SEQRITE

SEQRITE THREAT REPORT

Q2 - 2019

Enterprise Cybersecurity Solutions by Quick Heal

www.seqrite.com

Contributors

Quick Heal Security Labs

Seqrite Marketing Research Team

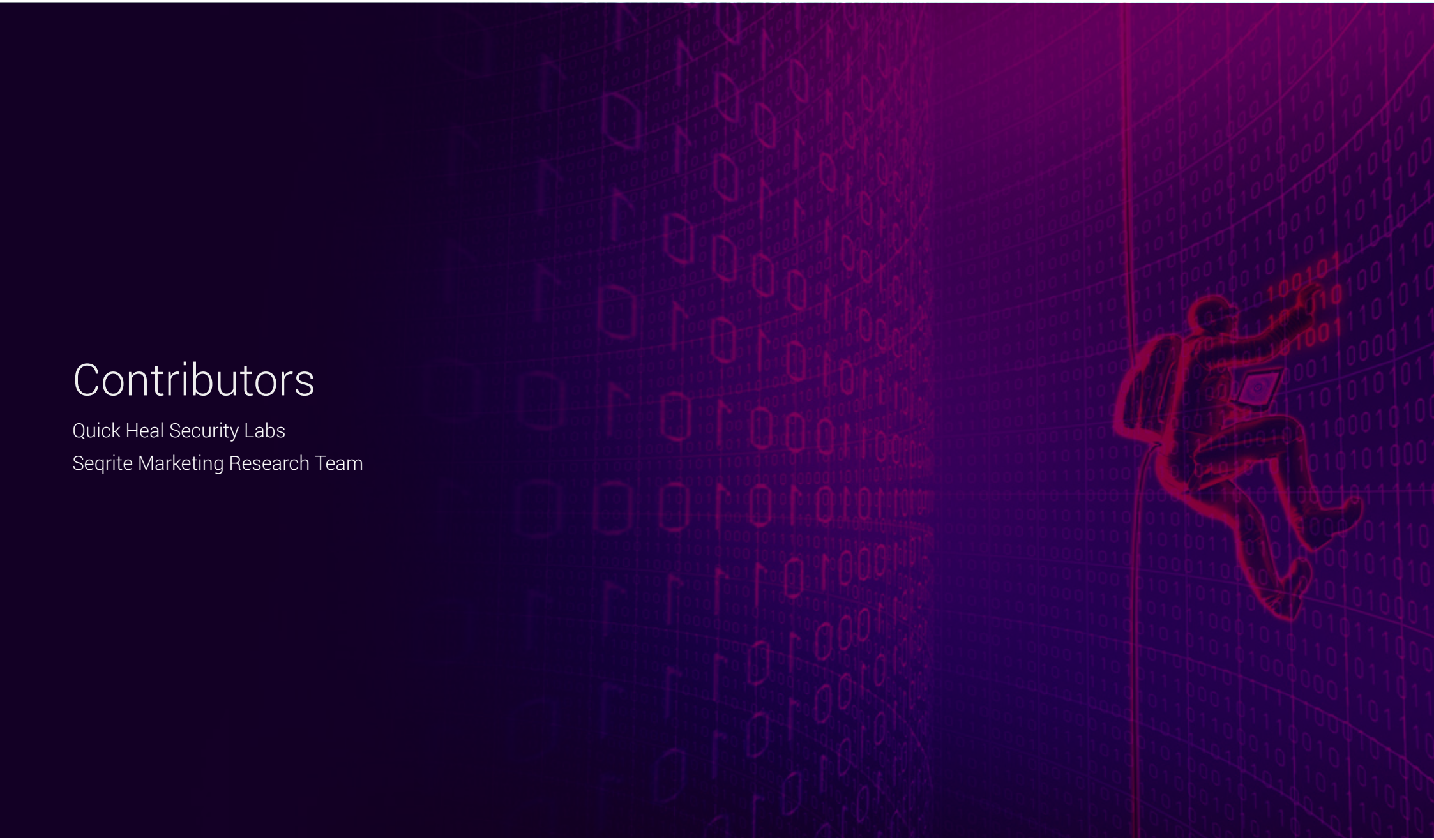


Table of contents

Introduction

The second quarter of 2019 saw some of the worst attacks in recent years. We begin with Amnesty International's Hong Kong office being attacked by Chinese hackers. Followed by this was Perceptics, a surveillance contractor for US customs and border safeguarding, attacked by hackers who stole pictures and license plates of 100,000 travelers. Lastly, in May, Brian Kerbs' discovery of a breach in First American, a real estate and title insurance behemoth exposed data theft of 885 million customers' sensitive financial information.

Seqrite's threat report reveals that 2019's second quarter saw an increase in malware count when compared with Q1 - 2019 by 6 million+ new threats. Overall, enterprises in the months of April, May & June were intruded by 34 million Windows malware. The month of June saw the highest detections at 12.30 million with Trojans continuing to dominate the quarter's threat chart at 40% of penetration – less by 6% than the previous quarter of this year.

While Trojan.KillAv.DR was the worst Trojan for Q2 2019, Worm.AUTOIT.Tupym.A, falling under the worm category had most detections throughout enterprises. Cryptojacking increased to 19K attacks per day from 17K a day last quarter validating Seqrite's Q1 prediction of cryptojacking malware to increase – this also adds up with the progressive rise of cryptojacking malware that we started reporting since last year.

It has also been observed that threat actors are increasingly targeting non-information technology industries such as automobile or manufacturing because such industries give secondary preference to cybersecurity. This is because their primary focus area on investment revolves around capital-intensive machinery. W32.Madang.A that attacked the manufacturing sector the most was designed to steal data.

