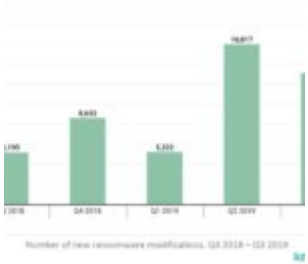
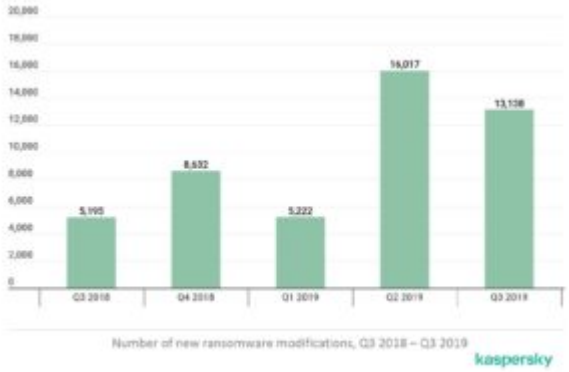
Kaspersky’s Q3 2019 report shows ransomware now targeting back-up data, Thailand ranks 4th among SEA countries





Kaspersky researchers have identified a new type of ransomware attack which is actively growing in popularity. Targeting Network Attached Storage (NAS), it poses new risks for back-up data usually stored on such devices. With NAS largely perceived as a secure technology, users often remain unprepared for the possibility of infection, putting their data at higher risk.

Encryption ransomware is a malware that applies advanced encryption methods so files cannot be decrypted without a unique key. This leaves the infected device owner stuck with a locked device and a demand to pay a ransom in order to regain access to files. While users are typically infected with ransomware via email or exploit-kits planted on websites, the new type of attacks on NAS devices use a different vector. Ransomware operators scan ranges of IP addresses looking for NAS devices accessible via the web. Although only web interfaces protected with authentication are accessible, a number of devices have integrated software with vulnerabilities in it. This allows the attackers to install a Trojan using exploits, which will then encrypt all data on the devices connected to the NAS.

“Previously encryption ransomware targeting NAS was hardly evident in the wild, and this year alone we have already detected a number of new ransomware families focused solely on NAS. This trend is unlikely to fade, as this attack vector proves to be very profitable for the attackers, especially due to the users being completely unprepared for them as they consider this technology highly reliable. NAS devices are usually purchased as complete and secure products, which as it turns out is not the case. Consumers and especially business users need to therefore remain cautious when protecting their data”, said Fedor Sinitsyn, security researcher at Kaspersky.

During Q3 2019, Kaspersky products detected and repelled encryption ransomware attacks on

229,643 Kaspersky products users worldwide, which is 11% less than during the same period last year. Thailand also has lesser numbers of users infected with ransomware, which is 0.85% in Q3 2019, while it was 1.43% in Q3 2018. Although the total number of affected users slightly decreased, the global report shows that the number of new encryption ransomware modifications grew from 5,195 in Q3 2018 to 13,138 in Q3 2019 marking 153% growth. This development signals cybercriminal interest in this type of malware as means of enrichment.

In Southeast Asians countries, Thailand ranks fourth among neighbors in terms of highest numbers of ransomware detections. Top Three countries are Indonesia, Vietnam, and the Philippines. Malaysia and Singapore rank fifth and sixth respectively.

At the same time, the infamous WannaCry Trojan family retained first place among the most popular Trojans with over a fifth of attacked users having been targeted with malware identified as belonging to this group. The top three most popular verdicts that account for almost half of users attacked by cryptors were Trojan-Ransom.Win32.Wanna (20.96% users attacked), Trojan-Ransom.Win32.Phny (20.01%) and Trojan-Ransom.Win32.GandCrypt (8.58%).

Other report findings include:
• Kaspersky detected and repelled 989,432,403 malicious attacks from online resources located in around 200 countries and territories around the world (4% growth compared to Q3 2018)
• Attempted malware infections that aim to steal money via online access to bank accounts were registered on 197,559 user computers (35% decline compared to Q3 2018)
• Kaspersky's antivirus file detected a total of 230,051,054 unique malicious and potentially unwanted objects (4% decrease compared to Q3 2018)
• Kaspersky mobile security products also detected 870,617 malicious installation packages (33% decrease compared to Q3 2018)

To reduce the risk of infection by encryptors, Kaspersky advises consumers and businesses to:
• Always update your operating system to eliminate recent vulnerabilities and use a robust security solution with updated databases
• Use a security solution that has specialized technologies to protect your data from ransomware such as Kaspersky Endpoint Security for Business and Kaspersky Security Cloud for consumers. Corporate grade endpoint security suites also have patch management and exploit prevention capabilities that would be helpful against these threats
• Always have fresh back-up copies of your files so you can replace them in case they are lost (e.g. due to malware or a broken device) and store them not only on the physical object but also in cloud storage for greater reliability
• Remember that ransomware is a criminal offence. You shouldn't pay. If you become a victim, report it to your local law enforcement agency. Try to find a decryptor on the internet first – some of them are available for free here: https://noransom.kaspersky.com
• Businesses can enhance their preferred third-party security solution with free Kaspersky Anti-Ransomware Tool
• To strengthen protection of NAS in corporate environments, implement specialized security solutions such as Kaspersky Security for Storage. This will ensure always-on anti-malware scans are carried out with flexible and granular configuration, while integration with NAS via native API means less impact on end-user productivity

Read the full version of the Kaspersky's IT Threat Evolution Report Q3 2019 on Securelist.com.

IT threat evolution Q3 2019