Implicazioni del COVID-19 nel campo della sicurezza cibernetica

Apulia CyberSecurity Forum

Pierluigi PAGANINI

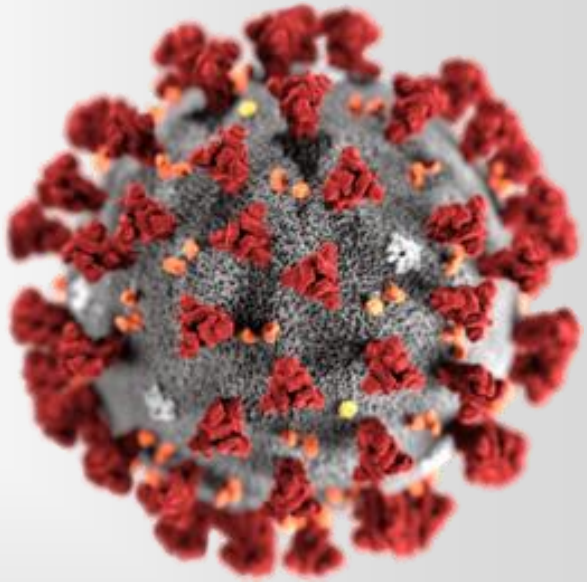
4 Novembre, 2020

Current scenario

- The current COVID-19 pandemic has brought significant changes in our society by forcing individuals and organizations to adopt new behaviors aimed at ensuring social distancing.

- New habits and the massive use of technological means have dramatically expanded our attack surface.

- Cyber criminals and nation state actors are attempting to maximize the effectiveness of their operations by exploiting the growing interest on the pandemic.



Current scenario

APR 2020

COVID-19: PEOPLE SPENDING MORE TIME WITH DEVICES

PERCENTAGE OF INTERNET USERS AGED 16 TO 64 IN SELECT COUNTRIES* WHO REPORT SPENDING MORE TIME USING EACH DEVICE IN RECENT WEEKS

SMARTPHONE OR MOBILE PHONE

76%

LAPTOP COMPUTER

45%

DESKTOP COMPUTER

32%

TABLET DEVICE

22%

SMART TV OR MEDIA STREAMING DEVICE

34%

GAMES CONSOLE

17%

SMART SPEAKER

11%

SMART WATCH

6.3%

SOURCE: GLOBALWEBINDEX'S CORONAVIRUS MULTI-MARKET STUDY (WAVE 2, APRIL 2020). ***NOTE:** FIGURES REPRESENT THE FINDINGS OF A SURVEY OF INTERNET USERS AGED 16 TO 64 IN AUSTRALIA, BRAZIL, CANADA, CHINA, FRANCE, GERMANY, INDIA, IRELAND, ITALY, JAPAN, NEW ZEALAND, PHILIPPINES, SINGAPORE, SOUTH AFRICA, SPAIN, THE UNITED KINGDOM, AND THE UNITED STATES. DATA COLLECTION (FIELDWORK) TOOK PLACE BETWEEN MARCH 31 AND APRIL 02, 2020. SEE GLOBALWEBINDEX.COM FOR MORE DETAILS.

Current scenario

APR 2020

COVID-19: INCREASE IN ONLINE AND DIGITAL ACTIVITIES

PERCENTAGE OF INTERNET USERS AGED 16 TO 64 IN SELECT COUNTRIES* WHO REPORT SPENDING MORE TIME ON EACH ACTIVITY IN RECENT WEEKS

WATCHING MORE SHOWS & FILMS ON STREAMING SERVICES

57%

SPENDING LONGER USING SOCIAL MEDIA

47%

SPENDING LONGER ON MESSENGER SERVICES

46%

LISTENING TO MORE MUSIC STREAMING SERVICES

39%

SPENDING MORE TIME ON MOBILE APPS

36%

SPENDING MORE TIME PLAYING COMPUTER OR VIDEO GAMES

35%

CREATING AND UPLOADING VIDEOS

15%

LISTENING TO MORE PODCASTS

14%

SOURCE: GLOBALWEBINDEX'S CORONAVIRUS MULTI-MARKET STUDY (WAVE 2, APRIL 2020). ***NOTE:** FIGURES REPRESENT THE FINDINGS OF A SURVEY OF INTERNET USERS AGED 16 TO 64 IN AUSTRALIA, BRAZIL, CANADA, CHINA, FRANCE, GERMANY, INDIA, IRELAND, ITALY, JAPAN, NEW ZEALAND, PHILIPPINES, SINGAPORE, SOUTH AFRICA, SPAIN, THE UNITED KINGDOM, AND THE UNITED STATES. DATA COLLECTION (FIELDWORK) TOOK PLACE BETWEEN MARCH 31 AND APRIL 02, 2020. SEE GLOBALWEBINDEX.COM FOR MORE DETAILS.

Current scenario

- More companies are going remote due to COVID-19
- Businesses and government organizations, are forced to review their internal processes to deal with the pandemic.
- To maximize damage to victims and their own profit, cybercriminals are focusing attacks on large companies.
- Governments and critical infrastructures are most exposed due to the role they play in the response to the pandemic.

