SOCRadar®

2020

THE YEAR IN CYBERSECURITY

Major Cyber Incidents

PREPARED BY
SOCRADAR CYBER INTELLIGENCE INC

DIFFICULT YEAR AHEAD

As companies, executives and consumers shift to digital-first interactions, threat actors have found opportunity in 2020.

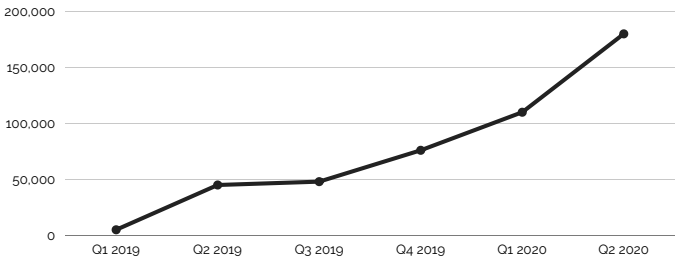
One of the trends in cybersecurity that should be noted is the continuing need to further improve the relevant cybersecurity rules. As technology companies operate with big data, it is up to cybersecurity experts to defy cybersecurity trends to prevent these attacks. Here we want to include the statistics that give us an idea of how the number of cyber attacks will increase in 2021.

Cybersecurity threats are everywhere, as statistics show the only thing that can help organizations and SOC teams who deal with them is to educate users about the threats. If we look at the possible trends in the following year, it becomes clear that 2021 will be a difficult year for cyber security professionals.

RANSOMWARE ATTACKS

Ransomware has become a common malicious tool for adversaries that threaten to damage governments, corporations, and individuals every day. The year 2020 has been a turning point for ransomware attacks. Global lockdown due to the COVID-19 pandemic has led to a huge increase in online transactions. For cybercriminals, more online transactions mean more attack possibilities.

AVERAGE RANSOM PAYMENT BY QUARTER

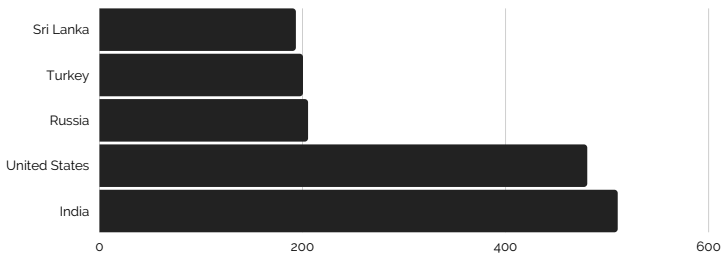


- 51% of surveyed businesses were hit by ransomware in 2020.
- ¼ of Ransomware victims make payments to Hackers.
- $5,900 is the average ransom for a small business.
- The average ransom demand in 2020 is $178,000.
- $50 is the average cost for ransomware kits on the Dark Web.
- It is predicted that every 11 seconds a company will be hit by ransomware in 2021.[1]

TOP 5 COUNTRIES IN 2020 Q3 AFFECTED BY RANSOMWARE

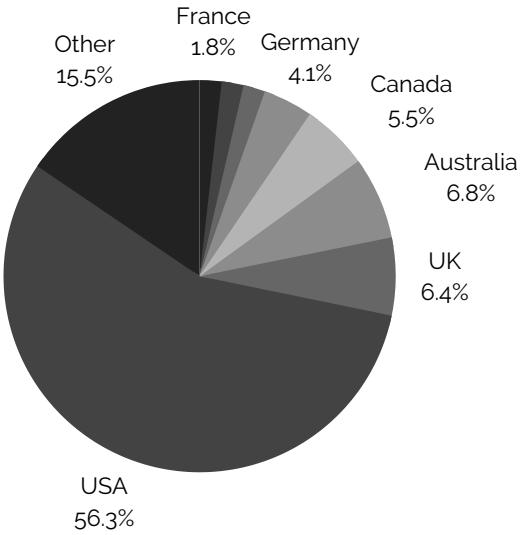
The top 5 countries affected by the ransomware are the US (98.1% increase), India (39.2% increase), Sri Lanka (436% increase), Russia (57.9% increase) and Turkey (32.5% increase). [2]

