CERT-EU

Cyber brief (July 2020)

CB 20-07 - Date: 03/07/2020 - Version: 1.0
TLP:WHITE

Europe and the European Union

According a French newspaper, France's Foreign Intelligence Agency DGSE attributed a 2018 cyberattack to the country's power grid to a Russia based threat actor.	Cyberwarfare Critical infra
The EU Disinfo Lab has uncovered a disinformation campaign in French alternative media. They report the operation to be liked to Russian Military Intelligence (GRU) unit 54777, responsible for psychological warfare.	Cyberwarfare Disinformation
European and Middle Eastern aerospace and military organisations were targeted by fake HR e-mails offering jobs. The researchers investigating the attack suspect North Korea's Lazarus Group to be behind the attack.	Cyberespionage Defence
Encrypted communication provider EncroChat has ceased operation after a malware attack they claim originated from government entities. Seen the popularity of their product among criminals, their hypothesis is not implausible.	Sovereignty Judicial
A remote access malware dubbed GuLoader was found to be quasi identical to protective software CloudEye from an Italian supplier.	Cybercrime Supply chain?
Austrian, German and Swiss victims of ransomware Thanos have refused to pay the criminals for decryption of affected systems.	Cybercrime Ransomware
Conduent, a large IT provider, fell victim to ransomware at the beginning of June. Its European operations were "temporarily hampered" – likely referring to the 9 hour downtime the company suffered.	Cybercrime Ransomware
Accessories giant Claire's was breached in an apparent credit card info stealing attack. Magecart, a Javascript stealer, was deployed.	Cybercrime Credit card info
A multi-level marketing company leaked more than 30.000 Italian sales agent's personal data through an unsecured Amazon S3 bucket.	Leakage Personal Data
Austria's largest telecom provider A1 admitted to a security breach following a whistleblower's complaint. The infection leads back to November 2019.	Telecom Whistleblowing

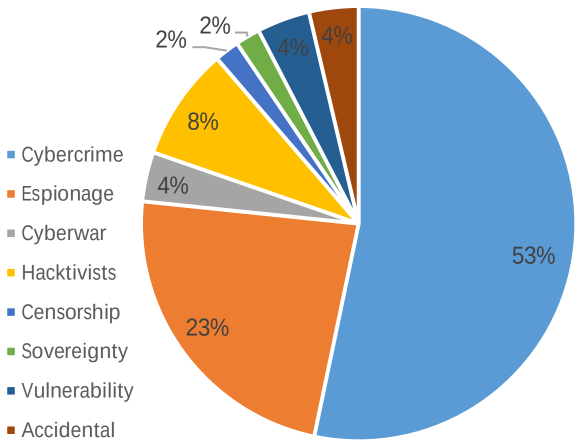
World

Australian authorities disclosed ongoing malicious cyber activity against Australian networks. Some Australian media quote 'senior sources within government' attributing the attack to China.	Cyberwarfare
Taiwan's Presidential Office was targeted by a tainted leaks campaign around the same time that a wave of ransomware campaigns hit at least ten Taiwanese companies.	Cyberwarfare Disinformation
Twitter announced it had discovered disinformation campaigns originating in China, Russia and Turkey, after having done the same with Saudi Arabian, UAE, Egyptian and Ecuadorian campaigns in the previous months.	Cyberwarfare Disinformation
Video conferencing platform Zoom was accused of censoring certain accounts held by users based outside China and related to the 1989 Tiananmen square massacre. The platform quickly reinstated the accounts, but the initial response highlights the issue of tech companies working in or with China.	Censorship Digital services
A Chinese software designed for paying local taxes was found containing malware. It reportedly targeted foreign companies operating within China.	Cyberespionage Tax
APT group InvisiMole, known for likely espionage through activation of microphones and webcams on victim machines, was shown having close relations with Russian-associated actor Gamaredon.	Cyberespionage
Researchers at IBM X-Force uncovered cyberattacks against supply chains for procurement of Personal Protective Equipment (PPE), a vital instrument in the treatment of COVID-19 patients.	Cyberespionage Health
Google's Threat Analysis Group announced another targeting of the US presidential campaign. With the trail leading to China this time, both Biden and Trump staff members received phishing e-mails.	Cyberespionage Elections
News reports this month disclosed the largest DDoS attack ever recorded. Targeting AWS last February, traffic peaked at 2.3 Tbps. The attack likely targeted a single AWS customer.	DDoS Cloud targeting
Ransomware operator REvil has started auctioning off data stolen from their victims to the highest bidder.	Cybercrime Ransomware

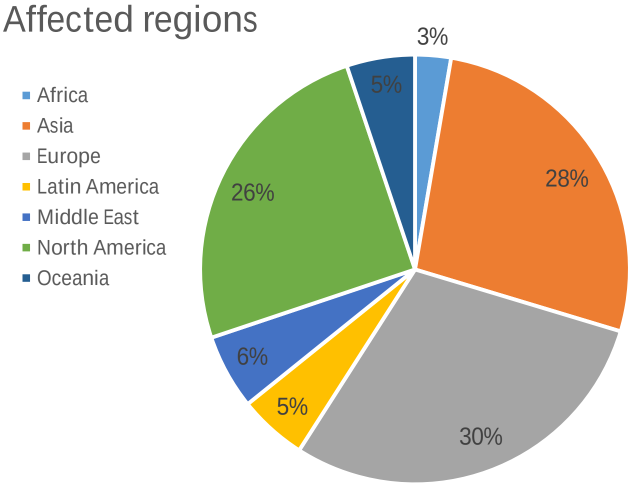
Threat statistics

(June 2020)

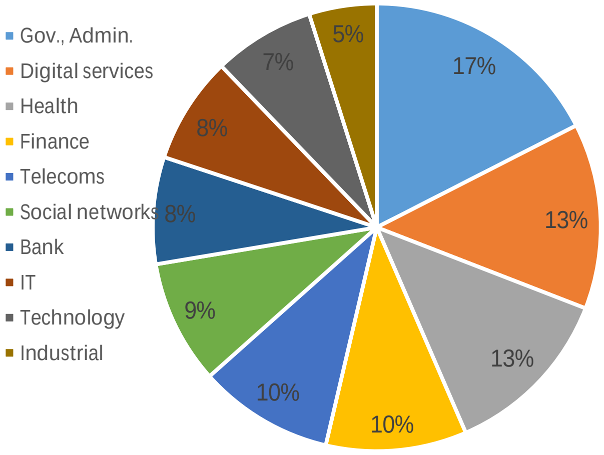
Threat categories



Affected regions



Top 10 affected sectors



Top 10 malware families

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