AO Kaspersky Lab
39A/2 Leningradskoe Shosse,
Moscow, 125212, Russia

+7 495 797 87 00
www.kaspersky.com
www.securelist.com

Annex to the second 'Pre-draft' of the report of the Open-Ended Working Group ('OEWG') on developments in the field of information and telecommunications in the context of international security

Kaspersky brief on the threat landscape during the pandemic

June 2020

As a non-governmental organization and cybersecurity company, Kaspersky welcomes the opportunity to share detailed information on the cyber threat landscape during the COVID-19 pandemic for Q1 2020.

The COVID-19 pandemic has affected us all in some way, and cybercriminals are no exception. Spammers and phishers[1] first sought to exploit the global health crisis (primarily through fraudulent emails purporting to offer health and safety tips from the World Health organization ('WHO')), but changes in the cyber threat landscape were not limited to these types of activities. While it is impossible to attribute all of the changes Kaspersky has observed solely to the pandemic, we can share some trends that seem to correlate with COVID-19.

Advanced Persistent Threat ('APT') Trends – Q1 2020

Since the WHO declared COVID-19 a pandemic, this topic has received increased attention from malicious cyber-actors. Cybercriminals have launched many of the phishing scams we have seen in order to cash in on people's fears about the virus. However, open source intelligence resources have also found that APT threat actors, such as Kimsuky, APT27, Lazarus, and ViciousPanda, have used COVID-19-themed lures to target their victims.

Kaspersky recently discovered suspicious command-and-control infrastructure that could have been used to target health and humanitarian organizations, including the WHO. While this infrastructure was initially registered before the COVID-19 pandemic in June 2019, and assigning it to any particular cyber-threat actor is not possible at this time, some private sources indicate that it may be related to the DarkHotel[2] APT actor. However, Kaspersky cannot confirm this information at the moment. Interestingly, some cybercrime groups have declared that they would not target health-related organizations during the pandemic in an effort to try and soften their public image.[3]

Kaspersky also sees continuous growth in malicious cyber-activity in Asia, and how some of the recently identified actors are now well established. On the other hand, long-standing APT actors seem more selective in their operations. The use of mobile platforms for infections and malware distribution is on the rise. Every actor seems to have some artifacts for these platforms, and in some campaigns, these platforms are the main target.

---

[1] Kaspersky report: spam and phishing in Q1 2020 https://securelist.com/spam-and-phishing-in-q1-2020/97091/
[2] The DarkHotel APT. APT report by Kaspersky GReAT https://securelist.com/the-darkhotel-apt/66779/
[3] Winder, Davey. "Hackers Promise 'No More Healthcare Cyber Attacks' During COVID-19 Crisis," Forbes, 19 March 2020, https://www.forbes.com/sites/daveywinder/2020/03/19/coronavirus-pandemic-self-preservation-not-altruism-behind-no-more-healthcare-cyber-attacks-during-covid-19-crisis-promise/#3b938479252b (accessed 11 June 2020).

APT actors have also sought to exploit COVID-19 via spear-phishing campaigns. While these types of attacks may seem unsophisticated, they remain highly effective and do not seem to represent a meaningful change in terms of the tactics, techniques, or procedures of these groups. In summary, here are some of the main trends that we have seen so far in 2020:

- APT actors such as, but not limited to, Kimsuky, Hades, and DarkHotel, as well as opportunistic cybercriminals, are exploiting the COVID-19 pandemic.
- It is clear from activities of various APT groups, including CactusPete, LightSpy, Rancor, Holy Water, TwoSail Junk, and others, that geopolitics continues to be an important driver of APT activity.
- Financial gain remains a motive for some APT actors, as demonstrated by the activities of the Lazarus and Roaming Mantis groups.
- Southeast Asia is currently the most active region in terms of APT activities, including established actors such as Lazarus, DarkHotel and Kimsuky, and newer groups such as Cloud Snooper and Fishing Elephant.
- APT actors such as CactusPete, TwoSail Junk, FunnyDream, and DarkHotel continue to exploit software vulnerabilities.
- APT actors continue to include mobile implants in their arsenal.

