Watching the whole world come to a grinding halt, streets emptying, chemical smell of sanitizer permeating the air, and the uneasy expectation of more bad news to come.

CYBERSECURITY DURING THE FIGHT AGAINST COVID-19

ROOT LEVEL RESOURCES

Coronavirus has upended the lives of people across the globe, forcing them to stay indoors and do their work remotely. From day one, many companies ran into the problem of building the technological systems necessary to adjust to the new normal. The reality is that remote work does not allow for the same level of cybersecurity easily achieved in an office setting. It might be a tough pill to swallow but cybersecurity capabilities of most companies were weakened by their switch to remote work. This, as we predicted, triggered a chain reaction: a surge in the number of successful cyber attacks on vital processing systems, SWIFT, banking networks and other payment systems. Two factors make cyber attacks more successful:

1

Incorrect connection of computers to internal servers through VPN, when a laptop used by an employee at home suddenly becomes out of reach of the company cybersecurity protections.

2

Employees working at home are unable to react to security threats in an efficient and coordinated manner.

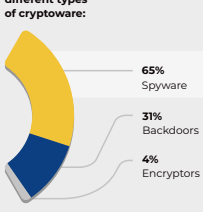
Another common problem is an increase in traffic, which often means servers are unable to take the strain and buckle under the pressure.

This situation is ripe for abuse by attackers. It is hard to think of another time when the risk posed by cyber threats was higher. From viruses causing system-wide crashes to more garden-variety cyberattacks. Those with the highest risk exposure are financial institution, telecom and tech company employees. The objective of an attacker is no longer to simply steal money or personal data but to break into the internal system of their target company. This is achieved by infiltrating personal computers of company employees.

Phishing emails during the pandemic

In the period from February 13 to April 1, top experts at CERT-GIB analyzed hundreds of phishing emails disguised as information campaigns and promotional offers related to COVID-19. Emails were written on behalf of well-known international organizations (WHO, UNICEF), as well as large Russian corporations and multinationals. These email campaigns targeted commercial and government sectors in Russia and CIS. The emails were successfully captured by the Threat Detection System (TDS).

Emails contained different types of cryptoware:



Spyware is capable of collecting information on the system and infected computers, downloading and activating corrupting files, taking screenshots, logging keystrokes, as well as stealing user data: logins, browser passwords, contact emails, debit and credit card numbers, banking account passwords, and more.

The most in-demand trojans:

Even though the total percentage of phishing emails which exploited COVID-19 was not high - they made up about 5% of malicious traffic during the recorded period - black hats are profiting off the public health crisis as evidenced by their messages on hacker forums and increase in malware sales.

As of February 2020, an underground forum is selling an interactive map for the tracking of COVID-19 which is really malware in disguise. The main method of infiltration is a phishing email campaign, capable of circumventing Gmail safeguards. Following infiltration, the user is presented with a map with real-time data from the WHO and John Hopkins University. In the meantime, "useful information" is being downloaded onto the computer, for instance, malware for the stealing of personal data. Overall, experts identified over 500 advertisements that were displayed on underground platforms and offered DDoD and spam campaign services. These ads featured discounts and promo codes: active for the duration of the pandemic. What could be better to create a sense of urgency among cyber criminals than a limited-time offer?

What is more, Group-IB experts recorded an emergence of false notifications about fines for the breaking of lockdown restrictions. Namely:

In April 2020, the Krasnoyarsk Region became a target of such a campaign, with SMS and social network messages being delivered to unsuspecting people. The messages even included the names and surnames of users. Many were notified they had to pay a fine of 4,000 RUB as required by a non-existent recree of the Federal Penitentiary Service.

As these notifications stated, the supposed fine had to be paid within a period of 24 hours by a direct bank transfer to an account based in the Krasnoyarsk Region. Those who called the phone number provided, were redirected to another number, which was supposed to be the number of the telephone directory of the Ministry of Internal Affairs of Russia.

Experts made a point of noting that the scammers test-drove their scheme last year: at the time users received notifications about "fines" for visiting porn sites.

It is also worth noting that so far - the lockdown was imposed on March 31 - the Krasnoyarsk Region leads when it comes to the number of cases of lockdown non-compliance. The criminal courts of the region were flooded with over 1,300 cases of administrative offences linked to 6.3 КоАП РФ (the breaking of regional rules governing sanitary and epidemiological welfare). As of today, over 1,000 are already resolved.

