Threat Landscape Report

Executive

Q1 2019

TLP:GREEN

CERT-EU
Computer Emergency Response Team for The EU Institutions, Bodies and Agencies
https://cert.europa.eu

Executive Summary

Direct Threats

Targeted attacks	CERT-EU has not observed any targeted intrusion attempt affecting EU institutions, bodies or agencies (EU-I). However, several advanced persistent threat (APT) groups were active in Europe, including Russia-based APT28 and Turla, North Korea-based Lazarus, and Chinese APT10. There was a Twitter hacktivist campaign, calling for disruptive action against the European Parliament (EP) and political parties in protest for the vote and approval of new amendments to the Directive of Copyright in the Single Digital Market. Some hacktivist-related denial of service attacks targeted public websites of EU-I. Some targeted phishing campaigns have impersonated other EU-I, colleagues, and an EU-I IT desk.
Common cyber-threats	There were no ransomware attacks affecting EU-I. Magento (online credit-card skimmer) and Emotet have been the main banking malware targeting EU-I end users. As it has been established over several observation periods, there were again appearances of new general purpose trojans. Limited cryptojacking activities were reported. Common phishing attacks (invoice, personal banking, purchase, shipping, etc.) have continuously affected EU-I. Credential leaks, that is username/password combinations discovered in publicly available repositories, have remained for several quarters the most widespread events identified with at least 39 impacted EU-I. Finally, successful password spraying attacks have been observed.

Broader Threats – Critical Sectors

Transport	Hackers and cyber-terrorists present an ever-evolving threat to air travel, constantly testing for new vulnerabilities, including the possibility that hacked drones could be used to throw planes off course. In the maritime sector, capsizing a ship with a cyberattack is a relatively low-skill undertaking, according to security researchers. In the automotive sector, executives of several EU car manufacturers are upset that GPS systems are vulnerable to attacks and spoofing.
Energy	Energy companies can become victims of severe, opportunistic and disruptive attacks (e.g. a Norwegian aluminium and energy producer was severely affected by ransomware). Energy companies in the US, Ukraine, South Africa and the Middle East were subject to intrusions by hackers of various origins (incl. Russia, Iran and China). Vulnerable electric vehicle charging stations can become an entry point for targeting electric grids.
Health	Health care entities in several countries (Sweden, US, Canada, Singapore and others) became victims of health data breaches mostly due to inadequate security measures or misconfigurations. Attackers may try to monetise these data by offering them for sale in illegal cybercrime markets. Researchers found new medical devices vulnerable to malicious manipulations over their wireless interface.
Banking& Finance	A major cyber heist has been reported in Bank of Valetta. The attack is highly likely related with cybercrime group Empire Monkey. Magecart group 12 accelerates credit card data collection with the use of supply chain infections. Cobalt group remains active with impersonations of credible companies. Ursnif malware evolves and targets some European countries.
Digital infra	Huawei is fighting back the Five Eyes ban on their 5G infrastructure products. BGP and DNS hijacking is still a major problem with several attacks abusing these protocols and services. Russia strives to control domestic access to satellite internet services and rehearses disconnecting from the global internet. Iran is also planning a similar action. Japan plans to proactively scan its citizens' IoT devices for vulnerabilities before the Olympic Games.
Digital services	Facebook is purportedly making an effort to stay ahead of fake news and election targeting on its platforms. On the other hand, it suffered the biggest outage in its history. Russia plans to ban what it deems to be fake news and insults on online platforms. As regards e-commerce, Magecart card skimming campaigns continue to make victims worldwide.
Defence diplomacy	Military and diplomatic entities in Eastern Europe were subject to targeted intrusions attempts from actors with alleged Russian ties. China and North Korea are in all likelihood using cyber-espionage to steal military technology (resp. naval and dual use technology). The US allegedly attempted to sabotage Iran ballistic missile project while Iran claimed to hack US drone operations. US experts helped the United Arab Emirates to spy on diplomats in the Middle East.