* Comparing to 2020 Q2

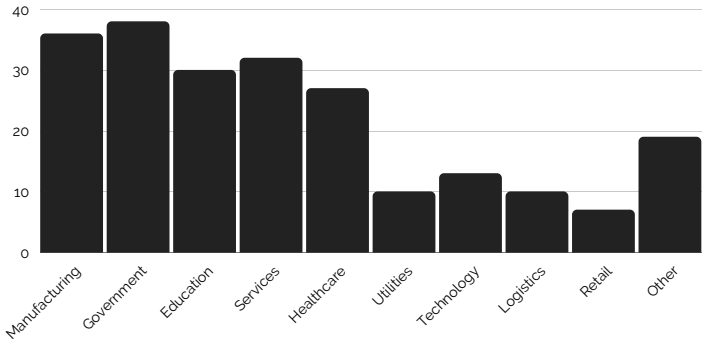


RANSOMWARE BY COUNTRY

The pie chart here shows how North American and European countries are affected by ransomware attacks in 2020. Among others, the US is the most affected country followed by the UK.



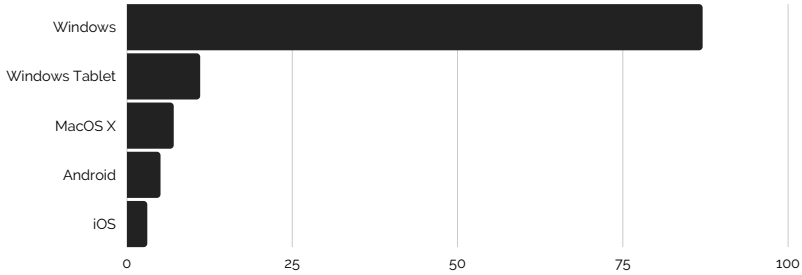
MOST TARGETED INDUSTRIES BY RANSOMWARE



According to statistics for 2020, about 38% of ransomware attacks target governments as the most targeted sector. The second most targeted sector stands out as the manufacturing industry with 36 percent.[3]

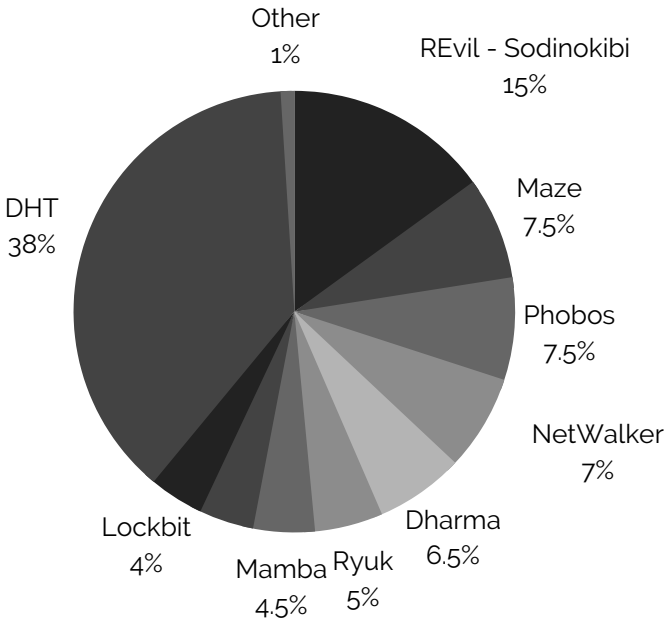
MOST TARGETED OS BY RANSOMWARE

The target of ransomware attacks is by far the Windows operating system. Windows is followed by MacOS and Android operating systems.