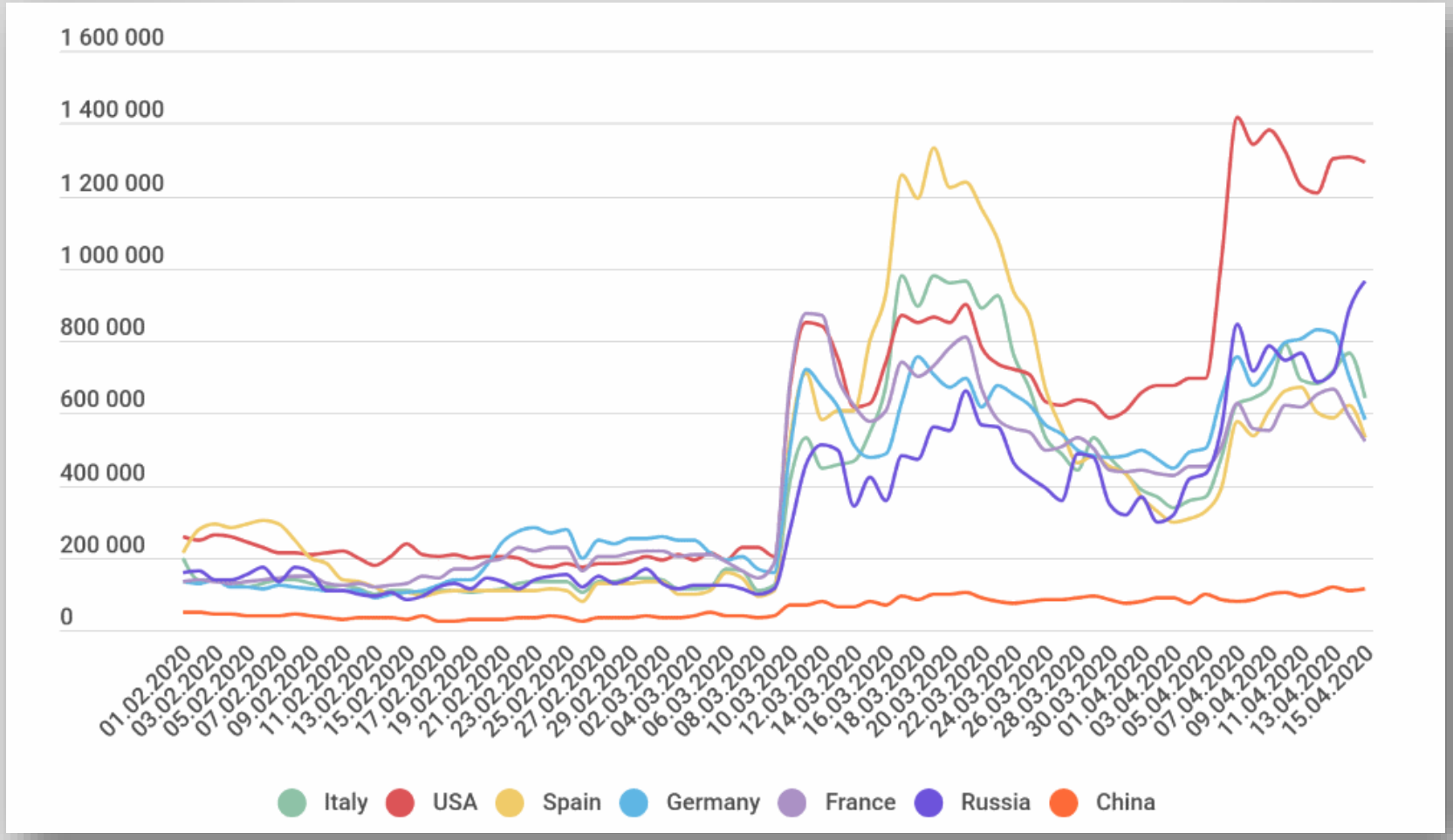
Current scenario

- In early April, researchers from IoT search engine Shodan reported a 41% increase in the number of RDP endpoints exposed online since the beginning the COVID-19 pandemic.

- Since the beginning of March, the number of Bruteforce.Generic.RDP attacks has rocketed across almost the entire planet.

- Threat actors are attempting to exploit vulnerabilities in systems and flaws in implemented processes to enable remote working (i.e. VPN).

