**Quick Heal Security Labs detected over 2.3 million infections and 13 families of Ransomware on Windows in Q2 2017**

* Over 1700 malware infections detected every minute on Windows; down 23% as compared to Q1 2017
* Trojan malware continues to lead with 37% detections, followed by Infectors, Worms and Adware & PUA
* Over 1 million Android infections detected; Android Ransomware rises 16%
* Android Banking Trojan increases 166% with the rise of digital payments

**Pune, August 02, 2017 – Quick Heal Security Labs, the Threat Research and Response division of Quick Heal Technologies,** the leading IT security solutions provider, **detected over 2.3 million infections and 13 families of Ransomware on Windows in Q2 2017.** According to the [Quarterly Threat Report](http://dlupdate.quickheal.com/documents/others/Quick_Heal_Threat_Report_Q2_2017.pdf) released by **Quick Heal Technologies**, malware detections saw a drop of 23%, but continued to emerge over 1700 times every minute. **With the advent of Ransomware attacks such as WannaCry and Petya (a.k.a NotPetya), Quick Heal Security Labs** observed that attackers are now shifting their attention towards attacks that make them more money and in an easier way as Ransomware campaigns have higher returns compared with data stealing and other malicious campaigns. **Quick Heal Security Labs continuously monitors the threat landscape and provides quality intelligence to Home users and Enterprise users under the brands 'Quick Heal' and 'Seqrite' respectively.**

**Apart from WannaCry and Petya, the active ransomware families which emerged in the quarter include Jaff, Crisis, Cry128/Cry9 among others.** Trojans continued to rise with 37% detections followed by Infectors, Worms and Adware & Potentially Unwanted Applications (PUA). According to the report, attackers are increasingly using Remote Desktop Services (RDS) feature to enter into targeted systems by acquiring weak login credentials, password stealer software and credential access techniques. RDS is a key feature that allows Windows users to take control of a remote computer over a network connection.

On the Android platform, **Quick Heal Security Labs** received over 1 million malware infections – a decline of 21%, while ransomware grew 16% in comparison to the first quarter. **Android Banking Trojan witnessed a massive growth of 166% as digital payments gained traction and became a popular source for banking transactions.**

**Sanjay Katkar, Joint Managing Director and Chief Technology Officer, Quick Heal Technology said,** "Although malware detections on Windows and Android saw a decline compared to last quarter, ransomware attacks have increased - WannaCry and Petya being the notable ones. This trend proves that cyber criminals are working on attacks that require fewer resources but at the same time, give higher returns. Even novice cyber criminals who may not be able to create a ransomware are outsourcing crimes through Ransomware-as-a-Service. WannaCry couldn’t have been the biggest attack in history if people were prudent enough to keep their operating systems up-to-date with security patches released by Microsoft way before the attack happened. It’s about time people paid heed to warnings, understand the types of digital threats, be wary of sharing their personal details and treat our digital lives in the same manner as we treat our real lives – with a sense of security."

**Trends and Predictions:-**

**Windows:-**

**1. Ransomware**

* With more users adopting the cloud to store their data, ransomware attacks on cloud server are expected to show up in the near future. There is an increased likelihood of massive attacks like WannaCry due to individual users and businesses failing to keep their systems patched and up-to-date.
* Ransomware attacks might increase on health care organizations.
* Newer, destructive and more advanced variants of the Wannacry and Petya are expected to surface.

**2. Adware**

Like fireball, we are expecting more and high-impact adware campaigns in the future. In these campaigns, adware might be used to spread ransomware.

**3. Targeted Attacks**

* Targeted attacks by using fileless and memory-based malware are expected to increase in the coming days. IoT (Internet of Things) devices are expected to be targeted at a higher scale as it was evident in the case of Mirai and Persirai botnet attacks.
* As digital payment gets increasingly mainstream, businesses running on digital wallet programs can become hot targets for attackers in 2017.

**Android:-**

**1. Fake applications are a major concern**

Scammers are distributing fake apps, labeling them with popular keywords to trick users into downloading them. These apps are mostly developed by novices are not coded properly which leaves security vulnerabilities in them. These ‘weak’ apps are then used by seasoned attackers to target mobile users. Faked applications are expected to increase in volume not only in third-party app stores but Google Play as well.

**2. Ransomware is growing**

As observed in the earlier sections, the top 10 Android malware list has included an Android ransomware and Q2 has registered a 16% spike in the malware compared to Q1. This only adds to the prediction that ransomware is going to get worse in the coming days.

**About Quick Heal Technologies Limited / Seqrite:**

**Quick Heal Technologies Limited** is one of the leading providers of security software products and solutions in India. Incorporated in 1995 with a registered office in Pune, Quick Heal has over 1,350 employees and a network of over 20,000 channel partners on 31st March 2017. It conducts sales and marketing activities across India through 36 branches in India and, through its subsidiaries that are present in Japan, Dubai, and Kenya.

Quick Heal Technologies portfolio includes solutions under the widely recognized brand names ‘Quick Heal’ and ‘Seqrite’ across various operating systems and devices. Since its incorporation, more than 24.5 million licenses of Quick Heal’s products have been installed and Quick Heal has over 7.6 million active licenses as on 31st March, 2017.

**Seqrite**, an enterprise business unit of Quick Heal Technologies Limited, **provides** a **full portfolio of perimeter security solutions, endpoints as well as mobile devices security solutions through centralized management, supervision and policies definition, on premise or on cloud, against advanced cyber threats.**

**About PartnerNET:**

**PartnerNET** is a value-added distributor of IP Telecommunications Products, Video Conferencing Systems, Wireless Network and Network Security Products as well as Cloud Back Up Software. **PartnerNET** represents some of the largest ICT manufacturers, worldwide, offering complete business solutions.

**PartnerNET’s** objective is to help businesses grow by finding and selecting the right technology products and solutions for our partners and their customers. We are uniquely positioned to address any technology needs and to provide flexible, tailor-made and affordable solutions for our customers. Our solutions cover all the needs of small and large companies and organizations, private and public, offering solutions in physical, virtual and cloud environments. We offer a full range of products, next business day delivery, as well as continuous pre-sales and after-sales support along with educational partner programs.

**PartnerNET** is an **exclusive distributor** of **Seqrite** solutions for the **EMEA** region.

To learn how **Seqrite** solutions can help your businessorfor a **free trial, call PartnerNET** at **210 7100000.**