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

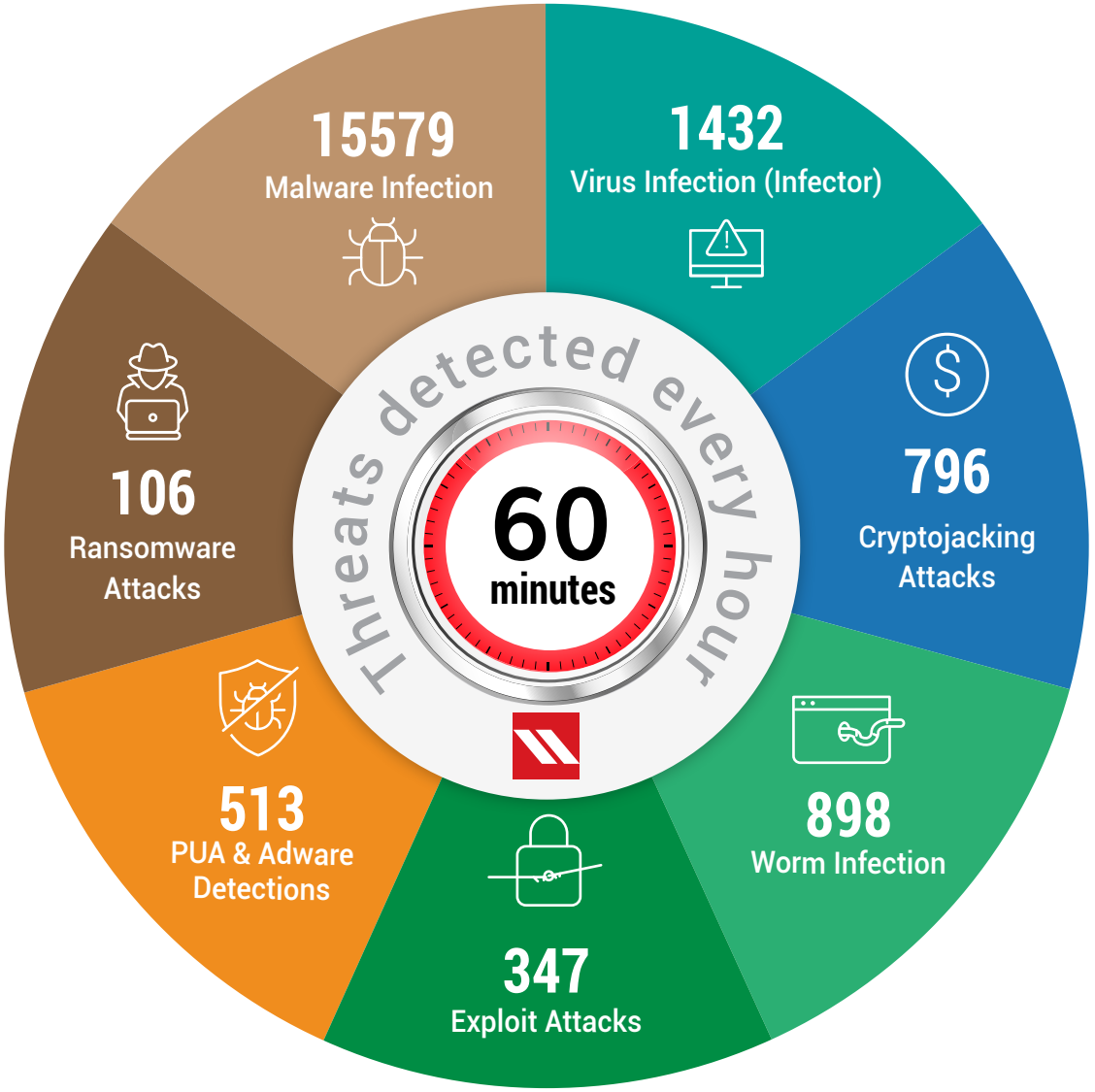
A leading source of threat research, threat intelligence and cybersecurity, Quick Heal Security Labs analyses data fetched from millions of Quick Heal products across the globe to deliver timely and improved protection to its users.

www.seqrite.com

Follow us on:

WINDOWS

Detection Highlights: Q2



Detection Statistics: Month Wise

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

Windows Malware Detection Count

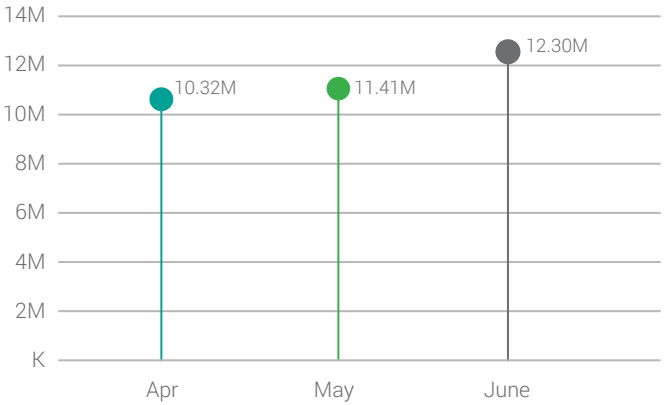


Fig. 1

Observations

- Seqrite detected over 34 million Windows malware in Q2 2019.
- June clocked the highest detection of Windows malware.

Detection Statistics: Week wise

Windows Malware Detection Count

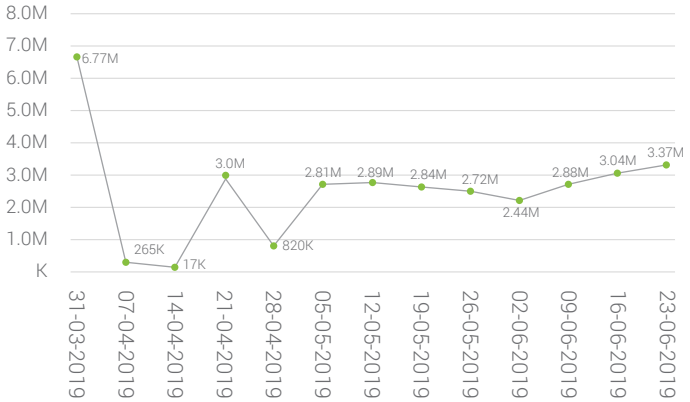


Fig. 2

Observations

- There was a major dip in the detection count in the month of Apr but the detections picked up by May and have been steady thereon.

Detection Statistics: Category-wise

Windows malware detection - Category Wise

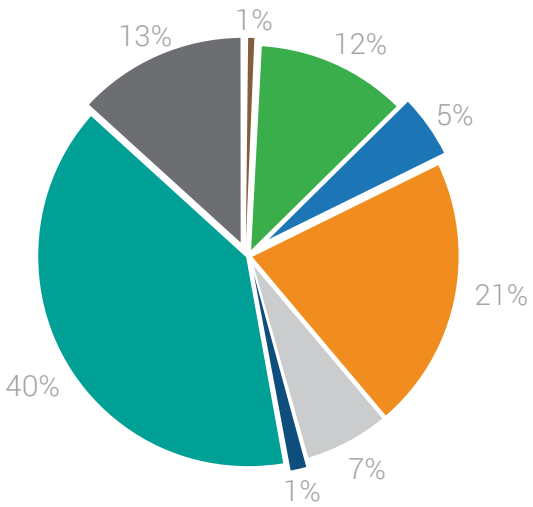


Fig.3

Observations

- Malware detection count was the highest for Trojan accounting to 40% of the detections followed by Infector and Worm.

