State Service of Special Communications and Information Protection of Ukraine

The War in Ukraine: Pulse of Cyber Defense

April 11, 2022

Weekly analytics from the State Service of Special Communication and Information Protection of Ukraine

UKRAINIAN CYBERHUB

The largest war on the European continent since World War II is continuing not only on the ground and in the air, but also in the cyberspace.

The State Service of Special Communication and Information Protection of Ukraine is responsible for the cybersecurity standards in the country and takes an active part in the defense. The lessons learnt during this war are extremely important for strengthening the defense of democratic states attacked by aggressive countries like russia.

In this regard, the SSSCIP initiates making available a public analytical report on the state and means of cyber defense. The SSSCIP CyberHub will make public its data and conclusions that may be used by the global cyber community for their own defense.

45 DAYS OF CYBER FRONT

Highlights

- A month and a half of war: situation is escalating on the cyber front;
- Cyber front trends: russia uses military hackers in the attempts to pursue their political ambitions; russian military hackers are targeting civilians and the EU countries; the data obtained as a result of phishing attacks is further used for the purposes of cyber aggression;
- Ukrainian critical infrastructure defense: how Ukrenergo repulses cyber attacks and what happened to Ukrtelecom on March 28;
- Five tips for Ukrainian and international companies on how to counter the RF aggression on the cyber front.

DETAILS

russia's cyberwar strategy and tactics

russia has been waging a war against Ukraine for eight years already both on the ground and in the cyberspace. During all this time, we have been witnessing escalation. Probably every cyber defense expert knows what BlackEnergy, NotPetya, attack13 cyber-attacks are.

Before the RF military incursion into our country, we also observed escalation at our cyber borders: on February 15, Ukraine suffered the worst DDoS attack in its history. However, due to coordinated action of cybersecurity entities, we quickly eliminated its consequences. Soon we got used to live with it as DDoS attacks continued. There were over 3,000 DDoS attacks with a 100 Gbps peak.

It has been a month and a half of war. Our foreign partners are well aware of the situation on our front. The government and the media, often risking (and sadly losing) their lives, are highlighting in detail the actions of the "second army in the world". They include rocket shelling of residential areas, destroying civilian infrastructure, looting, creating humanitarian catastrophes in the occupied territories and committing atrocities against civilians.

However, not everything is obvious on the cyber front. We often say that the cyberwar is a hidden part of russia's aggression against Ukraine, and it is true. Some actions of our enemy require identification, collection of evidence, examination, attribution, etc.

We'd like to dedicate this digest to a recap of the first month and a half of war on the cyber front and recommendations for Ukrainian institutions and our international partners on defense against the russian aggression.

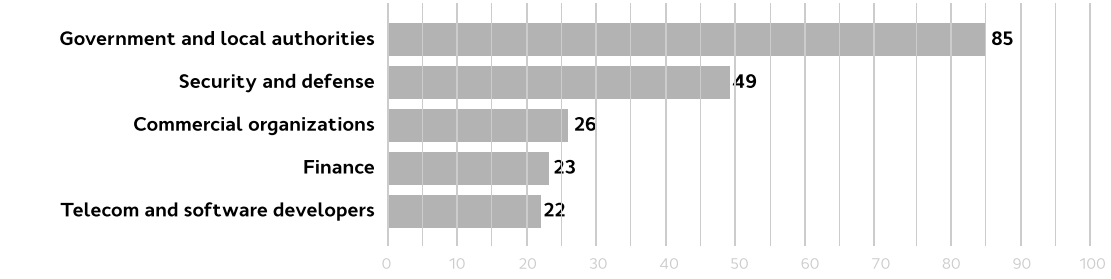
A MONTH AND A HALF OF WAR: SITUATION ON THE CYBER FRONT

During the first month and a half of war, Ukraine has suffered 362 cyber attacks. It is three times more as compared to the same period of the previous year (122 cyber attacks).

