicious activity and collects system information & sends it to CNC server.

4. W32.Brontok.Q

Threat Level: Medium
Category: Worm
Method of Propagation: Spreads through mail or infected USB & network drives
Behavior:

- This worm spreads through email or infected USB drives.
- It stores several copies of itself in 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 also modifies several system configuration parameters to disable the registry editor and command prompt, as well as modifies the safe boot shell to prevent the user from cleaning the machine.

5. LNK.Browser.Modifier

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

- Injects malicious codes into the browser which redirects the user to malicious links.
- Makes changes to the browser's default settings without user knowledge.
- Generates ads to cause the browser to malfunction.
- Steals the user's information while browsing like banking credentials for further misuse.

6. LNK.Exploit.Gen

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

- 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.

7. Trojan.Emotet.X4

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

- It arrives on victim's machine through malicious website or by execution of malicious powershell code.
- It drops self-copy and creates a service in victims machine and steals user's information
- Malware downloads different modules and other malware, also creates run entry for persistence.
- It is majorly known as threat distributor.

8. 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.

9. W32.Virut.G

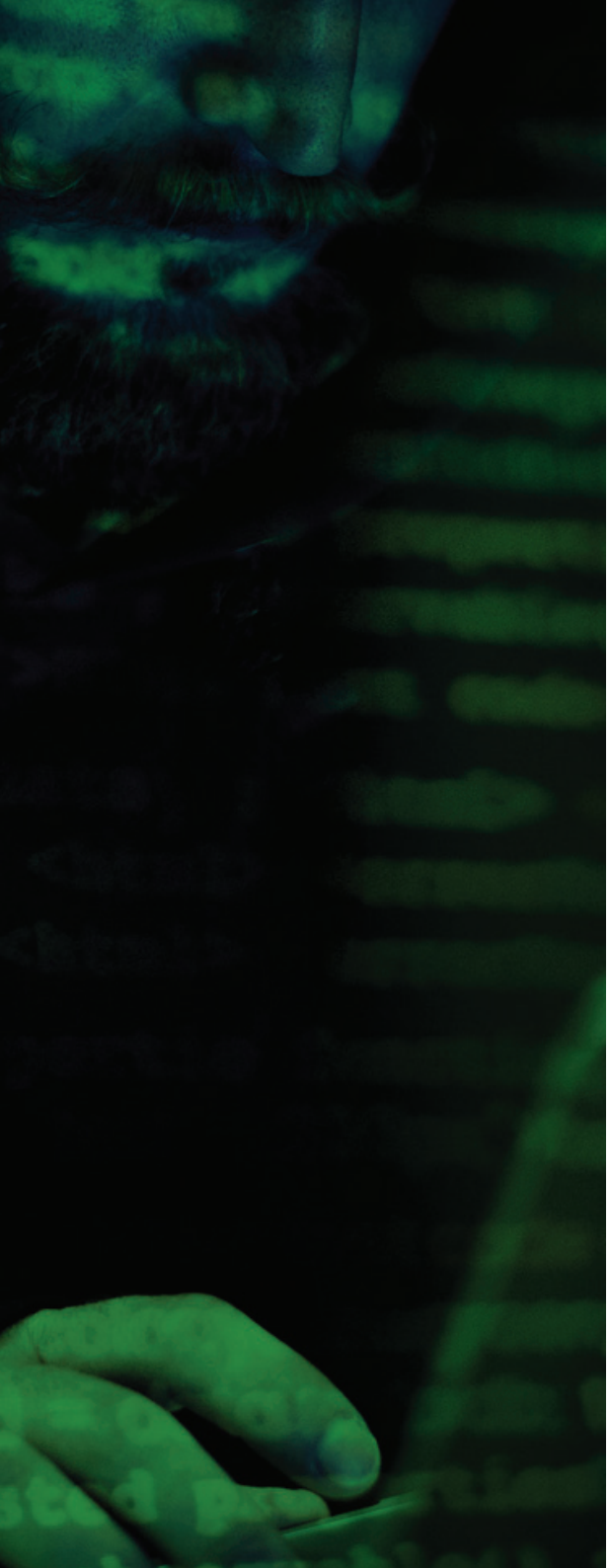
Threat Level: Medium
Category: Infector
Method of Propagation: Bundled software and freeware
Behavior:

