Cyber brief (June 2020)

CB 20-06 - Date: 03/06/2020 - Version: 1.1
TLP:WHITE

Europe and the European Union

The German authorities issued an arrest warrant for a Russian citizen in relation to the May 2015 breach of Bundestag IT systems. The activity is linked to APT28, associated with the Russian GRU intelligence agency.	Cyberespionage Political affairs
According to a report by the German security services, the Russian-nexus Berserk Bear threat actor has been on a long-term campaign to compromise German companies in the energy and water sectors.	Cyberespionage Energy Water
The Estonian Internal Security Service (KAPO) reported that in 2019, state-sponsored hackers had infiltrated the Estonian email provider Mail.ee targeting a small number of accounts belonging to "persons of interest."	Cyberespionage Political affairs
Since May 11, high-performance computing (HPC) services in several European countries have reported temporary shutdowns of their systems due to breaches. The activity has been linked to cryptomining.	Cybercrime Technology
A cyberattack on Norfund, the Norwegian government fund for developing countries, led to the transfer of $10 million to an account controlled by cybercriminals.	Cyberattacks Fraud
The largest European private hospital operator, Fresenius, suffered a ransomware attack that affected its IT systems.	Cyberattacks Healthcare
The airline EasyJet suffered a cyber-breach resulting in the leak of email addresses and travel details of approximately 9 million customers.	Cyberattacks Airlines
The UK Energy company Elexon experienced a cyberattack leading to the disruption of its IT network and preventing the use of employee laptops.	Cyberattacks Energy
The French newspaper Le Figaro exposed more than 7,4 billion records, including readers' personal, data due to a technical error.	Accidental Personal data

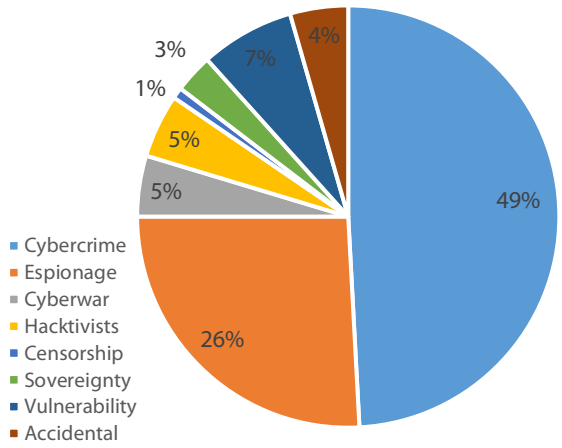
World

The US and the UK have issued alerts regarding Chinese targeting of organisations conducting COVID-19 research, in particular those involved in the search for a vaccine.	Cyberespionage COVID-19
Recent intrusions at the WHO and a major US pharmaceutical company have been attributed to the Iranian-nexus APT35 group.	Cyberespionage Health
The popular messaging and social media platform WeChat, of Chinese origin, contains communication surveillance features that also work on content shared by international users.	Cyberespionage Social media
The Chinese-nexus APT15 (also known as Ke3chang) has developed new malware dubbed Ketrum by merging features and code from their Ketrican and Okrum backdoors.	Cyberespionage
A hacker claimed a breach of Microsoft's Github account, accessing 500GB of internal code. Microsoft later confirmed the breach. The same actor started trading stolen data from at least 11 companies.	Cybercrime Leaks
Recent research has uncovered a new Emotet module that attempts to spread over WiFi networks. It enumerates wireless networks within its range and then tries to guess or crack their passwords.	Cybercrime
The highly organised, Russian-speaking cybercrime entity Netwalker is bringing together many recently emerged TTP trends and combining them into an efficient union of advanced crimeware.	Cybercrime
In a tit-for-tat reaction, Israel has highly likely conducted a cyber operation against the Iranian port of Hormuz that resulted in disruption of its services. This was in response for alleged Iranian attempts to disrupt Israeli water services.	Cyberwar Transport Water
Taiwanese authorities believe that the ransomware attack on a state oil company was a mainland Chinese operation by actors operating under the Winnti Umbrella group.	Cyberwar Ransomware
Researchers of the security company Checkpoint reported on a novel attack technique targeting corporate environments using an unspecified mobile device management (MDM) system.	Cyberattacks Corporate IT
Researchers from the Carnegie Mellon University analysed about 200 million tweets discussing COVID-19 since January and concluded that about 45 percent of all involved Twitter accounts were likely automated.	Disinformation COVID-19
Apple iOS v.13 has been described as "full of exploits" by the exploit broker Zerodium that lowered the prices offered for discovered issues.	Vulnerabilities IT

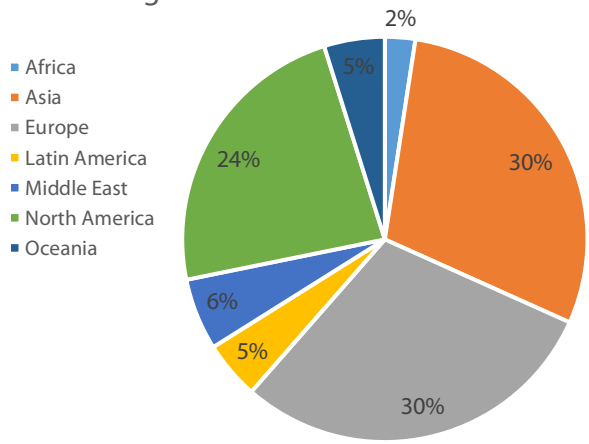
Threat statistics

(May 2020)

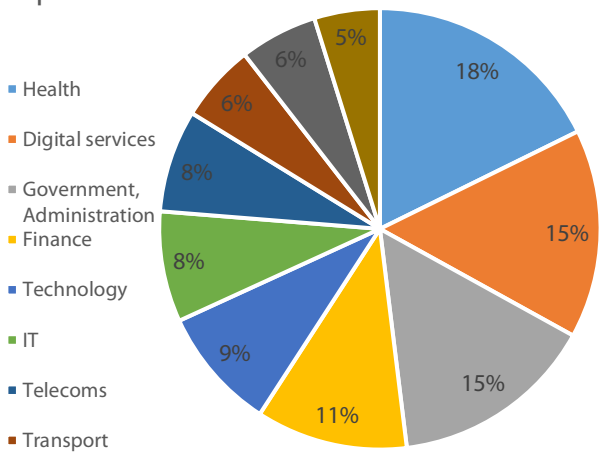
Threat categories



Affected regions



Top 10 affected sectors



Top 10 malware families

1	Mofksys
2	UrSnif
3	Qbot
4	DanaBot
5	GandCrab
6	Kovter
7	Agent Tesla
8	Emotet
9	Tinba
10	NjRAT