THREAT INTELLIGENCE REPORT 2021

rewterz

EXECUTIVE SUMMARY

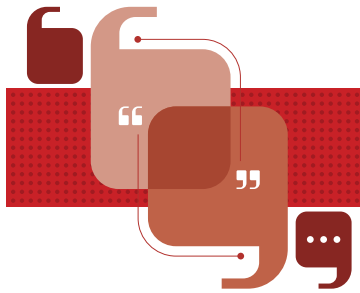
Rewterz has developed a unique space in the world of cybersecurity. So much so that its Managed Security Services and Threat Intelligence services are utilized by organizations all around the world for improved organizational security. Our cybersecurity experts provide holistic information security services on a large scale, and our Threat Intelligence teams release advisories, blogs, reports, and alerts. All of which are useful to keep cybersecurity professionals updated with relevant and emerging threats. Rewterz Threat Intelligence annually releases a consolidated Threat Intelligence report to summarize the most prominent cyber threats from this year, detected and highlighted by our various Security Operations Centers (SOC) and sensors.

Instead of a maze of complex numbers, we are here to transform the market by delivering well-researched data that you can utilize. The actionability of the data we offer provides organizations with a competitive advantage and obvious planning opportunities. We are employing our world-class abilities to analyze data from hundreds of thousands of protected endpoints and servers to track malware infection attacks, phishing campaigns, spoofing, identity theft, financial fraud, and other fraudulent activities.

To cope with the growing techniques of cybercrimes, our SOC team utilizes our Threat Intelligence capabilities and manages real-time data through our Security Orchestration Automation and Response (SOAR) platform, SIRP. Our orchestration and automation platform helps reduce the redundant processes of incident handling and lets analysts focus on more complex tasks. SIRP automates the usage of Threat Intelligence data for our SOC teams, equipping them for smooth incident handling, vulnerability management, access control regulation, and risk management, meanwhile saving a considerable amount of their time. We also create and deploy cybersecurity solutions to solve issues that clients have in a variety of sectors.

In a world of shifting cyber dangers, the rising risks in 2021 remind us that we must keep ahead of the curve to safeguard the next frontier of cyber resilience. It exposes how attackers are exploiting global unrest by targeting critical businesses and common weaknesses resulting from the move to remote labor. Threat actors are increasingly focusing on new industries, employing higher-pressure techniques to raise infection consequences and releasing payloads more quickly, making trusted detection technologies ineffective. The number of possible responses is growing.

We have perfected the art of threat intelligence and are now ready to assist you in strengthening your defense and mitigating risks. This detailed analysis investigates the most significant cyber-attacks that happened from 2020 to 2021. This extensive report contains an analysis of attacks detected from 2020 to 2021. It includes the top attacking countries, most common malware deployed, most active Advanced Persistent Threats, top phishing campaigns, top-targeted ports, most common attack vectors, most targeted industries, most exploited vulnerabilities, and much more. We hope that you find this report useful. Feel free to contact us with any feedback.



THREAT INTELLIGENCE FOR ENHANCED CYBER SECURITY

Threat Intelligence (TI) is the collection of data on current or emerging threats to assets, including context, tactics, consequences, and recommendations.

It is the information that is gathered and evaluated by a company to better understand the motivations, targets, and attack patterns of a threat actor. This information is used to prepare, prevent, and identify cyber threats looking to take advantage of valuable resources. Threat intelligence is an essential component of decision-making processes that aid in the development of information security plans. In the fight against breaches, threat information helps companies to make faster, more informed security choices and shift their behavior from reactive to proactive.

TI is gleaned from the most recent vulnerabilities that aid in determining the level of security coverage and threat exposure that these measures provide to an organization's cybersecurity. It also advises businesses on the kind of personnel training that their cybersecurity requirements necessitate. Threat Intelligence usually assists in identifying and targeting threat elements before they develop into an assault, allowing you to shift from a reactive to a proactive mindset.

THREAT ACTIVITY SUMMARY 2021

COVID-19 AS A VULNERABILITY

Cyberattack frequency increased by 400% during the COVID-19 pandemic.

Threat actors took advantage of the destruction and instability caused by the pandemic to exploit vulnerabilities and endpoints that were not secured before. The increase in remote workforce, VPNs (virtual private networks), and cloud services also provided attackers and cybercriminals with plentiful opportunities to steal data and conduct cyber attacks.

Phishing became the cyberattack of choice during the pandemic because even unsophisticated cybercriminals could conduct highly successful attacks using mediocre knowledge. To make matters worse, most employees working from home had little to no awareness regarding cyber security best practices and therefore, were more vulnerable to these attacks.

S.NO	TOP PHISHING EMAIL SUBJECTS
1	VISIT THIS LINK
2	Fancy a personalised winners logo for £50?
3	E-statement
4	paid invoice-transfer
5	Returned mail: see transcript for details
6	BUSINESS PROPOSAL/OFFER
7	Your New FedEx Biling Online invoice is attached
8	Failed delievery Attempt (Shipping Documents)
9	Hi.. i have an important transaction to discuss with you
10	Hi dear@,@

ACTIVE RANSOMWARE VARIANTS

A variant to software-as-a-service (SaaS), Ransomware-as-a-service (RaaS), is the latest trend in cybercrime.

Ransomware developers are selling their malware as a subscription service. The terrifying concept is a growing threat for businesses as petty cyber theft (low-level attacks and ransom demands) have become the norm and easily accessible to unsophisticated threat actors. With COVID-19 phishing schemes also on the rise, Ransomware-as-a-Service (RaaS) isn't going anywhere.

Financially and ideologically motivated threat actors and cybercriminals embrace RaaS. This is due to its higher efficacy and frequent updates by the distributors. REvil is a RaaS variant most active in the variant. Other ransomware observed in the region are mentioned below.

From these ransomware, REvil aka Sodinokibi has been most active in the region. The ransomware usually targets victims, infecting systems via Microsoft Office documents. After encryption, a ransom note is found on infected systems. Their targets are government officials and offices. Dridex and Ursnif are sophisticated strains of banking malware that target Windows platform, delivering spam campaigns to infect computers and steal banking credentials and other personal information to facilitate fraudulent money transfers. Ryuk and SNAKE are one of the nastiest ransomware going around. They will lock your files or systems and hold them hostage for ransom. This type of ransomware is used in targeted attacks, where the threat actors make sure that essential files are encrypted so they can ask for large ransom amounts.

