SEQRITE

QUARTERLY THREAT REPORT

Q2 | 2020

Enterprise Cybersecurity Solutions by Quick Heal

www.seqrite.com

Contributors

Quick Heal Security Labs | Seqrite Marketing Team

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:

Contents

The changing behaviour of Malware!

From a surge to a dip and then a spike again, the Coronavirus influenced lockdown and the subsequent unlock process impacted malware behaviour in the first six months of 2020. **22 million malware were detected and blocked by Seqrite products used worldwide.** The manufacturing industry was worst impacted with an increased trend of cyberattacks happening through business networks.

WINDOWS

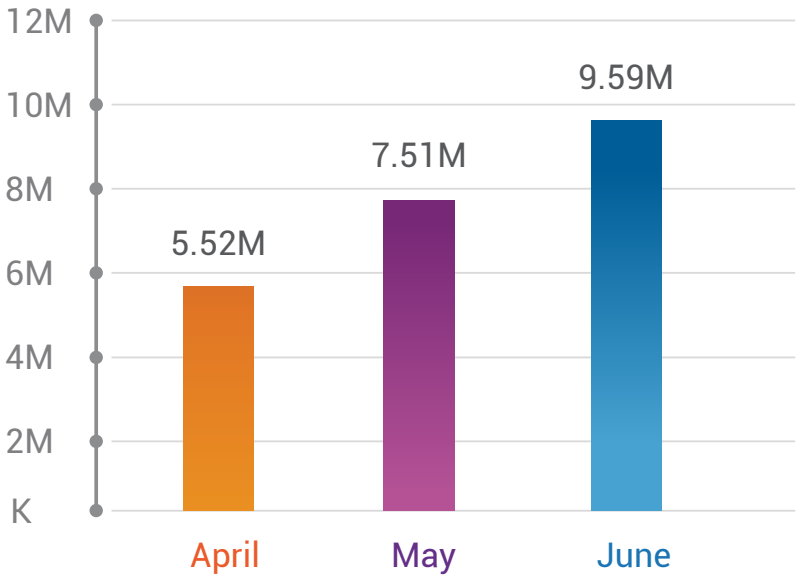
Detection Highlights – Q2 2020*

*Top seven 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 from April to June in 2020.

Month-Wise Detection Hits

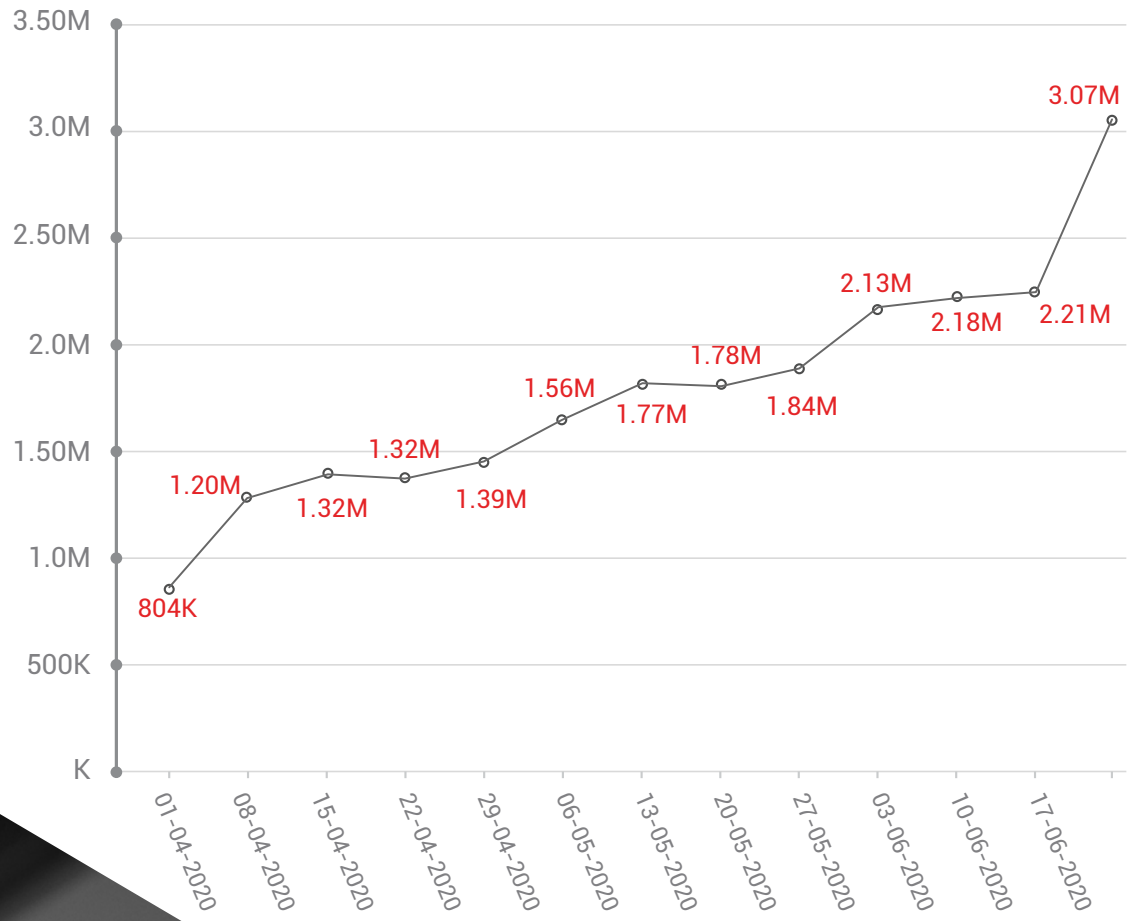


Observation

- Seqrite detected over **22 million Windows malware in Q2 2020.**
- June clocked the highest detection of Windows malware.

