Threat Landscape Report

Q2 2019

Executive

TLP:GREEN

Executive Summary

Direct Threats

Targeted Attacks

Some EU institutions, bodies and agencies have been affected by targeted intrusion attempts. The threat actors responsible for those attacks most likely include the Russia-based Turla group and another group with a distinct origin. Turla has infected victims since at least 2004 in over 45 countries, spanning a range of sectors including government, embassies, military, education, research and pharmaceutical companies. The group is sophisticated and stealthy, with a long record of attacking governments across Europe, in particular MFAs and ministries of defence.

Common Threats

Ransomware activity has remained rather limited. However, there were two notable events: an appearance of the Shade ransomware, and a distinct case with a ransom message without any corresponding malicious encryption. Magecart, the Magento web skimming cluster, and Emotet are still the main banking malware affecting EU-I, in addition to some limited activity Ursnif activity. The main exploited vulnerability concerned the Confluence platform (CVE-2019-3396). Another noteworthy vulnerability for which there were exploitation attempt(s) is an older (2017) Microsoft Office bug (CVE-2017-11882). A handful of trojans have been observed for the first time in 12 months, including Formbook, Bateleur, and Pteranodon. We have detected a higher level of activity in the area of cryptomining, involving mainly the new Rocke cryptojacking malware. DDoS events in this quarter were fairly limited but we observed a noteworthy email flooding attack. CERT-EU has launched the pilot phase of its social media assurance service (SMAS). The service has allowed to detect impersonation of EU-I officials' accounts, on Facebook, Twitter, and YouTube. 1600+ alerts have been handled which have generated 50+ cases. Targeted phishing emails have been observed impersonating EU-I, using a compromised email account of an EU-I employee in at least one case. Credential leaks have remained the most widespread cyber security event identified in EU-I, with at least 43 EU-I affected.

Broader Threats – Critical Sectors

Transportation

Cyber espionage groups from China collect sensitive information (technologies or business intelligence) that helps create competitive advantages in the global transportation market. Cybercrime groups cause disruption using ransomware attacks, especially in the aviation sector (manufacturers, airport). Smart cars are vulnerable to hacking that could cause personal data theft or remote control of steering wheels. In some geographical areas, Russia has likely been hacking the global navigation satellite system on a mass scale to misdirect ships and aeroplanes.

Energy

The US and Russia probe and deploy malicious code on each other's power grids. China executes cyber-espionage campaigns against the energy sector in several countries. Breaches and attacks compromise thousands of records of personal data related to customers of energy companies.

Health

Major personal and medical data breaches affect healthcare organisations around the world, and in one case, costs associated with the breach caused bankruptcy. China is aggressively conducting cyber-espionage to collect sensitive information on healthcare technologies. Additional medical devices – such as infusion pumps – contain severe vulnerabilities. Ransomware infections disrupt operations in a clinic and hospitals (USA and Romania).

Banking & Finance

US-CERT released two reports about malicious tools used by financially motivated North Korean threat actors. 'Silence group', a cybercriminal entity with powerful arsenal and a Russian nexus, has been seen active against European targets. Operators of the infamous banking trojan Emotet now offer it as malware-as-a-service.

Digital Infra

BGP routing errors continue to be a problem, with another significant case involving China Telecom. Malware is found preinstalled on several mobile device models. Hardware security modules are found vulnerable to code execution attacks.

Digital Services

In the e-commerce sector, Magecart is still going strong and the number of infections is increasing. Regarding messaging services, DDoS attacks are used to suppress Telegram messaging among protesters in Taiwan. On social networks, Facebook is purportedly working on reducing the number of inauthentic accounts on its platforms. Instant messenger users are required to ID themselves in Russia. As regards cloud services, cryptojacking threat groups are competing against one another for foothold on cloud-based infrastructure. Microsoft has closed an important security gap in its Azure Active Directory multi-factor authentication setup procedure. Microsoft, Google and a number of other web services suffered outages that affected users for a few hours. The root cause was issues with Google's Cloud service that powers apps other than just Google's own web services.

Defence Diplomacy	The US Cyber Command is allegedly authorised to conduct offensive online operations without receiving presidential approval. It has reportedly targeted Russia's electric grid as well as Iran's missile and rocket launch systems. For the first time, a military entity (Israel Defence Forces) launched a physical attack as a real-time response to a digital aggression, by Gaza-based Hamas. A Russian threat actor is conducting intelligence operations against global defence and military entities. Russia is promoting the export of facial recognition technologies for military use. An advanced Russian threat actor is targeting diplomatic organisations in Europe and the Middle East. Israel is using deceptive social media accounts to influence foreign politics.

Broader Threats – Geopolitical

US	The US suspends business with Chinese companies (chip manufacturers and Huawei) and indicts Chinese nationals in order to prevent or respond to Chinese cyber-threats. The US Cyber Command reportedly launches operations on electric grids (Russia) and missile launch systems (Iran). The US suspends Iran Islamic Revolutionary Guard Corps social media accounts (Instagram). The US authorities created fake social media accounts to identify people committing immigration fraud.
China	China employs a variety of surveillance systems (facial recognition in 'smart cities' and a backdoor in a hospital to track injured protesters in Hong Kong). China reinforces digital sovereignty with new regulation to seize the data of any firm (including foreign ones) operating in China. China strengthens censorship measures, denying (DDoS) access to a popular messaging app (Telegram) and blocking access to Wikipedia. China launches information operations on social media to build up foreign support for its Belt and Road Initiative. Chinese groups are presumably behind several cyber espionage campaigns (Middle East, Europe, the US), in the transportation, industrial, energy, health and foreign affairs sectors. China Telecom has still not implemented good practices to prevent internet traffic hijacking.
Russia	Russia intensifies digital sovereignty projects (domestic Linux-based operating system, internet isolation, blocking Facebook and Twitter domestically). Russia reinforces its monitoring legislation for instant messaging. Russian information operation campaigns address a variety of matters including portraying of 5G technologies as detrimental to health and inciting discord in Europe on Northern Ireland. At least two Russian advanced threat actors have been active in Europe and abroad (especially in the diplomatic sector) in 2019 Q2. Russia reportedly probes critical infrastructures (energy) and purportedly deploys disruptive malware (Triton).
Iran	Iran is reinforcing capacities to filter and monitor social media activities and target industrial control systems. Malicious tools used by advanced Iranian threat actors have been leaked (possibly by opponents to the regime). Iran continues information operations in foreign countries, using Facebook and Instagram.
North Korea	The North Korean regime participates to international programming contests and continues producing world-class cyber talents. North Korean threat actors continue to target the financial sector to generate revenues for the regime.