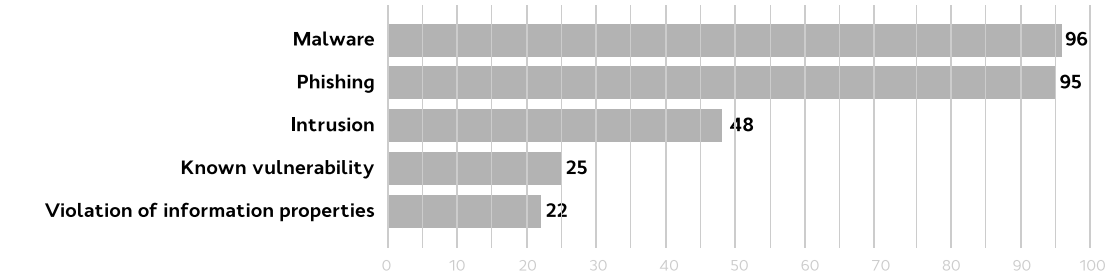
Cyber attacks on the government and local authorities, security and defense and commercial organizations accounted for a half of the total number. Over a half of attacks were made for the purpose of data collection or distribution of malware.

CYBER ATTACKS ON UKRAINE CRITICAL INFORMATIONAL INFRASTRUCTURE DURING THE FIRST MONTH AND A HALF OF WAR

KEY SECTORS TOP-5



KEY TECHNIQUES TOP-5



TOTAL OF ATTACKS WERE RECORDED OUT DURING THE PERIOD: 362

Each week we detect attacks made by the same groups that have attacked Ukraine during many years.

FIVE CYBERWAR TRENDS

russian military hackers make cyber attacks to pursue the political ambitions of their country's leadership

Hackers use cyber attacks to pursue the RF leadership's political ambitions.

According to the national transmission system operator, *Ukrenergo*, the number of cyber attacks has tripled since the beginning of the military action. The peak was observed during the connection of the Ukrainian energy system to ENTSO-E. During some of the attacks on Ukrenergo, russian hackers did not even try to hide their origin and used russian IP addresses to scan the national transmission system operator's network.

The russian army is not able to destroy Ukraine's communications infrastructure as our networks are decentralized and there is no "red button" in Ukraine to disconnect it from the Internet. Physical infrastructure attacks are of local nature, and their consequences are quickly eliminated by the providers.

That's why, as we can see during the war, the attacks by hackers on telecommunications networks have become more intensive. Triolan, Ukrtelecom and local providers in Odessa suffered from cyber attacks. It is evident that hackers are aiming at destroying the infrastructure or gaining control over it. It was confirmed by the investigation published by Viasat, a satellite communications provider. The same was also confirmed by the investigation of the cyber attack at Ukrtelecom. The attack consisted of two phases: the first phase included the discovery of the provider's network, during the second phase, there were attempts to destroy the infrastructure and gain control over the access to the provider's network and equipment.

russia also uses cyberattacks to spread panic among people and create mistrust in authority. In the same way as they try to block access of people to healthcare, food, humanitarian aid and evacuation in the temporarily occupied territories, they use hackers in the cyberspace to block the operation of services for people.

A week ago, there was a cyber attack on the Government Contact Centre. It is a tool for interaction between ordinary people and the government. As a result of the attack, virtualization servers were partially removed, which caused disruptions in the operation of the government's hot line and of the website.

Cyberattack at Ukrtelecom on March 28: what happened

Ukrtelecom saw an increase in the number of cyber attacks from the very beginning of the incursion into Ukraine. The attack that took place on March 28 was strong and complicated.

It consisted of two phases. The first phase included discovery. It was performed from the Ukrainian territory which was recently temporarily occupied by russians. For the purpose of reconnoitering, they used a compromised account of the company's employee. The cyber attack was quickly detected and counteracted by Ukrtelecom's SOC team.

The second phase involved a cyber attack on March 28, during which the hackers tried to disable Ukrtelecom's equipment and servers and to gain control over its network and equipment.

The second phase of the cyber attack was detected within 15 minutes from its start. Ukrtelecom's IT specialists took immediate measures to counteract the cyber attack. In order to protect the critical information infrastructure and ensure uninterrupted provision of services to the military and the country's critical infrastructure, Ukrtelecom temporarily limited the access to its services for private users and the business.

They started to restore the Internet access for their consumers in the evening, March 28. Next day, Ukrtelecom's services became almost fully available to all of the consumers.

Ukrtelecom notified the SSSCIP of the cyber attack and coordinated with the SSSCIP experts during its counteraction. Both national and international partners of the provider were engaged in the elimination of consequences of the attack, including Cisco, Microsoft and ISSP.

According to the current findings of the investigation, user data has not been affected by the attack and has not been compromised.

Ukrenergo in war: the number of attacks tripled to stop the connection to the European energy system

According to CERT-UA, Ukraine's energy sector has been one of the most popular targets of russian military hackers during the war. Despite that, electricity supply is stable in Ukraine.

