THREAT LANDSCAPE REPORT

VOLUME 1 / 11 JUNE 2021

TLP:WHITE

CERT-EU, CERT for the EU Institutions, Bodies and Agencies

Table of Contents

Executive Summary

In its review of the 2020 cyber threat landscape, CERT-EU identified the following 10 major threats.

1	Advanced Persistent Threats	The number of attacks conducted by Advanced Persistent Threats (APTs) attacks against EU institutions, bodies and agencies (EUIBAs) increased by 60% in 2020 compared to 2019.
2	Extortion	RaaS (Ransomware-as-a-Service) enabled threats and, to a lesser extent, DDoS (Distributed Denial of Service) and extortion attacks have surged in the EU but also globally, causing extremely damaging disruptions in crucial sectors such hospitals, administrations and various businesses. Luckily, and unlike some of their service providers, EUIBAs have not been directly affected.
3	Hack-and-leak	Stealing data from an organisation and publishing it online has been a frequently observed tactic. An EUIBA had been targeted by a hack-and-leak operation in 2020.
4	Malware and bots	Advanced cybercriminals have continued improving their arsenal and major malware strains. A number of EUIBAs were affected.
5	Attacks related to teleworking	Major threat actors, either state-sponsored or financially motivated, have stepped up their efforts to abuse teleworking technologies, especially VPNs, with a high level of success. The remote access services of several EUIBAs had been targeted.
6	Attacks targeting cloud services	Many organisations continue migrating their IT infrastructure, services or data to the cloud. Researchers have observed the successful use of innovating techniques to access the cloud assets of targeted organisations.
7	Supply chain attacks	These attacks, which are difficult to detect and mitigate in due time, demonstrated again how damaging they can be. The SolarWinds Orion campaign, one of the most sophisticated cyberattacks in history, affected some EUIBAs.
8	Attacks on service providers	The data and IT continuity of EUIBAs had been threatened by a number of breaches, especially ransomware, which affected high-profile service providers.
9	Identity abuse	Attackers have been pushing the principle of using legitimate assets of their victims to an unprecedented level. In addition to abusing legitimate software, they forge valid accounts to burrow into and stay inside the networks of their victims.
10	Artificial Intelligence and Machine Learning-based attacks	Academic studies show the potential role of AI and ML in empowering cyberattacks. Some cyber operations observed in the wild feature techniques and tactics that could have been facilitated by ML.

These threats are here to stay and may further increase in the foreseeable future.

1. Introduction

The cyber threat landscape is in constant evolution. Diverse threat actors carry out a large variety of malicious operations in the digital space, ranging from very narrowly targeted intrusions to indiscriminate, opportunistic campaigns. The prominent motives are diverse but change little: stealing sensitive information, making money, promoting a cause, manipulating public opinion, or undermining digital infrastructure. However, the tactics, techniques and procedures (TTPs) employed by threat actors keep evolving. The pace at which they conduct their cyberattacks is higher than ever, while their campaigns are increasingly sophisticated and automated, targeting exposed attack surfaces and quickly exploiting vulnerabilities. To mitigate these risks, a deep understanding of the most recent and prominent TTPs is necessary.

This document presents a synthetic overview of the principal cyber threats to which the EU institutions, bodies and agencies (EUIBAs)[1] are currently exposed or are likely to be prone to in the foreseeable future.

Three categories of observations were used to support the analysis on which this document is based:

1. Attempts to breach the IT infrastructure of EUIBAs. When successful, they are treated as incidents. Otherwise they are recorded as detections.
2. Threats detected in the proximity of EUIBAs, e.g. in their related sectors, their stakeholder communities, or in Europe.
3. Major threat trends observed globally.

Furthermore, the analysis takes into account major ongoing shifts affecting the way EUIBAs manage and use their IT infrastructure and services. These include:

- The general increase in teleworking. Teleworking became the norm in the aftermath of the COVID-19 pandemic. It is likely to remain a long-term trend.
- The migration to the cloud.
- The expansion of IT service outsourcing.

As a result, 10 major threats have been identified in 2020. They are detailed hereunder.

Note

During 2020, CERT-EU released a number of alerts and memos during 2020. See Annex 1 for further details.

2. Advanced Persistent Threats

The number of APT attacks against EUIBAs increased by 60% in 2020 compared to 2019. These attacks are tracked by CERT-EU as significant incidents.

A significant incident is a targeted intrusion operation in which the threat actor:

- successfully compromises critical information assets of its victims (e.g. mail servers, document management systems, etc.), and
- demonstrates advanced skills at key stages of the intrusion kill chain: initial access, credential theft, privilege escalation, lateral movement, persistence, defence evasion and/or exfiltration.

In half of the cases, the motivation of the attackers was not clear. However, CERT-EU determined that 25% of the significant incidents were highly likely caused by state-sponsored threat actors with a cyberespionage nexus. In other cases, the threat actor was especially interested in the collection of specific information.

CERT-EU also observed threat actors trying to abuse the trust inherent to information flows across EUIBAs. In some cases, they mimicked an EUIBA's identity, using spoofed domains or forged email addresses. In other cases, they compromised an element of an EUIBA's infrastructure or email accounts and used it as a beachhead to breach another EUIBA. These tactics allowed adversaries to blend in legitimate network traffic or create convincing phishing lures.

We assess that EUIBAs are highly attractive targets for APT groups.

[1] CERT-EU's constituency is composed of all the EU institutions, bodies and agencies (EUIBAs). As of this writing, there are 80 such organisations.

According to our observations, there are schematically three main motives for APT groups to target our constituents.

1	Targeting sensitive information on specific matters	The primary objective of the adversary is to steal sensitive information from a specific EUIBA depending on its sector of activity (e.g. diplomacy, health, energy, transportation, finance, etc.). During the financial crisis of 2008-2012, state-sponsored threat actors were looking for non-public EU political deliberations about finance, sovereign debts, etc. In the current COVID-19 pandemic, they are looking, among other things, for sensitive information on vaccines as demonstrated by the cyberattack against the European Medicines Agency[2].
2	Targeting the EUIBA community	EUIBAs form a group of stakeholders in which substantial information flows take place under well established, mutual trust. The threat actor's goal is to compromise a member of the community whose cybersecurity maturity is lower than others for further exploitation. Post-exploitation activity can then allow the adversary to move to other targets within the community. This may be done using several means such as blending in legitimate network traffic or sending spear phishing emails from a compromised email address of an EUIBA. Such tactics had been observed by CERT-EU.
3	Targeting EU communities of interest	All EUIBAs have close working relationships with an ecosystem of public and private organisations based in EU member states. APT groups can breach, abuse and blend in the flows within this ecosystem. Adversaries may compromise an EUIBA to facilitate attacks against various public or private organisations across the EU. Attackers can reuse compromised address books in phishing campaigns, breach an EUIBA's website in an EU-wide watering hole campaign, use a compromised email account as a launch pad for spear phishing, stealing, infecting official EU documents and redistributing them, etc. All these scenarios had been observed by CERT-EU in the past few years.