Detection Statistics – Week Wise

Week-Over-Week Detection Stats

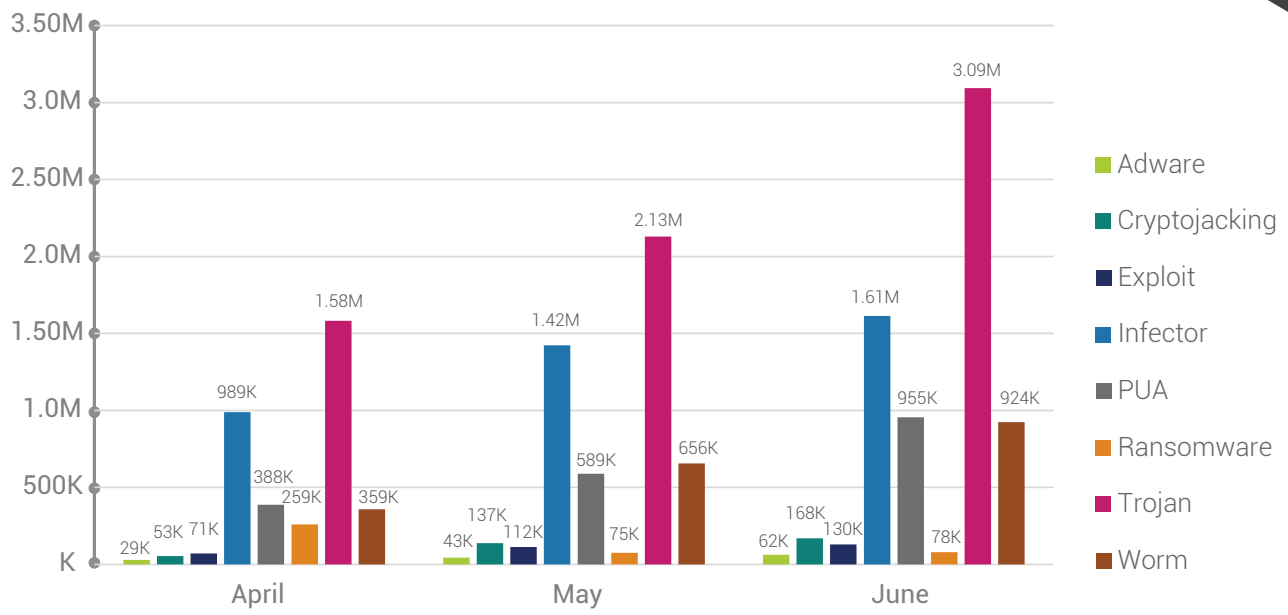


Observation

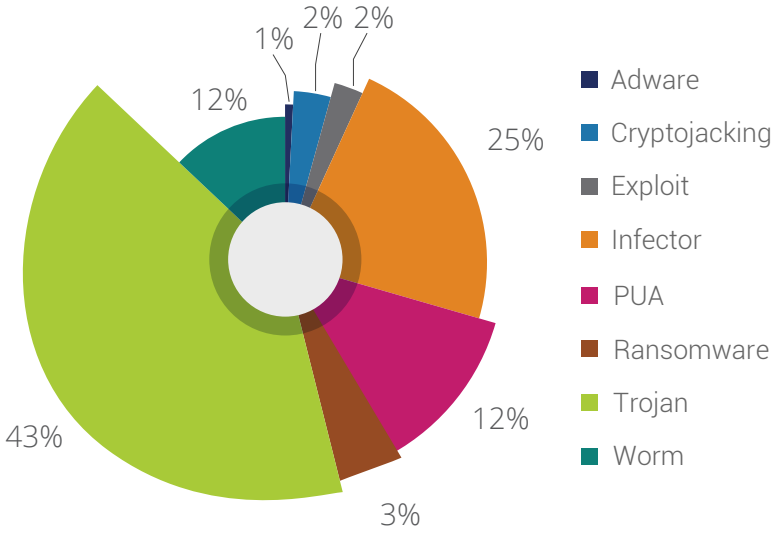
At **9 million + detections malware count** was at its peak in June attributed to a lot of sectors such as **Manufacturing, BFSI, Education, Healthcare**, etc. opening up after a long break.

