computer emergency response team | CERT-EU for the EU institutions, bodies and agencies

Threat Landscape Report

3rd Quarter 2018

V1.0 – 11/10/2018

EXECUTIVE VERSION

EXECUTIVE SUMMARY

PART I - DIRECT THREATS

- **Targeted intrusions**. No targeted intrusion attempts against EU institutions, bodies and agencies (EU-I) were observed. However, activities of at least two likely Russia-based dangerous actors – known as Turla and APT28 – have been detected in Europe. APT28 is highly likely affiliated to the Russian military intelligence (GRU), which has been publicly accused of cyber-espionage by the UK and the Netherlands. During summer 2018, both APT28 and Turla have employed new tools to maintain persistence (rootkit), and evade detection and analysis.
- **Other cyber-threats**. A limited number of ransomware infection attempts by GandGrab were observed. The banking trojan Emotet has been the most active cyber-crime threat for the fourth quarter in a row, with at least two spear-phishing campaigns that targeted specifically EU-I. Other cyber-crime activities have been dominated by the many Magento e-commerce payment skimmer occurrences and by constant illicit cryptomining attempts. Attackers attempted to exploit vulnerabilities mainly via malicious Microsoft Office and PDF documents. This quarter has seen a minor increase in DDoS attacks. Generic phishing activities employed the usual topics (inquiry, SWIFT, tax, payment, personal banking, quotation / purchase / sale order) and new subjects (telecom, remittance, real estate, diplomatic courier). Additionally, WhatsApp phishing was reported for the first time. Several spear-phishing attacks were observed having a EU-I nexus: spoofing a Member of the Parliament, distributing a weaponised official European Parliament document (on GDPR), impersonating an EU-I employee, or using compromised EU-I correspondent and trusted e-mail accounts. EU-I credentials leaks (in public sharing repositories) remain a permanent threat.

PART II - BROADER THREATS

- **Critical sectors**. In the energy sector, a gas pipeline manufacturing company and several petrochemical companies were subject to targeted intrusion attempts. The US DHS presented details on methods used by Russian actors to penetrate US and European electrical utilities in 2016 and 2017. The US Dept. of Energy is planning a hands-on test of the electrical grid's resiliency in November 2018. In the transportation sector, customers of an airline were subject to a massive leak of banking information, two port infrastructures (Europe and US) suffered disruptive security incidents, yet without significant damage, a Chinese shipping company suffered a large disruptive ransomware attack, and a US autonomous driving company was the subject of an espionage case by a Chinese national. The banking sector remains subject to large cyber-heists – executed by advanced threat actors with deep inner knowledge of banking systems, fake banking apps continue to be spotted on apps stores, and a global card skimming operation compromised seven thousand online stores equipped with Magento e-payment software. In the health sector, data breaches were observed in the US, UK and Singapore, and newly identified vulnerabilities keep affecting medical gateways and medical devices (pacemakers, insulin pumps) posing a threat to patients' health.
- **Digital infrastructures and services**. At the infrastructure level, multiple BGP hijacks and DNS redirection attacks highlight the need for more secure practices from providers. Additionally, exploitation of home routers by malicious actors to monitor network traffic shows again that the domestic segment of the digital infrastructure is increasingly leveraged. On the service level, social media have massively exposed data (Twitter direct messages), have been subject to account take over (potentially 50 million Facebook accounts) and have been aggressively used by Chinese intelligence (LinkedIn to recruit key persons). Viewing browsers as a strategic technology, China announced a "home grown" browser which turns out to be thinly veiled Google Chrome.
- **Defence and foreign affairs**. The US Department of Defence releases a new cyber strategy and names strategic adversaries (China and Russia). New US military data leaks are uncovered. The US military assesses that personal use of GPS in operational areas create increased risk to forces and missions. Russia is developing autochthonous military forensic technologies and testing resilience of military systems against foreign computer network attacks. Personal data of Israeli military personnel were collected and sold to marketing firms.
- **Geopolitical**. The US keeps reinforcing their policy and legislation: new cyber defence strategy, new cyber deterrence bill, less restriction for strike back, lawful end-to-end encryption breaking. China pushes replacement of foreign products and services with domestic ones in critical information infrastructure. New risks of China-based supply chain attacks were uncovered (e.g. Chinese telecom equipment and hardware authentication security tokens). Russia reinforces capabilities to filter and block internet content. Russian military intelligence attempted to procure exploits in the underground. Iran faces cyber domestic contestation and reinforces political surveillance operations and messaging / internet content control. North Korea plans to host an international conference on cryptocurrencies and blockchain technologies. Likely North-Korean actors keep targeting the cryptocurrency industry and banks for money gathering purposes. North Korea states that the hacker charged by the US Department of Justice as an alleged member of the Lazarus Group has nothing to do with North Korea.
- **Cyber conflicts.** Several countries engage in significant information operations (US against Iran, Iran against US and Israel, Russia against the US and possibly Italy), using news websites (sometimes inauthentic) and social media. Likely Russian entities attempted destructive operations (chemical plant in Ukraine) and tried to penetrate into German public broadcasting services, possibly for disruptive purposes.
- **Espionage.** Likely Chinese groups keep running large-scale targeted intrusions campaigns for economic and political espionage purposes. The UK and Netherlands publicly accused Russian military intelligence (GRU) of planning a cyber-