MOST COMMON RANSOMWARE TYPES

More than one form of ransomware is available, and it is difficult to follow up on them all with new ransomware attacks still emerging. Recently, Coveware published a report about the most common ransomware types. According to this report the most common ransomwares are REvil (Sodinokibi), Maze, Phobos, Netwalker, and Dharma. While REvil is responsible for 15 percent of all ransomware attacks, Maze and Phobos each caused ~7.5 percent of attacks. [4]



REvil (Sodinokibi - Sodin): This ransomware first appeared in a web attack on the Italian WinRAR tool in June 2019. Sodinokibi appears to be a tool of the popular cyber espionage group (FruityArmor), active since 2016. A number of countries in the world have been influenced by Sodinokibi. Taiwan has been the most targeted country with 17.56% of all reported Sodinokibi attacks. Germany (8.05%), Italy (5.12%) and Spain are the most attacked countries in Europe (4.88%).

Maze: This ransomware is a binary file of 32 bits, usually packed as an EXE or a DLL file. The malware begins planning such functions to save memory addresses in global variables, which are then used in dynamic calls later, but these functions are in fact not used later.

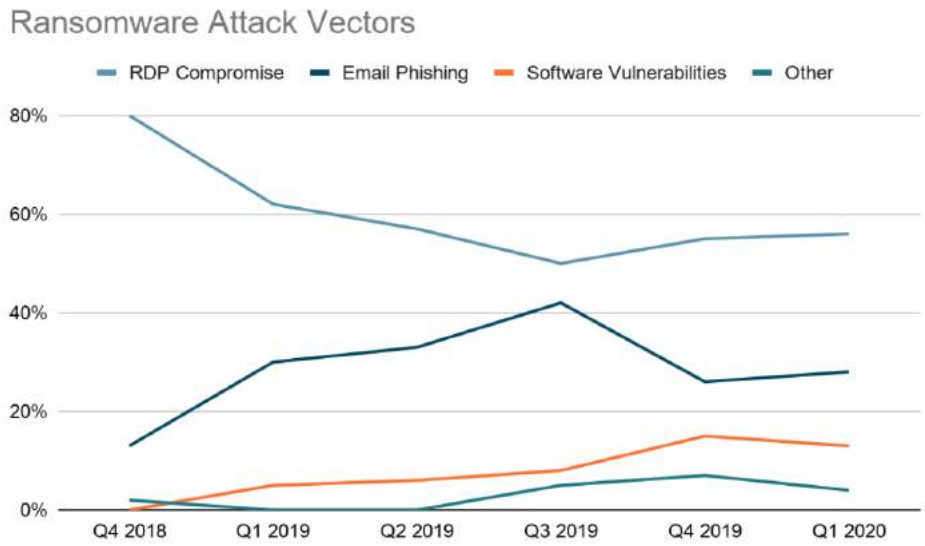
Phobos: Usually Phobos locks productivity documents files such as .doc, .docx, .xls, .pdf, among others. It is distributed via hacked Remote Desktop (RDP) connections. Through inserting the ".phobos" file extension, it would rename all encrypted data. It uses AES cryptography.

Netwalker: It was created by the cybercrime group known as 'Circus Spider' in 2019. As with other ransomware variants, Netwalker establishes an initial access through phishing emails, and then encrypts all critical data.

Dharma: It was first released in 2016 but new forms of Dharma are being developed. Not only does Dharma encrypt files of the victim, but it also destroys backups. In 2019, it infected files such as '.gif,' '.AUF,' '.USA', '.xwx,' '.best' and '.heets'.

RANSOMWARE ATTACK VECTORS

RDP is a formal process for remote system control of IT managers. However, hackers who have connections to RDP endpoints will use networks to gain territory on an enterprise network and continue to expand their rights by moving laterally and access even further. Organizations can take a variety of actions to lock RDP endpoints, including the security of them with complex passwords and multifactor authentication.



DECEMBER 2020

RANDSTAD

Randstad is a Dutch multinational human resource consulting firm headquartered in Diemen, Netherlands that have 280,000 clients and operations in 38 countries.