Detection Statistics: Category-wise

Category wise Detection

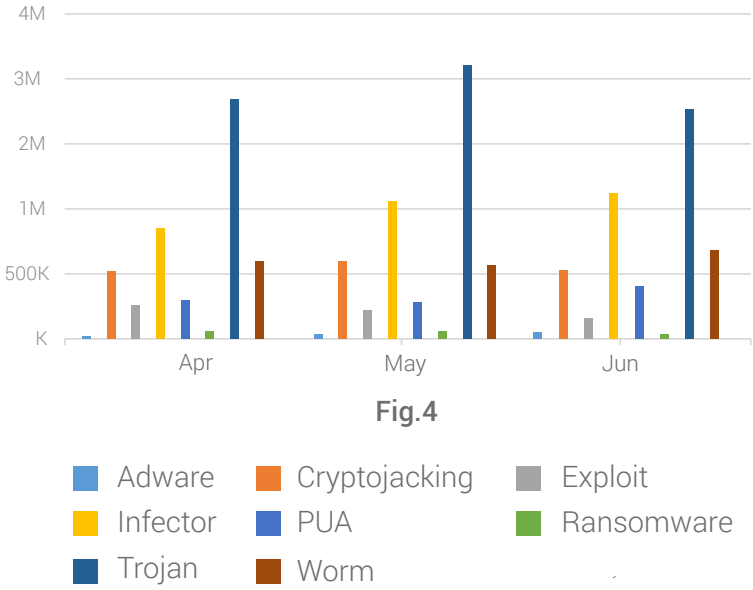


Fig.4

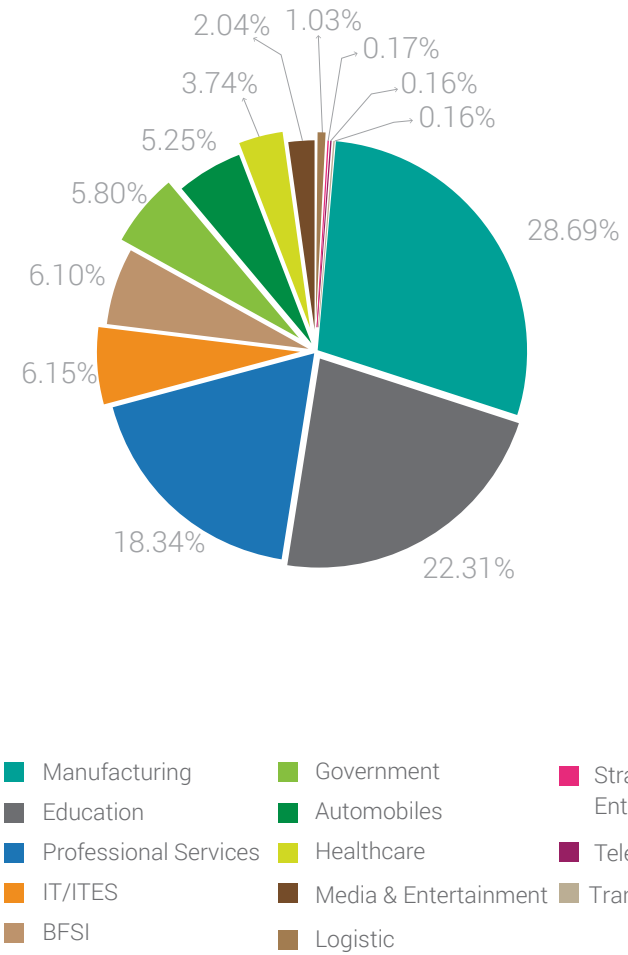
Observations

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

Industry Wise Detection Stats

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

Industry Wise Detection Stats



Industry Wise Top Detection:

Industry	Detection
Manufacturing	Worm.NSIS.NeksMiner.A
Education	Trojan.Shadowbrokers
Professional Services	W32.Pioneer.CZ1
Automobiles	W32.Madang.A
BFSI	W32.Pioneer.CZ1
Media & Entertainment	HTML.IframeRedirect.SK
Hospitality & Healthcare	PIF.StucksNet.A
Government	Trojan.KillAv.DR
IT/ITES	Trojan.Mauvaise.SL1
Logistic	TrojanDropper.Sality.U

Observations

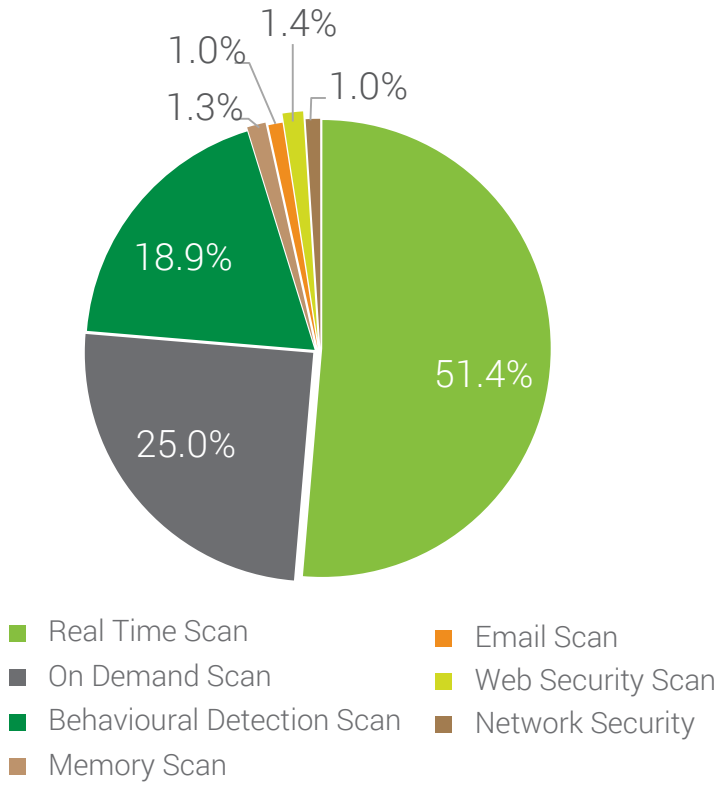
- Manufacturing industry had the maximum malware detections with over 28% of the total detections.
- The topmost malware affecting this industry was Worm.NSIS.NeksMiner.A.