- Creates a botnet that is used for Distributed Denial of Service (DDoS) attacks, spam frauds, data theft, and pay-per-install activities.
- Opens a backdoor entry that allows a remote attacker to perform malicious operations on the infected computer.
- The backdoor functionality allows additional files to be downloaded and executed on the infected system.

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.



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. 9 represents the top 10 PUAs and Adware detected in H2 2018.

Top 10 PUA

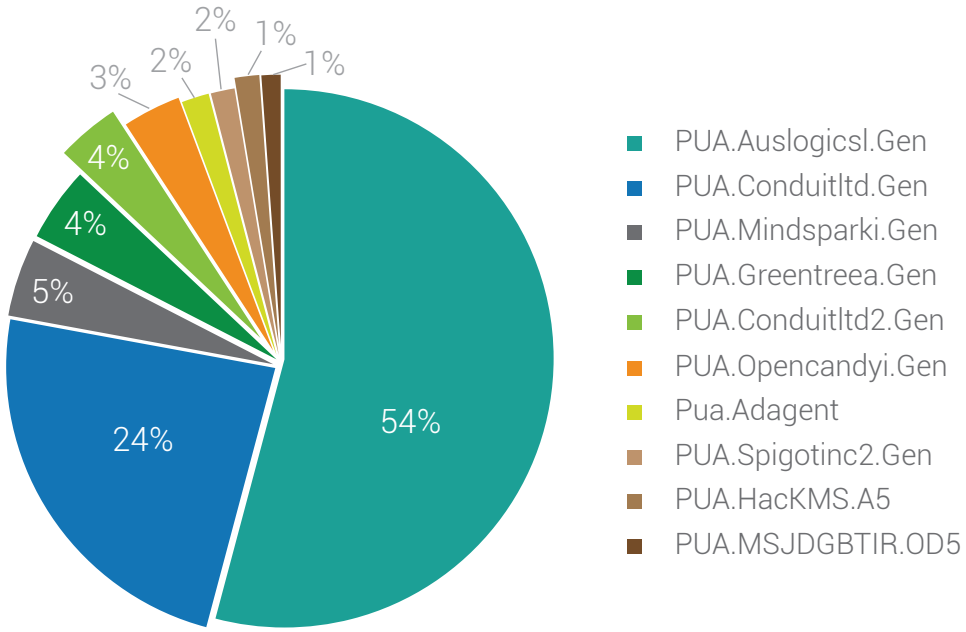


Fig.9

Observations

- With 54% detection, PUA.Auslogicsl.Gen is the top PUA in H2 2018

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

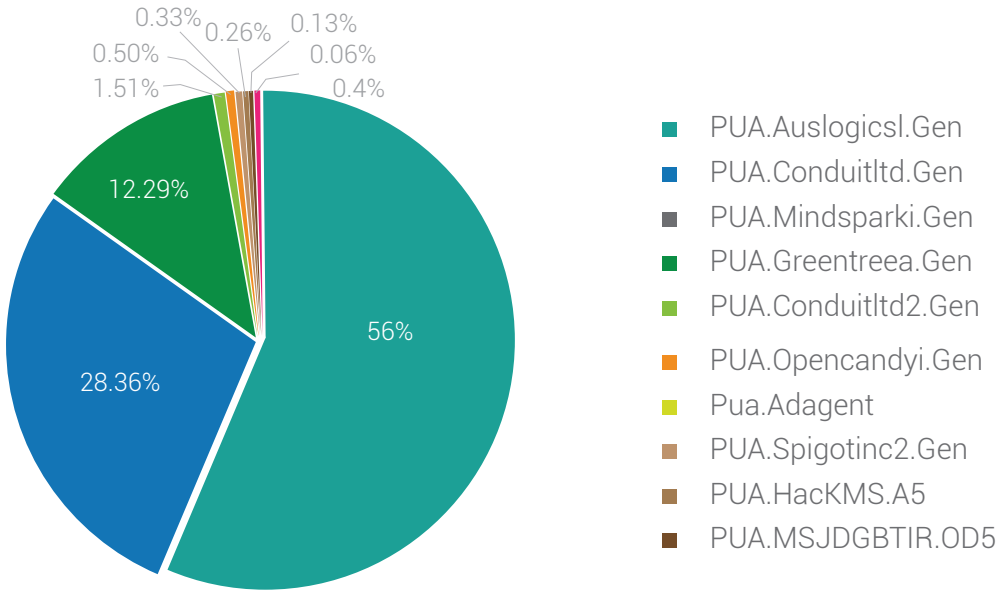
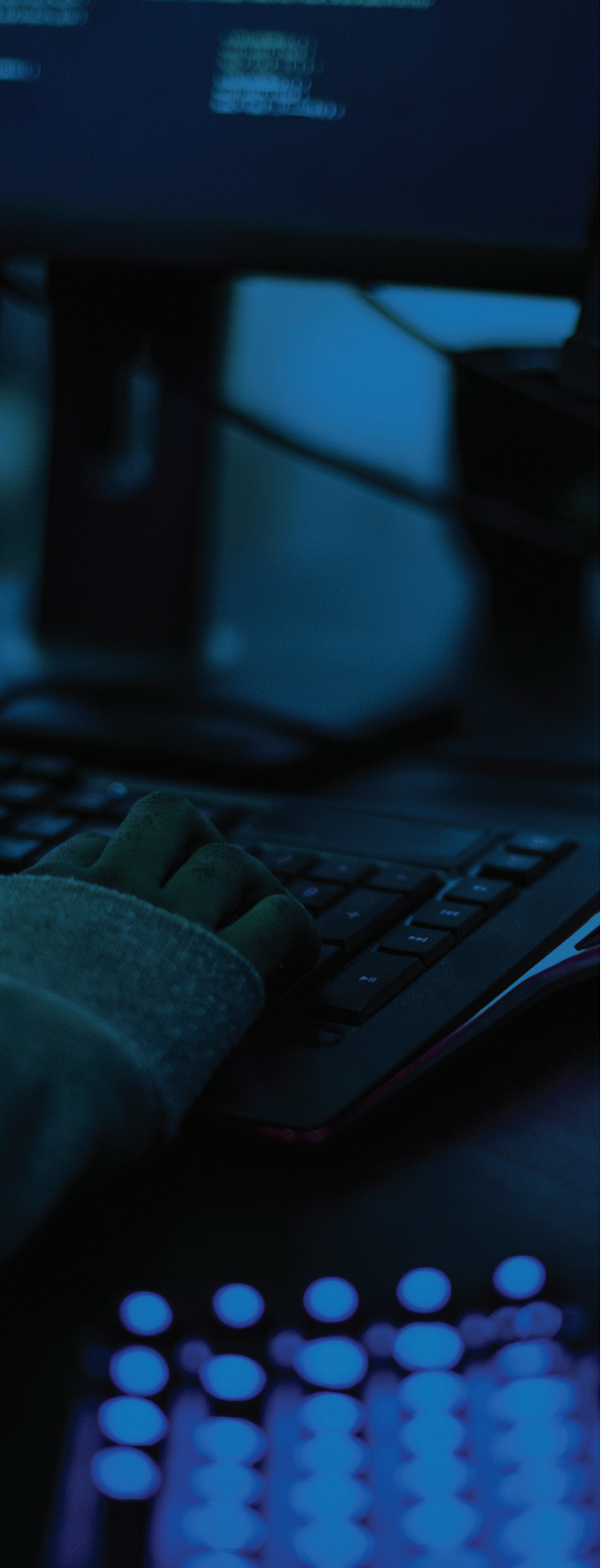