Detection Statistics – Category Wise

Category-Wise Per-Month Detection Stats



Category-Wise Detection



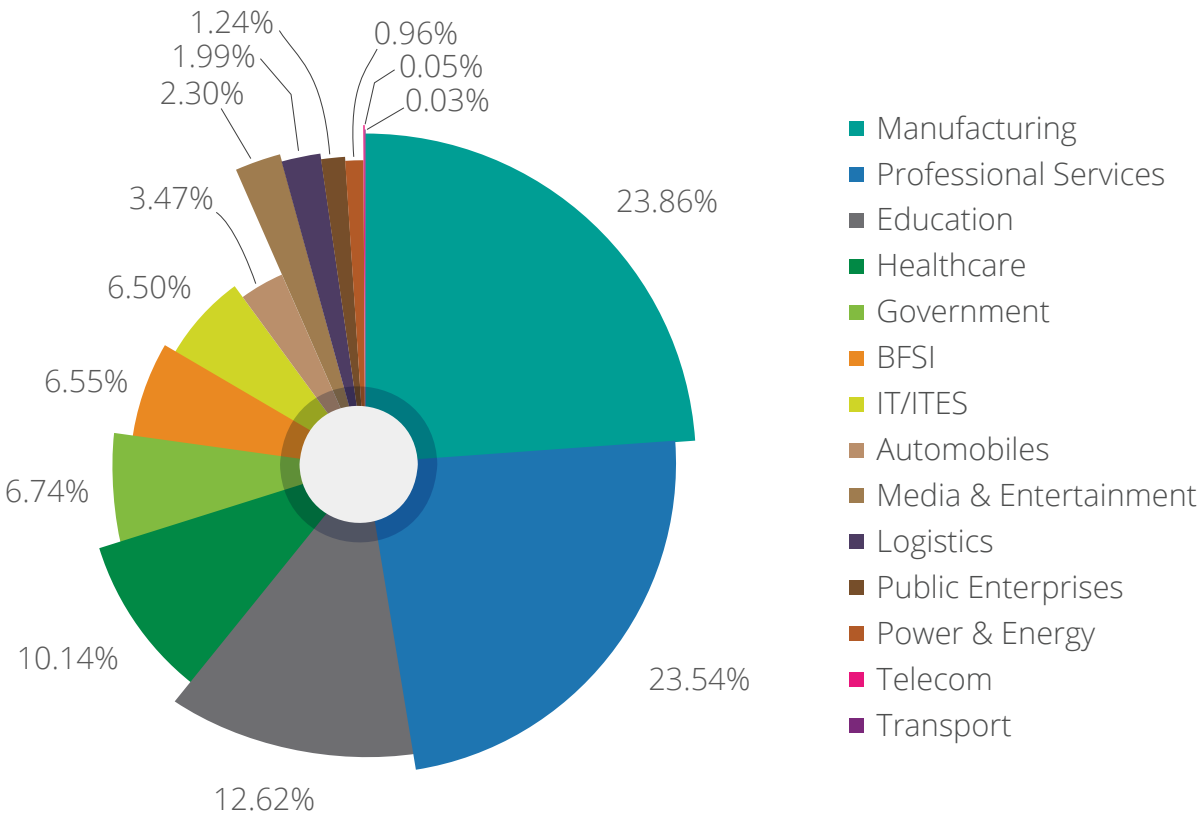
Observation

Malware detection count was the highest for Trojan accounting to **43% of the detections followed by Infector at 25%**. The trojan count was also the highest across all three months of **Q2 2020**.

Industry Wise Detection Stats

Below figure represents the malware detection count for various industries.

Industry Wise Detection Stats



Industry Wise Top Detections

Industry	Detection	Count %
Manufacturing	Worm.Agent	20.92%
Strategic & Public Enterprises	W32.Pioneer.CZ1	16.50%
Professional Services	PUA.Auslogicsl.Gen	16.17%
IT/ITES	W32.Pioneer.CZ1	10.11%
BFSI	Worm.Autoit.Sohanad.C	9.92%
Hospitality & Healthcare	W32.Sality.U	5.53%
Education	Trojan.Agent	5.35%
Government	Trojan.IGENERIC	4.24%
Power & Energy	W32.Brontok.Q	4.23%
Logistic	Trojan.IGENERIC	3.08%
Media & Entertainment	Worm.Tupym.A5	2.41%
Automobiles	Worm.Brontok.Q3	1.31%
Telecom	Trojan.Agent	0.10%
Transport	Trojan.Presenoker	0.07%