**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



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**

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

- **Memory Scan**

  Scans memory for malicious programmes running & cleans it

- **Email Scan**

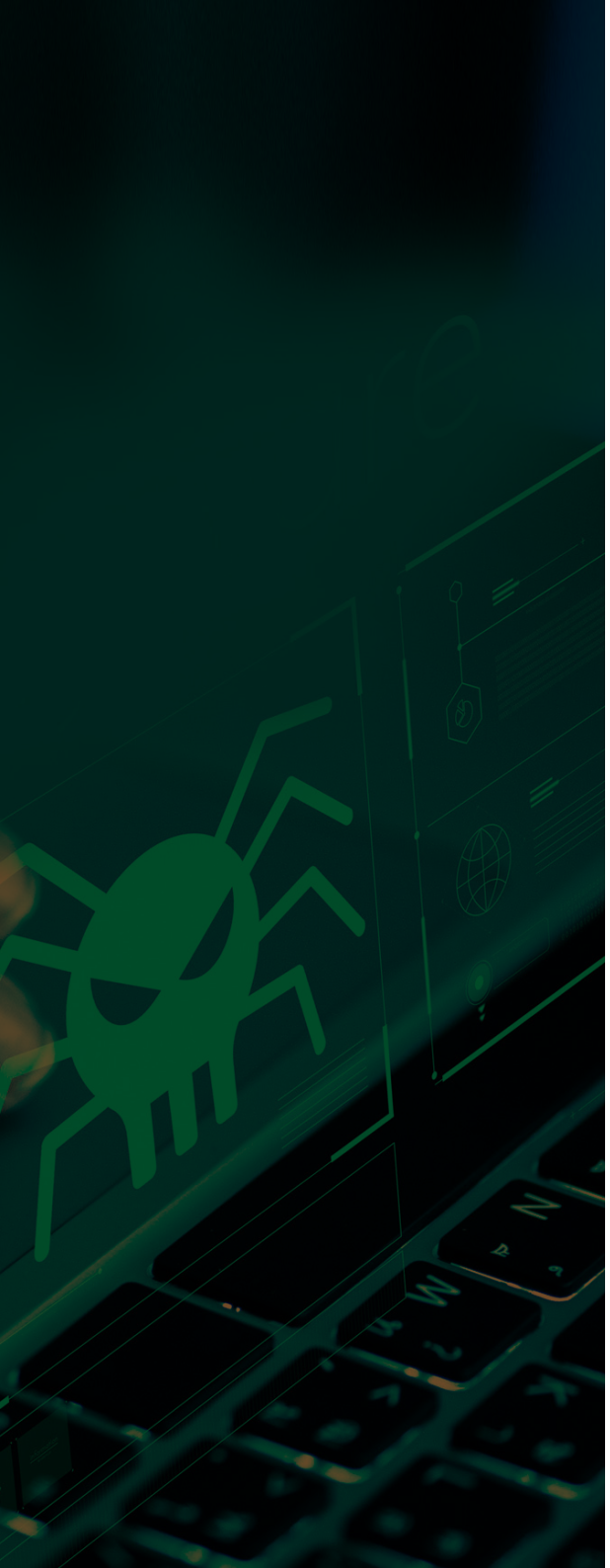
  Blocks emails that carry infected attachments or links to compromised or fake and phishing websites.

- **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 Q2 2019. These malware have made it to this list based upon their rate of detection from Apr to Jun.

Top 10 Windows Malware

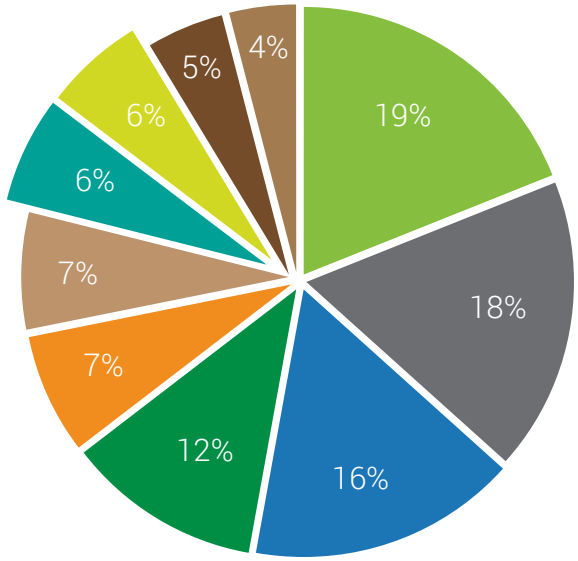


Fig.7

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

1. 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(s) and also modifies start page of browser to another site through registry entry.
- It also creates Run entry for same dropped file for persistence.

2. 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 C&C server.

3. W32.Sality.U

Threat Level: Medium
Category: File infector
Method of Propagation: Removable or network drives
Behaviour:

- IInjects 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.

4. Trojan.KillAv.DR

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

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

5. 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.

6. Worm.AutoIt.Sohanad.S

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

- It arrives in 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 file with a typical Windows folder icon.
- A user mistakenly executes this .exe assuming it as a folder and then it spreads over the network.
- It infects every connected USB drive too.

7. LNK.Exploit.Gen

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

Behaviour:

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

8. VBS.Dropper.A

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

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

9. LNK.Cmd.Exploit.F

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

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

10. LNK.Browser.Modifier

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

- 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.

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 Q2 2019.

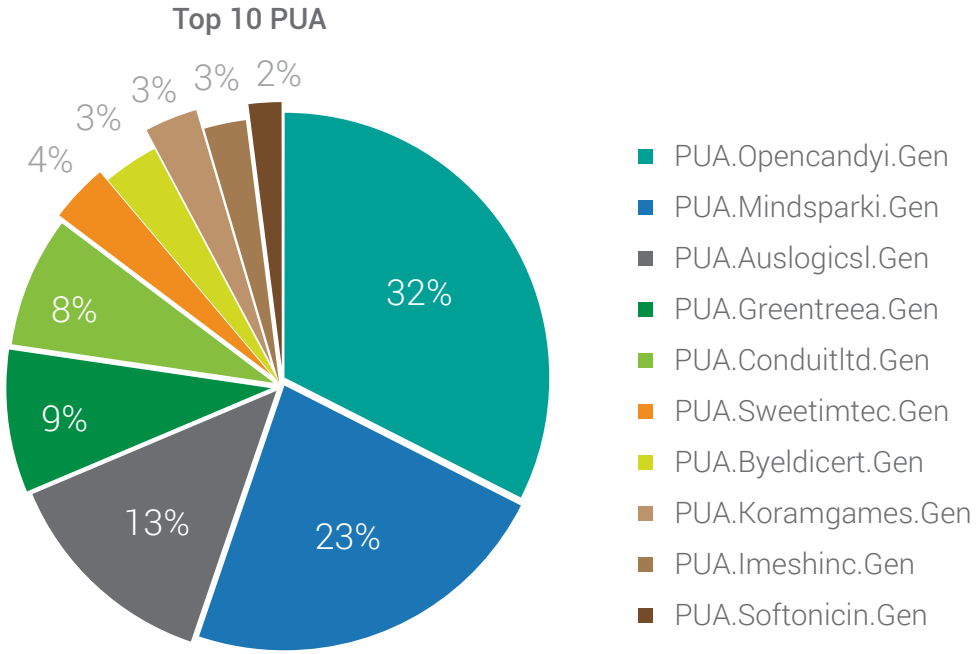


Fig.8

Observations

- With 32% detection, PUA.Opencandyi.Gen is the top PUA in Q2 2019

Top 10 Host-Based Exploits

A computer exploit is an attack designed by a hacker to take advantage of a particular security vulnerability the targeted system has. Below figure represents the top 10 Host-Based exploits of Q2 2019.