Current scenario



Growth in the number of attacks by the Bruteforce.Generic.RDP family, February–April 2019 (Source Kaspersky)

Current scenario

There are essentially two schools of thought con cyber attacks during the pandemic:

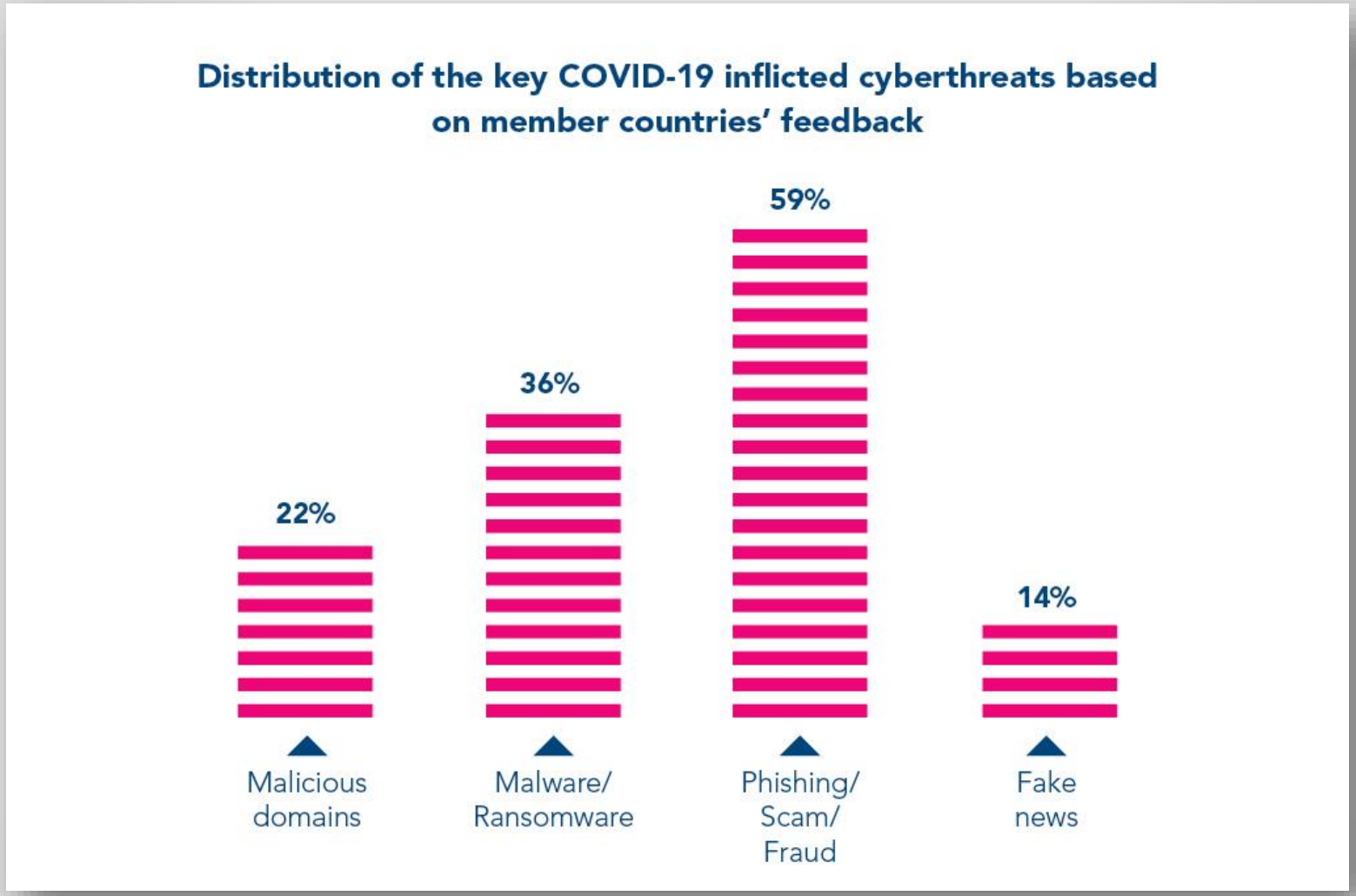
- Numerous companies and government organizations declare that they have observed a surge in cyber attacks since the beginning of the pandemic.
- Some companies claim that the number attacks has not increased significantly, only the way hackers are targeting organizations has changed, using the Coronavirus theme as bait.

Cybercrime

"Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19."Jürgen Stock, INTERPOL Secretary General

- *INTERPOL and its technical partner observed intense activity associated with the COVID-19 theme;*
- *Experts identifying approximately 907,000 spam messages, 737 incidents related to malware attacks and 48,000 malicious URLs.*
- *Threat actors are spreading malware for information theft, such as Remote Access Trojan (RAT), spyware, and obviously banking Trojans*

Covid-19 inflicted Cyber Threat (Interpol)



NATO call to action

- *In June, NATO issued a statement condemning cyber attacks against critical infrastructure involved in the response to the COVID-19.*
- *Threat actors are targeting health services, hospitals and research institutes endangering the lives of citizens.*
- *NATO calls alliance members to support each others.*
- *Cyber defense is a core element of NATO's advocated collective defense concept*