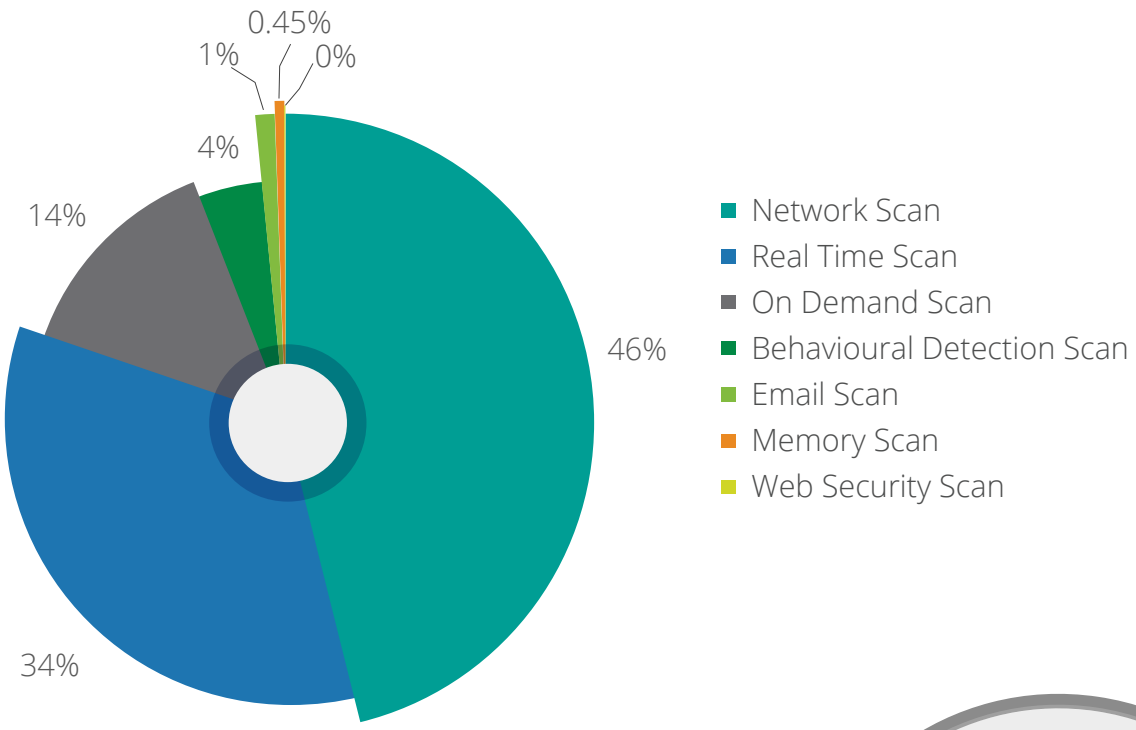
Observations

- The manufacturing industry had the maximum malware detections with **over 25% of the total detections**.
- The malware **Worm.Agent saw maximum attacks on the Manufacturing at 0.13 million hits.**

Protection Module Wise Detection Stats

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

Protection-Wise Threats



Observation

Most malware were detected by Network Scan at **46% followed by Real-Time scan Scan at 34%**.

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

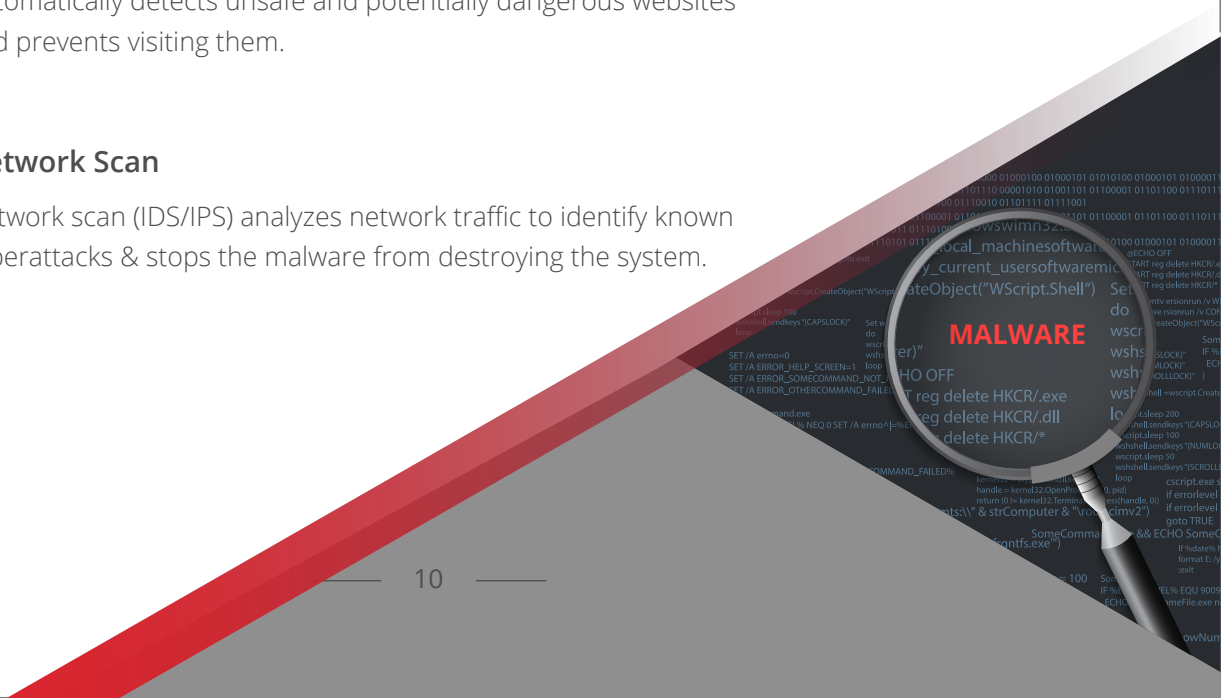
Blocks emails that carry infected attachments or links to compromised or fake and phishing websites.

Web Security Scan

Automatically detects unsafe and potentially dangerous websites and prevents visiting them.

Network Scan

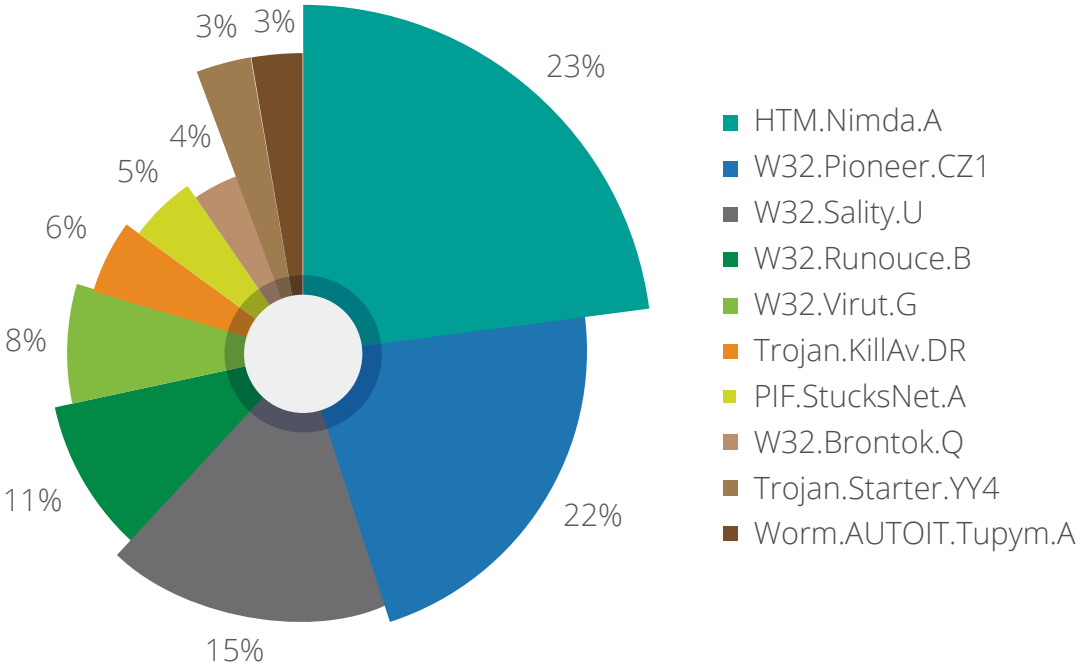
Network scan (IDS/IPS) analyzes network traffic to identify known cyberattacks & stops the malware from destroying the system.