Top 10 host-based exploits of H2 2018

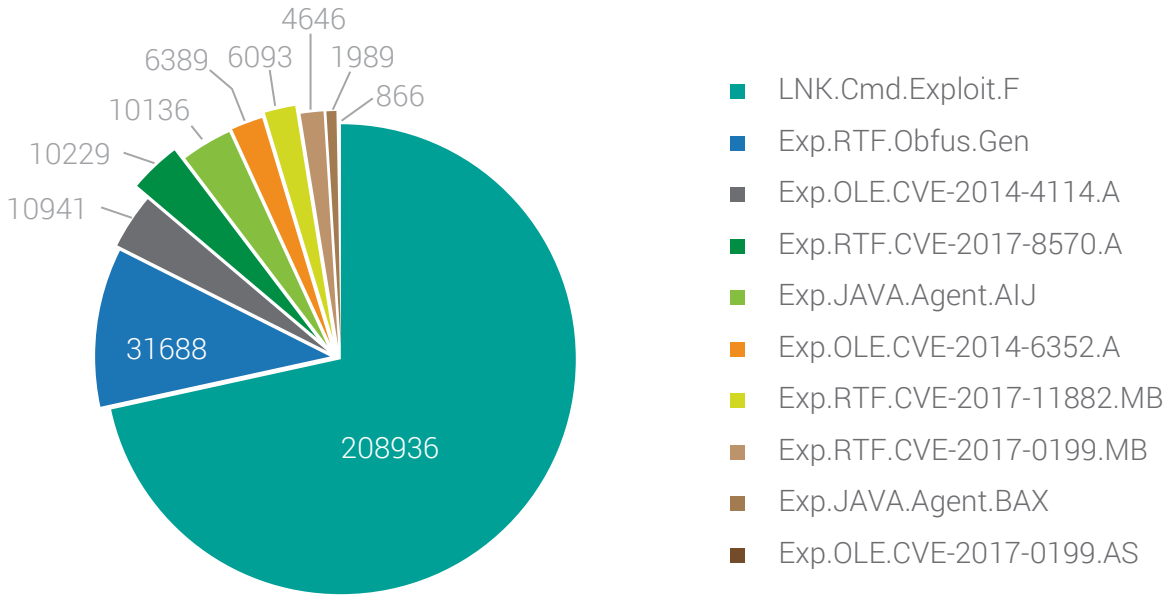


Fig.9

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.

Top 10 Network-Based Exploits

Below figure represents the top 10 Network-Based exploits of Q2 2019.

Top 10 host-network exploits

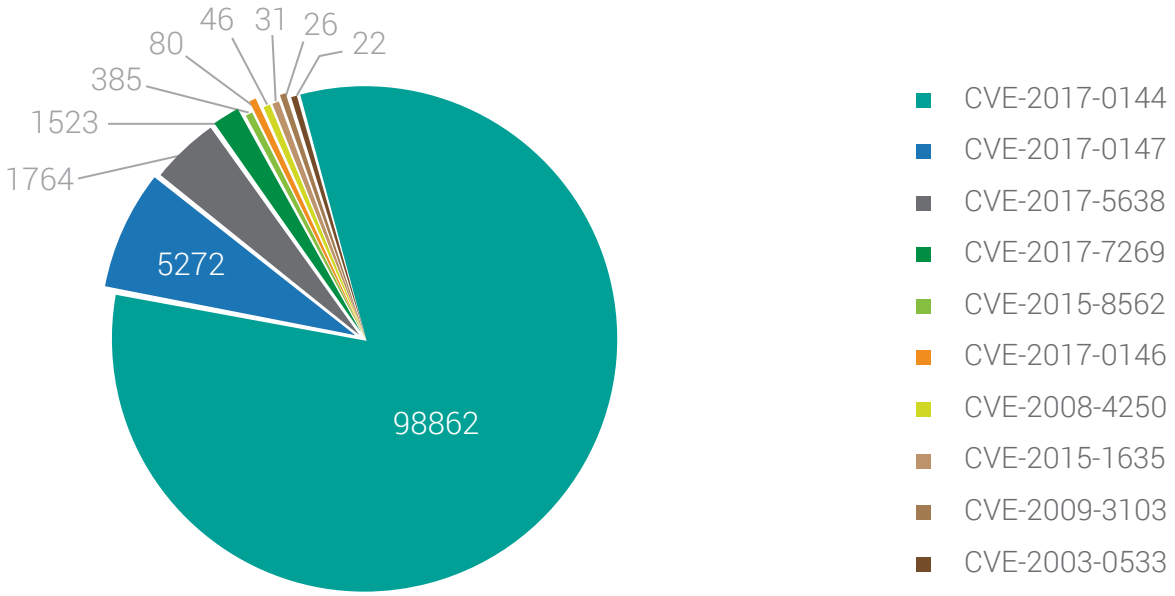


Fig.9

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).

Top 10 Commonly found malware file names

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

1. KMS-R@1n.exe	3. autorun.inf	5. Service_KMS.exe	7. autopico.exe	9. mssecsvc.exe
2. DOC001.exe	4. SECOH-QAD.dll	6. KMSEmulator.exe	8. DriverPackNotifier.exe	10. Public.exe

Trends in Windows Security

1. CVE-2019-0708 – A Critical 'Wormable' Remote Code Execution Vulnerability in Windows RDP

Microsoft recently released a patch for Critical Remote Code execution vulnerability found in Microsoft Windows Remote Desktop Service (RDP). The vulnerability is identified as 'CVE-2019-0708 – Remote Desktop Services Remote Code Execution Vulnerability.' As mentioned in the MSRC blog, "this vulnerability is pre-authenticated and requires no user interaction. In other words, the vulnerability is 'wormable', meaning that any future malware that exploits this vulnerability could propagate from one vulnerable computer to another vulnerable computer in a similar way as the WannaCry malware spread across the globe in 2017. While we have observed no exploitation of this vulnerability, it is highly likely that malicious actors will write an exploit for this vulnerability and incorporate it into their malware." This vulnerability is a special case, as Microsoft went out of the way to patch this vulnerability in Windows 2003 and Windows XP as well, which have reached the end of support quite a long time ago. Given the 'wormable' nature of this vulnerability, once a host is infected, it can infect other vulnerable hosts in the same network really fast. We have a few IPS signatures addressing this vulnerability through our AV. At the time of publishing this report, there were no known cases of this vulnerability getting exploited in the wild.