Fig.10

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. Public.exe	5. images.scr	7. Service_KMS.exe	9. Documents.exe
2. DOC001.exe	4. movies.exe	6. svchost.exe	8. IMG001.exe	10. iedvtoolex.dll

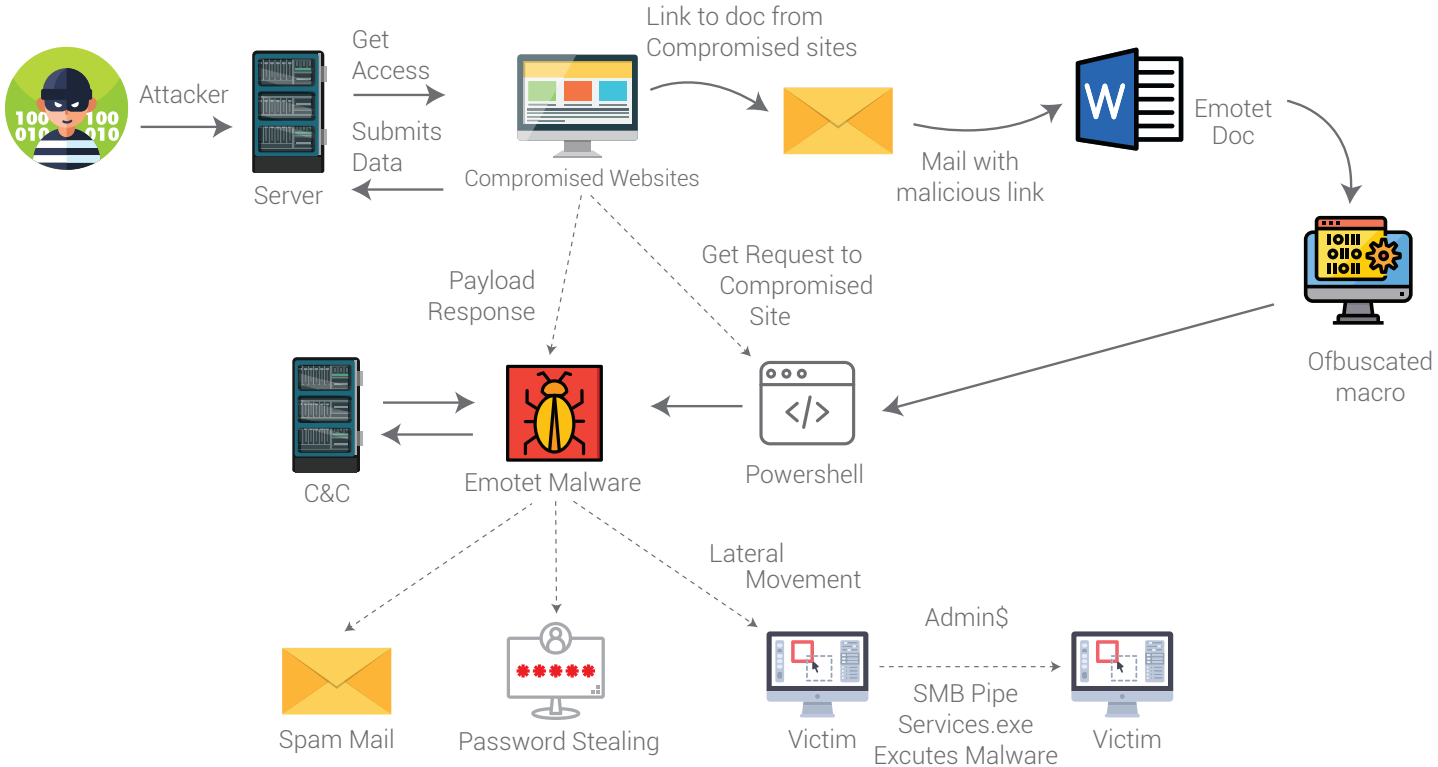


Trends in Windows Security

Emotet: A banking Trojan in trend

Emotet is also known as a malware distributor. Throughout the year, we have seen many different patterns in Emotet campaign's initial attack vector, which is malicious doc or xls file. These files contain highly obfuscated VBA macro code which ultimately executes cmd.exe through calls to Shell() and Run() functions. It further executes a second stage obfuscated PowerShell code to download and execute the malware from malicious domains. The PowerShell script holds 2 or more malicious URLs in case some domains are inactive. Emotet's obfuscated macro patterns have evolved over the year and has employed various obfuscation techniques to evade signature-based detection. Initially the macro was seen to be obfuscated with different mathematical functions like Mid, Sin, Tan, Trim and Shapes etc. Then it switched to using split string and string reverse patterns.

Emotet Complete Life Cycle



Ref: https://blogs.seqrite.com/beware-your-website-might-be-delivering-emotet-malware/

GandCrab: Evolving to secure the shell!

Change is a law of life. But even in information security, Ransomware authors like Gandcrab seems have taken this seriously. GandCrab was first observed in late January this year and within a month they claimed to have infected over 50,000+ nodes. This massive infection undoubtedly turned Europol's head and made them coordinate with a security firm to hack GandCrab servers for decryption keys. Malspam emails are being observed as a major attack vector in GandCrab

1st Version

Description: This is the first Ransomware which used Dash Currency. Office, database and other important processes like mail applications were stopped and files were encrypted so that no important file which might be in use is left behind without encryption. AES-256 was used for file encryption and AES-256 Key and IV was encrypted with RSA 2048.

Drawback: Poorly Protected C&C servers. Dependent on internet connectivity i.e. Encryption didn't continue until it finds a server, meaning if PC wasn't connected to internet at the time of infection, one could remove malware and data would be safe!

