




**State Service of Special
Communications and Information
Protection of Ukraine**



PULSE OF CYBER DEFENSE

Cyber Digest
April 2023



Malicious hackers, merged with russian special services, keep learning, changing their tactics and choosing some of the most dangerous types of attacks against Ukraine and its allies.

The SSSCIP experts have studied several tendencies, understanding which will help public institutions, businesses and private individuals protect themselves.

Malicious hackers, merged with russian special services, keep learning, changing their tactics and choosing some of the most dangerous types of attacks against Ukraine and its allies. The SSSCIP experts have studied several tendencies, understanding which will help public institutions, businesses and private individuals protect themselves.

We observe an increase in cyberattacks on commercial companies, especially the ones handling considerable amounts of citizens' personal data. The purpose of this campaign is still unclear.

Besides, the risks from using unlicensed software, published by

russian special services at popular torrent trackers, have increased. The SSSCIP specialists still observe such software being used across Ukrainian public and private sectors despite all the warnings.

CERT-UA has also [recorded](#) multiple cases of mass spyware emails to public authorities disguised as Windows security updates, ostensibly sent by the affected agencies' system administrators.

Phishing remains russian hackers' favorite tactics. Their phishing campaigns are well-planned and are massive in their nature. This type of attacks puts at risk not only employees of targeted organizations (public officials, employees of critical infrastructure-related companies), but each citizen as well. Through phishing, russian special agencies are trying to collect any possible information on Ukrainians, focusing on their personal data.

We also witnessed a new comprehensive tactics employed by russian criminals in April. It comes down to a simultaneous hacking of a ministry's network and an independent media website, followed by a fake news posted on both official website and