Broader Threats – Motives

Cyber Conflicts	In the last 10 days prior to the European Parliament elections, EU Member States reported more than 200 deceptive narratives or potentially false information campaigns. The USA / Iran escalating tensions led to cyber strikes executed by the US against Iran missile launch systems. The US and Russia have allegedly penetrated or probed each other's electric grid, likely for deterrence purposes. The USA have used their non-technical arsenal (technology ban, arrest of convicted persons) to react to Chinese cyber threats. Israel responded by military strikes to Hamas cyber-attacks.
Espionage	Chinese groups presumably conducted several espionage campaigns (energy, transportation, healthcare technologies, foreign affairs) in Asia, the Middle East, Europe and the US, using supply chain compromises and other techniques. Unidentified leaks have exposed the methods and tools used by several Iranian cyber-espionage actors. Russian threat actors show an interest for information gathering in several sectors (foreign affairs, military, maritime). The Russia's Data Localisation Law that collects personal data of Russian citizens gains more force through increased penalties. A WhatsApp flaw was uncovered enabling spyware to access mobile devices.
Hacktivism	Turkish, Iranian, Brazilian, Kurdish and Palestinian nationalist hacktivists actively respond through. DDoS, defacements and leaks to statements or situations perceived as hostile to their countries or communities. Political hacktivist collectives mobilise in several countries for causes such as the arrest of Julian Assange, the rise of extremist political parties, the fight against the global financial system, or the dissatisfaction toward governments.

Techniques, Tactics & Procedures

Malware The almost certainly Russian threat actor APT28 deploys a new malware family with RAT (remote access trojan) capabilities. The cybercriminal group behind the GandCrab ransomware announces they are discontinuing operations and retiring the tool, while Sodinokibi, another ransomware that is spreading quickly, appears to be filling the void left by GandCrab. European law enforcement agencies in cooperation with US counterpart, Europol and an IT security company released a decryption tool for the 4th generation of this ransomware. The Triton CIS malware is targeting critical infrastructure.

Techniques Weaknesses, suspected to be deliberate, were observed in Russian cryptographic algorithms submitted for standardisation. ASUS customers have been targeted by an extensive supply chain attack. ASUS cloud client software was possibly used for Person-in-the-Middle attacks. A SIM swapping campaign targets Portuguese-speaking nations: attackers take control of a victim's phone number by hijacking accounts and intercepting two-factor authentication methods in which the second authentication factor is an SMS message or a call placed to the mobile number.

Tactics The Rapid Alert System set up by the EU has allowed information sharing on more than 200 disinformation / potentially deceptive narrative campaigns on European traditional and social media in the last 10 days prior to the European Parliament election. Citizen cyber monitoring tactics are most likely employed by Chinese authorities in Hong Kong, while other countries are also employing similar tactics domestically. The US are accusing Iranian threat actors of using wiping tactics. Several cases of disruption and extortion tactics – in the form of ransomware attacks – are noted in various sectors, globally.

#	Attack	Type
1	In April, a targeted intrusion, likely executed by the Russia-based Turla threat actor, was detected in the EU delegation in Moscow.	Targeted attack Russia
2	In May, Israel Defence Forces airstrikes destroyed the headquarters of the main cyber unit for the Gaza-based Palestinian organisation Hamas.	Targeted attack Military
3	Amid protests against the extradition bill, the Hong Kong police were given backdoor access to the Hospital Authority's patient database. They used that information to find and arrest people injured in the protests.	Surveillance China
4	The US has allegedly infiltrated the Russian electrical grid with offensive malware, while a Russian threat group is reportedly probing US and Asian electrical grids.	Critical infrastructure Energy
5	The US allegedly launched cyber strikes that disabled the Iranian computer systems used to control rocket and missile launches and other systems used to track US ships.	United States Iran
6	A Chinese group dubbed APT27 compromised government organisations of two different countries in the Middle East, using tools that utilised the NSA-leaked EternalBlue exploit.	China Espionage
7	Belgium-based aeroplane parts and aviation structuring business ASCO Industries has been hit by a ransomware attack which caused the shutdown of the production in Canada, Germany, USA, Brazil, France and Belgium.	Transportation
8	In April, May, and June, the number of Magento infections by the Magecart malicious cluster has doubled every month. Magecart is a script that collects payment card data customers introduce on the checkout page of online businesses and exfiltrates it to a server controlled by the attackers.	Cybercrime
9	FIN7, a major cybercriminal ring created fake companies in order to hire remote pen testers, developers and interpreters to participate in their malicious business.	Russia Cybercrime
10	In the wake of Julian Assange's arrest at the Ecuadorian embassy in London on April 11, hacktivist groups mobilised and targeted numerous entities in the UK and Ecuador with DDoS attacks, data breaches, and defacements.	Hacktivism