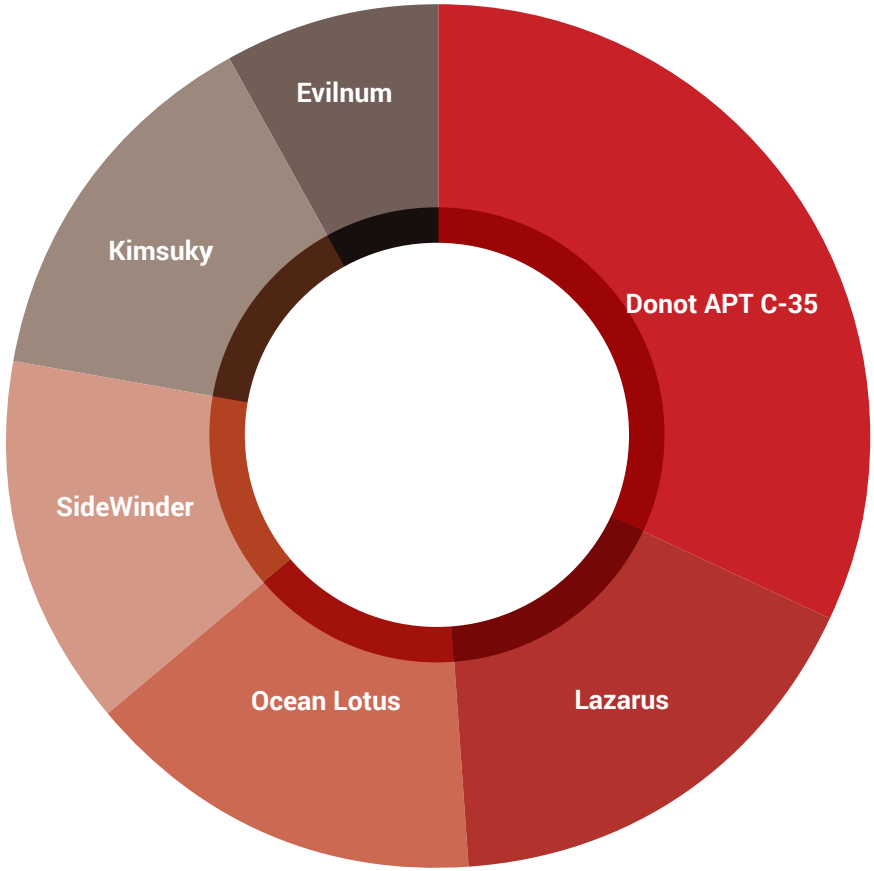
STATE-SPONSORED APT GROUPS

Advanced Persistent Threat (APT) groups are government-funded attackers that are built and endorsed to support nations or attack competing states. Some of the most common cyber espionage groups are from Iran, China, North Korea, Russia, Pakistan, India, Gaza, and Vietnam. These APT groups mostly target the financial, health, energy, and government sectors of opposing or enemy states and countries. However, the nuclear industry is the hot target of these groups.

The objective behind attacking these government, finance, and telecommunications sectors is to spy on enemy states and gather state secrets or to disable or destroy infrastructure. These APT groups have changed their stance from defensive to offensive and now proactively attack and target critical infrastructure.

TOP APT (ADVANCED PERSISTENT THREAT) GROUPS

S.NO	TOP APTS	%
1	Donot APT C-35	32%
2	Lazarus	17%
3	Ocean Lotus	15%
4	SideWinder	14%
5	Kimsuky	14%
6	Evilnum	8%



ZERO-DAYS EXPLOITED IN THE WILD

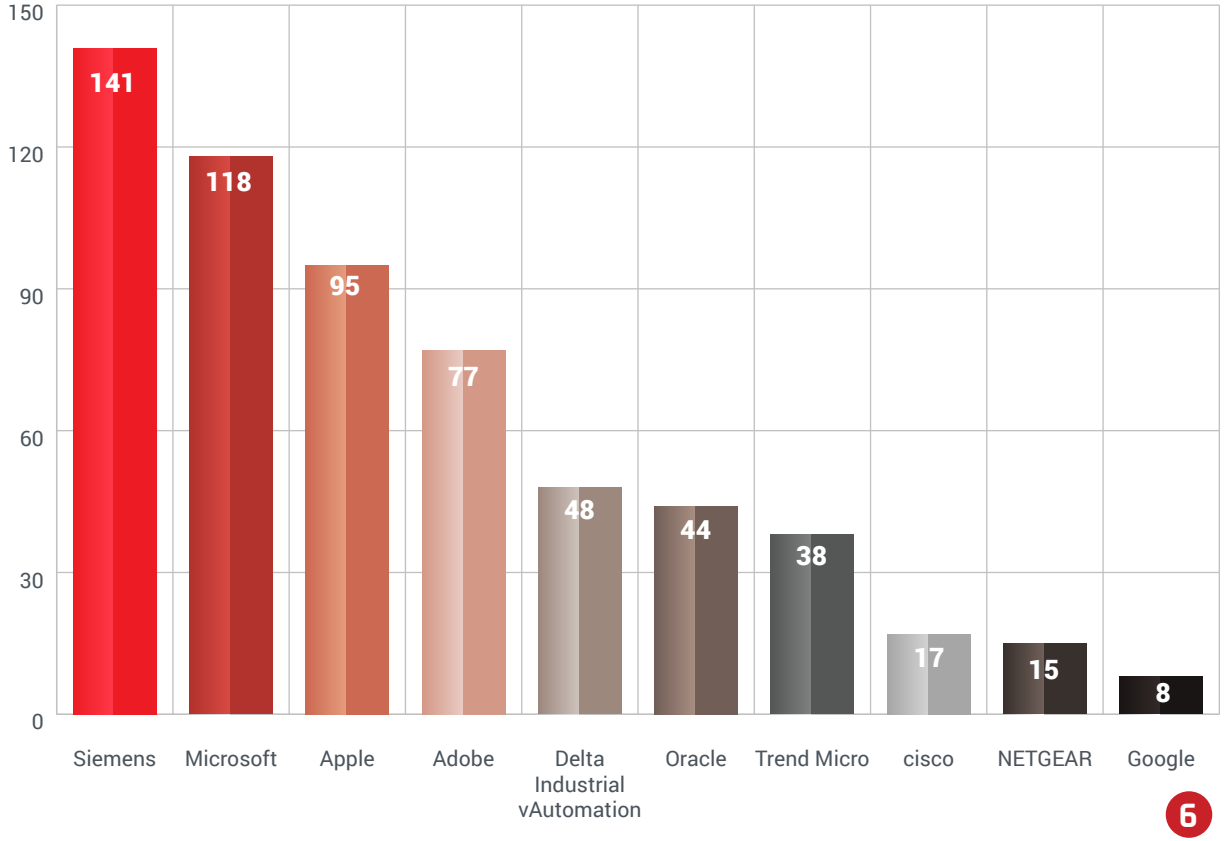
2021 has been a record-breaking year for zero-day discoveries.

Our Threat Intelligence team has reported more zero days this year than they did in previous years. This spike in zero-days can be attributed to better disclosure policies and enhanced detection capabilities. Vendors like Microsoft, Android, and Apple have been proactively informing clients about the exploitability of vulnerabilities in their products.

Another possible reason for this increase is that exploitation of zero-days is considerably easier than conducting other attacks. Zero-days also offer a more sophisticated and reliable attack vector than other attacks.