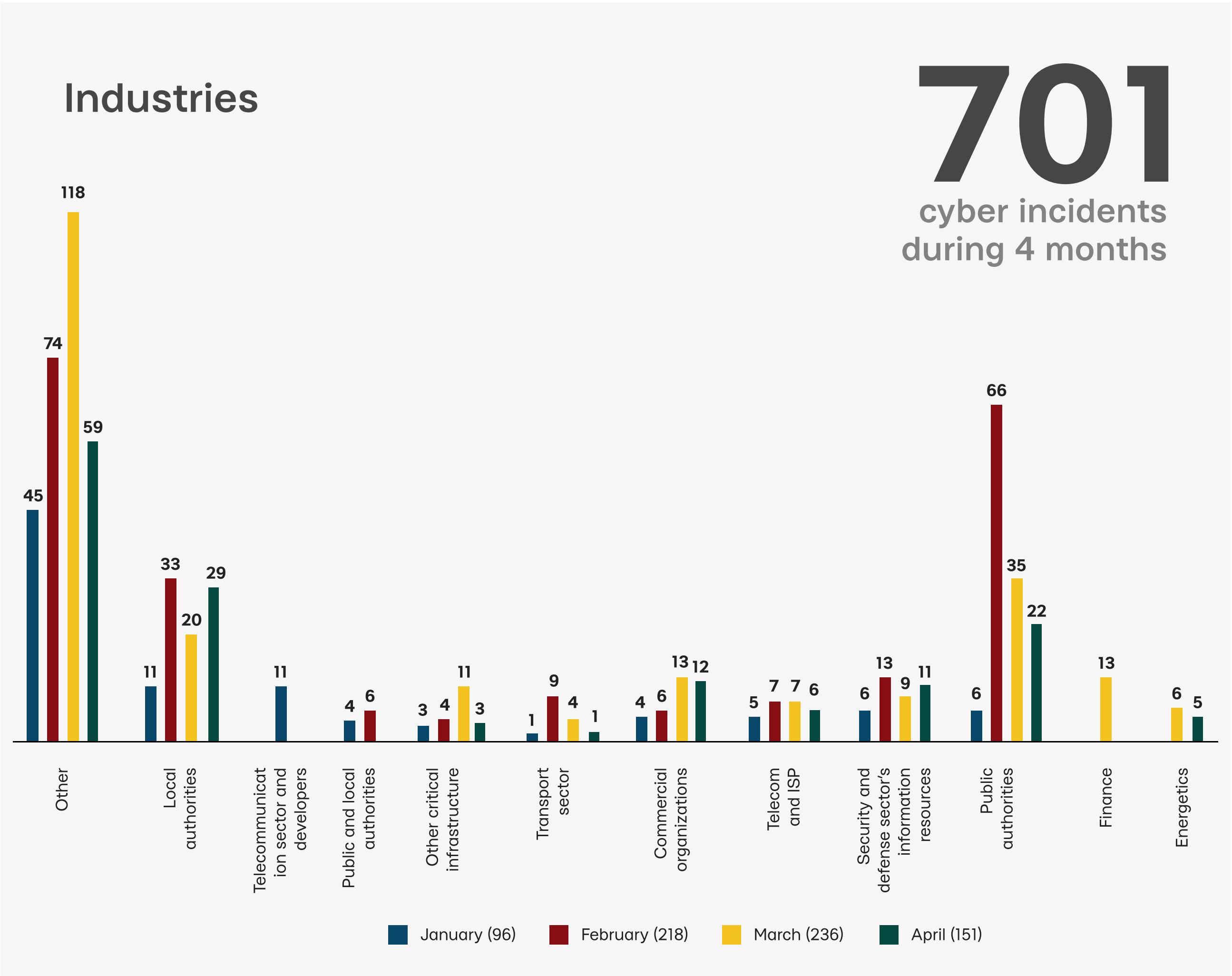


online media; a clear attempt to induce a wave of publications and reposts in order to compromise the credibility of the Government and independent mass media.

Following the rules of cyber hygiene is a prerequisite of protection, but it is hardly enough.

A comprehensive analysis of how companies and institutions protect their systems and networks as well as training of their employees is essential for them to be prepared to possible attacks.

The SSSCIP conducts such trainings and accepts applications from those organizations that require their cyber protection to be enhanced.