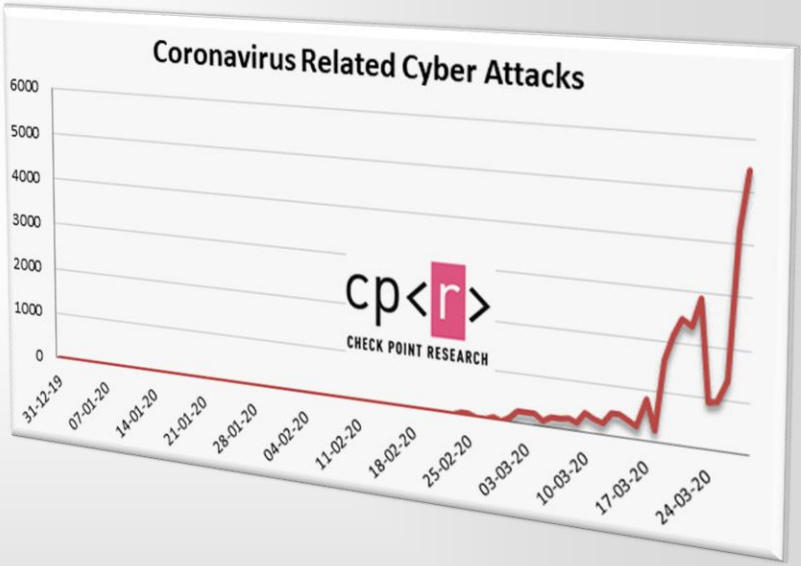
Healthcare industry under attack

- *FBI and the CISA published a joint alert to warn hospitals and healthcare providers of imminent ransomware attacks from Russia (Ryuk gang).*
- *Unlike other ransomware gangs, Ryuk operators did not announce to avoid targeting healthcare organizations during the COVID-19.*
- *Universal Health Services (UHS) shut down systems at healthcare facilities in the US after they were infected with the Ryuk ransomware.*
- *Dr. Reddy's, the Indian contractor for Russia's "Sputinik V" COVID-19 vaccine was hit with a cyber-attack.*

COVID-19 Themed attacks

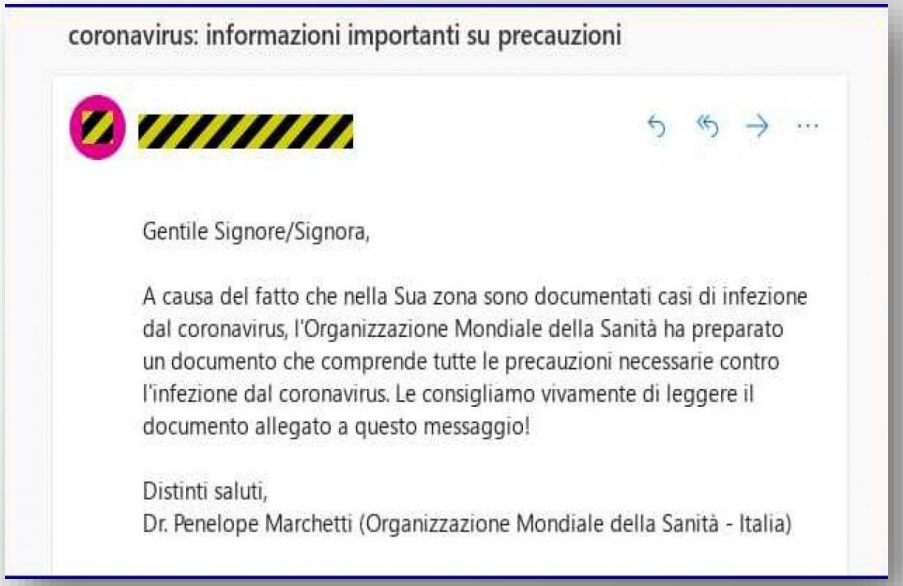
Which are the attack techniques employed by cybercrime organizations and how they exploited the COVID-19 theme?

- *Security companies and national CERTs / CSIRTs have seen a significant increase in the number of online scams and Covid-19 themed phishing campaigns.*
- *Threat actors impersonate world and local health authorities and government agencies to trick victims into providing personal and financial data or to download malware.*
- *In June, as the coronavirus spread globally, Google announced it had blocked more than 240 million of spam messages.*