Top 10 Windows Malware

The below figure represents the Top 10 Windows malware of Q2 2020. These malware have made it to this list based upon their rate of detection from April to June.

Top 10 Windows Malware



1. HTM.Nimda.A

Threat Level: Medium

Category: Worm

Method of Propagation: Spreads through emails

Behaviour: HTM.Nimda.A spread through email attachments infecting files on PCs and network drives.

2. W32.Pioneer.CZ1

Threat Level: Medium

Category: File Infector

Method of Propagation: Removable or network drives

Behaviour: W32.Pioneer.CZ1 injects its code into files and maliciously collects system information sending it to attackers.

3. W32.Sality.U

Threat Level: Medium

Category: File Infector

Method of Propagation: Removable or network drives

Behaviour: W32.Sality.U injects its code into system processes and gathers confidential information from affected machines.

4. W32.Runouce.B

Threat Level: Medium

Category: Virus

Method of Propagation: Spreads through emails

Behaviour: W32.Runouce.B sends a copy of self as an email attachment to email ids present on victim's contact lists creating a 'ChineseHacker-2' mutex.

5. W32.Virut.G

Threat Level: Medium

Category: File Infector

Method of Propagation: Bundled Software and freeware

Behaviour: W32.Virut.G creates a botnet that is used for Distributed Denial of Service (DDoS) attacks, spam frauds, data theft, and pay-per-install activities.

6. Trojan.KillAv.DR

Threat Level: High

Category: Trojan

Method of Propagation: Email Attachments and malicious/compromised websites.

Behaviour: Trojan.KillAv.DR drops a file when executed extracting IP address and other related information of victims.

7. PIF.StucksNet.A

Threat Level: High

Category: Trojan

Method of Propagation: Removable Drives

Behaviour: PIF.StucksNet.A drops a .LNK file, which is a shortcut to the main Trojan file, allows the attacker to execute arbitrary code on victim machines.

8. W32.Brontok.Q

Threat Level: Medium

Category: Worm

Method of Propagation: Spreads through emails or infected USB & network drives

Behaviour: W32.Brontok.Q spreads through emails or infected USB drives maliciously modifying system components present in a computer.

9. Trojan.Starter.YY4

Threat Level: High

Category: Trojan

Method of Propagation: Email attachments and malicious websites

Behaviour: Trojan.Starter.YY4 creates a process to run the dropped executable file and performs a plethora of activities such as stealing financial information, downloading more malware, etc.

10. Worm.AUTOIT.Tupym.A

Threat Level: Medium

Category: Worm

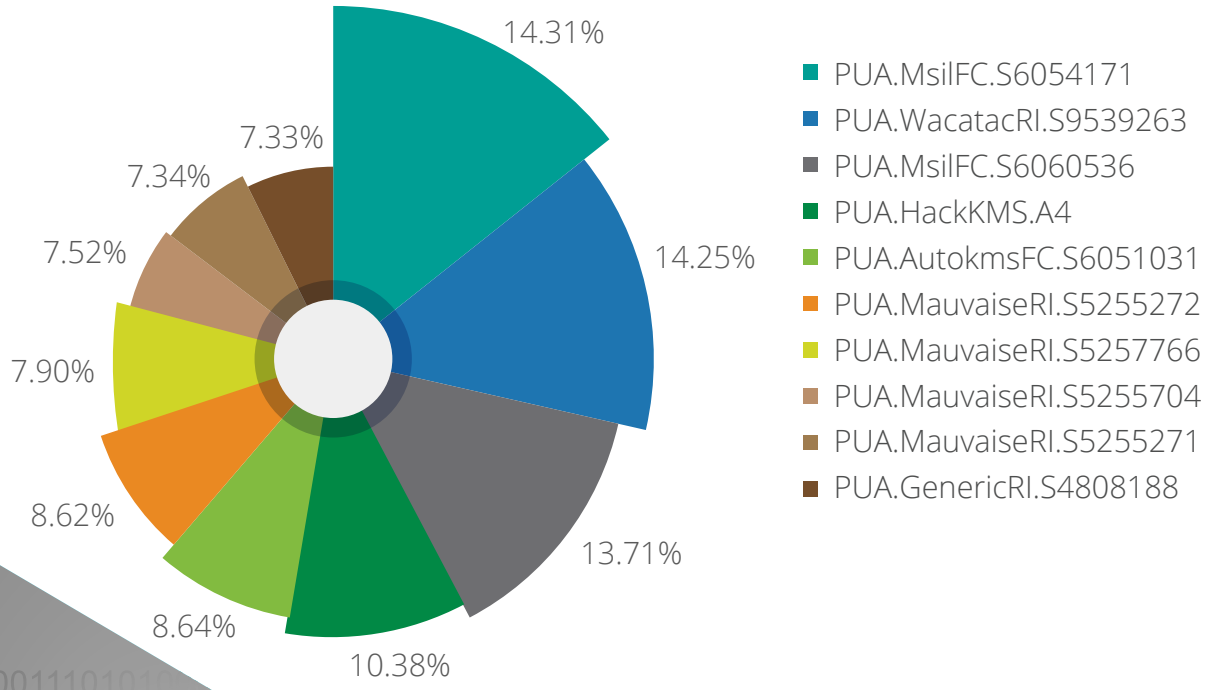
Method of Propagation: malicious links in instant messenger