Broader Threats - Geopolitical

US	The US charged, sentenced, arrested or disrupted assets of foreign hackers from Iran, China, North Korea and Romania. In the Middle East, the US allegedly attempted to sabotage Iran ballistic missiles project by slipping faulty parts into the supply chain and released a mobile spying tool to the UAE.
China	China deployed artificial intelligence-based security software for citizen surveillance purposes and reinforced legislation to inspect all kinds of networked units. China is suspected to benefit from its dominant position on the digital infrastructure segment (China Telecom rerouting international internet traffic – BGP hijacking – possibly for monitoring purposes, Huawei's involvement in 5G networks and undersea cable networks). Several Chinese groups are involved in cyber-espionage operations. Targets include technology firms in Europe and the US, a business conglomerate in Japan, gaming firms in Asia, naval technology with military applications in the US, Canada, and Southeast Asia.
Russia	Russia reinforces legislation on the independence and resilience of the Russian segment of the internet (RUNET). Russia presses foreign social media and internet search companies to comply with domestic internet control regulations. Russia is suspected of miscellaneous operations in Ukraine (intrusion in the energy sector, interfering into the presidential election, and spying on military) and the EU (e.g. entities dealing with international and security affairs). Facebook removed social media accounts tied to Sputnik for "coordinated inauthentic behaviour."
Iran	Iran removed US technologies from its national internet (NIN) and performed resilience exercises. Iran-based actors allegedly conducted a large DNS hijacking campaign to collect sensitive information on companies and government entities in the Middle East and Europe. Iran-based actors are purportedly conducting espionage operations against the aviation and telecom industry as well as diplomatic entities. Iran is training domestic actors for cyber and information operations while Facebook removed supposedly pro-Iranian accounts.
North Korea	North Korea's Reconnaissance General Bureau (RGB) maintains approximately 200 cyber units outside the country to generate revenue and gather intelligence for the regime. A United Nations panel of experts reported that cyberattacks on financial institutions to illegally transfer funds "have become an important tool in the evasion of sanctions and have grown in sophistication and scale since 2016". North Korea is suspected to have stolen the personal data of almost 1,000 North Korean defectors via cyber means.

Broader Threats - Motives

Cyber conflicts	Russia is suspected of miscellaneous operations in its neighbouring environment: Ukraine (intrusion in the energy sector, interfering in the presidential election, and spying on military) and in Moldova (information operations). Iran and the US are engaged in cyber-conflict involving various kinds of cyber-operations (sabotage, information operations, hijacking drones).
Espionage	Researchers found an online database that likely contains real-time surveillance data about Chinese Uyghur population. The Israeli NSO group's founder denies the company's involvement in Khashoggi's murder. China is accused of leveraging LinkedIn for spy agent recruitment. Russian lawful interception framework SORM will allow the country to get access to IoT devices and in addition to RUNET, there is plausibly a Russian-only IoT network in the making.
Hacktivism	Political hacktivism was triggered by legislative initiative (EU Copyrights Directive), opposition to a political party (Italy) or protests against a regime (in Venezuela, Algeria, Iran). In the Middle East, hacktivists continue to fight the influence of the Islamic State of Iraq and Syria (ISIS). Nationalist-hacktivist protest against violence on their compatriots (Syria, Lebanon), or entities perceived to be against national interests (Turkey). Hacktivists have employed different techniques, mostly denial of service, defacement, leaks and doxing.

Techniques, Tactics & Procedures

Malware	LockerGoga ransomware targets multiple industries, in likely targeted attacks, and causes great operational and financial damage. Scanbox reconnaissance watering holes are still in use. Russian APT groups develop new tools and redevelop old ones.
Techniques	Several malware, such as SLUB and RogueRobin use publicly available legitimate tools for command and control. Researchers describe ToRPEDO, PIERCER, and IMSI-Cracking attacks against mobile networks. Gmail services can be abused in several ways. ASUS laptops are involved in a massive supply chain attack. Heart defibrillators and smart car alarms are found to be vulnerable to cyber-attacks.
Tactics	Supply chain attacks have become a widely adopted tactic for hackers with different motives (criminals, espionage, sabotage): ASUS live update (espionage by a likely Chinese group), Magecart infecting payment website for card-skimming (cyber-criminals), the US suspected to sabotage Iran missile by slipping faulty parts into the supply chain (sabotage), US-based software provider compromised in a supply chain attack, tablets and smartphones from Polish, Chinese, and Hong Kong manufacturers were found to contain malware-infected firmware.

Selected Attacks

#	Attack	Type
1	A Chinese espionage group dubbed APT40 conducted espionage activities with the specific aim of theft of naval technology with military applications.	Global espionage China
2	A team of former US government intelligence operatives working for the United Arab Emirates hacked into the iPhones of activists, diplomats and rival foreign leaders.	Targeted attack Diplomacy
3	US reportedly attempted to sabotage Iran's ballistic missile and space rocket programs by slipping faulty parts into the supply chain.	Targeted attack US, Iran
4	A Chinese espionage group dubbed APT10 attempted to breach the networks of several European, US and Japanese firms: the Norwegian software firm Visma, HP, IBM and Keidanren conglomerate.	Global espionage China
5	APT28, a highly likely Russian threat actor, targeted an EU member state' civil-law institution dealing with international and security affairs.	Targeted attack Russia
6	Facebook removed hundreds of Russia-initiated accounts for "coordinated inauthentic behavior", including some linked to the state-owned news agency Sputnik.	Social media Russia
7	A DNS hijacking campaign dubbed "DNSpionage" targeted victims across the globe on an almost unprecedented scale, with a high degree of success.	Internet infra Iran
8	LockerGoga ransomware caused significant disruption in several countries (including a US chemical company, a Norwegian industrial firm and a French engineering company).	Malware
9	Between June and November 2018, a sophisticated supply chain attack dubbed ShadowHammer compromised the ASUS Live Update Utility and affected 500 000 computers.	Techniques Supply Chain
10	Bank of Valetta was the victim of a major cyber heist that led to fraudulent international payments totalling 13 million euros.	Bank Cyber-crime