Decryptor for this version was launched in late February.

2nd Version

Description: Started using Namecoin powered .Bit TLD (Top-Level-Domain) as Command And Control Servers (keys and data moved to a more secure location). Security researchers and police who hacked servers for keys were honoured by using their names for Hostnames. Ransomware had used autorun entry in RunOnce registry key

Drawback: Dependent on internet connectivity i.e. Encryption didn't continue until it finds a server, meaning if PC wasn't connected to internet at the time of infection, one could remove malware and data was safe!

3rd Version

Description: This time, ransomware had added desktop wallpaper. Also continued to use autorun entry in RunOnce registry key.

Drawback: This version could not execute correctly on Windows 7 PC. It resulted in users not being able to use access desktop.

4th Version

Description: Continued using Dash crypto currency. Instead of AES, it had started using SALSA20 algorithm for file encryption. Salsa20 made encryption process faster. Salsa20 key was encrypted with RSA2048, thus it made encryption impossible without the private key. Encryption process didn't wait for C&C server response. Distribution carried out by compromised websites.

Drawback: Continued to use DASH crypto-currency many users are unaware of.

5th Version

Description: Started Encrypting files with random extensions thus AV might not detect by extension. HTML ransom note also included. Network shares are also encrypted. Many variants of version 5 were launched.

At the end of the year 2018, GandCrab launched multiple variants. One variant was showing message box 'We will become back very soon :)!'. This may be an indication of a major update launching at the start of the coming year for a celebration of GandCrab's Birthday!

Ref: https://blogs.seqrite.com/gandcrab-says-we-will-become-back-very-soon/

Ghost Has Arrived

Quick Heal Security Labs observed new ransomware in wild – Ghost. Interesting fact about this malware is that it uses multiple components to encrypt user files. Main malware executable (Ghost.exe) is compiled using the DotNet Framework. The infection vector of this ransomware is still unknown, but this file may arrive on the victim's machine via spam emails, malvertising, bundled with other files, etc. It uses an icon of the spreadsheet to deceive the user to think he has received an invoice/quotation etc.