MOST ZERO-DAYS OBSERVED

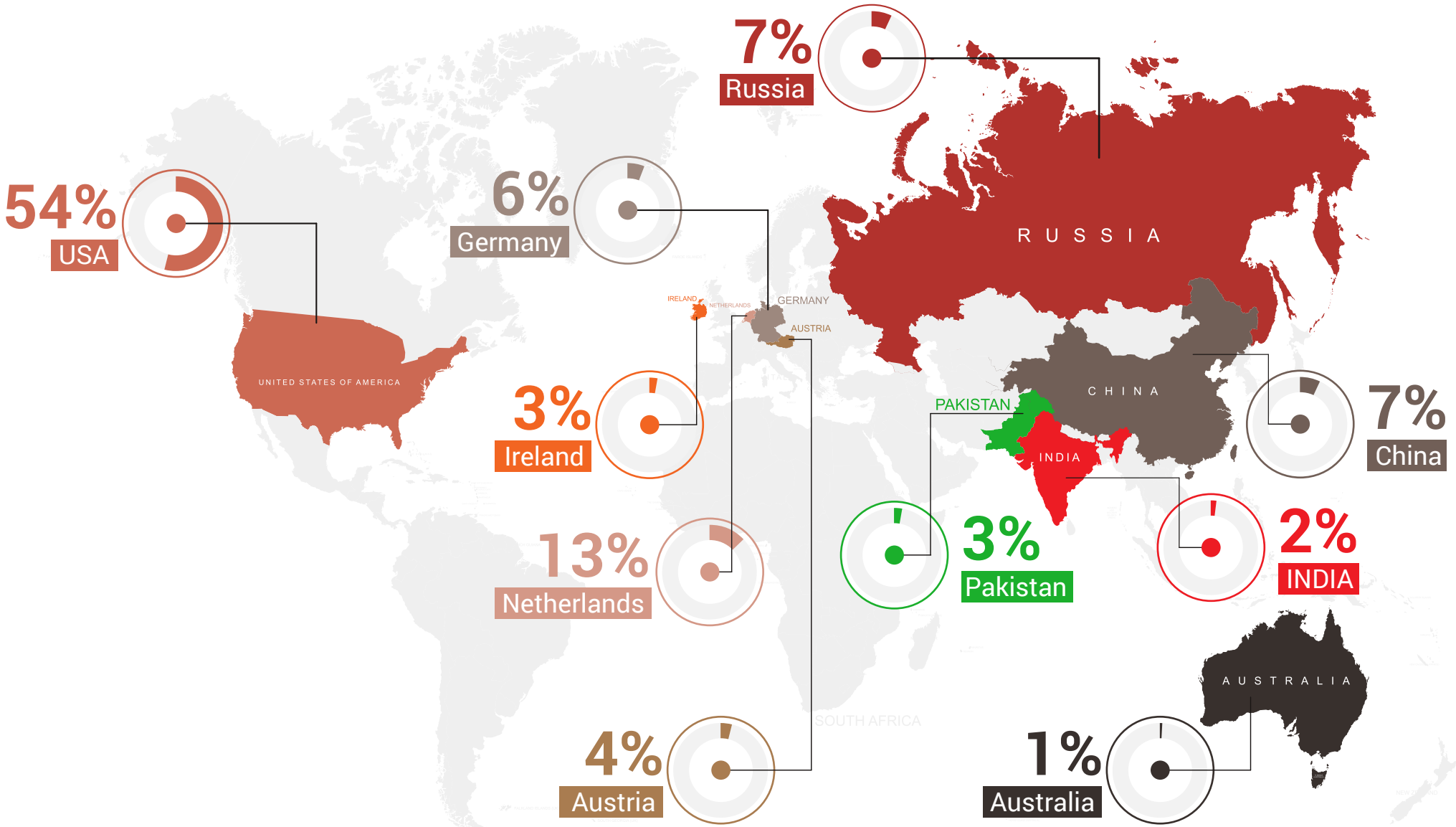
S.NO	VENDOR	COUNT
1	Siemens	141
2	Microsoft	118
3	Apple	95
4	Adobe	77
5	Delta Industrial Automation	48
6	Oracle	44
7	Trend Micro	38
8	cisco	17
9	NETGEAR	15
10	Google	8



CYBERSECURITY INSIGHTS

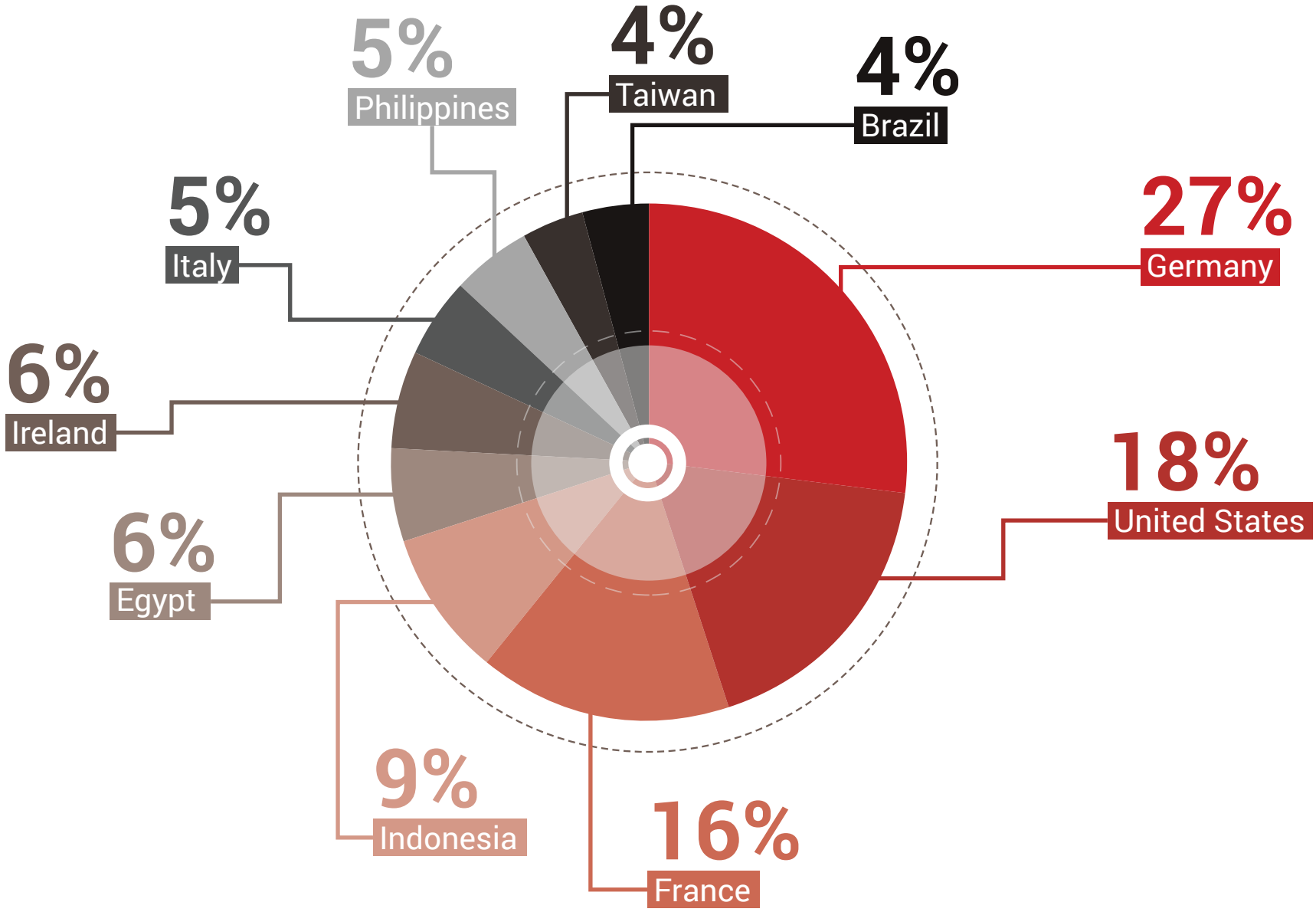
TOP ATTACKING COUNTRIES

When comparing the attacking countries from 2019 and 2020 to 2021, we notice that the United States has gone back to being the biggest attacking country, Russia that topped this list in 2020 has gone to 3rd place with the Netherlands emerging as a big threat. China is not far behind Russia and is responsible for a considerable number of cyberattacks. Below is a list of top attacking countries.