More detailed information is provided in the APT Q1 2020 report[4] by Kaspersky's Global Research and Analysis Team ('GReAT').

IT Threat Evolution Q1 2020

Kaspersky identified a number of key trends in the overall evolution of IT threats during Q1 2020,[5] as well as statistics that are based on detection verdicts for Kaspersky products received from users who consented to providing statistical data:

- **Ransomware programs**: ransomware attacks on organizations, as well as on city and municipal networks, did not decrease, on the contrary - more and more ransomware is starting to supplement encrypting files with data theft. To date, this tactic has been adopted by distributors of ransomware families, including Maze, REvil/Sodinokibi, DoppelPaymer and JSWorm/Nemty/Nefilim. If the victim refuses to pay the ransom for decryption (because, for instance, the data was recovered from a backup copy), the attackers threaten to put the stolen confidential information in the public domain. Such threats are sometimes empty, but not always: the authors of several ransomware programs have set up websites that do indeed publish the data of victim organizations.

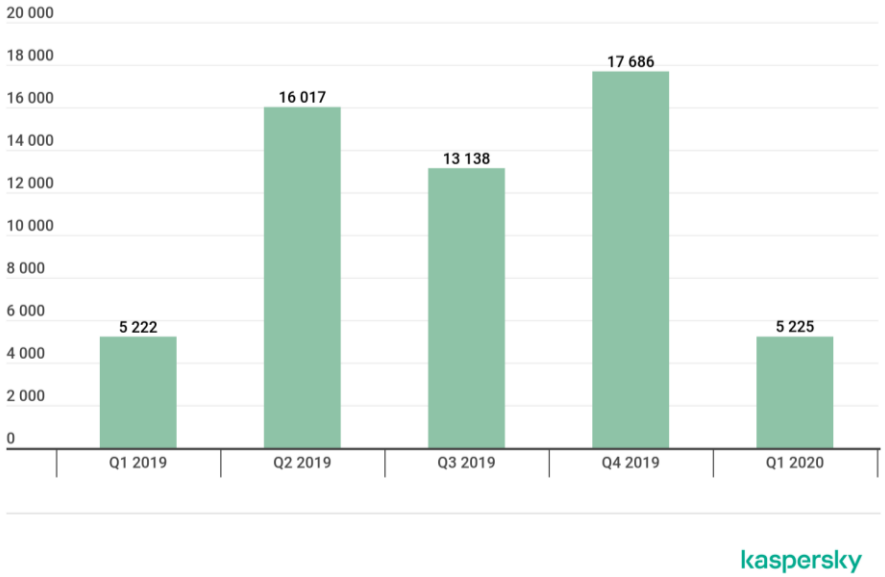
  In Q1 2020, we detected five new ransomware families and 5225 new modifications of these malware programs:

[4] APT trends report Q1 2020 by Kaspersky GReAT https://securelist.com/apt-trends-report-q1-2020/96826/