Impact on EUIBAs

The number of APT attacks against EUIBAs sharply increased in 2020 and shows no signs of abatement in 2021.

3. Extortion

Cyber extortion is a method cybercriminals use to attack or threaten to attack the IT assets of organisations and coerce them into paying a ransom. For several years, two main extortion tactics have emerged:

1. **Ransomware**: encrypting files to make systems unusable and threatening to release stolen information.
2. **DDoS extortion**: threatening to launch DDoS attacks to incapacitate the victims.

However, in recent months, cybercriminals have significantly refined their tactics to exert stronger pressure by causing multiple types of damage.

Ransomware operations remain the most dangerous cyber extortion scheme.

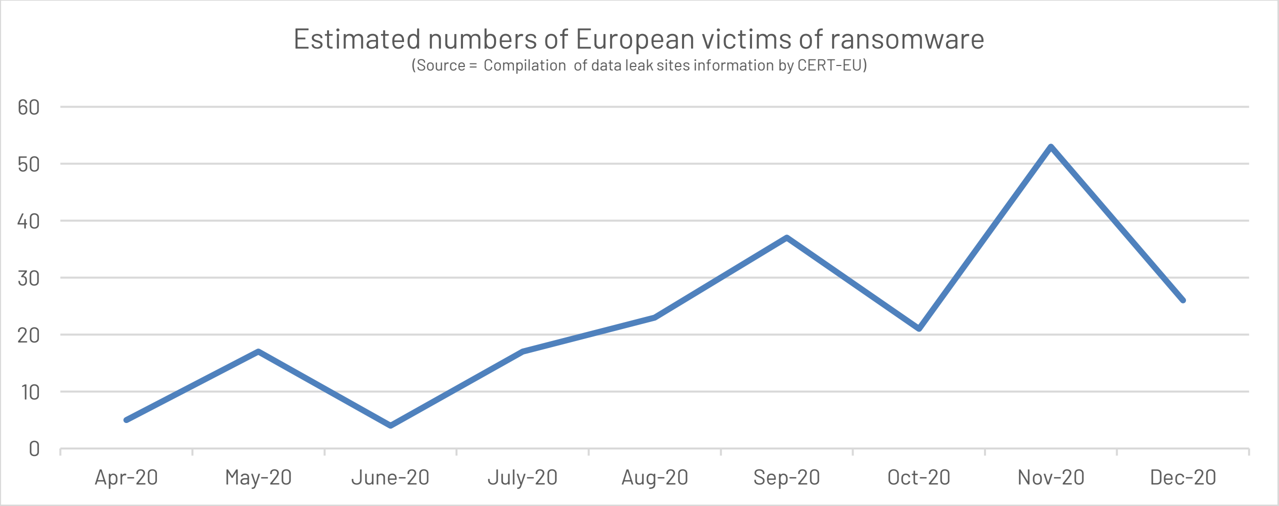
In 2017, a shift in ransomware operations was observed with the WannaCry, NotPetya and BadRabbit campaigns. However, these operations were atypical because they aimed at creating chaos rather than generate revenue and because they were most likely carried out by state-sponsored threat actors.

Starting from 2018, cybercriminals have begun to set up Ransomware-as-a-Service (RaaS) schemes, a practice which significantly expanded the volume of their activities.

[2] https://www.ema.europa.eu/en/news/cyberattack-ema-update-6

RaaS schemes involve two categories of cybercriminals: developers and affiliates, linked by what could be associated with a contractual relationship, albeit illegal.

Affiliates perform big game hunting (BGH) operations against large organisations, with ransom demands sometimes reaching millions of euros. Developers grant them access to a number of resources, such as the ransomware payload, a data leak site (DLS) on which affiliates will post the data stolen from their victims, and the mechanisms to monetise the breaches they perform. In return, the developers get a percentage of payments received from victims.



Affiliates of major ransomware operations have used multiple TTPs to intimidate and exert pressure on their victims. Double, then multiple extortion TTPs started to develop in the end of 2019. While ransomware activities were initially restricted to data encryption, cybercriminals now steal data and threaten to leak it publicly or auction it. Some also try to shame their victims by naming them publicly on dedicated blogs or websites, or threaten to disclose the data breach to regulatory authorities such as data protection supervisors.

Note

Annex 2 provides details on the major RaaS operations in Europe in 2020.

DDoS extortion. DDoS extortion attacks are not something new. This cybercriminal tactic became particularly popular in 2016 and 2017 with dozens of attacks reported in several regions and sectors. At that time four threat actors were especially active: D4BC (DDoS for BitCoins), Lizard Squad, Stealth Ravens, and Armada Collective.

Then, starting from Aug-Sep 2020, there has been a resurgence of DDoS extortion campaigns in multiple sectors, including banking, finance and retail. New Zealand's stock exchange was forced to halt trading for four days in a row[3]. Cybercriminals behind the campaigns claimed to be Fancy Bear or Armada Collective. It should be noted that Fancy Bear is the code name usually given to a Russian espionage threat actor, also tracked as APT28. It is highly unlikely that the latter is behind the DDoS extortion attacks. Instead, this "brand", abused by extortionists since 2017, is highly likely used to scare victims.

In addition, cybercriminals leverage DDoS botnets (e.g. Mirai). They flood networks using various protocols and techniques such as UDP, GRE, SNMP, TCP/SYN, NTP amplification, etc. The performance of the attacks varies significantly among threat actors. It typically starts at 10-20 Gb/sec and may go up to 200 Gb/sec and beyond. In some campaigns, attackers claimed traffic exceeded 2 Tb/sec.

Extortion demands start at a certain amount of money (5 to 20 bitcoins) then increase (10 to 30 bitcoins) if the deadline is missed, with another 5 to 30 bitcoins added for each day thereafter.