Ref: https://blogs.seqrite.com/ghost-has-arrived/

Obfuscated Equation Editor Exploit (CVE-2017-11882) spreading Hawkeye Keylogger

Cyber-attacks through phishing emails are increasing and generally, attackers use DOC embedded macros to infiltrate victim's machine. Recently, Quick Heal Security Labs came across a Phishing e-mail sample which uses Microsoft's equation editor exploit to spread Hawkeye keylogger.

Cybercriminals use different techniques to steal confidential data. Now they are offering advanced forms of malware to fulfil their purpose. That's why we are still observing actively evolving new threats. Hawkeye belongs to a family of keylogger. The latest Hawkeye v8 reborn uses Microsoft Office Equation Editor Vulnerability CVE-2017-11882 to infiltrate. This exploit uses new techniques to evade detection of AV product. It compiles its code while executing and loads payload in memory without writing it on the disk.

Ref: https://blogs.seqrite.com/obfuscated-equation-editor-exploit-cve-2017-11882-spreading-hawkeye-keylogger/

CVE-2018-15982- Adobe Flash Player use after free (Zero Day) vulnerability alert!

The recent zero-day vulnerability CVE-2018-15982 in Adobe Flash Player enables attackers to perform a Remote Code Execution on targeted machines. Adobe had released a security advisory APSB18-42 on December 5, 2018 to address this issue. According to Adobe, the in-wild exploit is being used in targeted attacks. This is a Use after free vulnerability in Adobe Reader which allows attackers to perform a Remote Code Execution on targeted machines. The vulnerability allows for a maliciously crafted Flash object to execute code on a victim's computer, which enables an attacker to gain command line access to the system. After successful exploitation, attackers can take control of the vulnerable system and executes extracted malware

Ref: https://blogs.seqrite.com/cve-2018-15982-adobe-flash-player-use-after-free-zero-day-vulnerability-alert/

Cryptojacking

What attracts more than a magnet? You might have guessed it right – it is money! And where there is easy money, there is a lot of hustle and bustle. Cryptojacking- which uses someone else's computer to generate digital cash, aka cryptocurrency, for an attacker as long as they want. Due to its ease of deployment and an instant return of investments, cryptojacking has replaced ransomware as the number one threat for consumers and enterprises.

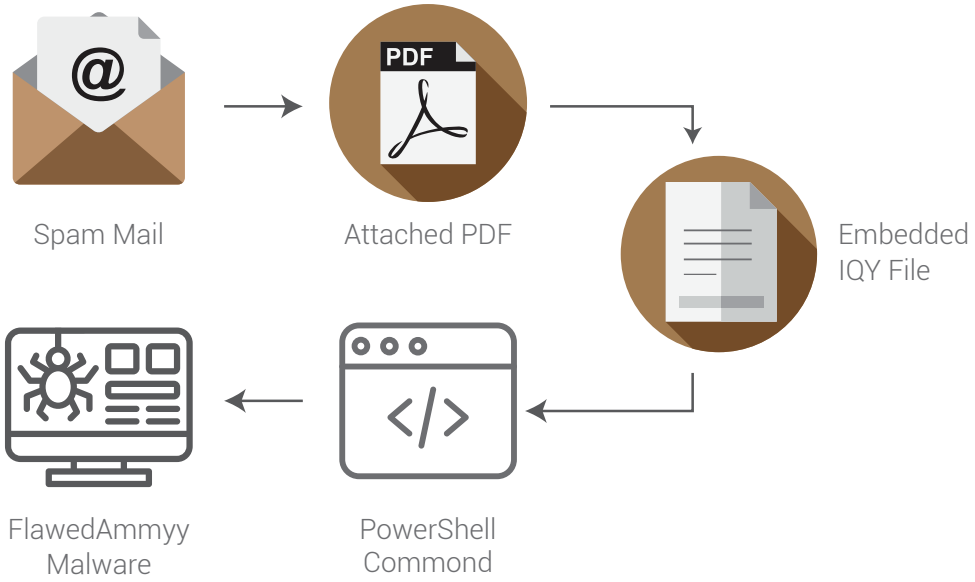
If one's computer is being used for cryptojacking, the only sign they might notice is slower performance or lag in execution. Most crypto mining scripts eat 100% of the targeted computer's CPU power which can significantly lower the lifespan of the hardware itself. In most cryptojacking cases that got reported, neither the owners of the compromised website nor its users were aware that they were the victims.

computer's CPU power which can significantly lower the lifespan of the hardware itself. In most cryptojacking cases that got reported, neither the owners of the compromised website nor its users were aware that they were the victims.