COVID-19 Themed attacks

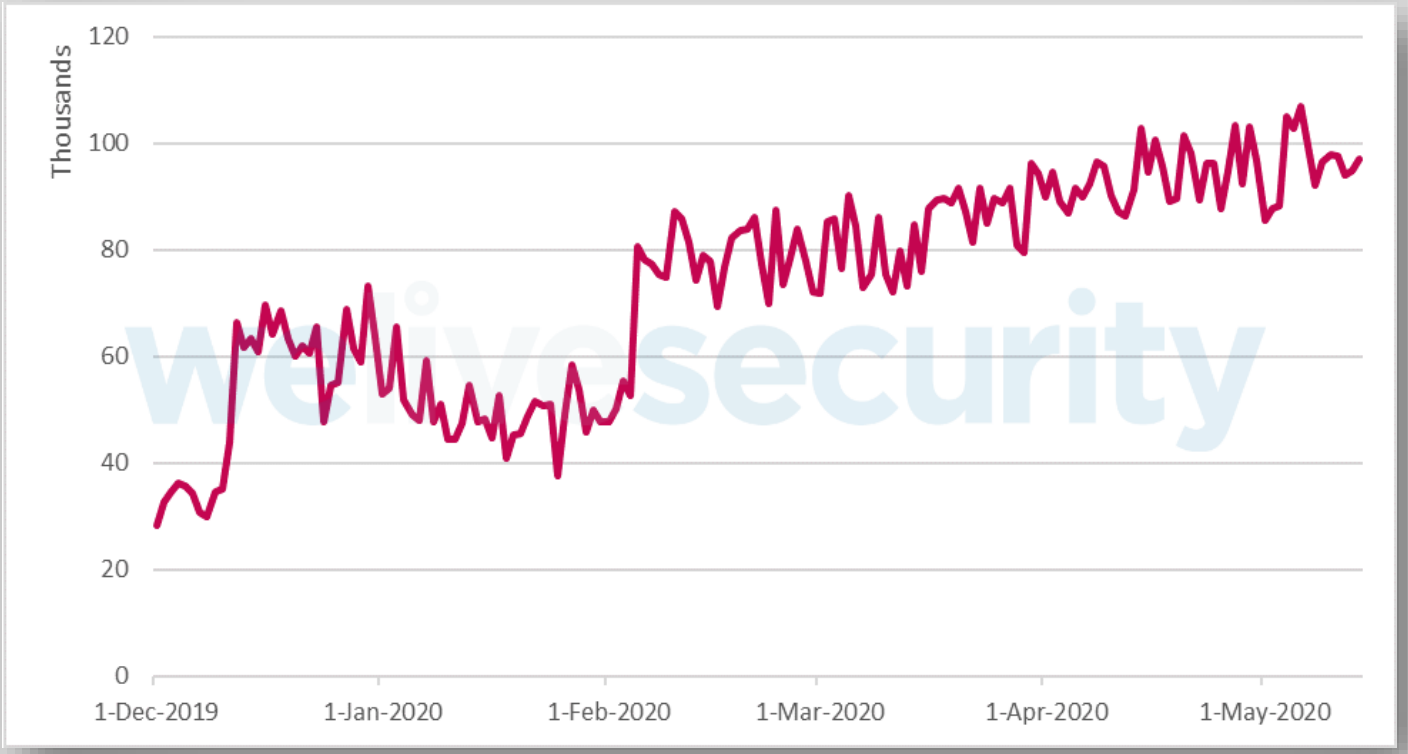
- Experts observed a surge in the Covid-19 themed attacks associated with peaks of emergency in specific countries (i.e. India, Brazil, UK)
- Microsoft confirmed a significant increase in COVID-19-themed attacks as the result of tactics change by threat actors.
- Most of the campaigns Microsoft observed were highly localized because attackers closely followed local developments in the crisis and the response of the population.



COVID-19 - increase in extortion practices

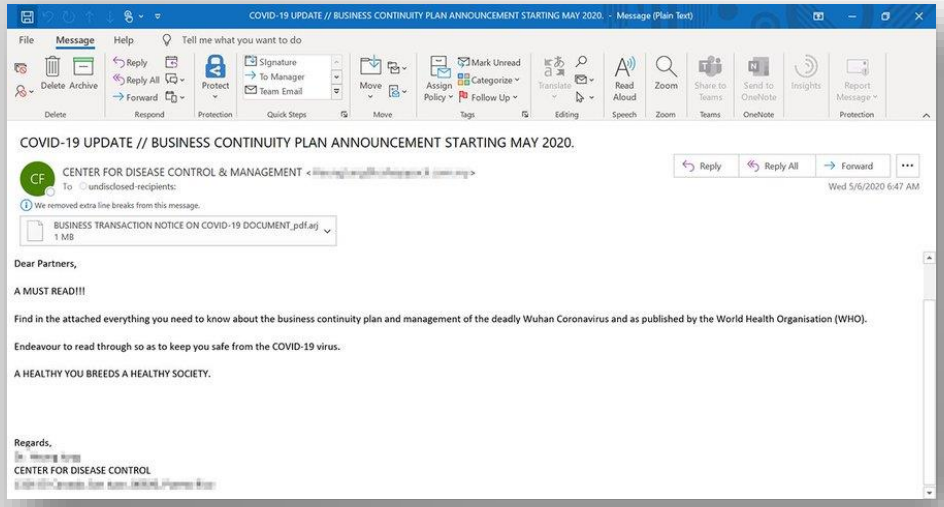
- Experts observed a significant increase in extortion practices, mainly through the spread of ransomware and Distributed Denial of Service (DDoS) attacks.
- A surge of attacks using known vulnerabilities in VPN systems and attempting to access systems exposed online via the Remote Desktop Protocol (RDP) have increased.
- RDP brute force attacks skyrocketed in March due to remote work imposed during the COVID-19 pandemic by many companies.
- ESET experts have observed numerous campaigns in which malicious actors attempted to exploit poorly secured RDP connections to access the networks of targeted organizations and install malware such as crytocurrency miners, backdoors, and of course ransomware.

COVID-19 - increase in extortion practices



- Between December 2019 and until February 2020, experts recorded an average number of attacks of between 40,000 and 70,000 on a daily basis, but the situation has changed dramatically since February, when the number reached and exceeded 80,000.