The DDoS extortion campaigns observed in Dec 2020 - Jan 2021 represent a strategic shift in attackers' tactics. In previous years, they would run annually for a few weeks ("seasonal event") targeting specific industries/companies before the cybercriminals would typically give up. Nowadays, cybercriminals are circling

[3] https://www.theguardian.com/world/2020/aug/28/new-zealand-stock-exchange-disrupted-by-fourth-offshore-cyber-attack

back to previous targets and demonstrating unusual perseverance. If an organisation had ever received an extortion demand, there is a high chance it will receive another one.

Impact on EUIBAs

No significant ransomware incident has been observed affecting EUIBAs. However, EUIBAs are frequently targeted by phishing campaigns trying to deliver the first stage of a typical ransomware infection chain.

4. Hack-and-Leak

Hack-and-leak is a tactic in which attackers steal data from an organisation and publish it online. The way the *leak* phase of the operation is carried out indicates the motive of the operation:

- When the leak is made on darknet forums, it usually marks a criminal motive with attackers trying to sell the stolen data.
- When it is made on regular internet websites, it probably indicates a political motive.

The latter may be performed by hacktivists wishing to promote a cause (e.g. expose the "bad practices" or "corruption" of the affected organisation). In some cases, the leak is performed by a front entity — acting on behalf of a foreign state — to sow public distrust or disinform people. As a consequence, breached organisations risk significant reputational damage. The reaction of the victim (adequate public communication and transparency, compliance to notification obligations, impact assessment on third parties, etc.) will be critical to mitigate the damage caused by the operation.

The cyberattack on the European Medicines Agency shows that an EUIBA that handles important information for a healthy European civil society can become the target of a politically oriented hack-and-leak campaign by state-sponsored threat actors.

A historical review of such campaigns shows that it is a global phenomenon. Although some, targeting US and European entities, have received significant publicity, other countries have also been affected. Some of these operations are run by domestic actors (e.g. hacktivists or dissidents), while others are likely conducted by front entities operating on behalf of nation states.

It is worth noting that, in a number of cases, hack-and-leak operations reportedly had a Russian nexus, underlining the importance of this type of activity for Russian threat actors in achieving their goals. Leaking of hacked content has been used as a public opinion influence tool at various moments, to cause election interference, to discredit or blackmail politicians, journalists, public figures, etc. Please refer to Annex 3 for details on historical hack-and-leak operations.

Impact on EUIBAs

1 EUIBA fell victim to a likely politically motivated hack-and-leak operation in 2020.

5. Malware and Bots

CERT-EU observed sustained and ongoing attempts by advanced cybercriminals to infect EUIBA networks with prominent malware strains or malicious tools such as Emotet, Agent Tesla, TrickBot, LokiBot, Cobalt Strike, etc.

The initial access vector is usually phishing. The victims receive email lures that either contain malicious attachments or links leading to attacker-controlled sites from where they download malware.

These threats should continue to be treated seriously because they have the potential to do significant damage:

- Certain types of malware and malicious tools can harvest information and/or credentials. Stolen data can be directly monetised in darknet markets or used in hack-and-leak operations, for example. Stolen credentials can also be used for lateral movement or privilege escalation within the organisation.
- Malware may sometimes be the first stage of an infection chain that leads to the deployment of ransomware.

- Once adversaries gain access to an EUIBA network, they may opt to not directly exploit it, proposing it instead for sale on darknet forums. There is indeed a very dynamic market for selling access and credentials.

Many major malware strains are highly modular frameworks. Their design allows extending core functionality or delivering additional malicious payloads. They include obfuscation and anti-detection features and their authors keep improving them to escape defences.

Before it was disrupted by a law enforcement operation in January 2021, Emotet was a long-running botnet, active since at least 2014, that had started as a banking trojan and developed into the preferred botnet-for-hire of several ransomware operators. Emotet was utilised to spread the TrickBot trojan or the Qbot (aka QakBot) backdoor on infected systems.

Agent Tesla[4], which have been active since at least 2014, is an information and password stealing RAT (Remote Access Trojan), focusing on acquiring data from a victim's system. It can record and exfiltrate keystrokes (i.e. account information, usernames, passwords, credit card numbers, etc.), as well as screenshots. Recorded information can then be used for cybercrime purposes. Used by multiple threat actors, Agent Tesla can be purchased as a "tool".

The most commonly occurring malware families within EUIBAs in 2020 are indicated in the table below.

Top 10 malware and number of affected EUIBAs

Malware	2020Q1	2020Q2	2020Q3	2020Q4
Emotet	20	2	21	19
Agent Tesla	12	10	5	10
LokiBot	11	0	6	5
Cutwail	0	0	0	19
Sunburst	0	0	0	13
Guloader	0	5	3	2
Cobalt Strike	0	2	2	5
Hworm	9	0	0	0
Azorult	6	0	0	0
TrickBot	5	0	0	0

Impact on EUIBAs

Up to 21 distinct EUIBAs observed Emotet, Agent Tesla or LokiBot infection attempts in each quarter of 2020.

6. Attacks Related to Teleworking

Remote access. In the wake of the COVID-19 pandemic, EUIBAs have, as many organisations, moved to teleworking as the norm. As a consequence, their attack surface increased and threats to VPN services have become especially prevalent.

Since spring 2020, several threat actors, including state-sponsored ones, have been intensively exploiting vulnerabilities in VPN products such as Citrix Gateway and Pulse Connect Secure.

The abuse of remote access services is clearly one of the preferred initial access methods by APT groups targeting EUIBAs (see the Advanced Persistent Threats section above).

[4] https://attack.mitre.org/software/S0331/

Collaboration apps. The use of videoconferencing and chat applications such as Zoom, WebEx, Houseparty, Google Meet, and Microsoft Teams increased significantly in 2020. While several threats and vulnerabilities related to these applications have been reported, a substantial number affected the Zoom platform.

Zoom has made very good progress in terms of security (e.g. they implemented end-to-end encryption by default in October 2020). However, in June 2020, prominent human rights activists – all of them located outside of China – accused[5] Zoom of disrupting or shutting down their accounts because they were linked to events to mark the anniversary of the 1989 Tiananmen massacre or because they were going to discuss China's measures to exert control over Hong Kong. Zoom reinstated the disrupted accounts and said they are developing technology that will let them remove or block participants based on their location.