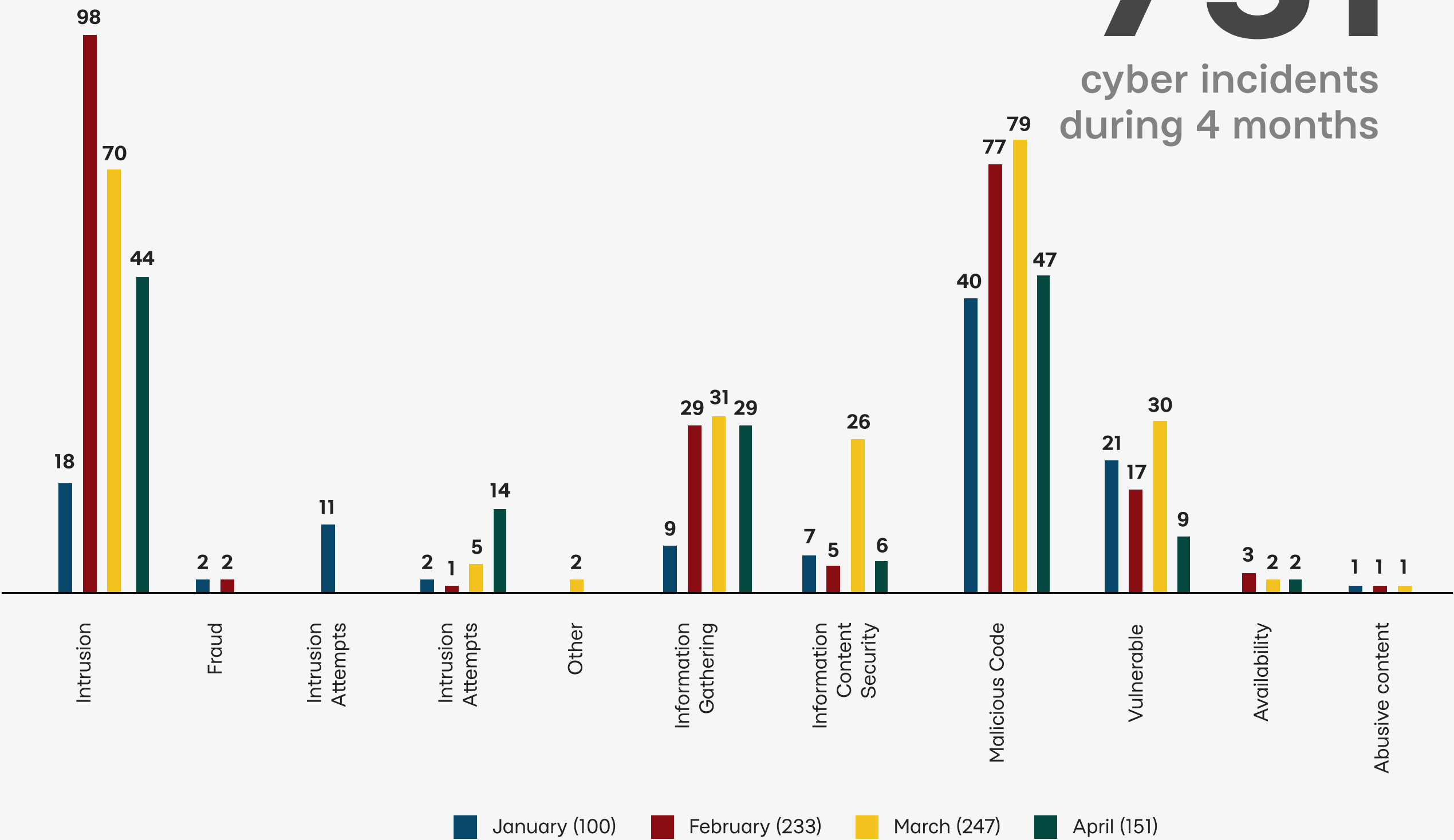




Categories

731

cyber incidents
during 4 months



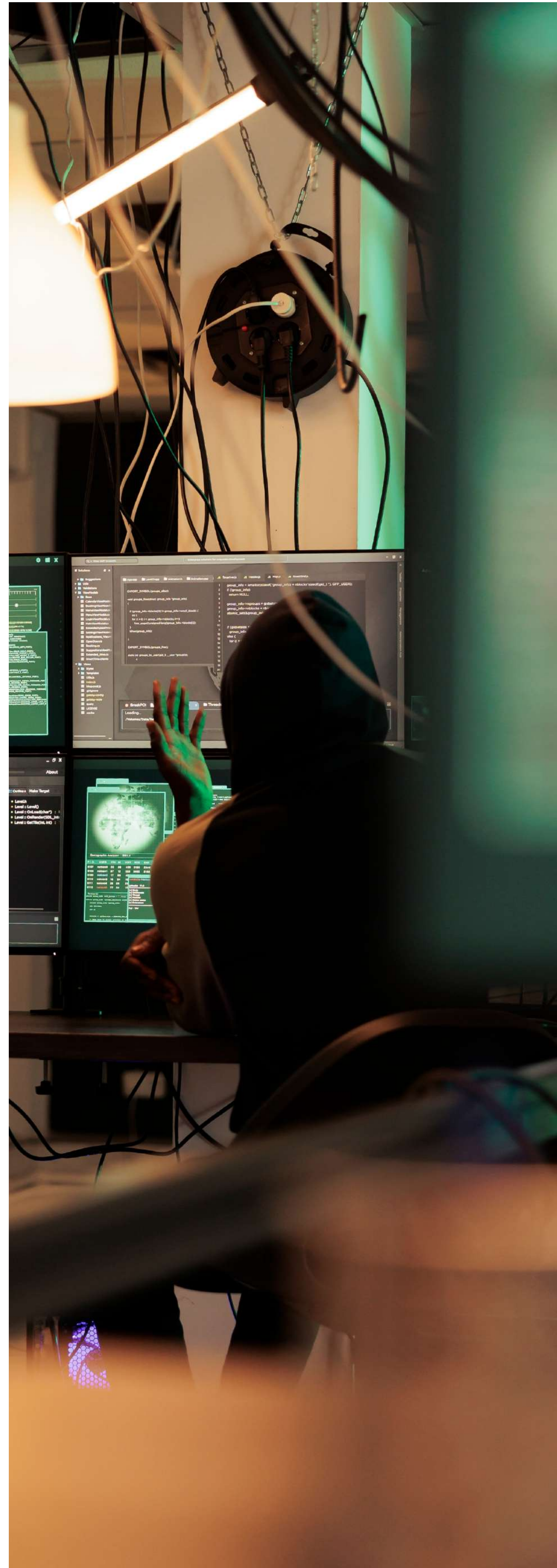


Danger posed by Software from Torrents: a distinct connection between using such software and russian hackers