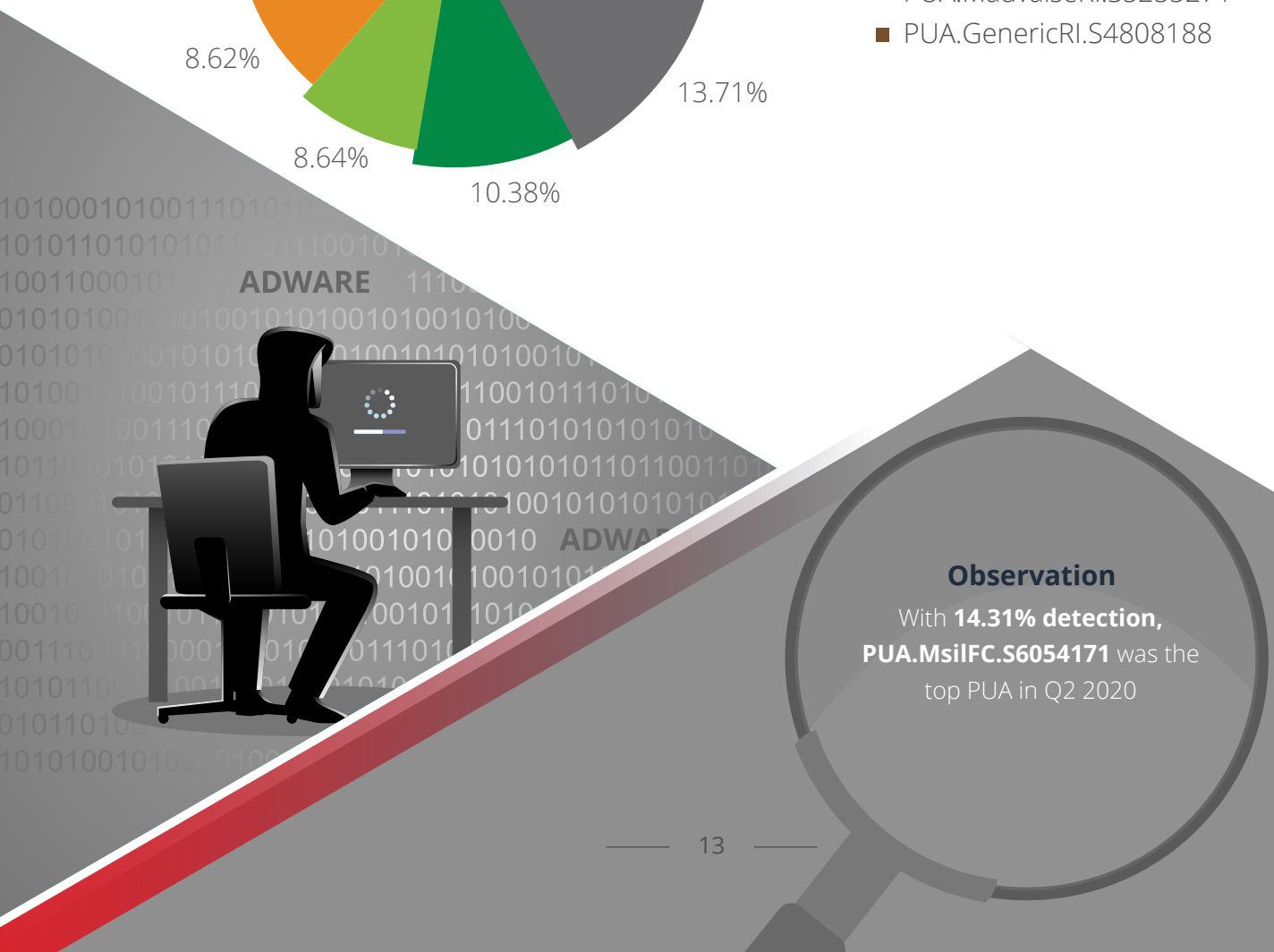
Behaviour: Worm.AUTOIT.Tupym.A connects to a malicious website, also modifies start page of browser to another site through registry entry.

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 2020.