On 20 November 2020, a Dutch journalist gatecrashed a confidential videoconference of EU defence ministers, thanks to a picture posted on the Dutch defence minister's Twitter account[6]. The picture in the now-deleted tweet included five digits of a six-digit PIN. The journalist only had to guess a single digit (0-9) to join.

Impact on EUIBAs

In 2020, more than one third of significant incidents affecting EUIBAs were made possible because of the exploitation of a vulnerability in remote access services.

An EU defence ministers' videoconference was gatecrashed by a journalist.

7. Attacks Targeting Cloud Services

While organisations worldwide are migrating their infrastructure to the cloud, threat actors have already developed techniques, tactics and procedures to breach cloud platforms.

According to recent analyses, threat actors have been using a variety of methods to access to the cloud resources of their targets. These include classic ones, such as spear phishing, use of stolen credentials, brute forcing and credentials stuffing, as well as more specialised techniques, such as Web Session Cookie[7], Pass-the-PRT[8]or Golden SAML[9].

Besides the typical flaws (e.g. misconfigurations, vulnerabilities or administration mistakes), the move to a digital infrastructure and software that is hosted and managed by a third party entails specific risks. Cloud environments are exposed to a number of threats, including APT groups.

Cyberespionage. A number of APT groups have been identified as the first to attack cloud services for espionage purposes. Between 2010 and 2017, in what became known as Operation Cloud Hopper[10], China's APT10 targeted many cloud providers worldwide.

In September 2020, Microsoft analysed[11] how the Chinese state-sponsored threat actor APT40 (aka Gadolinium) was abusing Microsoft cloud technology at several key stages of the intrusion chain. More specifically, the threat actor was using 18 Azure Active Directory applications for their malicious Command and Control (C2) infrastructure. This represents a shift to the "living off the cloud" tactic, which consists of abusing legitimate system applications to execute malicious actions.

Cybercrime. Cloud platforms are also targeted for immediate financial gain. In August and September 2020, researchers reported[12] how a cybercriminal group called TeamTNT was using a crypto-mining worm with

[5] https://www.theguardian.com/technology/2020/jun/11/zoom-shuts-account-of-us-based-rights-group-after-tiananmen-anniversary-meeting

[6] https://www.politico.eu/article/dutch-reporter-gatecrashes-eu-defense-ministers-videoconference/

[7] https://attack.mitre.org/techniques/T1539/

[8] https://stealthbits.com/blog/lateral-movement-to-the-cloud-pass-the-prt/

[9] https://www.sygnia.co/golden-saml-advisory

[10] https://www.pwc.co.uk/issues/cyber-security-services/insights/operation-cloud-hopper.html

[11] https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/

[12] https://www.intezer.com/blog/cloud-security/attackers-abusing-legitimate-cloud-monitoring-tools-to-conduct-cyber-attacks/

specific cloud platform features. The worm was indeed stealing AWS credentials and scanning the internet for misconfigured Docker and Kubernetes platforms. In addition, TeamTNT added the legitimate, open-source Weave Scope visualisation and monitoring software tool to its arsenal in order to more easily abuse misconfigured cloud environments.

Cloud service providers are also attractive for big game hunting cybercriminals because their customers create pressure points to incite them to pay the ransom. During the summer of 2019, for example, the cloud hosting provider iNSYNQ experienced[13] a ransomware attack that left customers unable to access their data.

It is important to remember that, in service-level agreements with cloud service providers, the responsibility for backup usually lies on the customer side. Therefore, organisations need to extend their backup strategies, which help them recover from ransomware attacks targeting their networks, to cloud environments.

Impact on EUIBAs

In 2020, CERT-EU observed regular attempts to steal or phish EUIBAs' cloud access credentials. These attempts are still ongoing.

8. Supply Chain Attacks

Supply chain attacks (SCAs) abuse the inherent trust that users and administrators place in hardware, software, and updates supplied by reputable vendors. This tactic has been used in a series of high-profile attacks, executed mostly by state-sponsored cyberespionage groups and, in some cases, by skilled cybercriminals.

On 13 December 2020, FireEye disclosed[14] that several high-profile agencies of the US government as well as numerous public and private organisations worldwide had been infiltrated via Orion, a popular network management system software made by SolarWinds. Shortly after, numerous publications were made by several organisations, including SolarWinds, Microsoft, CheckPoint, NETRESEC, CrowdStrike, CISA, and Volexity, detailing many aspects of one of the most sophisticated cyberattacks in history.

This is not the first time an SCA had been conducted. Previous SCAs targeted software made by Juniper (ScreenOS backdoor, 2015), MeDoc (NotPetya, 2017), NetSarang (ShadowPad, 2017), Piriform (CCleaner, 2017) and ASUS (Operation ShadowHammer, 2019) and this list is far from exhaustive.

SCAs have the potential for a devastating impact and their discovery is usually difficult as the malicious code is generally hidden within the modified application. For example, with 18.000 potentially affected organisations, including many high-profile ones, the SolarWinds Orion SCA may have had potentially wide-ranging implications given the unprecedented visibility and access level attackers could obtain by compromising such a central, highly popular application.

Attackers implementing supply chain compromises usually opt for two possible strategies:

- Regional/sectoral targeting. In such a case, they target software used in specific countries or sectors. This is the case for the StealthyTrident[15] and SignSight[16] operations.
- Global targeting. The attackers compromise software that is used globally. At a later stage, they can make a selection of the victims to which they want to deploy their espionage tools. This strategy was used in the SolarWinds and CCleaner cases.

CERT-EU has reviewed 14 significant SCAs that took place since 2014 (see details in Annex 4). An analysis of the origin of the attack, when attribution was possible, shows that:

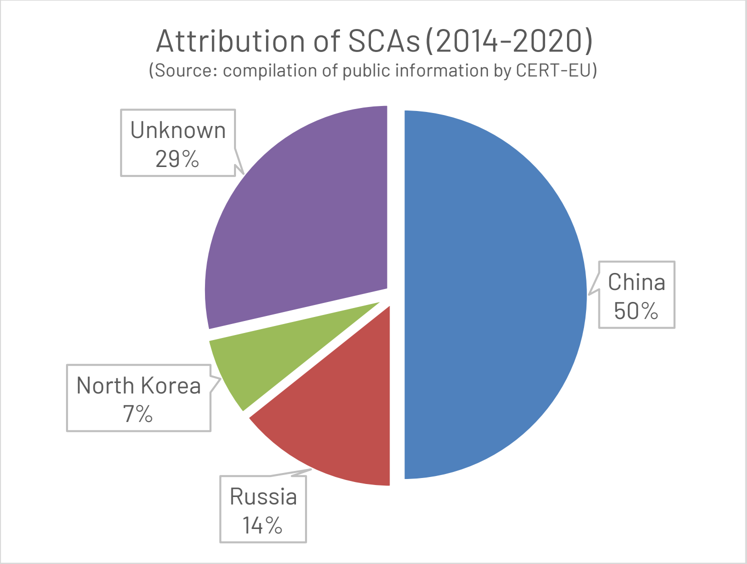
- 6 SCAs have been attributed to Chinese threat actors.
- 2 SCAs have been attributed to Russia (NotPetya operations and the SolarWinds Orion campaign).
- 1 SCA has been attributed to North Korea (Lazarus).