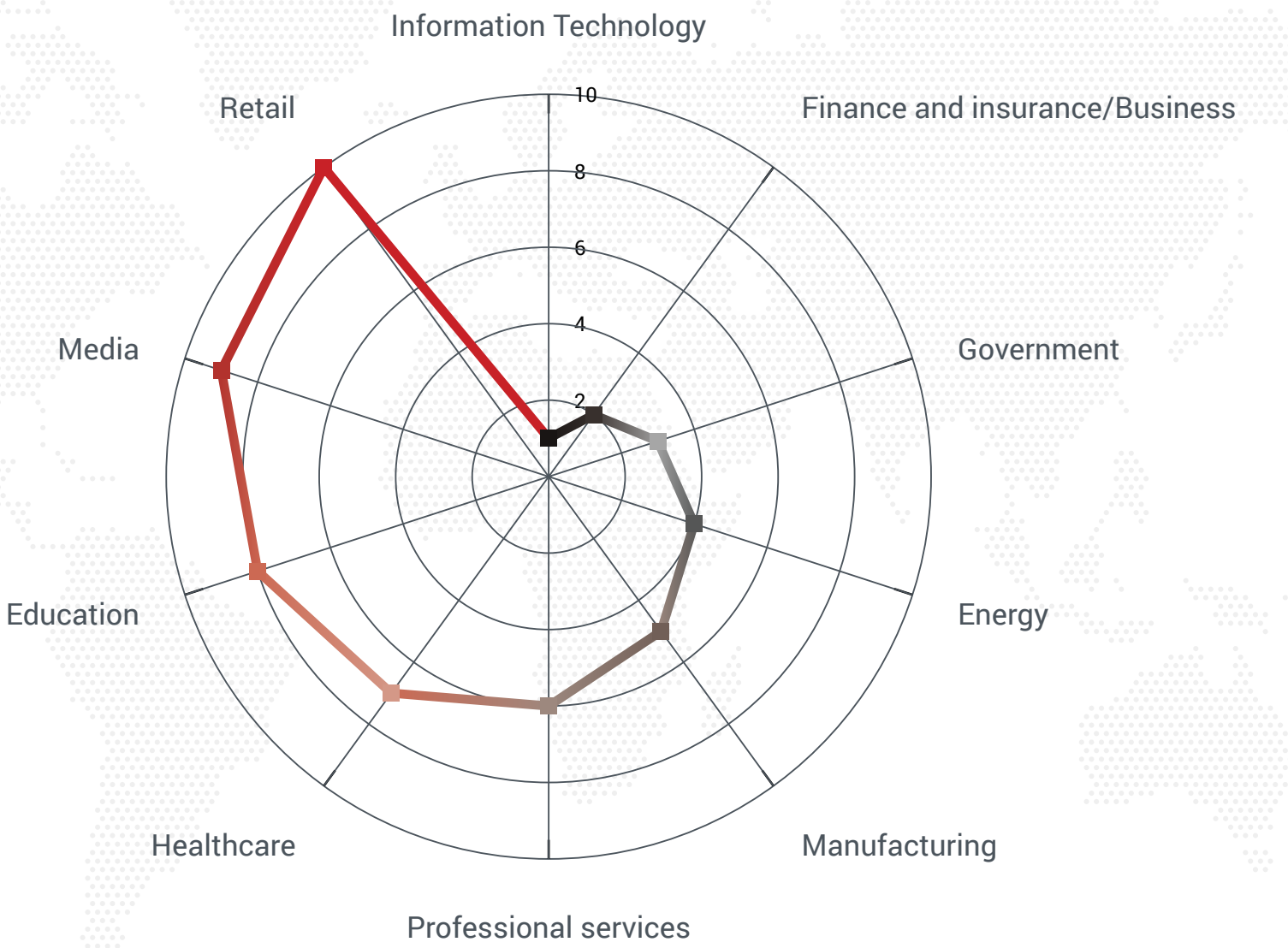
TOP TARGETED COUNTRIES

Cyberattacks have taken the world by storm. The USA tops the countries best prepared for cyberattacks, However, It is still the second most attacked country in the world. Germany emerged as the country which is at the greatest risk of cyberattacks. France, like the USA, is also on the list of countries most prepared for cybercrime, and yet also the recipient of major cyberattacks, the irony.



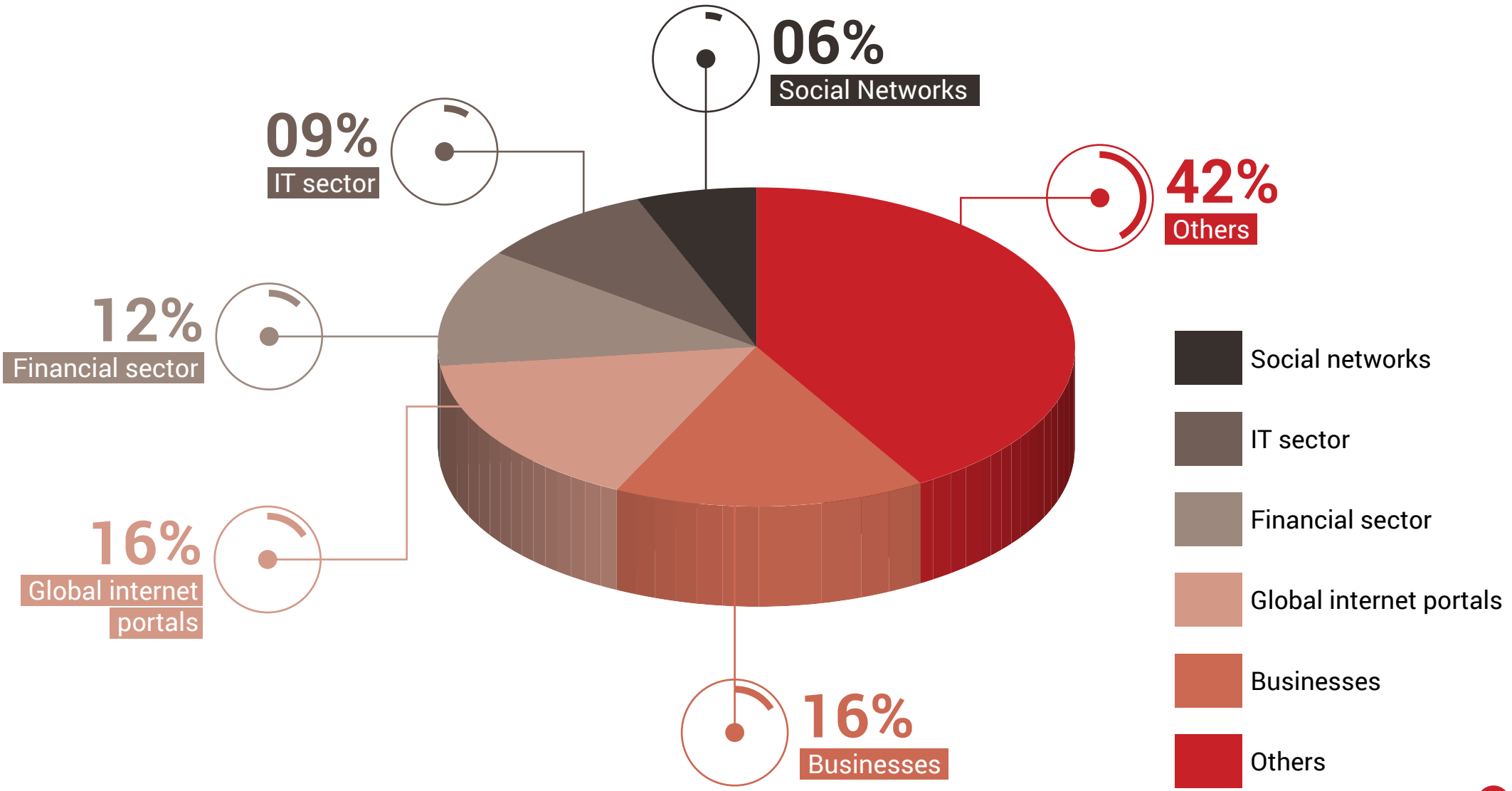
TOP TARGETED SECTORS

The most targeted sectors are Information Technology and Finance, and the same trend was observed in 2020. The Government and energy sectors have also undergone major cyberattacks.