Ref:https://blogs.seqrite.com/cve-2019-0708-a-critical-wormable-remote-code-execution-vulnerability-in-windows-rdp/

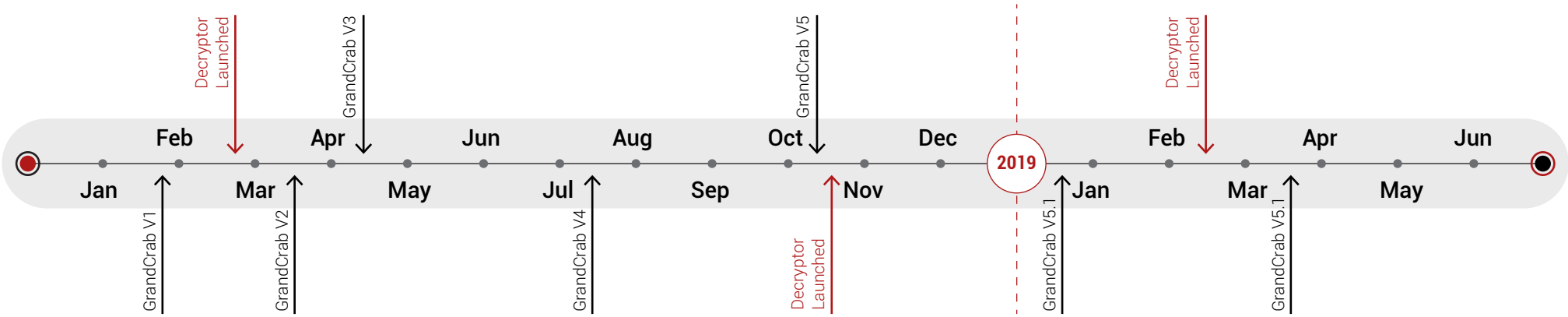
2. GandCrab retired?

One of the most prominent RaaS (Ransomware as a Service) ever, the evolving Ransomware GandCrab has announced its end this year after one and a half year since its inception!

Since the beginning, GandCrab had used almost every possible way to spread, like spam emails, malicious attachments, social engineering, various exploits in wild and bots to penetrate the systems, etc. Over the period they changed their way of encryption, extension generation, moved to secure C&C servers and almost everything which antivirus vendors tried to detect. The malware authors were continuously monitoring the solutions provided by various AV vendors and malware researchers. Also, they evaded those tricks and made fun of those vendors and researchers on the forum or through the next versions of GandCrab.

The retirement of Gandcrab also indicates that decryption keys will no more be available as infrastructure will shut down. The official page of Gandcrab RaaS on exploit.in was used to announce the retirement of GandCrab. The message stated in a sarcastic way with the phrase: "All good things come to end!"

The figures announced by authors are jaw-dropping. People who used this RaaS are believed to earn more than $2 billion with an average of $2.5 million per week. The authors themselves earned more than $150 million per year which sums up to $225 million for the period of their existence. And the best part is, the money earned by authors is already legalized!



GrandCrab has retired, or Has It?

3. APT-27 like Newcore RAT, Virut exploiting MySQL for targeted attacks on enterprise

Quick Heal Security Labs is observing increased use of cloud platform by threat actors for launching MySQL attacks. Due to the cloud platform, they can easily migrate and maintain their bot without any expenses. We observed a rise in a targeted attack on enterprises. Interestingly attackers are using MySQL & MSSQL as an entry point. Even though enterprises had patched all the vulnerabilities related to the OS, they failed to secure the server machine running MySQL, which is open to the public Internet.

According to resources available on the internet, there are approximately 4.9 million MySQL servers configured to run on Public IP. To execute malicious code, attackers require privileges such as admin rights, but MySQL is running as service hence, every process executed by it gets executed with system privileges.

In our lab, we observed more than 15 thousand attacks, of which, 34% attacks were targeted from Germany and rest of the attacks were centered with other countries including United States, France, China, Poland, and Russia.

Threat Actors Different Approaches:

Attackers were observed to be using two different approaches to abuse the MySQL server and to compromise the associated enterprise network.

1. They try to get an entry into the database server, drop existing tables and insert a ransom note as a blob in a newly created table.

2. They use MySQL or MSSQL as an entrance into Linux or Windows system and then drop a backdoor, miner or ransomware into the victim host.

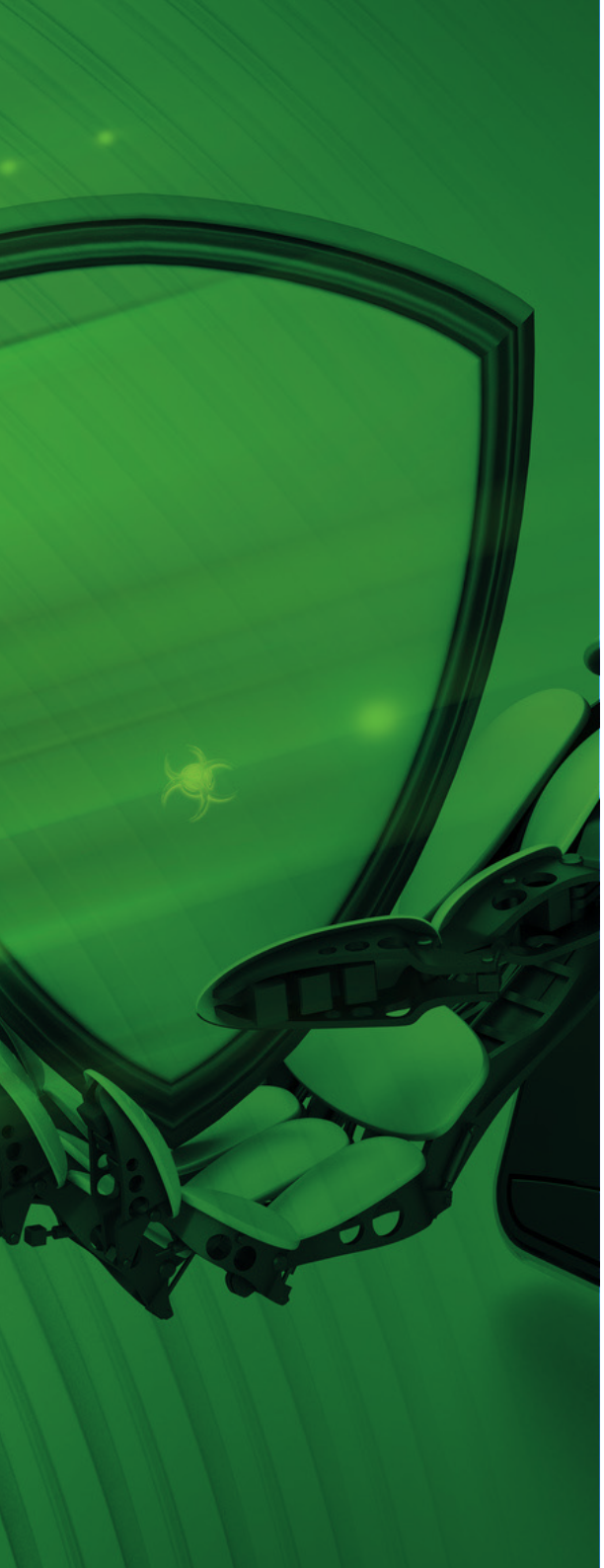
Threat actors are abusing the MYSQL server by exploiting weaknesses such as default credentials like root:toor, scott: tiger and brute force attacks with 1000+ well-known passwords and SQL injections. Apart from this approach, attackers also make use of WebShell as we presented in Emotet paper and authentication bypass vulnerability that allows them to take control over the server without any credentials to manipulate the data and even delete it or steal it. Attackers are using the user-defined MySQL functions through which they are dropping .dll files containing a definition for their user-defined function like downloading and executing any malware component. Every application executed by mysqld.exe will run with system privilege. They evade traditional detections and can be used to launch file-less malware attacks with the help of PowerShell. Alongside, there are various malware distributed using MySQL as a source which includes a virus, backdoor, miner, ransomware, and RAT.

