10 years CERT-EU

Cyber brief (May 2022)

June 1, 2022 - Version: 1.1

TLP:WHITE

Europe and the European Union

Cyber policy

The EU formally accused Russia of coordinating the cyber attack which targeted Viasat's KA-SAT satellite network on February 24.

Attribution

EU lawmakers reached a provisional agreement on a new network and information security directive dubbed NIS2 that seeks to strengthen cybersecurity resilience. The framework establishes new incident reporting rules, stricter enforcement requirements, and aims to improve information sharing at the national and EU levels.

Regulation

Cyberespionage

The Russian Turla threat actor has been running a phishing and reconnaissance campaign against several European targets (Baltic Defence College, Austrian Economic Chamber, and a NATO eLearning platform).

Defence, Russian threat actor

The Russian Gamaredon threat actor targeted Eastern European governmental entities using foreign military help lures.

Government, Russian threat actor

A years-long phishing campaign has targeted German companies in the automotive industry, attempting to infect their systems with password-stealing malware. The targets include both car manufacturers and car dealerships in Germany.

Automotive

Cybercrime

ASST Fatebenefratelli Sacco — an Italian public healthcare entity in Milan that manages regional hospitals and healthcare facilities — was reportedly breached with ransomware.

Ransomware, Healthcare

The Vivalia Hospital in Belgium was targeted in a LockBit ransomware attack. According to the Belgian media, it is the second attack against a healthcare organisation in Belgium since the beginning of 2022.

Ransomware, Healthcare

Threat actors named Bulgaria's State Agency for Refugees under the Council of Ministers (SRA) as a victim on LockBit dedicated leak site (DLS). The SRA is responsible for granting asylum and humanitarian status to foreigners in the Republic of Bulgaria.	*Ransomware*, *Government*
The BlackCat ransomware gang, also known as ALPHV, hit the Austrian federal state Carinthia and demanded a $5 million to unlock the encrypted computer systems. The breach temporarily halted the issuance of passports and traffic fines and disrupted the state administration's telephone system, email service, and website.	*Ransomware*, *Public administration*

Hacktivism

The Romanian Ministry of Internal Affairs confirmed that a Romanian national had been arrested in the UK on May 2 for assisting the pro-Russia hacktivist group Killnet during a recent DDoS campaign targeting Romania.	*DDoS*, *Arrest*
In May, Killnet claimed a series of DDoS attacks against a number of entities (i.e. the ministry of defence, an email service provider, a cloud service provider, a mail service provider, an airport operator, a national parliament) in several European countries, including Italy, Latvia, Germany, Estonia, Poland, and Romania.	*DDoS*, *Defence*, *Email services*, *Cloud services*, *Mail services*, *Airport*, *Parliament*
A new pro-Russia hacktivist group called Legion Cyber Spetsnaz — a self-proclaimed "project of Killnet" — claimed DDoS attacks against the websites of various German companies.	*DDoS*, *Companies*

Information operations

According to Google and the former head of the UK Secret Intelligence Service, the Russian threat actor Callisto carried out a successful hack-and-leak operation via a website titled "Very English Coop d'Etat", targeting several leading proponents of Britain's exit from the EU.	*Russian threat actor*, *Hack and leak*
According to cyber security firm Mandiant, an information operation promoted the narrative that a Polish criminal ring was harvesting organs from Ukrainian refugees and illegally selling them via social media.	*Fake narrative*, *Ukraine*
Still according to Mandiant, the Russian threat actor APT28 has been using a Telegram channel to disseminate content to weaken Ukrainians' confidence in their government and undermine support for Ukraine from its Western partners.	*Russian threat actor*, *Social media*, *Ukraine*

Disruption

The Russian threat actor Sandworm is improving its tools used to load disruptive (wiper) payloads by making them more stealthy and capable of being activated at a specified time.	*Ukraine*, *Wiper*

New disruption attacks were observed targeting Ukrainian internet and telecom services providers.	*Ukraine*