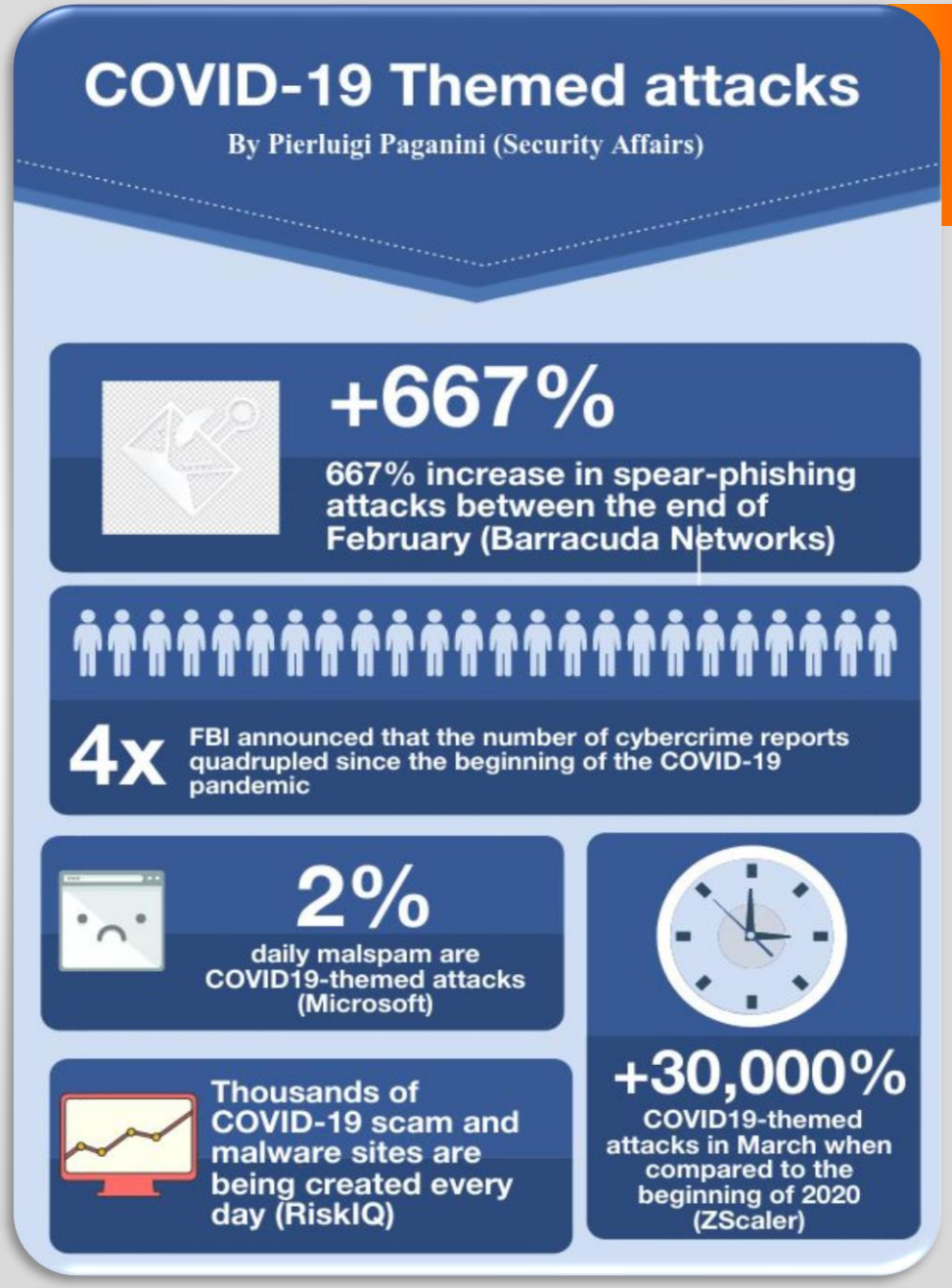
COVID-19 – Themed malware campaigns



- Spam campaigns use decoy docs that promise to provide information on the pandemic and the procedures recommended by governments and companies for containing the virus.
- The infection process starts every time these documents are opened and the victims have been tricked into enabling macros.
- In May alone, the Microsoft observed numerous COVID19-malware campaigns spreading the info-stealer LokiBot and the banking Trojan Emotet.

COVID-19 – Themed malware campaigns

- Threat actors created thousands of malicious domains on a daily basis to spread malware or to arrange phishing campaigns.
- The increased demand for medical supplies has supported a major increase in the number of domain name registrations containing keywords, such as "coronavirus" or "COVID".
- These fraudulent domains were used for multiple criminal activities. From February to March 2020, there was a 569% increase in the registrations of malicious domains according to Interpol.



Nation-state hacking

- In April, Google TAG identified at least a dozen nation-state groups using COVID-19 as bait in attacks on healthcare organizations and entities involved in the development of vaccines and possible drugs for the containment of the virus.