Chairman of the Board of NEC Ukrenergo Volodymyr Kudrytskyi told Interfax how the defense is organized at Ukrenergo and how it works during the war.

Ukrenergo is a heart of the transmission system in Ukraine. The company unites electricity generators, interacts with the energy systems of neighbouring countries and ensures electricity export and import.

Since the beginning of the incursion, the number of attacks on the company's perimeter has tripled as compared to the pre-war period. February and March saw the highest number of attacks, and the peak was observed before the connection to ENTSO-E and before the incursion.

All cyber attacks proved to be unsuccessful. However, they still continue.

russian hackers do not even try to hide. During some phases, they scanned the system using russian IP addresses. The main goal of hackers was to prevent Ukraine's energy system from connection to ENTSO-E. Ukraine cannot and is not going to let it happen.

The fact that, before and during the incursion, Ukrenergo did not suffer from cyber attacks can be attributed to the past two years of work during which the company built a strong cyber defense system. The cyber defense system protects both the management network related to the Internet and the service network, being the heart of the energy system. The security level of the latter is multiple times higher.

"All of our systems comply with the highest global standards, so are the performance of our team, which is second only to the SSSCIP team in the cyber defense competition, and investment in the equipment, in particular in the data centre. We were able to defend ourselves because we prepared in a right way", told Volodymyr Kudrytskyi.

Heavy cyberattack on Ukraine's energy sector

On 12th of April CERT-UA reported a Sandworm (UAC-0082) cyberattack on Ukraine's energy infrastructure suing Industroyer2 and CaddyWiper malware.

The attackers attempted to take down several infrastructure components of their target, namely:

- *Electrical substations — using Industroyer2 malware. Every executable file contained a statically configured set of unique parameters for one of the target substations.*

- *Windows-operated computing systems (user computers, servers, APCS workstations) — using CaddyWiper destructive data wiper.*
- *Linux-operated server equipment — using malicious destructor scripts.*
- *Active network equipment.*

The target organization suffered two attack waves. The initial compromise occurred not later than in February 2022. And on Friday evening, April 8, 2022, the attackers planned shutting down the electrical substations and taking down the enterprise's infrastructure. However, the malicious intent has been prevented.

To determine whether there is a similar threat for other Ukrainian organizations, the information, including malicious software samples, has been shared with the international partners and Ukraine's energy sector enterprises.

The Computer Emergency Response Team of Ukraine CERT-UA expresses its special gratitude to Microsoft and ESET.

Cyber attacks as one more way of spreading false information and propaganda

In order to disseminate disinformation, hackers compromise the media, the websites of local authorities and those of the Internet providers and publish false information thereon. However, Ukrainians do not trust in the russian government that has shown its true face.

According to Meta, belorussian military hackers from the Ghostwriter (UNC1151) group also attack the Facebook and Instagram accounts of Ukrainian military men. They compromise the accounts using phishing links which they send to the e-mail address and urge to lay down the arms on behalf of those users. Meta blocks those posts.

Phishing attacks against civilians

Almost 200 children were killed by russian invaders, over 100 healthcare facilities and ambulances were affected. There is a humanitarian catastrophe in some cities. russia's attacks against civilians are becoming more and more aggressive.

According to multiple witness accounts, in the occupied cities, they check the smartphone content and can detain innocent people because of the content in their gadgets.

In the same way, russia uses its weapons against civilians in the cyberspace. Before the beginning of the military action, the activities of the russian hackers working for the military or under their management were targeted mainly at public authorities and the critical information infrastructure. However, we currently detect sending phishing e-mails to civilians. russians are probably trying to obtain at least any information to be used against the army, the government, commercial and volunteer organizations.

On March 18, CERT-UA warned about malicious e-mails allegedly sent by public authorities. They were related to the payment of benefits and contained a link to the dangerous resource.

On March 30, CERT-UA published information on mass sending of e-mails containing a malicious file which activated malware that was classified as MarsStealer and could damage the computer. It collects the information about the computer, steals credentials from browsers, crypto wallet plug-ins and multi-factor authentication applications, steals files and downloads files making screen snapshots.

On March 5, CERT-UA informed about the fact of sending e-mails to Ukrainians, which contained a malicious link to the alleged Telegram website allowing the hackers to gain an unauthorized access to the accounts, with the possibility to capture a one-time code from an SMS. Ukrainian cybersecurity experts blocked the hosting from which the attacks were made, but trespassers tend to relocate to the RF hostings.