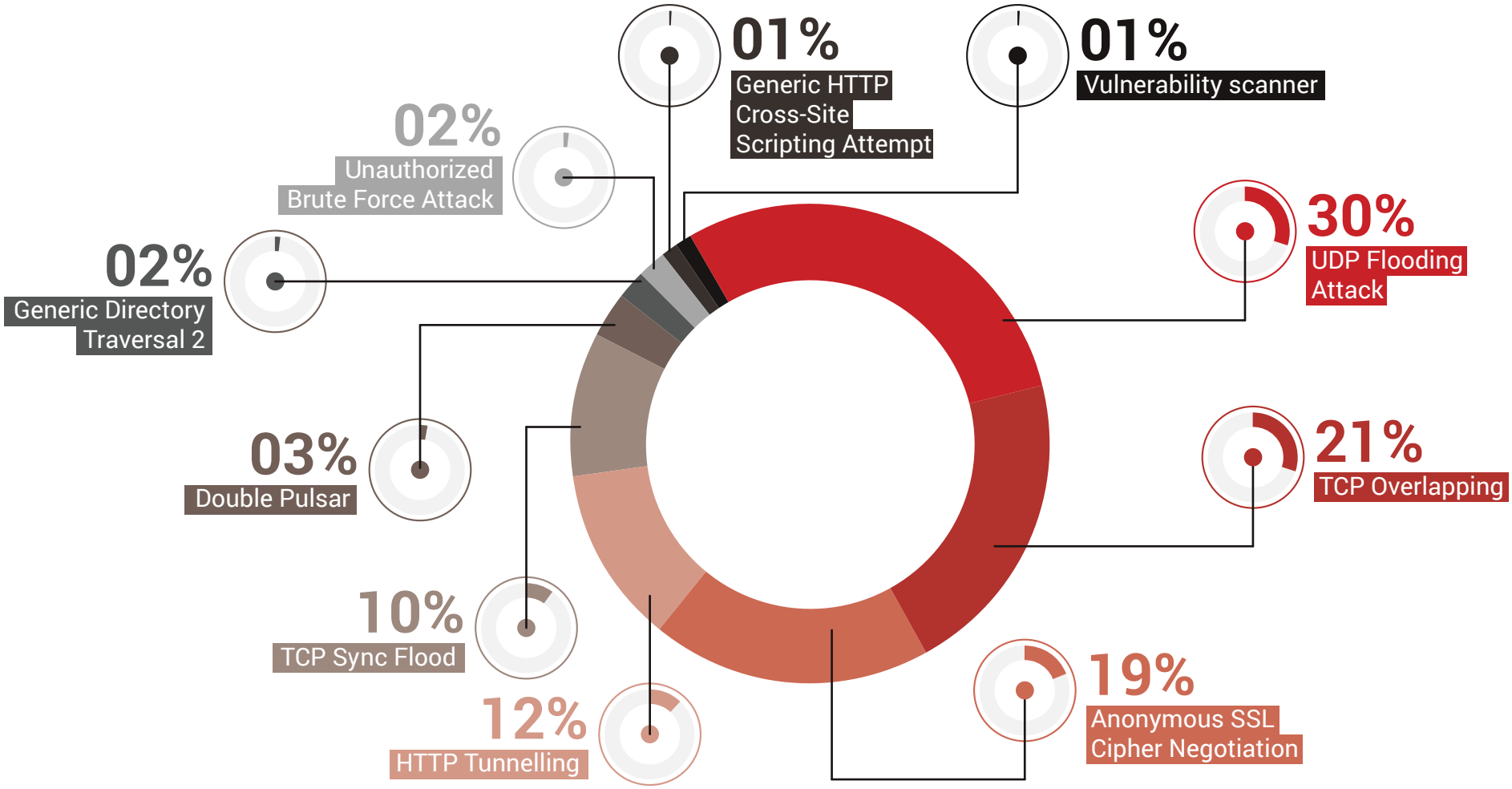
TOP SECTORS ATTACKED BY PHISHING

While businesses and global internet portals have been most impacted by phishing attacks, the financial sector is next in line. The other sectors include retail, government, healthcare, and energy. Within these sectors, C-suites, Finance, IT support, and HR are the most targeted departments.



TOP ATTACKS OBSERVED

Payloads (viruses and malware) or malicious software are delivered to targeted workstations and servers using “attack vectors.” These vectors are pathways or methods through which attackers and attackers gain access to your systems. Following are the top attacks detected by our Security Operations Centers and sensors:



Almost 30% of the attacks are UDP flooding attacks, followed by 21% of attacks caused by TCP overlapping, and anonymous SSL cipher negotiations are the third most used tactic for causing cyberattacks. HTTP tunneling and TCP sync floods are also on the list of most attacked types used.

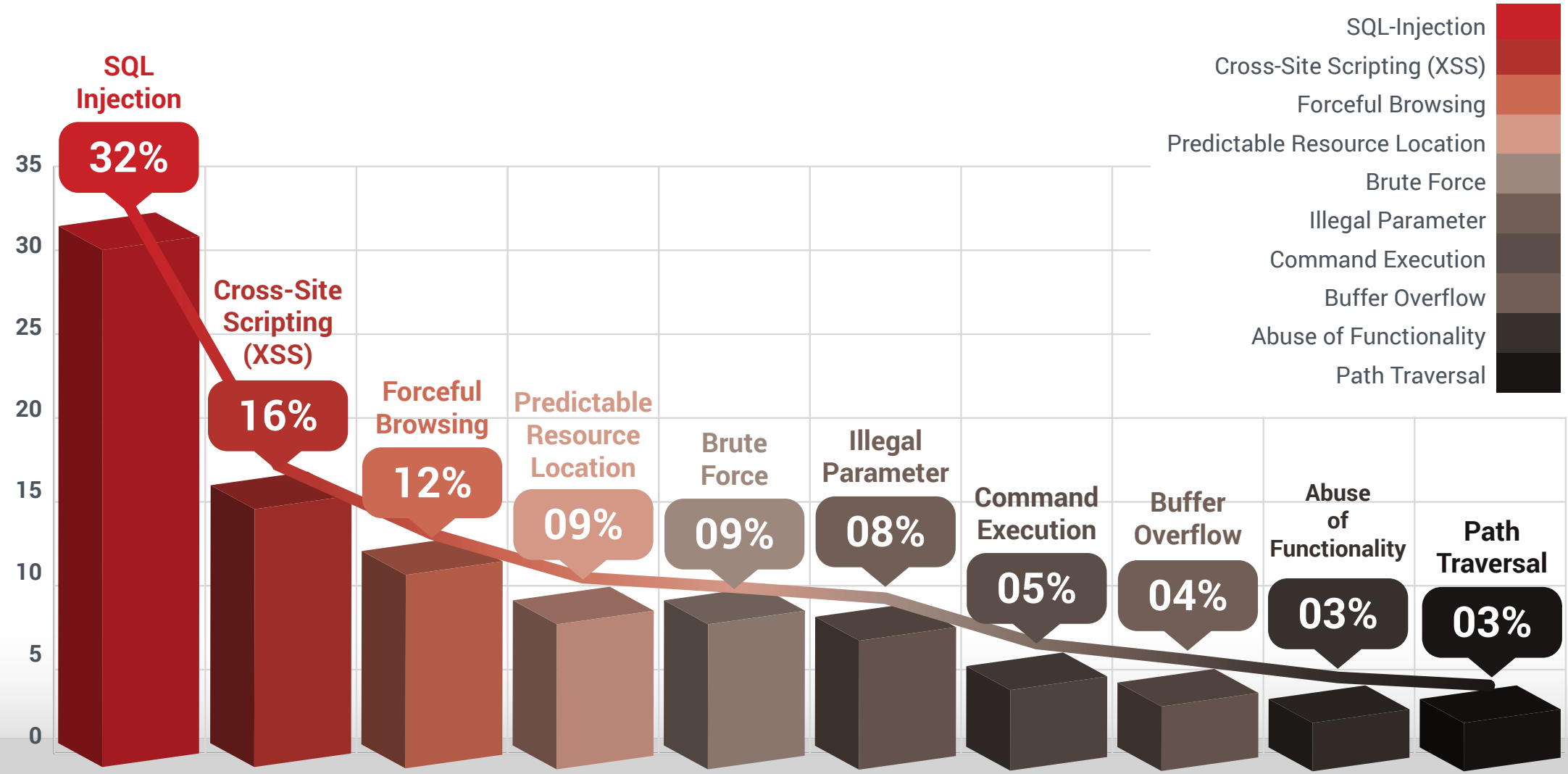
TOP CNC (COMMAND-AND-CONTROL) SERVERS OBSERVED