- In July, the UK's National Cyber Security Center revealed that the Russian government-linked APT29 group is responsible for cyber-espionage campaigns targeting British, US and Canadian orgs working on a vaccine.

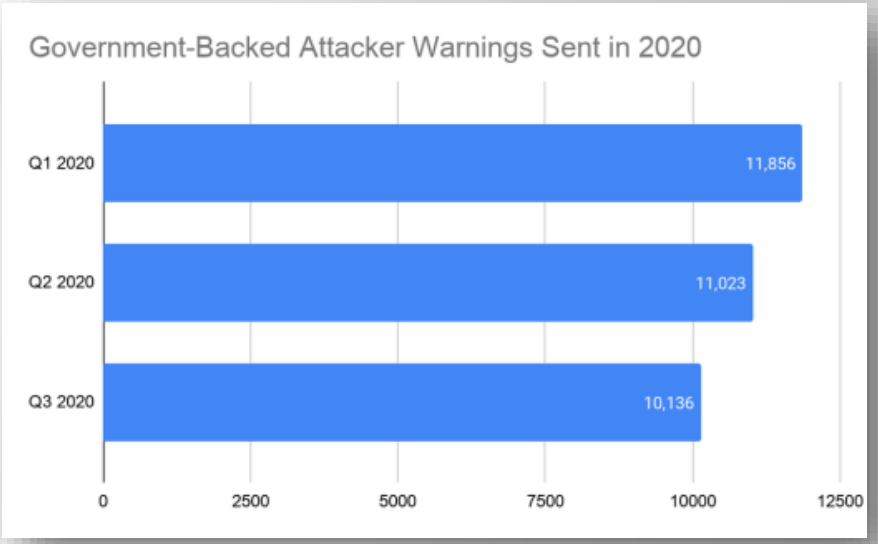
- Since the beginning of the pandemic multiple nation-state actors have carried out disinformation campaigns, mainly Russia and China.

Nation-state hacking

- Google delivered over 33K alerts to its users during the first three quarters of 2020 to warn them of attacks from nation-state actors.

- During the last summer, Google observed threat actors from China, Russia, and Iran targeting pharmaceutical companies and researchers involved in the development of a vaccine.

- In September, Google experts started to observe attacks carried out by multiple North Korea-linked APT groups aimed at COVID-19 researchers and pharmaceutical companies, especially those based in South Korea.



Nation-state hacking

- US authorities warned healthcare and scientific researchers that China-linked hackers were attempting to steal research related to treatments and vaccines for COVID-19. (May 2020).

- Chinese hackers have stolen information from Spanish laboratories working on a vaccine for COVID19, El Pais newspaper revealed. (Sept 2020).

Nation-state hacking – The Chinese arsenal

1) CVE-2019-11510 – In Pulse Secure VPNs, ® 7 an unauthenticated remote attacker can send a specially crafted URI to perform an arbitrary file reading vulnerability. This may lead to exposure of keys or passwords.

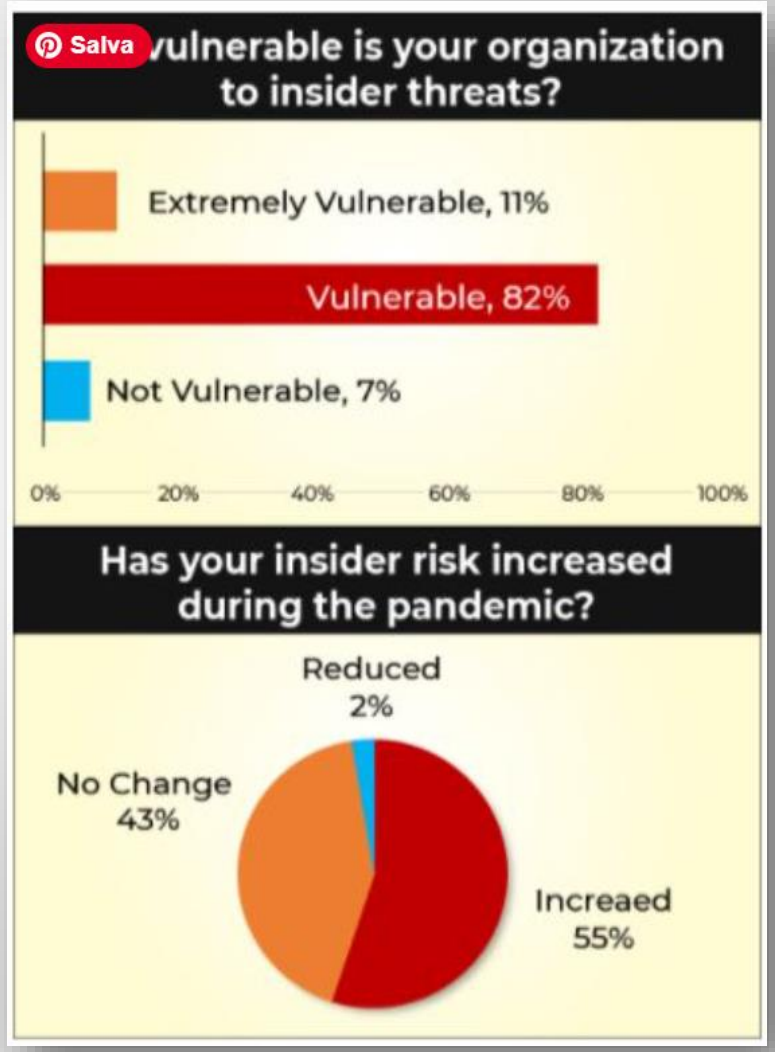
2) CVE-2020-5902– In F5 BIG-IP® 8 proxy / load balancer devices, the Traffic Management User Interface (TMUI) – also referred to as the Configuration utility – has a Remote Code Execution (RCE) vulnerability in undisclosed pages.