Top Ten Potentially Unwanted Applications (PUAs)





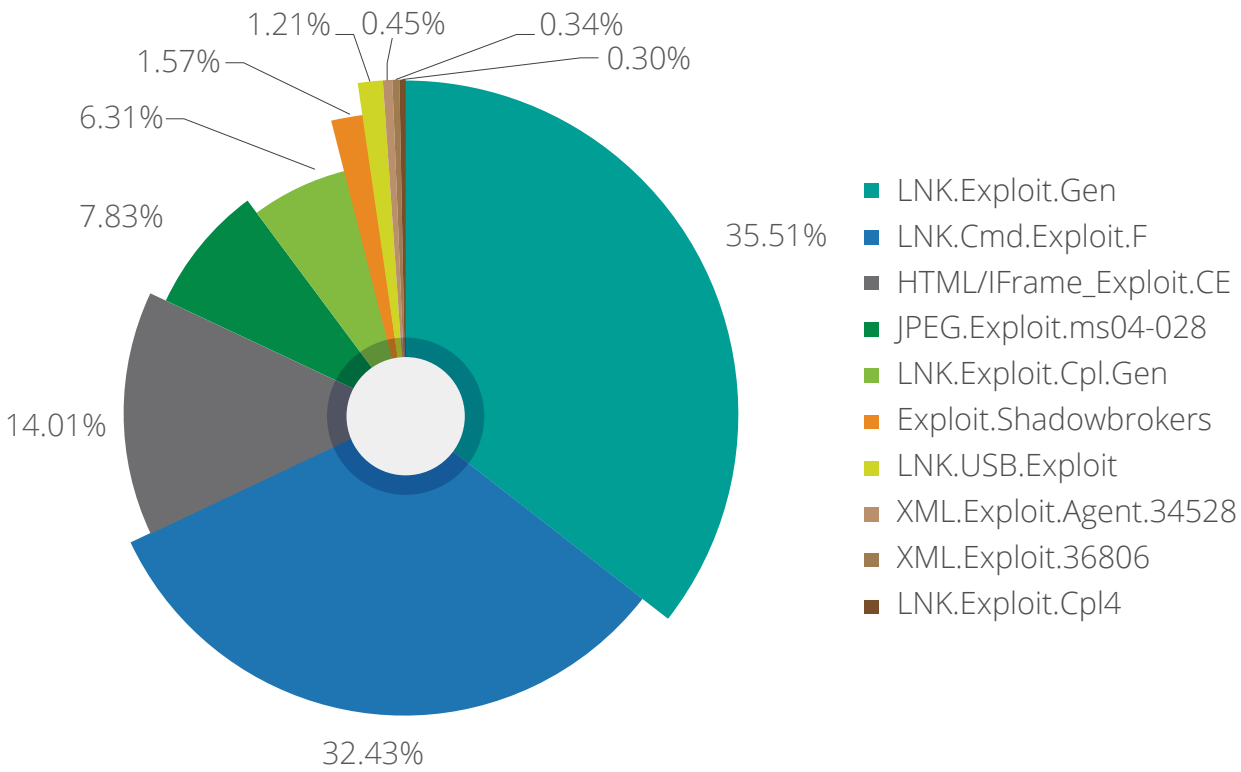
Observation

With **14.31% detection, PUA.MsilFC.S6054171** was the top PUA in Q2 2020

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 for Q2 2020.

Top 10 Host-based Exploits



What are host-based exploits?

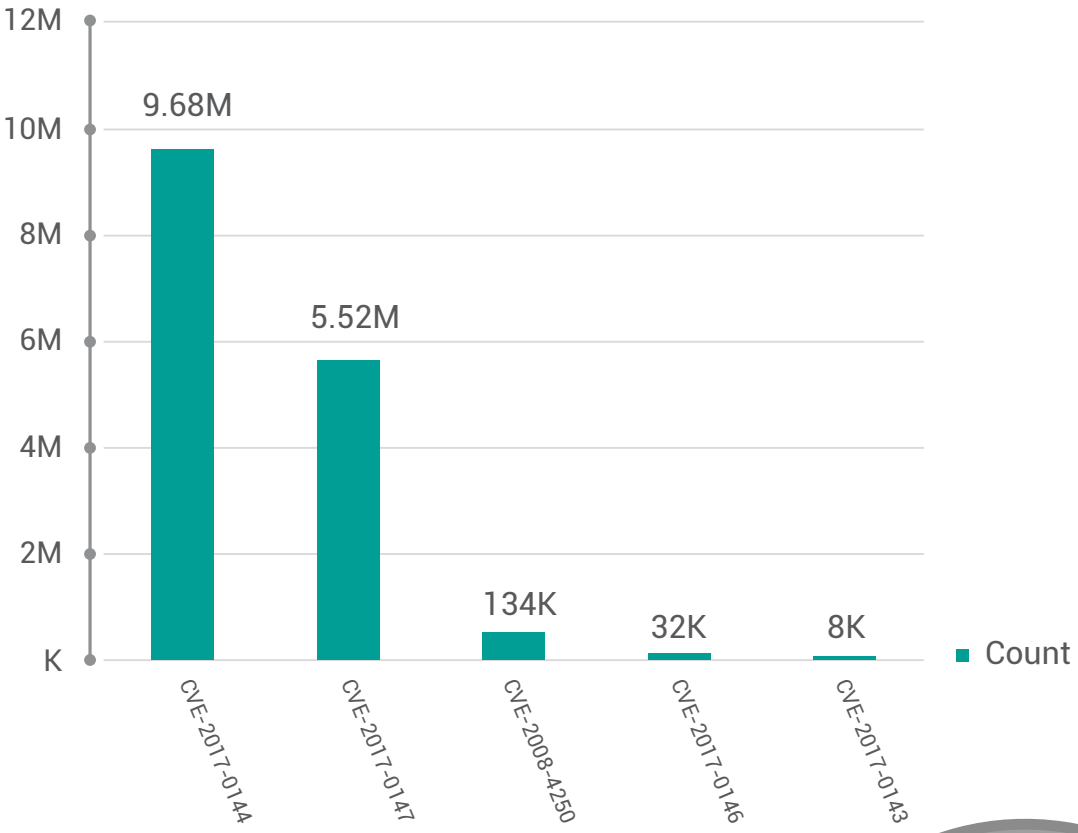
Host-based exploits are those that target security vulnerabilities found in host-based applications (host is a computer or other device connected to a computer network). These exploits are detected by endpoint detection modules such as Virus Protection, Email Protection, and Scanner.