The leading malware detected by our Security Operations Centers (SOC) in the past ten months is Emotet (63.83%), with most attacks originating from the UK. It was followed by Crilock(14.89%) and PDF Phishing(14.59%), both originating from the USA. Below are the CnCs, IP addresses, and geolocations associated with these malware attacks.

MALWARE	CNC SERVER	IP ADDRESS	GEOLOCATION	%
Emotet	ccanet.co.uk	91.199.212.52	United Kingdom	63%
Crilock CNC	216.21.13.14	216.21.13.14	United States of America	15%
PDF Phishing CNC	weebly.net	199.34.228.53	United States	14%
HTMLPHISHER	ovh.net	213.186.33.17	France	4%
Smokeloader	getresponse-mail.com	104.160.64.9	United States of America	1%
Kryptik	singlehop.net	69.175.87.74	United States of America	1%
MPCDotCash	bluehost.com	162.241.218.28	United States of America	1%
BAT/Miner.VS!MSR	agafurreetor.com	139.45.195.210	Netherlands	1%

TOP WEB APPLICATION ATTACKS

The data from our Security Operations Centers reveals that 32% of all web application vulnerabilities were that of SQL injection attacks. 16% of the attacks were carried out using cross-site scripting. Forceful browsing attacks amounted to 12%. Others are listed below.



TOP ATTACKING IP ADDRESSES

A high percentage of detected cyberattacks (37.63%) originated from the IP address 77.68.122.128. This was followed by around 15% of the attacks originating from the IP address 74.208.223.188. Our SOC also detected other malicious IP addresses, some of which are given below.

TOP PORTS ATTACKED

Port 443 has maintained its position as the most targeted port since 2020, bearing almost 89% of the detected attacks, up from 50% in 2020 and 40% in August 2019. Other ports like 25, 80, and 389 continue to appear in the list of top-targeted ports. Ports 53 and 137 have emerged as new highly targeted ports.

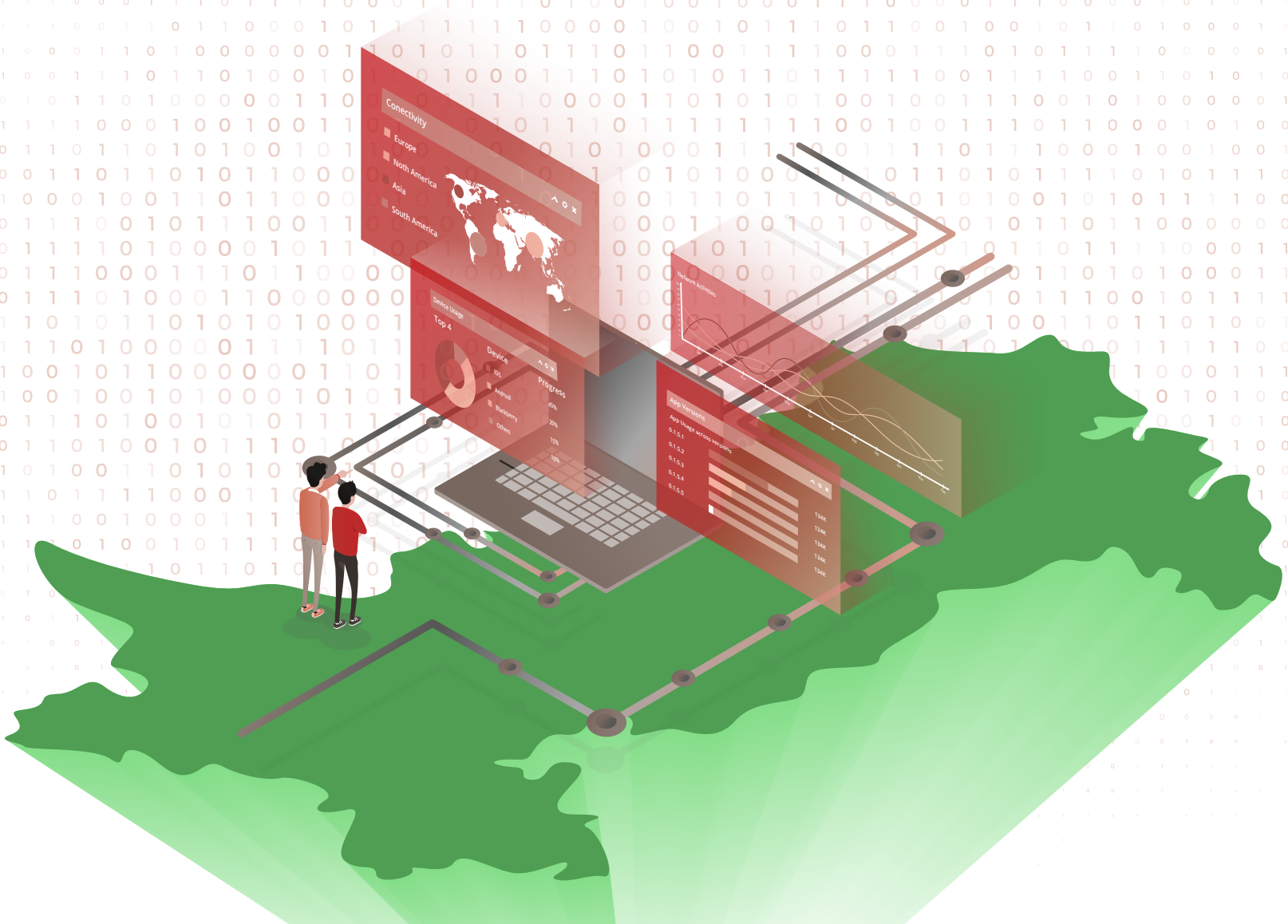
PORTS	%
443 (HTTPS)	85%
25 (SMTP)	3%
80 (HTTP)	2%
389 (LDAP)	2%
53 (UDP)	1%
445 (SMB)	1%
137 (NetBIOS)	1%
3389 (RDP)	1%
123 (NTP)	1%
993 (IMAPS)	1%
4500 (IPSec)	1%

TOP MALWARE DETECTED

The Highest detected malware was W32/Malicious_Behavior.SBX followed by VBA/Agent.FB32!tr. These top malware include file infectors, email worms, trojans, keyloggers, and unwanted applications. These are listed below.

