RANSOMWARE ATTACKS

ROOT LEVEL RESOURCES

As the world confronts the novel pandemic, borders close, businesses teeter on the brink of solvency, and political conflicts between countries escalates, one index that keeps rising steadily is cybercrime.
During the pandemic, the number of cyberattacks has been rapidly increasing, the culprits being either "unaffiliated" cybercriminals or pro-state hacker groups taking advantage of the COVID-19 agenda with spyware, encryption tools, and backdoors. Attackers have been honing their skill of penetrating corporate networks by targeting remote workers and infecting their computers with malware, through which they gain access to the employer company's network.

Some of the main sources of problems for companies are vulnerable versions of software in public services as well as weak passwords. Exploiting these vulnerabilities, perpetrators use ransomware with the goal to halt business applications and encrypt valuable business data, thus rendering both the data and the applications unavailable to the owner.
Ransomware has become so popular that ready-made Ransomware-As-A-Service projects for Linux, MacOS and Windows – such as RAASNet – can be found on GitHub.

Ransomware partner programs

Not always ransomware developers have sufficient means and capabilities to penetrate corporate networks. Recently they started to solve this problem by offering two types of affiliate programs:

Public

involving open search for partners on underground forums

For instance: Revil; BuranZeppelin; NetWalker; Lockbit; Avaddon; Exorcist; Thanos; Phobos; SunCrypt.

Private

clandestine and intended as a way to collaborate with other cybercrime groups (e. g., APT groups) and trusted users

For instance: Maze; JSWORMNemty; Ako.

It's noteworthy that many affiliates choose to keep a low profile and only the analysis of the hacker community activity and of the incident response information allows for identifying some of them.

Compromise vectors

The following table reveals cybercrime affiliate programs and the methods of gaining initial access used by those running them:

Ransomware	Phishing	Exploit Public-Facing Application	External Remote Services	Supply Chain Compromise
Revil	✓	✓	✓	✓
MegaCortex	✓		✓	
Maze	✓	✓	✓	
Dharma			✓	
JSWORM → Nemty	✓	✓	✓	
Buran → Zeppelin	✓	✓	✓	
NetWalker	✓		✓	
Ako	✓	✓	✓	
Lockbit			✓	
Avaddon	✓	✓		
Thanos	✓		✓	

Post-compromise strategy

After the initial break-in, many ransomware operators first try to gain higher-level access rights (via exploits or post-exploitation frameworks), then attempt to gain access to other user accounts utilizing specialized software (Mimikatz, LaZagne, and the like) or bruteforcing.

Perpetrators may also survey targeted networks in advance using quite legitimate network scanners or frameworks (e. g., Cobalt Strike, Metasploit), gaining information about the system, groups, network resources, password policies, domain trust relationships, etc.

The table below shows different frameworks used by ransomware operators:

Ransomware	Cobalt Strike	Metasploit	CrackMapExec	PoshC2	Koadic	PowerShell Empire
Ryuk	✓	✓				✓
REvil		✓	✓			
Maze	✓	✓				
DoppelPaymer				✓	✓	
Clop	✓	✓				
Lockbit			✓			

Stealing and publishing data

In the past, attackers would only encrypt important data and demand ransom from users, but since 2020 they have been employing a new technique: before encrypting the data, they copy it all to their servers with the idea of continuing to blackmail the victim. Typically they use for this standard protocols – HTTP, HTTPS, FTP – and legitimate cloud storage (in rare cases, email and messengers are used).

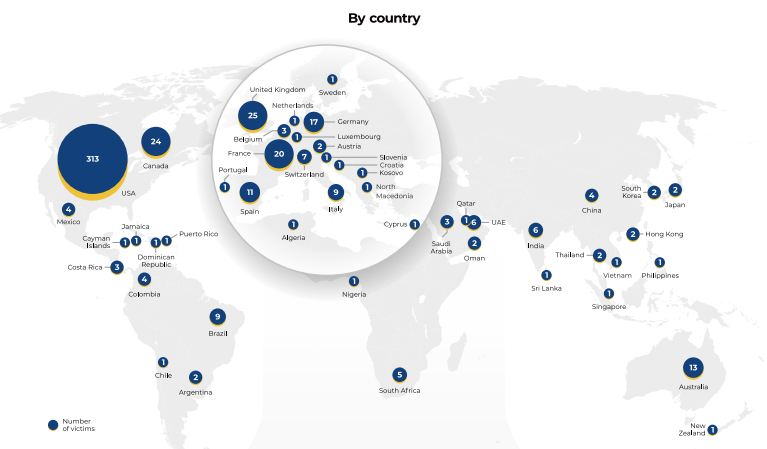
At this point, if the victim refuses to pay the ransom, the valuable data will not be just lost to them but made publicly available by the ransomware operators. To increase profits, some groups may choose to auction off the data instead of simply posting it online.