Observation

With **35.51% attempts, the LNK.Exploit.Gen** was the top detected host-based exploit

Top 5 Network-Based Exploits

Below figure represents the top 5 Network-Based exploits for Q2 2020.



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).

Observation

With **9.68 million attempts, the CVE-2017-0144** was the top detected network-based exploit in Q2 2020.

Top 10 commonly found Malware file names

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

Filename
1. Time.exe
2. autorun.inf
3. SECOH-QAD.dll
4. SECOH-QAD.exe
5. mssecsvc.exe
6. clean.exe
7. VID001.exe
8. autorun.inf
9. Doublepulsar-1.3.1.exe
10. Video.UI.exe

Trends in Windows Security

1 Indian Co-Operative Banks Under Attack

The Adwind Java RAT malware attacked India cooperative banks in April 2020 through email attachments — sample email subject lines and attachments names were as mentioned below.

Email Subject	Attachment Name
Urgent – COVID measures monitoring template	Covid_19_measures_Monitoring_Template-Final_xlsx.zip
Query Reports for RBI INSPECTION	NSBL-AccListOnTheBasisOfKYCData_0600402020_pdf.zip
Moratorium	Gazette notification&RBI_Directives_file-00000120_pdf.zip
FMR returns	Fmr-2_n_fmr_3_file_000002-pdf.zip
Assessment Advice-MH-603	MON01803_DIC_pdf.zip
[874890897] – MIS for NEFT/RTGS, 06-04-2020 [1]	FIXEDCOMPNULL_xls.zip
Deal confr.	SHRIGOVARDHANSING0023JI001_pdf.zip
DI form	DI_form_HY_file_00002_pdf .zip

2 Zloader Riding on Excel 4.0 Macro Wave

Excel Macro 4.0 was widely used by attackers in malspam Campaigns with the below mentioned file-names -

- req_data-6794349.xls
- Covey_Planning.xls
- Efa-4314.xls
- Rva-1968.xls
- price list 2020.xlsx
- inform-2020-06-01_7985395.xls
- FOH DAILY CASH- REMMITANCE 24-05-2020 NIGHT SHIFT (version 1).xls

3 A New Era in Ransomware

Multiple ransomware attacks happened throughout the second quarter of 2020 — the prominent ones are mentioned below.

1. **WoL (Wake on Lan) in Ryuk Ransomware**

   Wake on Lan (WoL) is a hardware feature that allows a computer to be turned ON or awakened by a network packet.

   Ref: https://blogs.quickheal.com/deep-dive-wakeup-lan-wol-implementation-ryuk/

2. **Process Hollowing in Mailto aka Netwalker Ransomwar**e

   The Mailto or Netwalker performs process hollowing in explorer.exe — this helps in evading the Anti-Virus software (AVs) to easily perform the encryption.

   Ref: https://blogs.quickheal.com/mailto-ransomware-hiding-under-explorer-exe/

3. **HorseDeal & Gigabyte Ransomware**

   HorseDeal & Gigabyte Ransomware use spoofed ECC certificate to evade detections.

   Ref: https://blogs.quickheal.com/horsedeal-riding-curveball/

4. **RagnarLocker Ransomware Hides in Virtual Machine.**

   RagnarLocker Ransomware is deployed inside a Windows XP virtual machine to hide the malicious code from security products.

5. **PonyFinal and Tycoon Ransomware**

   PonyFinal and Tycoon Ransomware use JAVA as the language/file format for Encryption

4 Maze ransomware continues to be a threat to the consumers

Maze is a recently highlighted ransomware among the ever-growing list of ransomware families. The ransomware is active from the past one year, Maze ransomware came into limelight due to its new approach of publishing sensitive data of infected customers publicly.

5 Emerging of new SMB exploits

SMB and RDP attacks were also on the rise in Q2 -2020.

SMBGhost [CVE-2020-0786]

CVE-2020-0786 is an integer overflow bug in the decompression mechanism of SMBv3.1.1 affecting both, the client and the server. Users connected to hacked systems are at high risk.

SMBleed [CVE-2020-1206]

Just three months after Microsoft had patched SMBGhost, another similar vulnerability called SMBleed was disclosed affecting Windows 10 versions 1903, 1909 and 2004.

SMBLost [CVE-2020-1301]

CVE-2020-1301 is an integer underflow bug in SMBv1 (srv.sys) causing Out-of-Bound kernel to write from data under the attacker's control.

6 COVID-19: Specific sectors getting incessantly affected during the lockdown and the subsequent unlock period.

The number of attacks against customers in certain sectors such as Manufacturing, Healthcare, BFSI, etc. has increased considerably since Feb 2020, the onset of COVID-19 pandemic. We saw a dip in attacks for a brief period but the number of attacks is seen to be increasing again after the unlock process began.

Inference

These are tricky times for all entities, be it governments, businesses, individuals or even cybersecurity vendors. However, to **safeguard the critical collective, we need to evolve, adapt and come to terms with the current global situation**. Businesses need to have extensive discussions with cybersecurity vendors on integrating optimum and useful solutions to safeguard their business from the spectre of cyberattackers.