Quick Heal has detection capabilities on user-defined .dlls, as well as behavior-based and IDS/IPS solution for the second type of attack. It is recommended to always apply critical security patches to Operating Systems & important applications too. Also, the use of complex passwords is strongly recommended and it is also essential to backup important data.

4. Script kiddies using Open Source projects: A Smarter Way

The availability of free and open-source tools, scripts, obfuscation frameworks, etc. pose a significant risk for systems, networks, and a pain area for security researchers to analyze them.

AV industry has faced a huge challenge on blocking such scripts/tools as these are originally intended for pen-testing as a part of security testing. A few of such scripts/tools are also in use for administrative purposes. Script kiddies heavily abuse them to spread ransomware, steal information and for crypto jacking attacks. This



has caused thousands or millions of dollars in lost revenue or damage to the enterprise segment. So, do script kiddies become smarter as the years pass?

Recently, Quick Heal Security Lab observed that many fileless scripts, obfuscation frameworks and tools like Powersploit, Invoke-Obfuscation, etc. are easily available on GitHub. These are being used by script kiddies to spread cryptojacking malware, ransomware attack and evading various security products. Some of them were detected by our telemetry since the late 2018 - early 2019 period.

Quick Heal Security Labs also observed a crypto miner malware, a bit recursive in nature, which typically targets Windows servers. On execution, it creates a backdoor which will convert that machine to a bot and simultaneously download and execute a payload which contains the source code of infamous Windows version of Mirai Botnet. It has used a combination of Powershell script and WMI database for making persistence on the system and used Mimikatz to extract and steal passwords. The components used in this attack are linked to different open source projects. Nowadays Script kiddies are modifying open-source projects according to their need and generating revenue quickly.

5. Older vulnerabilities still being exploited

We noticed that cybercriminals are leveraging older vulnerabilities to target the SME sector in India. Here is the list of top 5 vulnerabilities which attackers are trying to exploit even today.

1. NTP Amplification Attacks Using “monlist” Command (CVE-2013-5211)

NTP Reflected DDoS Attacks using the amplified response to a ‘Monlist’ command was quite a popular and wide-spread attack during late December 2013 and early January 2014. It exploited a vulnerability (CVE-2013-5211) in NTP. Though a patch for this vulnerability was made available in January 2014 itself, we still see multiple scan attempts being made by malicious threat actors over the internet to find open NTP servers. This attack can cause a DOS attack on enterprise networks, disrupting normal operations.

2. Microsoft IIS WebDAV Remote Code Execution Vulnerability (CVE-2017-7269)

This is a buffer overflow vulnerability in the ScStoragePathFromUrl function in the WebDAV service in IIS 6.0 in Microsoft Windows Server 2003 R2. It was zero-day and the vulnerability was exploited in the wild. This vulnerability allows remote attackers to execute arbitrary code via a long header beginning with "If: <http://" in a PROPFIND request to a WebDAV server. We still see several attack attempts being made to exploit this vulnerability even today. A successful attack can result in remote code execution and eventually obtain full control of the target host.control of the target host.

3. Windows SMB Remote Code Execution Vulnerability (CVE-2017-0143/MS17-010)

This is probably the most talked about and widely exploited vulnerability ever. The infamous ransomware WannaCry used 'exploit' for this vulnerability in SMB v1.0 protocol to infect millions of nodes worldwide. Microsoft has patched this vulnerability in March 2017. A hacker group named Shadow Broker got access to exploits/tools related to this vulnerability (and many others) and leaked the exploit dump on April 14, 2017. The same exploit was also used to carry out the 2017 NotPetya cyberattack on June 27, 2017, and reported to be used as part of the Banking Trojan since at least September 5, 2017.
Ref.=https://en.wikipedia.org/wiki/EternalBlue

We see lots of vulnerability probing and exploit attempts related to this vulnerability happening even today.

4. Apache Struts arbitrary command execution through crafted HTTP headers (CVE-2017-5638)

The vulnerability is seen in Jakarta Multipart parser in Apache Struts introduced because of incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary code on the vulnerable server. It was exploited in the wild in March 2017. The high profile, high-impact data breach at Equifax was due to this same vulnerability in Apache Struts. This incident again emphasized the importance of applying software patches immediately. Exploiting this vulnerability is quite easy and hence we see attacks exploiting this vulnerability to still be active.