Hackers attacking public authorities in Ukraine also attack the EU Member States

It was repeatedly confirmed by the Computer Emergency Response Team of Ukraine (CERT-UA), acting under the SSSCIP.

For instance, e-mails containing links to malicious RAR archives with the names “Assistance.rar”, “Necessary_military_assistance.rar” were sent to the e-mail address of one of the Latvian public authorities. Each of those archives contained malicious shortcut files with English names relating to the humanitarian aid for our country.

The attack is attributed to the UAC-0010 (Armageddon) group, the same group which sent malicious e-mails to Ukrainian public authorities.

russian hackers use the data obtained through phishing e-mails to make further attacks on the critical information infrastructure

Phishing attacks aimed at stealing user account details is a part of the cyberwar. Stolen user account details can be used by hackers to make further attacks for the purpose of stealing public information or interfering with the system operation.

For instance, during the last attack on the Ministry of Foreign Affairs, hackers used the credentials which were allegedly stolen during the previous phishing attack.

CONCLUSIONS AND RECOMMENDATIONS

In view of the experience gained by Ukraine in fighting the russian war machine, the SSSCIP is willing to share its recommendations with the states that plan to strengthen their defense against the RF pernicious influence.

Invest in the simplest defenses

In the past few years, the most popular cyber attack techniques of russian military hackers included:

- phishing e-mails through which they can obtain credentials for the access to information systems;
- disseminating malware aimed at stealing data or destroying the infrastructure;
- using known vulnerabilities.

It is possible to prevent those cyber attacks and minimize their risks through the compliance with the cyber hygiene rules, a responsible attitude to the password use policy and timely software updates.

Therefore, the highest level of defense is achieved through the investment in the simplest cyber defenses.

Identify your cyber defense weaknesses and strengthen them

Hackers are continuously conducting reconnaissance in Ukraine. If they target you, they will find your weaknesses and attack using them.

There are no 100%-protected systems. However, the easier it is to hack your system, the higher the hackers' motivation is likely to be. The aforementioned compliance with the cyber hygiene rules boosts the cyber resilience of institutions. Therefore, it makes life harder for hackers.

Each Ukrainian is at risk

During the first month of war, the Ukrainian critical information infrastructure managed to avoid damage. It proves both that we have become stronger and that the hackers' capacity could have been overestimated. It seems that, both in the cyberwar and in the military action on the ground and in the air, russia uses a lot of low-skilled force that is not able to inflict severe damage.

However, we treat the threat with the utmost seriousness and expect probable escalation on the cyber front.

Each institution has to realize that it is at risk as russian hackers attack even ordinary people to steal their data. It poses a threat for both ordinary users and employees of certain institutions.

The military and statesmen are at particular risk. Cyber hygiene must become no. 1 habit for those people.

Physical security of the critical information infrastructure users is as important as the protection of their accounts

As one of the recent cyber attacks showed, russian hackers can use the credentials of users staying in the temporarily occupied territories. Companies, especially those included in the critical infrastructure, have to realize that physical security of their employees is, inter alia, an investment in their cyber defense.

In addition, we'd like to remind that the SSSCIP State Cybersecurity Centre and the Computer Emergency Response Team of Ukraine (CERT-UA), jointly with the teams of the best Ukrainian cybersecurity companies and the world's major producers of solutions provide comprehensive assistance in establishing multiple-tiered cyber defense systems of the IT infrastructure for institutions and organizations, irrespective of ownership.

It is free of charge.

All of us must stay resilient to external challenges, continue providing services to people and ensure the functioning of the business and the economy in whole.

Please, send your requests to our official e-mail address cert@cert.gov.ua, and we will provide you with targeted assistance in defense against cyber attacks, security monitoring, migration to cloud environments, deployment of state-of-the-art systems to defend your workstations and servers against cyber attacks, etc.

The analytical document is prepared by the experts and analysts from the State Service of Special Communication and Information Protection of Ukraine.

If you want to receive regular updates, please subscribe to our analytical mailing at https://forms.gle/qWJWGqAUd5habwiz5

Follow the State Service of Special Communication and Information Protection of Ukraine:

www.cip.gov.ua

www.facebook.com/dsszzi

www.Instagram.com/dsszzi

www.t.me/dsszzi_official

www.twitter.com/dsszzi

www.linkedin.com/company/dsszzi

Prepared with the support of the European Union