Attack statistics

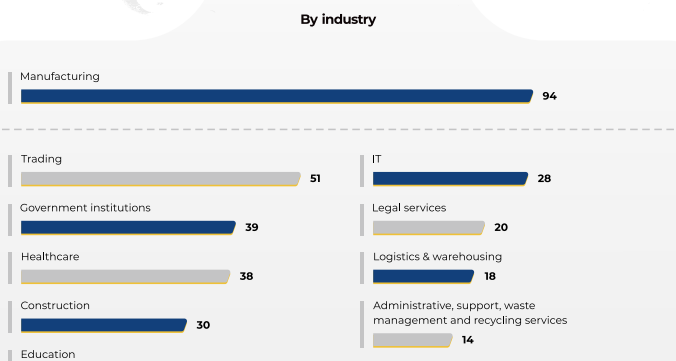
ROOT LEVEL RESOURCES

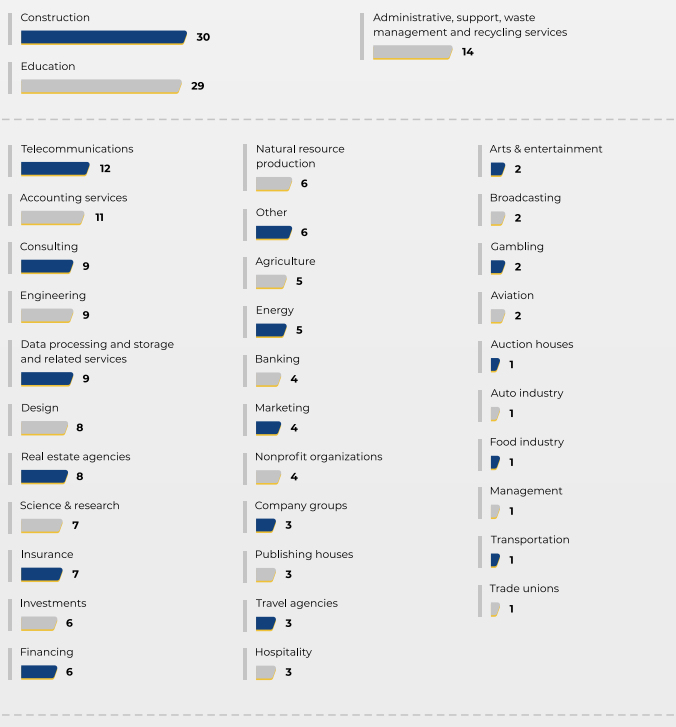
Both small local companies and transnational giants fall victim to ransomware attacks. Last year more than 500 successful cyberattacks targeting companies in over 45 countries have been detected. The total number of successful attacks is much larger, but many affected companies prefer to pay the ransom without reporting the incident. In other cases, the data obtained from the attack has been kept private.

By country



By industry





Maze and REvil are the most active ransomware titles since 2020, accounting for over 50% of successful attacks. The second tier is comprised of Ryuk, NetWalker, and DoppelPaymer.

Number of victims and damage estimate

ROOT LEVEL RESOURCES

Manufacturing has been the most heavily targeted sector. In general, half of all attacks have targeted manufacturing, trading, government institutions, healthcare, construction industry, and educational institutions. However, affiliates tend to choose the easiest targets for their attacks, which explains the broad distribution across different industries.