Unlicensed/pirated software has become an increasing threat, as russian hackers are constantly trying new ways to gain unauthorized access to Ukrainian organizations' and citizens' information systems. Such software is being distributed even through Ukraine-hosted torrents.

In late 2022, the Mandiant reported public agencies having been infected with trojanized Windows 10 installation files downloaded from a popular Ukrainian torrent tracker Toloka and the russian Rutracker. This activity was associated with the UNC4166/ Invisimole group (russia's foreign intelligence service).

It is not a sporadic case. It is now a growing trend for commercial and public organizations.





How russian pirated software works

Once a piece of pirated software is installed, the host gets infected with malware and a primary compromise of information systems occurs. Then hackers install additional software for remote access and proceed with lateral advancement through the organization's systems.

It means that even a single 'cracked' app, be it an office software package or a solitaire game, installed on a PC, may reveal the organization's information to russian foreign intelligence service or other special services.

In most instances, hackers use legitimate remote management or vulnerability testing software

(such as DWAgent, Stowaway) to gain extra access. This makes tracking such access with cybersecurity tools more difficult.

Such a vector of primary compromise has been increasingly encountered. Apart from Microsoft Office software, CERT-UA is also aware of device infection cases resulting from installing operating systems and other applications (scanners, password recovery tools, etc.), downloaded from unofficial resources. Execution of the above actions on the system administrator's PC and/or under a privileged user account contributes to the implementation of the malicious plan.

CERT-UA has studied multiple cyber incidents that involved hacking information systems through the installation of pirated Windows OS copies. In such cases, a supposedly clean host already has built-in backdoors for criminals to access it remotely. Besides, protection services, update features and access to Microsoft resources are disabled in



such OS, making it easier for hackers to carry out further unauthorized activities while staying unnoticed by the PC user.

We can conclude that the use of this cyberattack vector will only keep increasing. More and more new users will appear at Ukrainian torrent trackers to disseminate infected pirated software.

Hackers' motives may vary depending

on the type of affected organizations: from cyberspying and destructive actions to financial operations involving stealing credit card data followed by theft of money and infecting devices with ransomware.

This is why we re-emphasize that using unlicensed software is unacceptable, especially in corporate environment.

[Read more about some cases of such cyberattacks.](#)

Double Hacking for PsyOps

An unusual operation was performed by Russian hackers in April, involving a double cyberattack and an information impact operation. It was aimed at achieving people's complete distrust to any information in media and public resources.

This operation consisted of a cyberattack on one of Ukrainian ministries followed by an attack on one of Ukrainian media outlets.

The hackers broke into the resource and published the news on the ministry getting hacked, along with some criticism of the Computer Emergency Response Team of Ukraine (CERT-UA).

This operation is an example of Russia not making a distinction between cyberattacks and information attacks, using both of them to reinforce each other, which puts the targeted countries in even greater danger.





A New Security Threat: insurance companies being hunted by russian 'hacktivists' to steal Ukrainians' personal data.

In April, russian so-called 'hacktivists' launched a number of cyberattacks aimed at retrieving Ukrainians' personal data. They managed to access four of top 10 Ukrainian insurance companies. Personal data of several millions Ukrainians were stolen and published as a result. Depending on the source, those included contacts, addresses, employment, travel, vehicle data, personal data, etc. of their clients.

All those are sensitive information that has become available to russian special services due to the leak and can be used to plan further operations. Such as information and psychological influence campaigns or campaigns against individuals by threatening them with revealing the data they don't want to see published, or physical threats, especially to those living in russia-controlled areas.