World

Cyber policy

The US President J. Biden signed a national security memorandum (NSM) asking government agencies to implement a set of measures that would mitigate risks posed by quantum computers to US national cyber security. The NSM outlines the risks of cryptanalytically relevant quantum computers (CRQC), such as their likely ability to break current public-key cryptography.	*US*, *Cryptography*, *Quantum computers*
The US Department of Justice (DOJ) announced a revision of its policy on how prosecutors should charge violations of the Computer Fraud and Abuse Act (CFAA), exempting security research conducted in "good faith" from prosecution.	*US*, *Regulation*
The Government of Canada announced its intention to ban the use of Huawei and ZTE telecommunications equipment and services across the country's 5G and 4G networks.	*Canada*, *Foreign technology ban*
The Russian President V. Putin signed a decree instructing heads of departments in administrations and regions, state funds, state corporations, strategic and systemic enterprises "to authorise deputy head of the body to ensure information security, including on revealing, preventing and liquidating the consequences of computer attacks and responding to computer incidents."	*Russia*, *Regulation*

Cyberespionage

Researchers at Sentinel Labs have identified a new China-aligned cluster of malicious cyber activity tracked as Moshen Dragon, targeting telecommunication service providers in Central Asia.	*Chinese threat actor*
According to the cyber security firm Cybereason, the China-linked Winnti threat actor has been running a sophisticated and elusive cyberespionage operation, dubbed CuckooBees, that has remained undetected since at least 2019. The goal of the campaign is stealing sensitive proprietary information from technology and manufacturing companies mainly in East Asia, Western Europe, and North America.	*Chinese threat actor*
Researchers reported about a highly-evasive Chinese surveillance tool, dubbed BPFDoor, present on "thousands" of Linux systems for at least five years. The threat actor targeted the telecommunications, government, education and logistic sectors accross the Middle, Asia, and Europe.	*Chinese threat actor*
A previously unknown Chinese threat actor known as 'Space Pirates' is targeting enterprises in the aerospace industry with phishing emails. Victims include government agencies and enterprises involved in IT services, aerospace, and electric power industries located in Russia, Georgia, and Mongolia.	*Chinese threat actor*

A newly discovered malware campaign, dubbed SilentMarten, stores malicious shellcode in Windows event logs, using this technique to conceal malware from the filesystem. The campaign also uses custom tools alongside commercially available penetration testing suites, such as Cobalt Strike and NetSPI (formerly known as SilentBreak).	*Fileless malware*
Google's Threat Analysis Group (TAG) released a report on zero-day vulnerabilities in the Android OS and the Chrome browser, which are being exploited by the private sector offensive actor (PSOA) Cytrox for surveillance on mobile devices. The bundling of the exploits by Cytrox is sold to government-backed actors.	*PSOA*

Cybercrime

After a year-long investigation that involved Interpol and several cybersecurity companies, the Nigeria Police Force has arrested an individual believed to be in the top ranks of a prominent business email compromise (BEC) group known as SilverTerrier or TMT.	*Business email compromise, Arrest*
Popular libraries used by Python and PHP developers were compromised in supply chain attacks. The goal of the attackers was to steal developers' secrets such as Amazon AWS keys and credentials.	*Supply chain attack, IT*
The cloud platform service Heroku confirmed unauthorised access to an internal customer database resulting from the theft of GitHub-integration OAuth tokens. Upon investigation, Heroku learned the actor also exfiltrated hashed and salted passwords associated with customer accounts. Heroku forced a password reset for all customers.	*Cloud services*
Compromised YouTube accounts started to post deepfake videos featuring interviews with multiple well-known business personalities — including SpaceX CEO Elon Musk — promoting a fraudulent cryptocurrency platform called BitVex.	*Deepfake, Scam*
Several ransomware strains have been linked to APT38, a North Korean-sponsored hacking group known for targeting and stealing funds from financial institutions worldwide.	*Ransomware, North Korean threat actor*
The REvil ransomware operation has returned amidst rising tensions between Russia and the US, with new infrastructure and a modified encryptor allowing for more targeted attacks. The operation had been shut down in October 2021 by law enforcement authorities but has now returned.	*Ransomware*
The Conti ransomware gang claims to have hacked the Peru Ministry of Economy and Finance – Dirección General de Inteligencia and stolen 9.41 GB.	*Ransomware, Finance, Intelligence services*
The Costa Rican President Rodrigo Chaves has declared a national emergency following cyber attacks from the Conti ransomware group on multiple government bodies.	*Ransomware, Government*
The US Department of State offered up to $15 million for information that helps identify and locate leadership and co-conspirators of the Conti ransomware gang.	*Ransomware*