Close behind is the Republic of Tatarstan where lockdown restrictions on freedom of movement were introduced on March 30. In the Republic, 6.3 КоАП РФ regulation-related cases exceed 800.

To make matters worse, there has been a surge in the number of scam websites and messages on the topic of coronavirus, with crooks angling for vulnerable users' money or personal data.

Fake electronic passes

The pandemic has changed the daily lives of Russian citizens, which, in turn, provided the perfect breeding ground for scammers, offering their services and electronic passes.

Experts were able to identify the first attempts of internet scamming related to the fight against the COVID-19 pandemic as early as the end of March. This was before the first lockdown measures and the system of electronic passes were introduced. Based on the data provided by Group-IB, at the very beginning of the quarantine, experts recorded a spike in dubious offers of electronic passes promising freedom of movement in Moscow, Saint-Petersburg and Krasnodar on a popular messaging app. To get the pass, the scammers said, all one had to do was send their passport details, and, if the order was for a vehicle pass, their license number.

Another key condition was pre-payment for the service which could set you back anywhere between 2,500 and 6,000 RUB, depending on the electronic pass type and the website in question. Upon the transaction, the gullible customer was left empty-handed, all communication would stop, and that person would be blocked so they would not get in the way of communication with new candidates who were lining up to get the coveted electronic pass.

At least in one case, law enforcement authorities were able to track down two admins of such an internet platform — they turned out to be young people of 19 and 23. Both of them were apprehended on April 21. The Office of the Ministry of Internal Affairs in Moscow has already opened a fraud case against them (part. 1 law. 159 УК RF). It is not out of the question that the case might make its way up in the courts and will be found more "severe" based on the existing legislation of the Russian Federation.

The data collected by the Innovation, Brand and Intellectual Property Protection department of Group-IB indicates that 126 scammer platforms offering electronic passes have already been identified:

35 groups and accounts on social networks — **25 websites** — **66 Telegram channels**

Zoom Accounts for Sale

One of the most popular video-conferencing platforms to make a name for itself during the lockdown was Zoom. The company, Zoom Video Communications, offering a video-conferencing service of the same name, was founded back in 2011. Still, it was the lockdown that propelled it to global success. Daily usage worldwide in March 2020 was 20 times that of December 2019. Zoom hit 200 million users.

Group-IB experts soon identified banners advertising the sale of Zoom users' personal information on three different underground platforms. The total number of unique account records available for sale at the moment is 4153. Among these are 31 user accounts with an email address ending in .ru. But it doesn't appear possible to confirm whether or not these accounts really belong to Zoom users.

Earlier, Bloomberg reported on two lawsuits filed against Zoom, accusing the video-conferencing company of mishandling confidential user information. This includes a lawsuit, filed by a private individual in the San-Jose court of California, alleging the company collects user data without a requisite consent during the process of Zoom app installation, then this data is alleged to be shared with third parties, the most prominent of these is Facebook.

The Foreign Ministry of Germany has imposed strict restrictions on the use of the application among their employees due to security concerns, as reported by the Handelsblatt publication which links back to an internal document of the Ministry. Financial Times has also reported that the U.S. Senate recommended government staffers against using Zoom for video-conferencing due to fears related to data privacy.

ROOT LEVEL RESOURCES

Some rightly point out the post-covid world will never be the same. Even as lockdowns are gradually lifted across the world, a significant number of office workers will continue to work from home. This creates a major cybersecurity risk for firms — it is a challenge having to ensure all the necessary safety measures are in place.

In a situation like this one it is more important than even to follow the basic rules of cybersecurity. First and foremost, every employee who is working from home on their own device and who has access to confidential company information must have a programmatic system installed on this device for cyber threat detection and protection. This is the only way to safeguard against phishing emails, malware and spyware.

Apart from the basics of cybersecurity, we recommend that you also follow the principles of cyber-hygiene. This will help you maintain the safety of your devices and will allow for timely detection of suspicious activities of attackers even after life has returned to normal.

1 - The citizens of Moscow city are at the threat of paying a 5 thousands rubles fine for violating the of self-isolation law. Besides, the breachers of self-isolation regime can be sentenced to bigger fines - from 15 to 300 thousands according to the federal Code of Administrative Offenses (breach of sanitary and epidemiological wellness legislation).