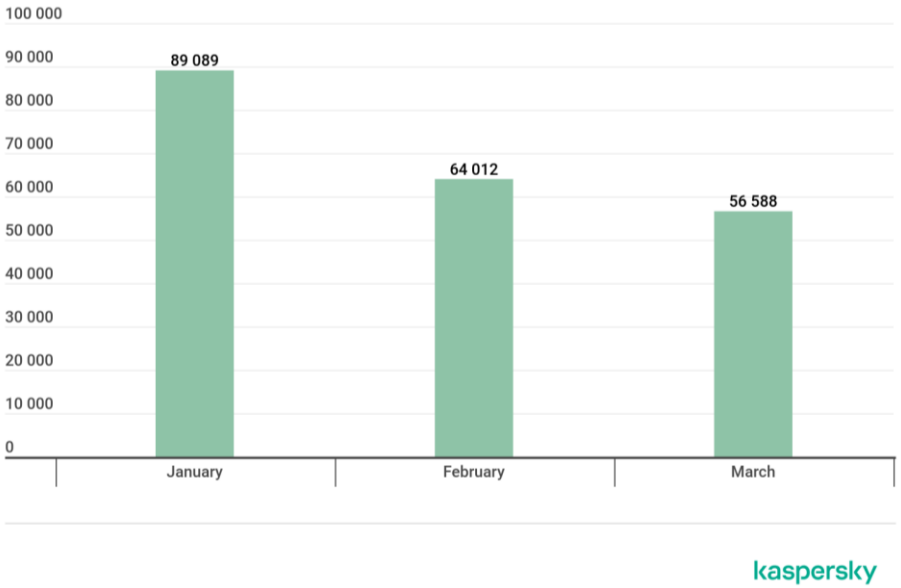
[5] IT threat evolution Q1 2020 report by Kaspersky https://securelist.com/it-threat-evolution-q1-2020/96886/ and separately IT threat evolution Q1 2020 statistics https://securelist.com/it-threat-evolution-q1-2020-statistics/96959/

AO Kaspersky Lab
39A/2 Leningradskoe Shosse,
Moscow, 125212, Russia

+7 495 797 87 00
www.kaspersky.com
www.securelist.com



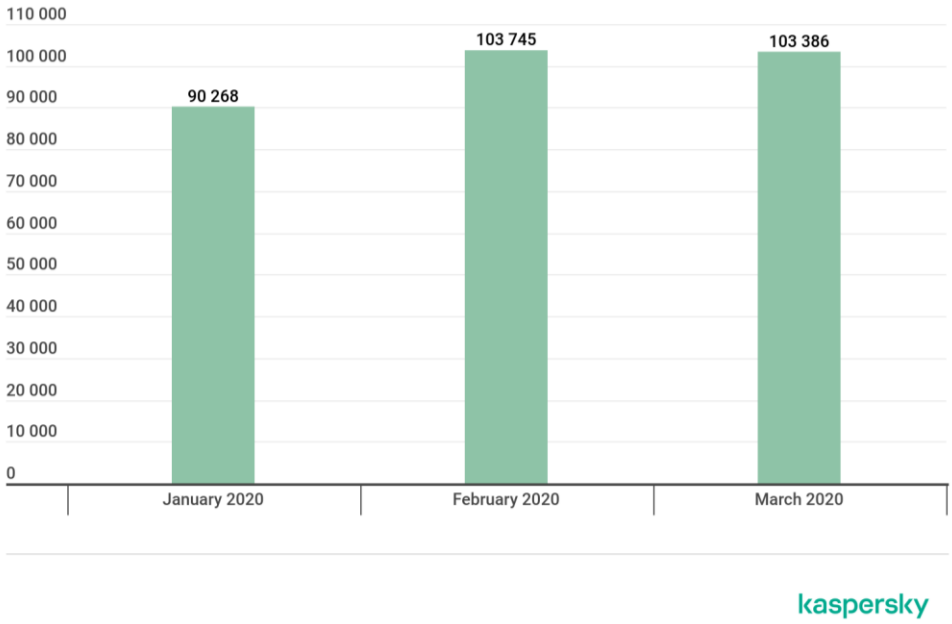
In Q1 2020, Kaspersky products and technologies protected 178,922 users from ransomware attacks. The number of unique users attacked by ransomware Trojans in Q1 2020 is illustrated below:



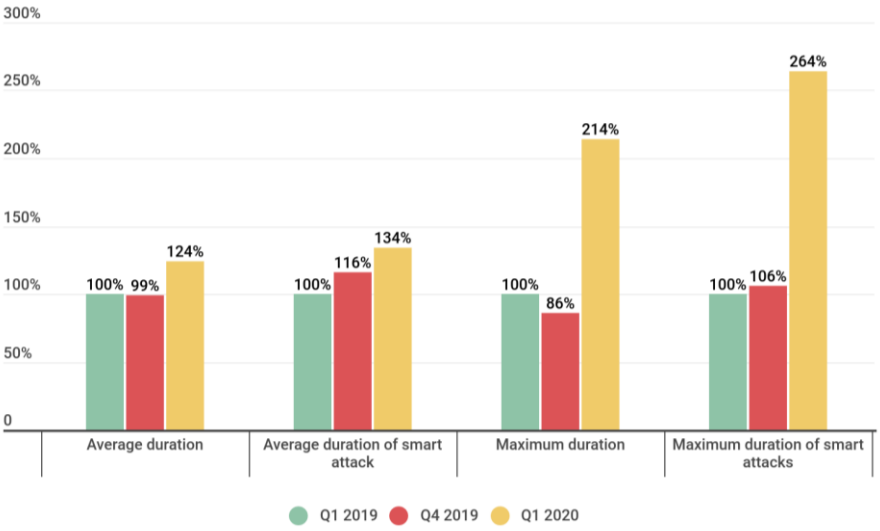
- **Financial threat statistics**: In Q1 2020, Kaspersky solutions blocked attempts to launch one or several types of malware designed to steal money from bank accounts on the computers of 249,748 users. Number of unique users attacked by financial malware is illustrated below:

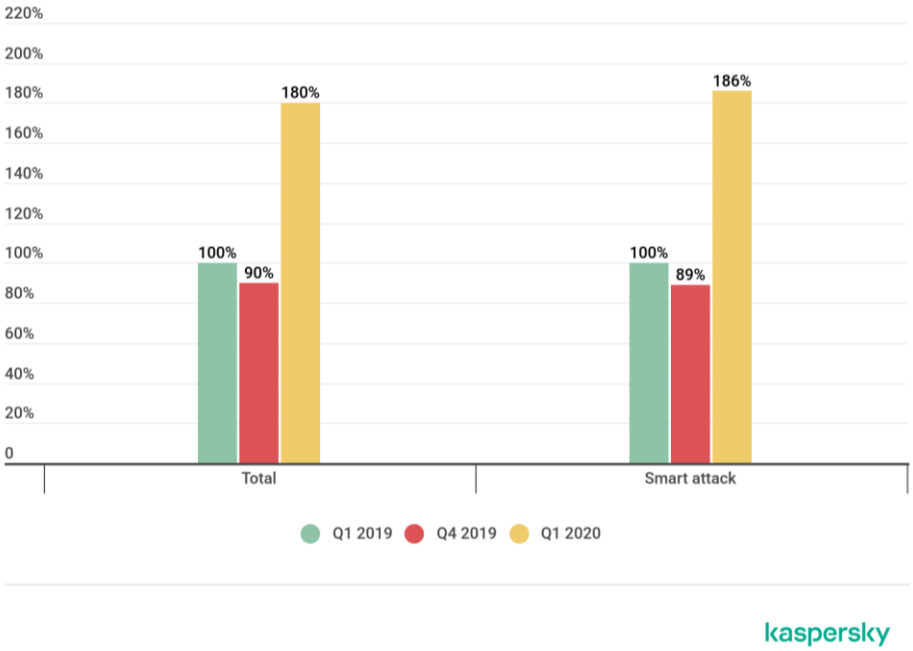
AO Kaspersky Lab
39A/2 Leningradskoe Shosse,
Moscow, 125212, Russia