3) CVE-2019-19781 – An issue was discovered in Citrix® 9 Application Delivery Controller (ADC) and Gateway. They allow directory traversal, which can lead to remote code execution without credentials.

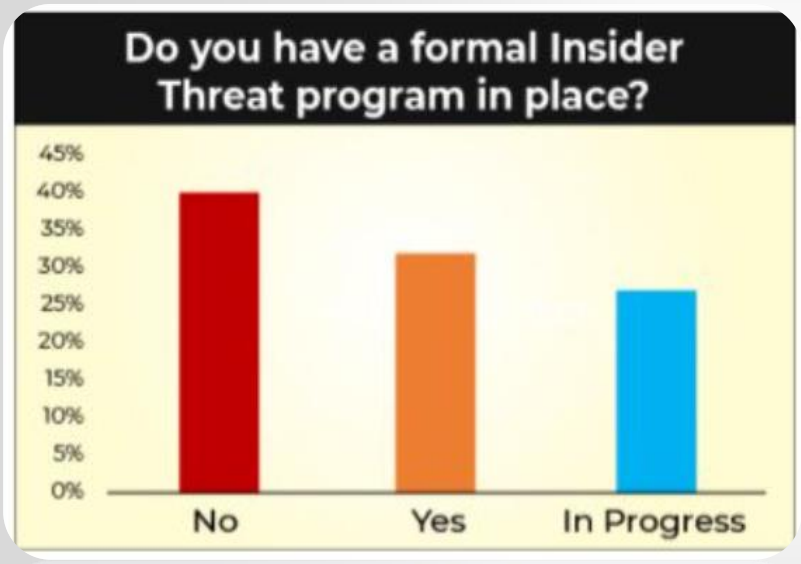
- The US National Security Agency (NSA) has shared the list of top 25 vulnerabilities exploited by Chinese state-sponsored hacking groups in attacks in the wild.
- The report includes well known vulnerabilities that have been already addressed by their vendors.

Insiders

- Amazon, Twitter, and Shopify recently faced serious security breaches from insiders (i.e. employees, partners, suppliers and contractors, past and present).
- Pandemic fallout creates perfect conditions for insider threat
- Insider threats increased during the # COVID-19 pandemic, challenging corporate cybersecurity teams, Legal, HR and communications staff.
- According to Forrester, a third of all security incidents in 2021 will be caused by insiders.



Insiders



- Motivations that compel employees to become malicious insiders include financial distress, disgruntlement, and announcement or fear of layoffs.
- The use of traditional technologies, such as DLP (Data Loss Prevention) tools, PAM (Privileged Access Management) solutions or other point solutions are no longer sufficient to detect the behavior of insiders today,
- Use a ML behavioral anomaly technique that combines the occurrence of a rare event together with anomalies that indicate suspicious or abnormal usage

Disinformation campaigns

- One of the most dangerous phenomenon observed during the pandemic is represented by the numerous disinformation campaigns aimed at spreading fake news related to COVID-19.
- The campaigns observed are mainly attributed to nation-state actors who have worked to destabilize the political context of other countries by sowing fear and undermining trust in their governments.
- i.e. Fake link between 5G technology and the spread of Coronavirus.

Conclusion

- Overlap between digital and real-life is significant.
- The pandemic caused a burst in the penetration of technology in our society with consequent security issues.
- Security is still considered a cost to cut.
- More to come!

About me

About Pierluigi Paganini:

Pierluigi Paganini is a member of the ENISA (European Union Agency for Network and Information Security))Threat Landscape Stakeholder Group, member of Cyber G7 Workgroup of the Italian Ministry of Foreign Affairs and International Cooperation, Adjunct Professor in Cyber Security at Luiss University.
He is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing, and a strong belief that security is founded on the information sharing lead Pierluigi to launch the security blog "Security Affairs" recently awarded as the Best European Personal Security Blog.
Author of the Books "The Deep Dark Web" "Digital Virtual Currency and Bitcoin" and "Digging the Deep Web: Exploring the dark side of the web",

Ing. Pierluigi Paganini

Chief Technology Officer & Founder Cybaze SpA.

Founder Security Affairs

http://securityaffairs.co/wordpress

pierluigi.paganini@securityaffairs.co


Thank you