[13] https://krebsonsecurity.com/2019/07/quickbooks-cloud-hosting-firm-insynq-hit-in-ransomware-attack/

[14] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[15] https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/

[16] https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/



Impact on EUIBAs

At least 6 EUIBAs were affected by the SolarWinds Orion SCA[17].

9. Attacks on Service Providers

EUIBAs, like most professional organisations in the world, are dependent on an increasing number of companies for the management of their IT infrastructure and provision of digital services. This dependency creates a number of risks including:

- Risks to data. Third parties are in possession of data belonging to an EUIBA. A security breach at the third party will put this data at risk of being stolen.
- Risks on continuity. EUIBAs may rely on these third parties for infrastructure and service continuity. A breach affecting the third party may put service continuity at risk.
- Risks of infection propagation. In case of data flows, and particularly automated ones, between the infrastructures of the third party and the EUIBAs, compromise of the third-party infrastructure may ripple through the EUIBAs through lateral movement, API access, etc.

Several major managed service providers were compromised in 2020.

In May 2020, the US-based digital services company Blackbaud was breached[18] in a ransomware attack that had adverse effects to several of its customers in the US and Europe. The attackers copied a subset of the customer data and asked for a ransom to delete it. The company gave in and paid the requested sum. In August 2020, a US resident filed a class action lawsuit against the company for actions which resulted in the leakage of his personal data.

That same month, a large number of customer accounts associated with Sendgrid, a global email service provider handing over 70 billion emails per month, were compromised[19]. Stolen passwords are sold in darknet marketplaces and abused in phishing campaigns.

In October 2020, cybercriminals reportedly planned to compromise US-based managed service providers common to healthcare facilities[20] (e.g. a provider of electronic health records). Their objective was to cripple the providers with the Ryuk ransomware and create an impact on its customers (hospitals, clinics, etc.). Up to

[17] https://www.europarl.europa.eu/doceo/document/P-9-2021-001112-ASW_EN.pdf

[18] https://www.zdnet.com/article/cloud-provider-stopped-ransomware-attack-but-had-to-pay-ransom-demand-anyway/

[19] https://www.bleepingcomputer.com/news/security/hacked-sendgrid-accounts-used-in-phishing-attacks-to-steal-logins/

[20] https://krebsonsecurity.com/2020/10/fbi-dhs-hhs-warn-of-imminent-credible-ransomware-threat-against-u-s-hospitals/

400 different healthcare facilities were at risk. A few days after the plan was set, already 4 healthcare facilities had been affected.

In the same month, the German software giant Software AG fell[21] victim to a Clop double extortion ransomware attack that encrypted enterprise files and resulted in data theft. Attackers claimed to have stolen 1 TB of data and were demanding a $23 million ransom. A few days later, the attackers started to leak some of the stolen information, including contract data and possibly files of other customers, on their dedicated blog "CLOP^_-LEAKS".

In November 2020, a report uncovered[22] a large-scale cyberespionage operation attributed to the Chinese APT10 threat actor. Among other sectors, the campaign targeted managed service providers.

Impact on EUIBAs

EUIBAs are customers of several prominent managed service providers that were breached in 2020. However, no direct impact on EUIBAs had been observed by CERT-EU as a result of these breaches.

10. Identity Abuse

The SolarWinds Orion campaign was not just another sophisticated supply chain attack. An analysis of the key tactics showed the unprecedented level of sophistication the adversaries leveraged to abuse their victim identities for later movement and stealthy operations. They remained undetected for more than six months in the network of hundreds of compromised organisations.

Identity abuse essentially consists of using valid accounts and legitimate applications to perpetrate malicious activities in a persistent and stealthy way. Attackers abuse the inherent trust in any action associated with authenticated users or authorised applications. Identity abuse can be seen as an extension of the living-off-the land (LOTL) tactic where an attacker makes use of legitimate tools to remain undetected, whereas, through identity abuse, the attacker will additionally make use of legitimate accounts.

In the SolarWinds Orion campaign, the adversaries abused the high-privileged accounts the application uses; these accounts ultimately underpin identity in an organisation's environment.

Impact on EUIBAs

CERT-EU noticed cases in which attackers used or created valid accounts within the infrastructure of EUIBAs. In many significant incidents investigated by CERT-EU, the attackers possessed valid credentials for several EUIBA users.

Additionally, most organisations use a large variety of software running with high privileges. Like in the SolarWinds Orion case, these can be abused.

11. Artificial intelligence and Machine Learning-Based Attacks

Artificial Intelligence (AI) and Machine Learning (ML) are double-edged swords: cybersecurity vendors try to leverage these novel technologies in their prevention and detection products, but AI/ML can also likely be used by threat actors to improve their TTPs and tools.

[21] https://threatpost.com/software-ag-data-clop-ransomware/160042/

[22] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage

There have been a few[23] academic[24] studies[25] analysing the potential role[26] of AI and ML to empower cyberattacks. Some observed cyberattacks also indicate possible signs of AI or ML use.

Scale and efficiency. Automation brought by AI would alleviate the existing trade-off between the scale and efficiency of attacks. In particular, labour-intensive cyberattacks (such as spear phishing) would expand in scope. To be successful, attackers need to carefully prepare their operation: impersonate a legitimate sender, find recipients in the address book or group of stakeholders, blend into a legitimate flow of information (email threads, chat platforms, social networks, etc.), weaponise a payload (for example using a stolen legitimate document), craft a convincing message, etc. Several of these steps could be automated using large language models such as GPT-3 and other AI/ML technologies.