+7 495 797 87 00
www.kaspersky.com
www.securelist.com



- **IoT threat statistics**: In the IoT field, Telnet, Secure Shell (SSH) and web servers are the most common services available and, therefore, the most-attacked ones. One of the most popular attack and infection vectors against devices remains cracking Telnet passwords. For Telnet and SSH, Kaspersky stores not only malicious payloads but also initial login credentials. This data enables us to identify targeted devices due to the default username/password combinations mainly used by the attackers. In Q1 2020, the share of IP addresses from which attempts were made to attack Kaspersky Telnet traps increased significantly. Their share amounted to 81.1% of all IP addresses from which attacks were carried out, while SSH traps accounted for slightly less than 19%. It was a similar situation with control sessions: attackers often controlled infected traps via Telnet (60.38% vs. 39.62% attacks at SSH traps).
- **DDOS attacks**: Contrary to our forecast in 2019, in Q1 2020, we observed a significant increase in both the quantity and quality of Distributed Denial of Service, or DDoS, attacks. The number of attacks doubled against the previous reporting period, and by 80% against Q1 2019. The attacks also became longer: we observed a clear rise in both the average and maximum duration. The first quarter of every year sees a certain spike in DDoS activity, but we did not expect this kind of surge. The comparison of the total number of DDoS attacks in Q1 2020 and Q1 and Q4 2019 (Q1 2019 is taken as the 100% reference value):



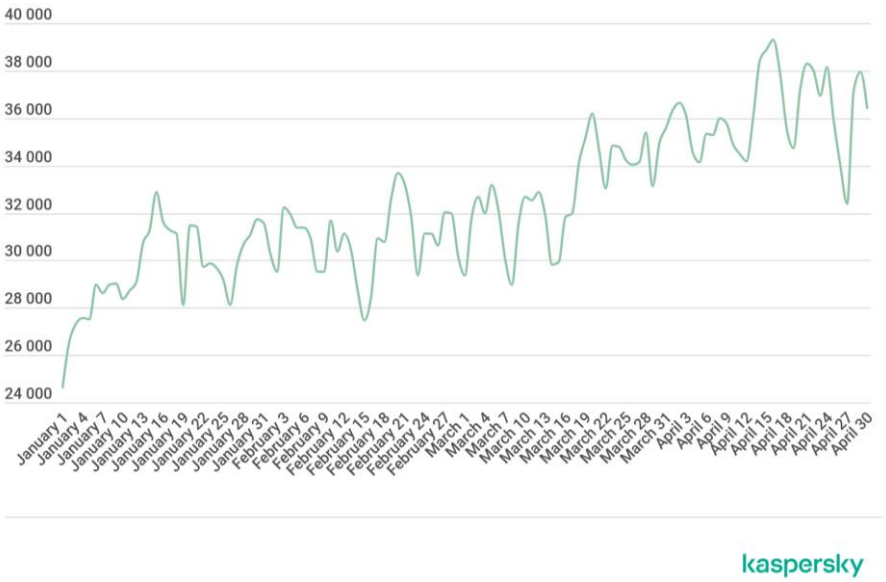


More details are in the Kaspersky DDoS attacks report, Q1 2020[6].

- **Attacks on servers and remote access tools:** From an information security standpoint, an employee within the office network and an employee connecting to the same network from home are two completely different users. It seems cybercriminals share this view, as the number of attacks on servers and remote access tools has

[6] Kaspersky DDoS attacks report, Q1 2020 https://securelist.com/ddos-attacks-in-q1-2020/96837/

increased as their usage has grown. In particular, the average daily number of brute-force attacks[7] on database servers in April 2020, was up by 23 percent from January:



Cybercriminals use brute force to penetrate a company's network and subsequently launch malware inside its infrastructure. We are monitoring several cybercrime groups that rely on the approach.

The payload is usually ransomware, mostly from the Trojan-Ransom.Win32.Crusis, Trojan-Ransom.Win32.Phobos and Trojan-Ransom.Win32.Cryakl families. More detailed analysis of these attacks is provided in a separate report[8].

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters to them most. Learn more at www.kaspersky.com. Readers who would like to learn more about Kaspersky intelligence reports or request more information on a specific report are encouraged to contact intelreports@kaspersky.com.

[7] This is a method for guessing a password (or the key used to encrypt a message) that involves systematically trying all possible combinations of characters until the correct one is found.

[8] "Remote spring: the rise of RDP bruteforce attacks" by Kaspersky GReAT https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/