S.NO	VIRUS NAME	%
1	W32/Malicious_Behavior.SBX	17%
2	VBA/Agent.FB32!tr	12%
3	PUA.Keygen.KMS	12%
4	Hacktool	12%
5	Virus.Win32.Virut.ce	12%
6	PUA.Keygen.KMS!g3	12%
7	Virus.Win32.Nimnul.a	8%
8	Trojan.Gen.2	7%
9	Email-Worm.Win32.Runouce.b	5%
10	Trojan.Win32.Starter.yy	5%

REGIONAL DATA AND REWTERZ THREAT INTELLIGENCE



APT ATTACKS ON PAKISTAN

Rewterz Threat Intelligence (TI) team observed and detected targeted attacks on Pakistan's infrastructure and government sector. Out of these cyberattacks, the most commonly occurring or impactful were attacks carried out by SideWinder, Agrius, Donot, Confucius, and Emotet. Phishing attacks have been on the rise since the beginning of the pandemic, these attacks also took place in Pakistani government departments. The purpose of these attacks was to target confidential information and intellectual property of South Asian organizations, especially the government and business sector of Pakistan. Confucius targeted South Asian organizations using pegasus malware while other APT groups used RaaS and specialized malware.

S.No	Threat Actors	Month & Year	Region
1	APT C-35 (Donot)	October 2020	India
2	APT C-35 (Donot)	December 2020	India
3	APT C-35 (Donot)	January 2021	India
4	APT C-35 (Donot)	February 2021	India
5	APT C-35 (Donot)	March 2021	India
6	APT C-35 (Donot)	March 2021	India
7	APT C-35 (Donot)	April 2021	India
8	APT C-35 (Donot)	June, 2021	India

S.No	Threat Actors	Month & Year	Region
1	Confucius	November 2020	India
2	Confucius	February 2021	India
3	Confucius	June, 2021	India
4	Confucius - using Pegasus	August 2021	India

S.No	Threat Actors	Month & Year	Region
1	PatchWork	January 2021	India
2	PatchWork	July, 2021	India

S.No	Threat Actors	Month & Year	Region
1	Bitter APT	April 2021	India
2	Bitter APT	September, 2021	India

S.No	Threat Actors	Month & Year	Region
1	Gallium	May 2021	China

S.No	Threat Actors	Month & Year	Region
1	Sidewinder	August 2020	India
2	Sidewinder	November 2020	India
3	Sidewinder	November 2020	India
4	Sidewinder	January 2021	India
5	Sidewinder	January 2021	India
6	Sidewinder	February 2021	India
7	Sidewinder	March 2021	India
8	Sidewinder	April 2021	India
9	Sidewinder	May 2021	India
10	Sidewinder	June, 2021	India

S.No	Threat Actors	Month & Year	Region
1	APT38	February 2021	North Korea

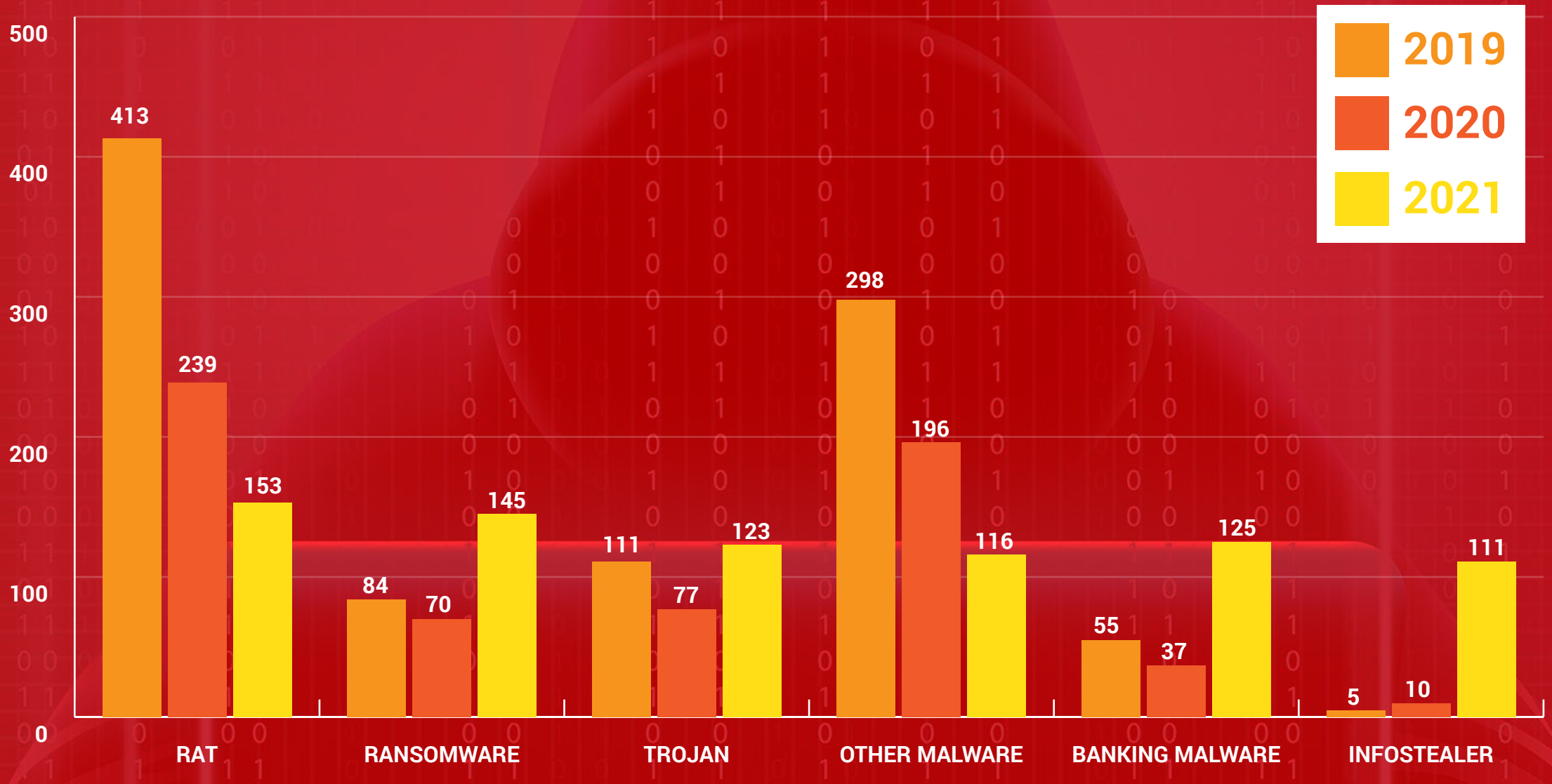
S.No	Threat Actors	Month & Year	Region
1	APT39	May 2021	North Korea

S.No	Threat Actors	Month & Year	Region
1	Muddywater	January 2021	Iran
2	Muddywater	February 2021	Iran