Emerging trend of spreading malware through IQY files

Attackers are constantly in search of finding new ways to spread malware; and delivering malware through IQY files is gaining lots of attention lately. IQY file is an Excel Web Query file that is used to download data from the internet. Attackers use Spear Phishing campaigns and spam mails with attached PDF or IQY files. In PDF, the 'importDataObject' function is used to import iqy file, and when the security checks are enabled, .iqy file is downloaded at %temp% location of victim machine and executed. Attackers have used this attack to deliver RATs like FlawedAmmyy RAT (remote access trojan).

Blog: https://blogs.quickheal.com/emerging-trend-spreading-malware-iqy-files/



MaaS Moving Towards APT as A Service?

Our last year's prediction in Quick Heal Annual Threat Report about the new pillar of MaaS (Malware as a Service) that is RaaS (Ransomware as a Service), became true.

Initially interested only in the development of ransomware payload, RaaS developers started selling entire attack package along with the intrusion mechanism for a lucrative cut in the loot. Newer versions of SATAN Ransomware like DBger were spread in the first half of the year 2018 using RaaS. Satan conceived modular approach by using different templates but similar encryption technique. Here percentage of ransom was given to RaaS developers as a cut for their services. Again, others like FilesLocker ransomware developers are paying affiliate around 70% of their ransom.

This evolution of RaaS is actually pointing towards the future possibility of As-a-Service model for APTs too. We all know that planning and execution of APT (Advanced Persistent Threat) requires lots of skills, resources and time. Hence, in future, malware authors may invest their time to find generic loop-holes in particular sectors like health, banking or cloud and then they will sell a well-organized attack vector to the attackers. Also, another possibility of APTs against particular countries, large organizations, government agencies, law enforcement systems, etc. may become a new pillar of 'Malware as a Service philosophy'. As roots of MaaS are spreading fast, we must be prepared with strengthened security shields against this organized cybercrime.

Conclusion

Data breaches are bad news and H2 2018 saw a plenty of them. Whether it's the CEO, the CISO or a network administrator, data breaches represent a significant threat which can have potentially catastrophic consequence. The threat of data breaches has only increased in recent years leading to the biggest enterprises rushing to understand, identify and secure this threat.

Enterprises should ensure they guard against breaches by employing a strong multi-layered cybersecurity strategy. Deep Learning & Computer vision techniques are making progress in every possible field. With growing computing powers many organizations can use them to resolve or minimize many day-to-day problems.

Governments across the world are strengthening their infrastructure to protect the digital lives and identities of its citizens. There is no exaggeration in the statement that 'future wars will be fought in the cyber domain'. Important elections are coming up in many different countries, including India's General Election in 2019 and it is up to the election officials to ensure there is a fair and free vote without interference from external forces. Considering India's neighbourhood, its place in the world as among the fastest-growing economies and the number of non-friendly actors around it (China, Pakistan, etc.), the chances of state-sponsored cyber-attacks can be high.

Don't try a one-size-fits-all approach-- The digital world is a dynamic and fast-changing world where the environment, threat detection and risk management change drastically. In such an environment, security teams should not try to create one specific approach and be inflexible about imposing it across the enterprise. There should be 'horses for courses' approach with the approach readily flexible to adjust to changing realities.

We operate in an extremely agile and scalable environment. With the help of cybersecurity, organisations must now increase the resilience of their network infrastructure, secure endpoints, and mobilize their workforce while ensuring the critical data is absolutely secure.