Ransomware/ Total number of victims	Country	Industry	Average ransom amount/ Potential damage
Maze 155	93 USA 8 Canada 6 France 6 Italy 6 United Kingdom	30 Manufacturing 19 Trading 15 Construction 8 Administrative, support, waste management, recycling services 7 Healthcare	$2 420 000 $375 100 000
REvil 103	63 USA 7 United Kingdom 5 Australia 4 Switzerland 3 Canada	20 Manufacturing 17 Trading 10 IT 6 Legal services 4 Government institutions	$300 000 $30 900 000
Ryuk 62	53 USA 5 Spain 1 Australia 1 United Kingdom 1 Germany	16 Government institutions 14 Education 14 Healthcare 3 Publishing houses 3 IT	$1 451 500 $89 993 000
NetWalker 49	28 USA 6 France 4 Canada 2 United Kingdom 1 Austria	14 Manufacturing 6 Healthcare 5 Education 4 Trading 3 Logistics & warehousing	$720 000 $35 280 000
Pysa 25	5 USA 3 United Kingdom 2 Canada 2 France 2 Mexico	5 Healthcare 3 Government institutions 3 Manufacturing 2 Construction 2 Education	Unknown Unknown
DoppelPaymer 53	35 USA 5 France 3 Canada 1 Saudi Arabia 1 Qatar	8 Trading 7 Government institutions 6 Manufacturing 4 Logistics & warehousing 3 Construction	$1 143 500 $60 605 500
Nefilim 13	3 Brazil 3 India 1 Germany 1 France 1 Switzerland	4 Manufacturing 2 Construction 2 Natural resource production 1 Logistics & warehousing 1 Administrative, support, waste management, recycling services	$100 000 $1 300 000
Ragnar 10	7 USA 1 Portugal 1 Germany 1 Singapore	2 Marketing 2 Legal services 1 IT 1 Manufacturing 1 Construction	$7 750 000 $77 500 000
Clop 15	7 Germany 2 USA 1 Spain 1 Austria 1 United Kingdom	6 Manufacturing 2 IT 2 Logistics & warehousing 1 Gambling 1 Government institutions	$400 000 $6 000 000
Ako 9	6 USA 2 United Kingdom 1 Canada	2 Construction 1 Legal services 1 Design 1 Engineering 1 Manufacturing	$300 000 $1 800 000
Avaddon 1	1 USA	1 Construction	$7 500 $7 500
Sekhmet 6	3 USA 1 Brazil 1 United Kingdom	2 Manufacturing 1 Legal services 1 IT	Unknown Unknown
Snake 3	1 Germany 1 Argentina 1 Japan	1 Healthcare 1 Energy 1 Company groups	Unknown Unknown
MegaCortex 1	1 USA	1 Data processing and storage and related services	Unknown Unknown
Conti 16	13 USA 2 Canada 1 Spain	3 Manufacturing 2 Hospitality 1 IT 1 Insurance 1 Healthcare	$200 000 $3 200 000
SunCrypt 2	1 USA 1 Canada	1 Manufacturing 1 Design	$400 000 $800 000
WastedLocker 1	1 USA	1 Manufacturing	Unknown Unknown

Unfortunately, the actual damage is difficult to assess. The estimate must include the amounts paid by victims, losses incurred during downtime, and costs of restoring normal operation, not to mention the fact that finding out about an attack may be a challenge unto itself, since many companies choose to pay ransom and keep the whole thing quiet.

The data above describes is related to known incidents only and shows the lower estimate of damage. But this is just the tip of the iceberg. For example, there are only 62 known incidents involving Ryuk, which was actively spread by the banking trojan Trickbot. At the same time, according to Group-IB data, the owners of the Trickbot botnet have successfully encrypted over 2,500 different networks over the past year, using ransomware like Ryuk (later Conti), Kraken, and Thanos. The 62 known incidents are only 2.5% of this total, which means the actual damage is much greater.

Selling data by groups close to intelligence agencies

ROOT LEVEL RESOURCES

In an effort to secure additional funding, some pro-state hacker groups turn to selling access to corporate networks or using ransomware, like common criminals. The following are just a few known examples of pro-state groups making money with ransomware:

The group known as Lazarus returned to ransomware development and attacked European companies using VHD Ransomware. The hackers gained access via a vulnerable VPN gateway, upgraded their privileges to administrator, and installed the DacIs backdoor. Then they spread across the victim's network and encrypted files with a combination of AES-256 in ECB mode and RSA-2048.

In May 2020, Taiwanese authorities blamed the Chinese hackers from APT41 for a ransomware attack on the island's energy and technology companies, including the state-owned shipper of oil products CPC Corp. The attack did not affect CPC's operation directly but prevented customers from using CPC Corp. payment cards to buy gas. This wave of attacks involved a new ransomware, ColdLock. Analysis has revealed similarities between ColdLock and two previously known ransomware families, notably Freezing and the EDA2 educational ransomware.

In the spring of 2020, a group of Chinese hackers called IronTiger used the HybirdRansom ransomware against companies in the Asia Pacific region. The ransomware included several components, Locker, Loader, and Cryptor, that would run one after another to lock the compromised machine and encrypt files.

ROOT LEVEL RESOURCES

It is our firm belief that constant data exchange, joint efforts to maintain global cyber-stability, and development of partnership ties between private companies and international law enforcement agencies constitute an effective way of fighting cybercrime. Worldwide awareness of cybersecurity will help preserve and protect the freedom of communication and common opportunities of the cyberspace.