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

Threat Landscape Report

4th Quarter 2018

V1.0 – 15/01/2019

EXECUTIVE VERSION

EXECUTIVE SUMMARY

PART I - DIRECT THREATS

- **Targeted intrusions**. Spear-phishing attacks executed by two threat actors (APT28 and APT29), almost certainly based in Russia – using Brexit as a lure document or impersonating the US State Department – were observed in a few EU institutions / bodies / agencies (EU-I). These two groups also attacked entities in several European countries.

- **Other cyber-threats**. For the first time in several years, no successful ransomware attacks were reported by EU-I in the last quarter. Two popular banking trojans (Emotet, Trickbot) repeatedly attempted to infect EU-I systems, yet unsuccessfully. The "Hall of Fame" programme of CERT-EU encouraged again white hat hackers to report vulnerabilities affecting EU-I assets. Instances of the Magento skimmer variations were detected but the number of cases has gone down. Occurrences of cryptojacking were observed affecting at least four EU-I. A serious DDoS incident affected at least three EU-I. There was a steady inflow of targeted, specific phishing emails, with appropriate subjects and content to lure EU-I personnel. Attackers also spoofed, masqueraded or typo-squatted EU-I domains or websites to lure EU-I employees or IT administrators. The majority of phishing attacks were however mass-produced, generic spam, reaching constituents only occasionally. Credential leaks remained (even if somewhat decreased) the most widespread events identified in EU-I.

PART II - BROADER THREATS

- **Critical sectors**.
  Transportation: GPS jamming – possibly Russia-initiated – disrupted airlines and maritime navigation in Nordic countries. The aerospace sector remained an attractive target for cyber-espionage activities, likely China-based. Several airports and railway operators became the victims of cyber-criminal attacks (ransomware, scam, hacking). Supply chain compromise tactics were used to attack the naval industry. Researchers found new vulnerabilities in smart cars.
  Energy: New variants of the Shamoon wiper (a malware that originally targeted Saudi oil companies in 2012 and 2016) were spotted in several countries globally – including Italy and France – and impacted a European company for the first time. The US Defence agency DARPA gained valuable experience in an electric grid recovery exercise.
  Health: The healthcare sector remained a key target of cybercriminals both for data breaches and ransomware attacks. Healthcare providers handle a wealth of medical and personal data, which attract cyber-criminals. Security vulnerabilities were uncovered in software used in medical imaging devices, cardiac devices, and ambulance services. Likely Iran and North-Korea-based threat actors attempted to steal healthcare related intellectual property.
  Banking and finance: Details of attacks against financial institutions by the highly likely North-Korean group Lazarus were made public. The attacks confirm the group's know-how on various banking IT technologies.

- **Digital infrastructures and services**. At the infrastructure level, researchers accused China Telecom of exploiting their network points of presence to hijack traffic. The US asked allies to avoid Huawei products, especially in 5G infrastructure. On the social media level, Twitter released information about accounts related to state-sponsored operations of Russia and Iran, while Facebook left millions of non-public photos exposed. Ukraine introduced social media control under the martial law, Russia enforced instant messenger user verification. As regards e-commerce, under the umbrella name "Magecart", several different groups (at least seven) are exploiting electronic payment systems to gain access to customer credit card information; they are diverse in their technical approaches and choice of victim retailer sites. US authorities accused a Chinese group dubbed APT10 of targeting cloud services providers across the globe. This group is suspected by US authorities of having connection to the Chinese Ministry of State Security.

- **Defence and foreign affairs**. Russia executed cyber-attacks (espionage, denial of service, information operations) against various military and diplomatic entities in the EU, Ukraine, NATO and the US. US revealed that several critical military systems (ballistic missile defence, weapon systems) demonstrated weaknesses, in order to accelerate remediation. The US Defence dept. started a new large bug bounty programme and began publicly sharing malware samples affecting US Defence. Likely Russian actors impersonated the US State Department in a global spear-phishing attack.

- **Geopolitical**.
  The US continues to legislate to expand the Department of Justice's powers to prosecute foreign hackers. US authorities deployed a complete judicial arsenal (charges, arrests, complaints, seizures) against foreign hackers from China, Russia and Iran.
  China reinforces domestic sweeping power to collect information "related to cybersecurity". Chinese entities ran cyber-espionage campaigns globally for diplomatic and industrial purposes. China leveraged dominant positions on the IT segment to execute supply chain attacks. China Telecom re-routed large amount of Internet traffic through China.
  Russia attempts to reinforce control over digital services. Likely Russia-sponsored state-actors executed targeted intrusion operations in Europe and abroad. Likely Russian entities ran information operations in various sectors (military, sport, social networks). Security experts linked a destructive malware (Triton) to a Russian government research institute.
  Iran based groups attempted intrusions against Kurds and globally in the telecoms and heath sectors. Iranian entities ran information operations (including disinformation) targeting dissidents, journalists and foreign countries. Iranian cybercriminals were involved in ransomware, extortion and fraudulent activities.
  A North Korea based entity executed a global cyber-espionage campaign targeting nuclear, defence, energy and financial companies. North Korean threat actors were involved in ATM breaches, cryptocurrency exchanges theft and financial heists.