intrusion against the Organisation for the Prohibition of Chemical Weapons (OPCW). The surveillance software made by the Israeli firm NSO group has been detected in 45 countries (including in Europe). A Chinese espionage operation has allegedly targeted an Australian university.

- **Hacktivism.** Turkish nationalist hacktivists targeted a variety of websites or social media accounts hosted in countries perceived as hostile to the Turkish government. In Spain, political hacktivists launched DDoS attacks against government and political institutions as part of "Operation Catalonia". In Russia, political hacktivists targeted government officials (leaks, defacement) as part of Operation Russia.
- **Cryptocurrencies**. Cryptocurrency exchange sites remain vulnerable to targeted cyber-criminal attacks (in one instance an official EU document related to GDPR was weaponised and used as a lure to infect victims) while various instances of malware target users' cryptocurrency wallets.
- **Internet of Things (IoT)**. The discovery of a new large IoT botnet (Torii) and the proliferation of Mirai variants demonstrate ongoing threat actor interest. Researchers demonstrated how attack to water management IoT devices could have strong impact on water controlling infrastructure. California has passed legislature to regulate IoT-s.
- **Data protection**. Data breaches affected many sectors: social networks (Facebook: 50 million accounts impacted), airline companies (British Airways: 380,000 payment data), retail, IT, defence, hotels, telecoms, web hosting, health, industry, and government. The main causes of breaches are flaws in social media apps, vulnerable third-party e-payment software, misconfigured cloud servers and, in fewer cases, hacking.

PART III – TECHNICAL TRENDS

- **Exploits and vulnerabilities**. New serious vulnerabilities affect all IT sectors: computers' operating systems, CPU and Chips, network equipment, servers, virtualisation & cloud, application, platforms, cryptocurrency, browsers, mobile, connected and storage devices. Potential consequences include total system compromise, access to sensitive information, privilege escalation (to the highest level), denial of service and remote code execution.

10 SELECTED ATTACKS

#	Attack	Type
1	APT28 (aka Fancy Bear, Sofacy) Russia-based threat actor targeted at least three US Senators via spear-phishing attacks. In this campaign, 80+ malicious domains were mimicking legitimate domains associated with US political think tanks.	Targeted attack
2	A Border Gateway Protocol (BGP) hijack affected the encrypted Telegram Messenger service in Iran. Note: a successful BGP hijack permits malicious operators to reroute network traffic and potentially exposes data to capturing and monitoring efforts.	Digital Infrastructure
3	A global economic espionage campaign was observed emanating from an IP address associated with Tsinghua University ("China's MIT").	Espionage
4	A chemical and biological laboratory in Switzerland was reportedly targeted by hackers likely linked to the Russian government.	Espionage
5	A malicious trading application, allegedly associated with a North Korean hackers, was observed targeting cryptocurrency exchange users in South Korea.	Targeted attacks
6	Suspected Iran-based actors were observed conducting influence operations using inauthentic news and social media sites (Western countries, Russia, Middle East).	Information Operation
7	Likely Russia-based threat actor executed targeted attacks against German public broadcasting services (ZDF and WDR).	Targeted attacks
8	Facebook discovered that hackers manipulated a feature to steal 50 million users' access tokens.	Social media
9	"Magecart" eCrime group infected seven thousand e-commerce sites using Magento payment software and stole payment information (British Airways: 380.000 payment cards, Ticketmaster, etc.).	Cyber-Crime
10	US Counterintelligence reported on aggressive efforts by Chinese intelligence agencies using LinkedIn to recruit Americans with access to sensitive government or commercial information.	Social media