Vulnerability exploitation. Use of AI could empower social engineering[27] and expand the exploitation of software vulnerabilities[28].

Fine targeting. Finely targeted attacks could become more prevalent thanks to AI and ML. Attackers sometimes need to tailor their attacks to certain targets. Analysing workflows and digital interactions which are specific to an organisation or a group of stakeholders could be facilitated with AI and ML. In 2020, CERT-EU observed some campaigns in which attackers were sending phishing emails that used hijacked email threads from compromised victims. Hijacking email threads to deliver malware is a technique that leverages trust between people. The phishing emails were typically sent as replies to genuine emails. Attackers leveraged email conversations between colleagues, suppliers and customers. The phishing links or documents were sent as replies to emails which had been discovered in the compromised account's mailbox. This was giving the email messages an inherited sense of trust.

Autonomous cyber weapons. Development of autonomous cyber weapons is also expected. Currently, most malware variants need some sort of communication between the deployed agents and a C2 server. AI features embedded into a malware framework would allow the deployed agents to behave appropriately in the victim environment without interaction with a "controller", just like autonomous vehicles. This would also allow attackers to exploit segregated systems more easily. On this specific topic, Stuxnet, used to disrupt the Iranian nuclear program, can be seen as a precursor. Indeed, Stuxnet had the ability to operate without receiving commands once it infected the victims' computers.

12. Outlook

The threat landscape is changing on an ongoing basis and it is important to revaluate threat models and update them regularly to account for the threats of most concern to one's organisation. We believe however that the threats identified in this report are here to stay and may increase in the foreseeable future. This assessment is supported by two main factors:

1. Most of the threats identified in this document did not appear for the first time in 2020. Threat actors keep improving certain TTPs. When these TTPs reach a sufficient degree of maturity, they guarantee a certain ratio of success and they are adopted by more threat actors.
2. The elements of context (migration to the cloud, teleworking, growing reliance on AI and ML, etc.) that influence these TTPs will likely have long-lasting effects on the threat landscape.

It is also important to note that some threat actors are tactical and/or technical pioneers. And while emerging TTPs may not be adopted immediately by a large number of threat actors, that does not mean they are not dangerous from the onset. One should look no further than the SolarWinds Orion campaign for a stark example.

[23] https://arxiv.org/abs/1905.10615

[24] https://www.rte.ie/documents/news/2018/02/ai-report.pdf

[25] https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter-wp.pdf

[26] Enjeux et défis de l'intelligence artificielle en cybersécurité, Institut intelligence et données, ULaval. https://www.youtube.com/watch?v=IzMDe6FXTZ0

[27] e.g. through the use of speech synthesis for impersonation or to mimic human interactions on social media.

[28] e.g. finding and exploiting vulnerabilities by leveraging deep learning techniques.

13. Conclusion

EUIBAs are highly attractive targets. As clearly described in this report, they are facing highly skilled and very well-resourced threat actors as well as several types of threats.

In 2020:

1. CERT-EU tackled 1432 incidents, **the highest number ever recorded in our 10 years of existence**, averaging 119 incidents per month, up from 688 (or, on average, 57 incidents/month) the year before.
2. **The number of forensics images we analysed in 2020 more than tripled in comparison to 2019**, which was already a record-setting year.
3. **The number of significant incidents in EUIBAs had risen more than tenfold since 2018.** Playing the long game, the adversaries behind these attacks are professional, systematic and persistent.

While hack-and-leak operations are a tangible danger and ransomware remains a very potent threat, service providers, cloud services and IT software are also attracting the attention of various adversaries. Moreover, supply chain attacks, as demonstrated by the recent SolarWinds Orion campaign, one of the most sophisticated cyberattacks in history, can have devastating effects and their scope may never be fully grasped.

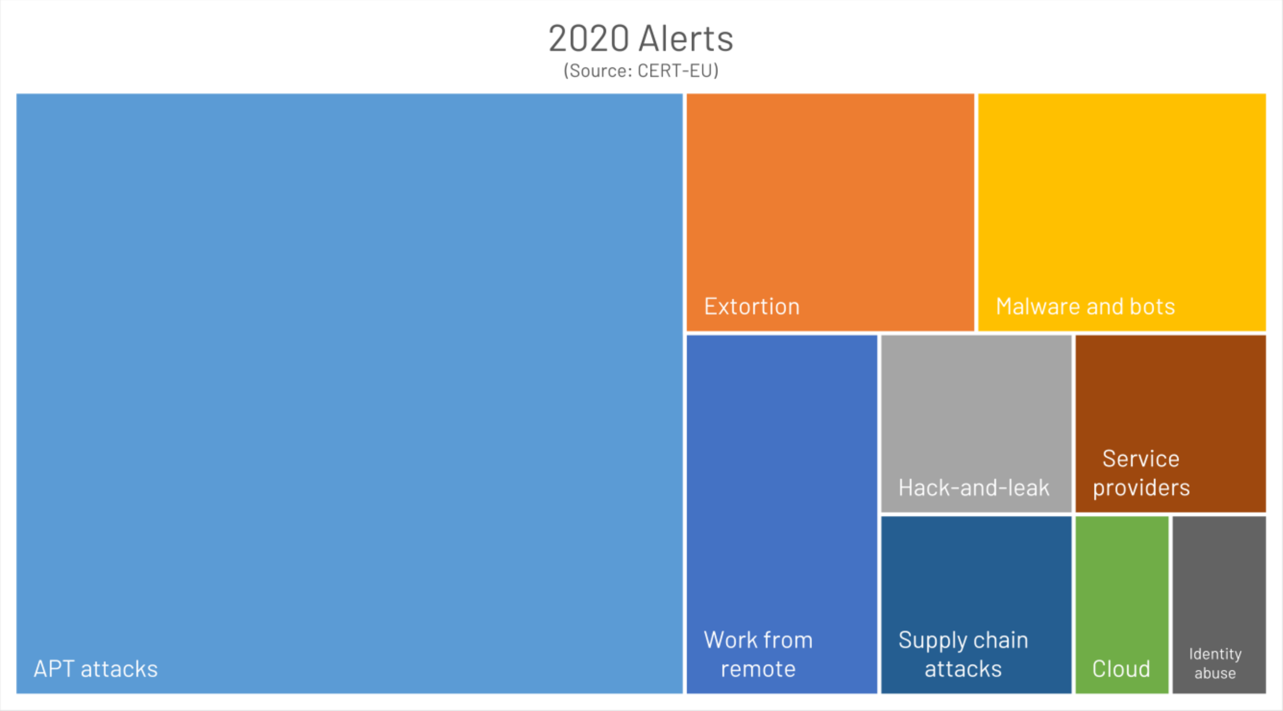
Far from abating, the number and variety of cyberattacks continue to increase and the pace at which they do is accelerating. Thanks to their investments in automation, many threat actors have scaled up and improved their campaigns. And as strides continue to be made in artificial intelligence and machine learning research and applications, and the barrier to entry is lowered, it is highly likely that AI/ML technologies will be used or abused by adversaries to intensify their attacks and further their objectives.