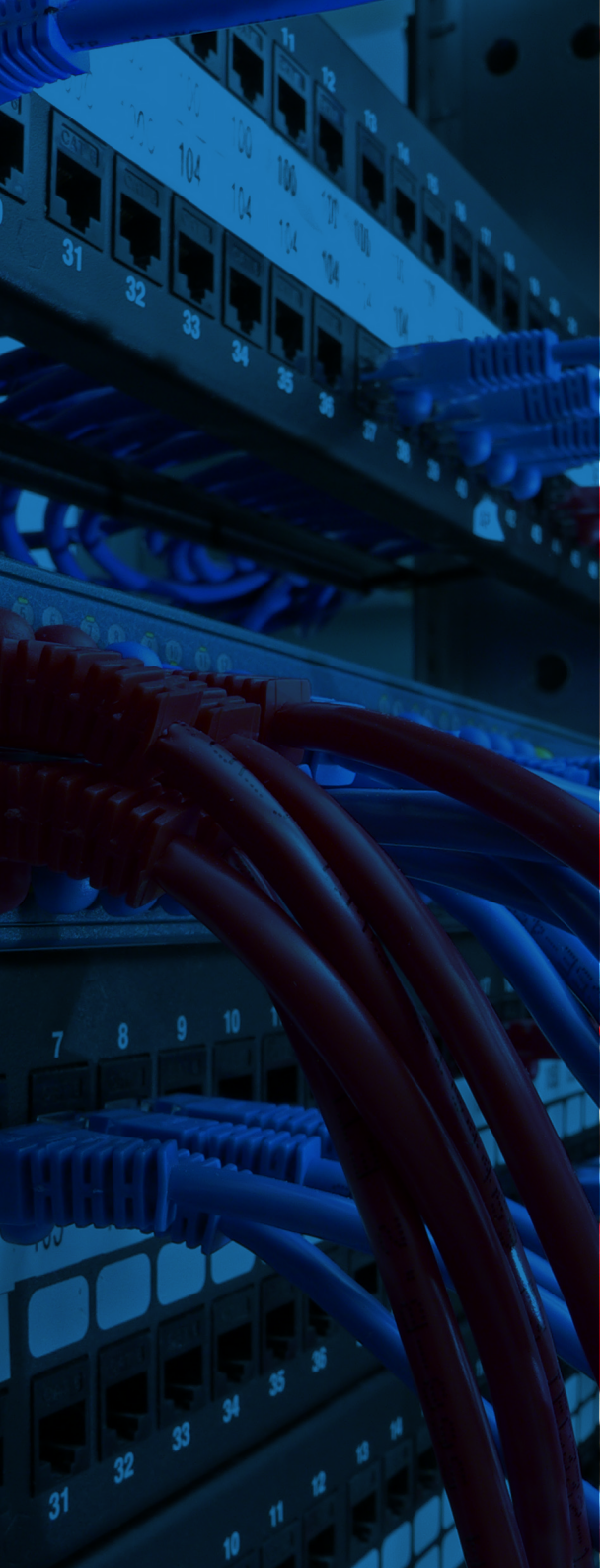
5. Apache Struts CVE-2017-12611 Remote Code Execution Vulnerability (CVE-2017-12611)

This is another remote code execution vulnerability in Apache Struts which can be exploited through a crafted URI containing a sequence of commands to be executed on the Apache server. We noticed that attacks against this vulnerability are still prevalent.

This observation again emphasizes the importance of patching enterprise applications. Especially the vulnerabilities for which public exploits are available, exploitation is much more likely. If one can't patch a system because of some challenges like fear of breaking existing functionality, the risk should be mitigated with virtual patching solutions like Seqrite Unified Threat Management.

6. Era of Cloud storage and the saga of data loss

Your cloud storage may have been compromised and you might be unaware of it. This has been the new strategy that malware actors tend to adapt to spread the nuisance.



In the recent past, we observed many security breaches where cloud systems were soft targets. Shanghai Jiao Tong University leaked 8.4TB of email metadata due to misconfigured Elasticsearch database. It was found that the server was running unprotected database. This open database contained 9.5 billion rows of data which amounts to 8.4 TB of data. This leaky Elasticsearch hosted database had leaked 8.4 TB of email metadata - this massive data leak was found to be a database which was set up without any authentication, according to the cybersecurity and privacy analyst who discovered this data leak.

In another incident, a misconfigured Elasticsearch database left nearly 1.68 million records exposed to the public. According to the respective security analyst, this leak exposed 34GB of data containing 1,679,993 records with information that included individuals' names, birth dates, addresses, phone numbers, email addresses, gender, marital statuses, and financial status, as well as communication notes. As acknowledged by UChicago Medicine, certain records also contained the names and clinical areas of physicians who treated patients listed in the database. Thankfully the database did not include information from patients' medical records nor did it hold financial information or Social Security numbers, the school asserted.

In a third incident, cloud storage Amazon S3, storing more than 540 million records of Facebook users, was exposed. It was found that these S3 buckets were weakly protected and thus were publicly accessible. In addition to weak protection, the respective app owners of this S3 store had stored app passwords, account names, user IDs, interests, relationship status, and much more in simple plain text form. And this is really very dangerous. This shows that even big companies like Facebook are faltering and that's a serious concern.

One thing that is common in these three incidents is the lack of adequate protection for data storage. Datastores were configured without proper care.

Cloud services are definitely useful however misconfigured cloud services may backfire on organizations. Cloud configuration must not be taken lightly, nor should one assume that simply storing the data in the cloud makes it safe. Adoption of certain best practices can strengthen an organization's cloud security and prevent their data from being publicly exposed. One should not assume that the default configuration is good enough to prevent their data from being compromised.

Certain best practices, as given below, can be adopted to strengthen security of cloud assets:

1. Keep all the data stores password protected and make it a point to use strong passwords. In addition, keep changing passwords on regular basis.
2. Use Access Control Lists for setting up data stores to prevent your datastore from getting compromised.
3. Except IT administrator, root access should not be given to any user of the data store.
4. Your cloud services should be regularly run through audit trial to check for signs of misconfiguration.
5. Use of separate subnets such as private and public, is also one of the best practises to follow.

Conclusion

The reports make it clear that cyber threats still loom large for enterprises. The observations in this report are in-line with Seqrite's Q1 – 2019 threat report where the conclusion essentially hinted that enterprises display exemplary behavior of utmost vigilance towards cybersecurity. As enterprises deploy cutting-edge system defenders to protect their valuable IT assets, threat actors only seem to be constantly evolving and finding newer ways to break-in.

What makes it so easy for threat actors to break into enterprise-grade security? Here is an interesting insight that might answer the question - the top ten malware attacking Windows operating systems are essentially penetrating the enterprise from email, removable drives, and Instant messengers. Businesses' will paralyze without these tools. With so much intelligence available to secure, say specifically these three channels, the penetration of threat actors seems to be directly proportional to the amount of security applied.

Nowadays, threat actors are essentially attacking to steal data. This is because data is the new gold! A plethora of start-ups are mushrooming that are built around market and business data. Couple that with the invasion in 'Artificial intelligence (AI) for everything' & AI's need to ingest a very large volume of data for it to function.

This data, when moved through the correct channels gets the top dollar. This is the recent trend and gain of the current hacker community. Worm.AUTOIT.Tupym.A, malware that was discovered on Windows OS wanted to steal enterprise data.

Such an environment is confusing for enterprises to decide upon building a roadmap for the future. Seqrite provides a range of customized solutions for end-to-end security for the entire enterprise.