A threat actor named Stormous Group continues to claim victims - inluding the Coca-Cola Company - and threaten to leak their data on the Stormous Group DLS. The actor — best known for hacktivist operations — is now likely also involved in cybercrime. The group is also know for its large number of unverified hacking claims.	*Ransomware*
The Conti ransomware operation decided to shut down and split into smaller units in order to gain mobility and better evasion of law enforcement.	*Ransomware*
According to researchers at NCC Group, the Clop ransomware is now back after effectively shutting down their entire operation between November 2021 and February 2022. The ransomware group added 21 new victims to their data leak site in April.	*Ransomware*
GitHub disclosed that an attacker stole the login details of roughly 100,000 npm package manager accounts during a mid-April security breach, commited with the help of stolen OAuth app tokens issued to Heroku and Travis-CI. The threat actor successfully breached and exfiltrated data from private repositories belonging to dozens of organisations.	*Breach*, *IT*

Information operations

According to the cyber intelligence firm Nisos, a subcontractor to the FSB, the Federal Security Service of the Russian Federation has been developing a botnet code named Fronton which aimed to creating and deploying trending social media events en masse to support coordinated inauthentic behaviour on a great scale.	*Russian threat actor*, *Social media botnet*

Hacktivism

Anonymous affiliates began calling for a revival of #OperationJane in response to the leaked draft of a US Supreme Court opinion that would overturn Roe vs. Wade — a landmark case that legalised abortion nationally in 1973. Anonymous affiliates first launched #OperationJane in early September 2021 to protest the Heartbeat Act banning abortion in the US state of Texas following the detection of embryonic “cardiac activity”.	*US*, *Government*
The pro-Russia hacktivist group called Legion, an affiliate of Killnet (see above in chapter “Europe”), claimed DDoS attacks against at least several US entities: a business-to-business database provider, the CIA, a defence and aerospace corporation, and a defence contractor whose weapons systems had been sent to Ukraine.	*US*, *Defence*, *Aerospace*, *Intelligence*

Vulnerability exploitation

Several cyber security agencies, including CERT-EU, warned of the active exploitation of critical F5 BIG-IP network security vulnerability (CVE-2022-1388). See also CERT-EU SA 2022-032.	*F5 BIG-IP*
The Department of Homeland Security's cybersecurity unit ordered Federal Civilian Executive Branch (FCEB) agencies to urgently update or remove VMware products from their networks due to an increased risk of attacks. See also CERT-EU SA 2022-036.	*VMware*
Splunk released a security advisory for a critical path traversal vulnerability (CVE-2022-26889) in a search parameter that can potentially allow external content injection. An attacker can cause the application to load data from incorrect endpoint URLs, leading to outcomes such as running arbitrary SPL queries. See CERT-EU SA 2022-037.	*Splunk*
Microsoft warned of brute-forcing attacks targeting internet-exposed and poorly secured Microsoft SQL Server (MSSQL) database servers using weak passwords. See also CERT-EU TA 22-060.	*SQL Servers*
Independant security researchers have discovered a new Microsoft Office zero-day vulnerability, dubbed Follina and tracked as CVE-2022-30190, that is being used in attacks to execute malicious PowerShell commands via Microsoft Diagnostic Tool (MSDT) simply by opening a Word document. See CERT-EU SA 2022-039.	*Microsoft Office*