Yet, the cybersecurity posture, detection and response capabilities of EUIBAs vary quite significantly while, at the same time, any EUIBA can be used as a beachhead to compromise others, as already witnessed by CERT-EU, or target EU communities of interest.

Annex 1 – Threat Alerts and Memos In 2020

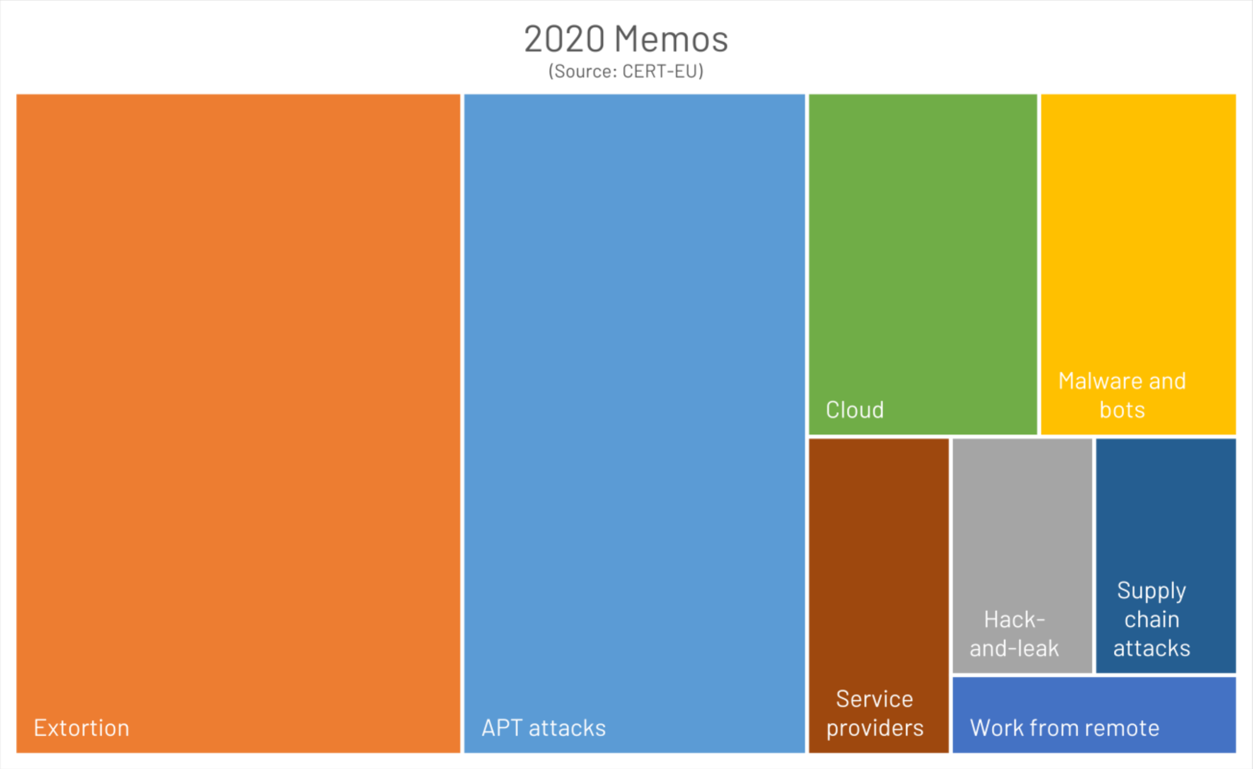
In 2020, the top 5 threat categories for which CERT-EU released threat alerts, which are actionable deliverables, were:

1. APT attacks
2. Extortion
3. Malware and bots
4. Work from remote (teleworking)
5. Hack-and-leak.



In 2020, the top 5 threat categories for which CERT-EU released threat memos, which are informational deliverables, were:

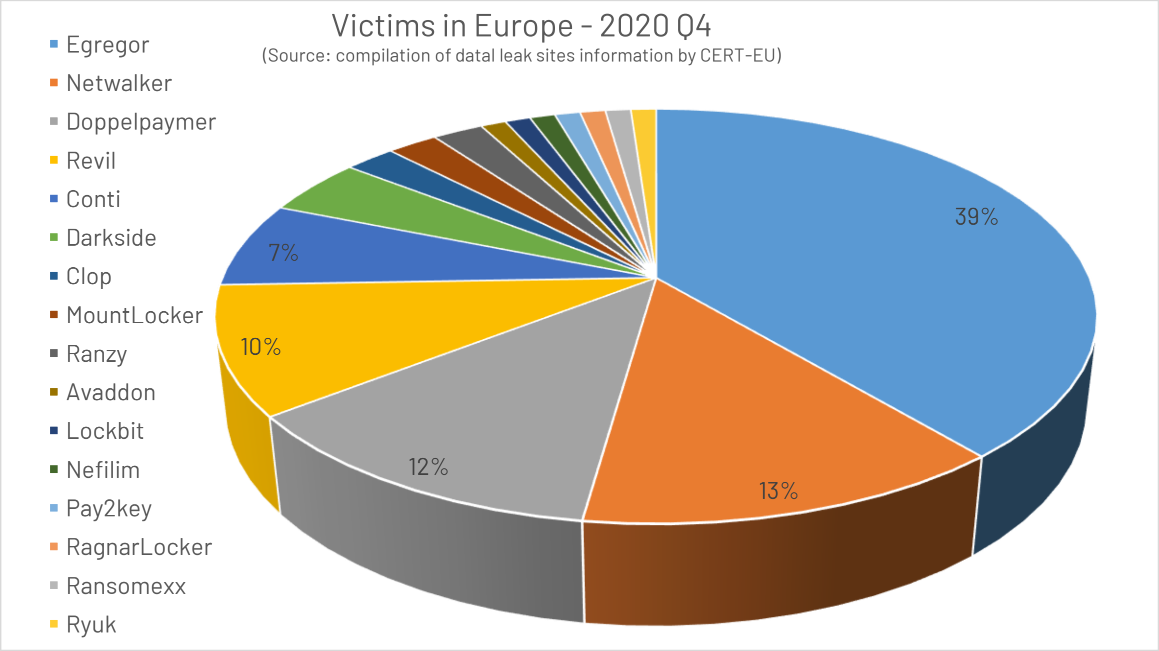
1. Extortion
2. APT attacks
3. Cloud
4. Malware and bots
5. Service providers.