- **Cyber conflicts.** Russia was accused by Ukrainian authorities of several cyber-operations (information operations, targeted intrusions, reconnaissance) against critical targets (government, media, judiciary, telecoms, military). Russian entities were

suspected to have been behind information operations of various nature (defacements, fake SMS, disinformation, social media campaigns) in several EU countries. In the Middle East, Iran and Israel engaged in regional cyber-operations against their neighbours.

- **Espionage**. A newspaper reported that the 2013 Belgacom hack was the work of the UK GCHQ. The aviation satellite communications (SATCOM) systems sector was targeted by a cyber-espionage operation aiming at bulk data collection for intelligence purposes. Huawei was accused by an Australian intelligence official of facilitating Chinese espionage.
- **Hacktivism.** A series of politically motivated hacktivist attacks have surfaced in France and Spain. Turkish nationalistic hacktivist group Ayyildiz Tim conducted a series of attacks against entities perceived as hostile to Turkish national interests.
- **Elections**. US authorities accused a Russian woman, Elena Husyainova, of interference in the political system of the US, specifically in midterm elections. The US Cyber Command reportedly targeted individual Russian operatives to try to deter them from spreading disinformation that would interfere in mid-term elections. Ahead of the 2018 US midterm elections, researchers found 20 different state voter databases available for purchase on the dark web. Bahrain authorities accused Iran of "disturbing" elections by disseminating SMS messages to Bahraini citizens telling them they were not registered to vote. On the day of Latvian parliamentary elections, the domestic social media site Draugiem was targeted with a Russian nationalistic defacement.
- **Data protection**. Data breaches affected many sectors: space, hotels, gaming, social networks (Facebook), transportation, sport, dating, construction, culture, education, health and defence. Main causes of breaches include flaws in social media apps, vulnerable third-party e-payment software, misconfigured cloud servers, and in fewer cases, hacking. Consequences include attempts to reputation damage, loss of trust by users and extortion threatening.

PART III – TECHNICAL TRENDS

- **Malware, tools, techniques**. A new kind of malware known as Overlays runs on top of legitimate applications and steals user inputs in applications including banking, social media, email, and payment. Overlays enable an attack technique known as Tapjacking. This technique uses the Android Toast functionality to present a piece of malware as a legitimate app and tricks users into granting it various privileges and providing sensitive information. The Btlejacking attack, demonstrated at the DefCon conference in Las Vegas, allows an attacker to jam or take control of any Bluetooth Low Energy device. SMS messages were used in a hybrid / disinformation campaign in Ukraine and Poland.

10 SELECTED ATTACKS

#	Attack	Type
1	The almost certainly Russia-based group APT28 used weaponised documents related to Brexit to target several governmental entities in Europe.	Targeted attack Government
2	Highly likely Russian actors (possibly APT29 / Cozy) impersonated the US State Department in a global spear-phishing attack.	Targeted attack Diplomacy
3	US authorities accused hackers working for China's Ministry of State Security of being responsible for the Marriott data theft (500 million customers affected since 2014).	Global espionage China
4	China Telecom hijacked BGP to reroute large amounts of Internet traffic from the several countries through China for over two and a half years.	Digital infrastructure
5	In a new global campaign North-Korea based Lazarus targeted nuclear, defence, energy, and financial companies.	Global espionage North Korea
6	Russian actors launched coordinated cyber-attacks against Ukrainian government / military before and during the attack and seizure of Ukrainian ships on 25 Nov.	Targeted attacks Military
7	On 27 Nov, Polish authorities identified distribution in south-eastern Poland of false information via SMS related to the imposition of martial law in Ukraine.	Info Ops Social media
8	Several new samples of Shamoon 3 – a new variant of the likely Iranian disk-wiping malware – were spotted in several countries globally, including in Italy and France.	Destructive malware
9	A series of hacktivist attacks have surfaced in France under the hashtag #OpFrance. The attacks are believed to be related with the ongoing Gilets Jaunes movement	Hacktivism Finance
10	The New York Times, referring to US security firm Area 1 (founded by former NSA employees), disclosed EU diplomatic cables reportedly stolen by Chinese hackers.	Leaks Diplomacy