Services provided by insurance companies in Ukraine are used mostly by people with average or above-average incomes, working for international or major domestic companies, probably system-shaping and essential for the country's economy. This is why such leaks jeopardize Ukraine's national security. Besides, the stolen data are probably

going to be sold in the Darknet, putting those concerned at a greater risk.

The SSSCIP reminds that company owners are the ones responsible for security of their clients' data.

Regardless of their ownership, the companies having access to sensitive information should immediately report any cyber incidents or cyberattacks to CERT-UA, their partners and other relevant organizations within the sector.

Other companies are strongly recommended to do the same, because timely reporting to CERT-UA and partners can help prevent an attack from spreading, facilitate its research and neutralize its consequences.



Russian tech companies are sanctioned for 10 years

The President of Ukraine Volodymyr Zelenskyy imposed sanctions against russian technology companies. Over 250 russian companies were [sanctioned](#), including Yandex, 1C, VK, Positive Technologies, etc. Using their products is a threat to Ukraine's national security.

Still, despite the danger posed by russian software, despite all the sanctions, some of which had already been in force, some Ukrainian organizations keep using software made in the aggressor country. Some of them even keep purchasing it.

The SSSCIP would like to remind that using russian software in Ukraine not only finances the aggressor's economy, but also enables russian special services to access the users' data.

To verify the software origin, organizations can check it using the [@checker_products_bot](#), created by the State Cyber Protection Center SSSCIP. The chat bot takes relevant data from russian service databases.

The website [Replace russian software with Ukrainian solutions](#) offers information on Ukrainian equivalents to russian software products.

Central executive authorities (except those for whom it is mandatory) may apply for procurements of secure software to the Centralized Procurement Organization [SoE USS CPO](#) that verifies all the counterparts and origin of the software products.



Ukraine is getting ready to legislate application of the NIST standards and functioning of the Prohibited Software Registry.

Ukraine is preparing to adopt a more systematic solution of the hazardous software issue. The draft law No. 8087 “On amending certain Laws of Ukraine as regards urgent actions to enhance cyber protection capacities of public information resources and critical information infrastructure” that envisages creation of the Prohibited Software Registry.

This draft law also allows to regulate the development of information protection systems, based on the NIST Cybersecurity Framework Standards and risk-oriented approach. This will



enable Ukrainian organizations to adopt advanced approaches to cyber defense.

This draft law has been highly evaluated by international experts, and the SSSCIP emphasizes the importance of its immediate enactment.



Cybersecurity Trainings:

Please refer to the SSSCIP for available programs

To help Ukrainian organizations protect themselves better, the SSSCIP arranges a series of educational programs for various specialists, ranging from students to Category A managers:

- educational programs for managers of public institutions (Category A) and information security specialists in the public sector (Categories B, C), supported by the EU-funded Project “Support to comprehensive public administration reform in Ukraine” (EU4PAR), the National Agency of Ukraine for Civil Service (NAUCS) and the High School of Public Governance;
- wartime cybersecurity workshops that involve CERT-UA specialists;
- Critical Infrastructure Resilience Exercises (CIREX), designed based on the guidelines by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and supported by the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity;
- the National Student Competition in Cybersecurity in the Capture-the-Flag format (UA30CTF), supported by the EU4DigitalUA Project;
- and others.

Ukrainian public agencies and critical infrastructure facilities can apply to the SSSCIP for detailed information on the scheduled future trainings, or share their own training needs that would help them enhance their cyber protection by email to: edu@cip.gov.ua.



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.

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:

<http://eepurl.com/hZS6Xj>



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.

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.youtube.com/channel/UCIZRZt90fMKxEKeSgY4LB9Q

www.t.me/dsszzi_official

www.twitter.com/SSSCIP

www.linkedin.com/company/dsszzi

Prepared with the support of the European Union and the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity



This publication is made possible by the support of the American people through the United States Agency for International Development (USAID) and the support of the European Union. The authors' views expressed in this publication do not necessarily reflect the views of USAID, the U.S. Government or the EU.



State Service of Special Communications and Information Protection of Ukraine