Annex 2 – RaaS Activity in Europe in 2020

The RaaS threat landscape is very dynamic and frequently changing. The figure below provides a snapshot of the RaaS landscape in 2020 Q4. During that quarter, CERT-EU observed 16 main active RaaS operations in Europe.

Out of these 16, Egregor and Netwalker accounted for half of the infections. This is one likely explanation why law enforcement authorities attempted to disrupt these operations in January and February 2020.



Annex 3 – Major Hack-and-Leak Operations Since 2016

Date	Region, country or entity	Category	Type	Attribution[29]	Platforms	Details
Dec-20	EU	Unknown		Unknown	Darknet	In December 2020, the European Medicines Agency was affected by a cyberattack. Then, documents stolen from the agency were advertised on darknet forums.
Aug-20	Lebanon	Hacktivists		Unknown	Twitter	In August 2020, an entity dubbed @CyberTeamOFC claimed on Twitter to compromise and leak data from five Lebanese government websites.
Jun-20	US	Hacktivists		Unknown	Twitter	In June 2020, the hacktivist group "Distributed Denial of Secrets" leaked 269 GB of law enforcement data. Twitter suspended the @DDoSecrets account on 23 June 2020.
Apr-20	Europe, US	State sponsored	Tainted	Russia	Blog, Reddit	This campaign disseminated fake official US government documents.
Dec-19	UK	State sponsored		Russia	Reddit	This operation disseminated leaked US-UK trade documents.
Jan-18	IOC-WADA	State sponsored		Russia (Fancy Bears' International Hack Team)		This campaign disseminated documents from the Internal International Olympic Committee, World Anti-Doping Agency (IOC-WADA) to discredit the Russia-punishing decisions these organisations had taken.
May-17	France	State sponsored	Tainted	Russia	Wikileaks, Pastebin	An unknown actor dumped thousands of documents, obtained via data breaches, from the campaign of then French presidential candidate Emmanuel Macron on the website Pastebin. WikiLeaks and several researchers have identified links in the leaked documents to at least one Russian actor. The original hack has been linked to APT28.
May-17	Russia	State sponsored	Tainted	Russia		Documents were stolen from Russian journalists and used to create "tainted leaks" to discredit domestic and foreign critics of the Russian government.
Sep-16	US	State sponsored	Tainted	Russia (GRU created persona, "DC leaks")	Twitter, Web	This operation leaked email exchanges of government officials.

[29] When an operation has been attributed, the source of the attribution is provided.

Date	Region, country or entity	Category	Type	Attribution[29]	Platforms	Details
Sep-16	IOC-WADA	State sponsored		Russia (Fancy Bears' International Hack Team)		This operation leaked athlete's medical data.
Jun-16	US	State sponsored	Tainted	Russia (GRU created persona, "DC leaks", Guccifer 2.0)	Website	This operation targeted the US presidential election candidate Hilary Clinton. Leaked documents were acquired by breaching the Democratic Party National Committee and the candidate's campaign IT systems.

Annex 4 – Major Supply Chain Attacks Since 2014

Date	Compromised vendor	Malware	Description	Targets	Sector	Attribution[30]
Dec-20	SolarWinds	Sunburst	Compromise of SolarWinds Orion software.	Global (primarily the US)		Russia (SVR / APT29)[31]
Dec-20	Able Desktop	HyperBro	Operation StealthyTrident in Mongolia. Attackers compromised a chat app called Able Desktop.	Country (Mongolia)		China (APT27)
Dec-20	SignSight	PhantomNet	Operation SignSight in Vietnam. Attackers breached the website of the Vietnam Government Certification Authority (ca.gov.vn).	Country (Vietnam)	Government	China
Nov-20	WIZVERA VeraPort		WIZVERA VeraPort is a South Korean application that helps manage additional security software.	Country (South Korea)		North Korea (Lazarus)
Apr-19	ASUS	ShadowHammer	Trojanised ASUS Live Updater file (setup.exe).	Global		China (APT41)[32]

[30] When a supply chain attack has been attributed, the source of the attribution is provided.

[31] https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

[32] https://content.fireeye.com/apt-41/rpt-apt41/

Date	Compromised vendor	Malware	Description	Targets	Sector	Attribution[30]
Mar-19	Electronics Extreme		Two games and one gaming platform application were compromised to include a backdoor.	Region (Asia)	Game	Unknown
Jul-18	Infestation PointBlank		Southeast Asian video game distributor Infestation PointBlank.	Region (Asia)	Game	China (APT41)[33]
Sep-17	CCleaner		Backdoor was included in version 5.33 of the CCleaner application.	Global		Possibly China (APT41)[34]
Aug-17	NetSarang	ShadowPad	Software produced and distributed by NetSarang was modified to include an encrypted payload that could be remotely activated.	Global		China (APT41)[35]
Jul-17	M.E.Doc	NotPetya	Supply chain-focused attack on M.E.Doc software that delivered a destructive payload disguised as ransomware.	Global (primarily Ukraine)		Russia
Dec-15	Juniper Networks		Juniper Networks found "unauthorised" code embedded in an operating system running on some of its firewalls.	Global		Unknown
Sep-15	Apple iOS apps	XCodeGhost	XcodeGhost malware modifies Xcode IDE to infect Apple iOS apps. At least two popular ones were infected, including WeChat.	Global		Unknown
Dec-14			Online games distributed by a Southeast Asian video game distributor (Path of Exile, League of Legends, FIFA Online).	Region (Asia)	Game	Possibly China (APT41)[36]

[33] ibid.

[34] ibid.

[35] ibid.

[36] ibid.

10 years CERT-EU

THINK CONSTITUENT
CREATE VALUE

https://cert.europa.eu

secretariat@cert.europa.eu

@CERTEU