S.No	Threat Actors	Month & Year	Region
1	RedDelta	June 2021	China

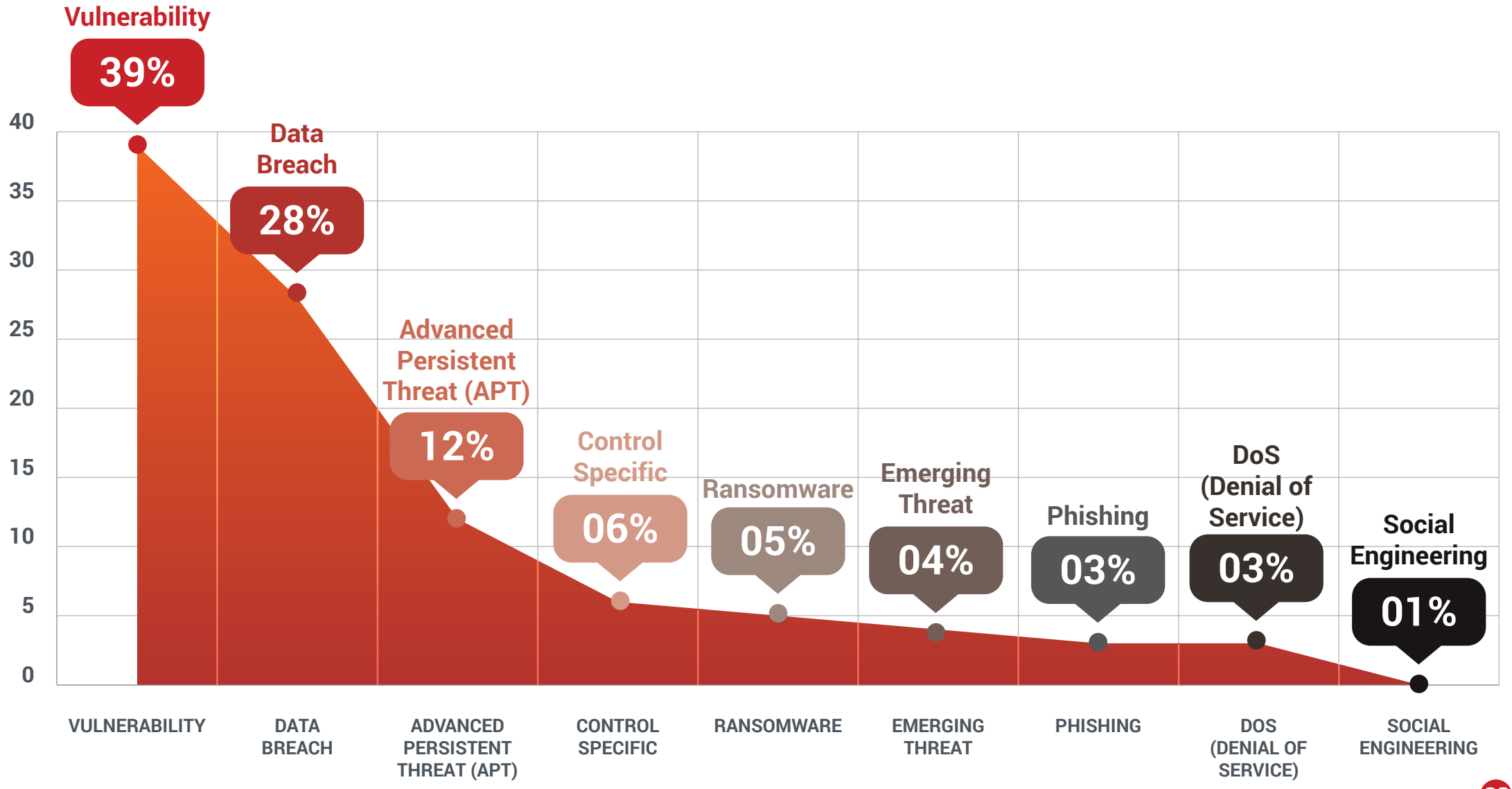
MALWARE TRENDS IN REWTERZ THREAT UPDATES 2019-2020-2021

Given below is the trend of malware occurrence according to Rewterz Threat Updates. Remote Access Trojans continue to be the most popular tools in cybercrimes, with the highest reported threats in both 2019, 2020, and 2021 so far. However, we have observed that ransomware has increased exponentially during the pandemic and this also reflects in our data. Banking malware and Trojans have increased a lot since 2021, as compared to their occurrence in 2020. Infostealers have also detected more than 2020 and 2019.



THREAT CATEGORIES COVERED IN REWTERZ ADVISORIES

Rewterz Threat Intelligence has reported around 1400 threats and vulnerabilities in the past year. Of these, 39% were vulnerability advisories and followed by data breaches at 28%. 12% of the alerts reported were APTs, whereas 6% of them were control specific. Below is the categorization of these reports.



CYBER SECURITY TRENDS TO LOOK FOR IN 2022

- Working from home became a necessity in 2020, but soon people realized that many businesses can be easily carried out with the help of VPNs and video conferencing. While it was the need of the time, work from home significantly increased the cyber threats, crime, and vulnerabilities. Remote workforces introduce weaknesses in the systems that can be exploited by adversaries to carry out many cyber attacks. These threats have carried on from 2020 to 2021 and will continue in 2022 .
- SIEM (security information and event management) and SOAR (security orchestration, automation, and response) have been combined for improved security. To obtain visibility across networks, SOAR and SIEM platforms have become more commonly used. They will continue to be more widely used in 2022.
- XDRs (Extended Detection and Response) will have a broad industry impact and contain significant potential.
- Transition to cloud data storage became a trend in 2020, and 2021 has become the year for cloud security threats. Cyber security professionals will have to work extra hard to enhance cloud security in 2022.
- Artificial Intelligence (AI) and Machine Learning (ML) will accelerate the automation of cybersecurity tools in medium and small businesses to protect data and critical infrastructure.
- Phishing attacks have soared in recent years, but 2021 has significantly increased the phishing attack frequency. Data is at risk because even unsophisticated threat actors can deploy phishing campaigns using online tools and 2022 will see a rise in these phishing attacks.
- Ransomware was the most commonly used cyber attack in the first quadrant of 2021. And it will continue to rise in 2021 and be carried out into 2022.
- Another threat caused by remote working is Insider threats. This trend will carry its wrath into 2022 as awareness regarding insider threats is lacking in most employees and organizations.
- Supply chain attacks have persistently shocked the business community in 2020 and 2021. The PrintNightmare and SolarWinds' supply chain attack is proof that vulnerabilities and zero-days will cause plentiful damage in 2022.
- Speaking of Zero-days, Zero-days have also been widely reported and exploited. These zero-days are exploited-in-the-wild by threat actors and cybercrime groups to target organizations with unpatched software. We expect that 2022 will be the year where Zero-Days detection and exploitation will skyrocket.

RECOMMENDATIONS

- Update software and patches regularly against all known vulnerabilities.
- Use secure, trusted, reputable, and updated VPNs only.
- Use the least privilege policy to limit access of each employee to job requirements alone.
- Maintain and test backups regularly to not be vulnerable to ransomware attacks.
- Set up systematic logging of all access and activities of your infrastructure equipment (servers, firewall, proxy…), and workstations.
- Monitor remote connections and maintain logs of all activities.
- Keep track of users with admin privileges and access to critical infrastructure.
- Where possible, keep unused ports closed. If possible, implement segmentation of IT and OT networks.
- Implement a strict and strong password policy along with a password change policy every few months.
- Whenever possible, limit VPN access to only authorized devices. Any attempt to connect from another device should be denied.
- You should also activate two-factor authentication on remote sessions, especially for connections to the corporate network.
- Update spam and anti-phishing software and configurations to increase security.

rewterz

www.rewterz.com

info@rewterz.com

UAE Oman Pakistan USA Australia