At the beginning of December in 2020, Randstad's systems were targeted by a ransomware named Egregor. According to Randstad's statement "To date, our investigation has revealed that the Egregor group obtained unauthorized and unlawful access to our global IT environment and to certain data, in particular related to our operations in the US, Poland, Italy and France. They have now published what is claimed to be a subset of that data. The investigation is ongoing to identify what data has been accessed, including personal data, so that we can take appropriate action with regard to identifying and notifying relevant parties."

The hackers have leaked about 60Mb of data from Randstad networks so far. The leaked files are primarily financial records, particularly PDFs and Excel files, claiming that they only represent one percent. On their website, Egregor named 176 victims September 25 and December 2. A majority of victims are in the United States (82), followed by France (19), Italy (15) and Germany (9).

SEPTEMBER 2020

UNITED HEALTH SERVICES | US & UK

Universal Health Services, one of the largest healthcare providers in the U.S. It has 400 hospitals and healthcare facilities in the U.S. and the U.K.

At the end of September, UHS confirmed that its systems were hit by a ransomware attack. It is believed that a phishing attack followed by an email hack caused the attacks. UHS officials did not announce the system disruption until the next day, when they recognized that all 400 US facilities operated under the protocol of Electronic Medical Record EHR downtime, as the IT team responded to fix them from the ransomware attack.

In their official statement UHS said "UHS has deployed a significant number of IT and clinical resources to the hospitals, to support the resumption of online operations. The go-lives will continue on a rolling basis; in the meantime, those working toward go-live are continuing to use their established back-up processes including offline documentation methods''.

APRIL 2020

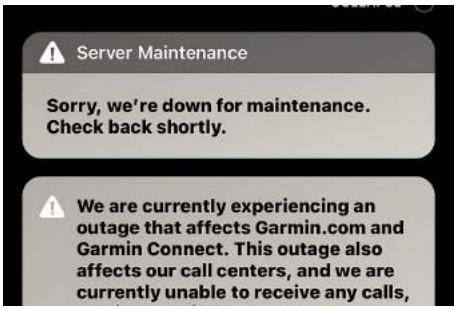
TRAVELEX

Travelex is foreign currency exchange company that has over 1,000 stores and 1,000 ATMs in 26 countries. In April 2020, It was reported that hackers have accessed Travelex's systems and downloaded 5 GB of data. According to the reports, unpatched vulnerability in Pulse Secure VPNs (CVE-2019-11510) caused the adversaries to remotely execute malware that is known as Sodinokibi, also commonly referred to as REvil or Sodin. After weeks of negotiation, Travelex agreed to pay a ransom of $2.3 million, or about 285 bitcoins.

JULY 2020

GARMIN

Garmin Ltd. is a multinational technology company whose revenue was $3.35 billion in 2018. Garmin is mostly known for GPS wearables.On July 23rd of 2020, Garmin's wearables, apps, website, and even its call centers became offline for several days. Couple days later, Garmin confirmed the cyber attacks.



According to the reports hackers deployed the ransomware tool WastedLocker to encrypt sensitive data. It is believed that the Russian hacking group known as Evil Corp is behind the attacks. According to the unconfirmed reports, Garmin paid $10 million ransom to save its data. On July 27th, many of Garmin's services were starting to come back online. Today, threat actors such as Evil Corp seem to have relocated their focus to Fortune 500 companies, with millions of random demands. Garmin could only be the start of a new age of ransomware affecting major American companies.

JANUARY 2020

CPI

In mid-January of 2020, CPI (Communications and Power Industries) suffered a ransomware attack. Based on the investigation by a third-party the main reason behind the attack was clicking on the malicious link by a domain admin. Researchers said, "Controlled use of administrative privileges, including running with the lowest level of privilege is CIS Control 4. Network segmentation, particularly for older operating systems such as XP, is key to not only restrict lateral movement but also mitigate shortfalls in legacy system security". It is claimed that the company paid hackers a $500,000 extortion fee.

DATA BREACHES

NUMBERS SPEAK:

Hackers attack every 39 seconds, on average 2,244 times a day.

53% of companies had over 1,000 sensitive files open to every employee.

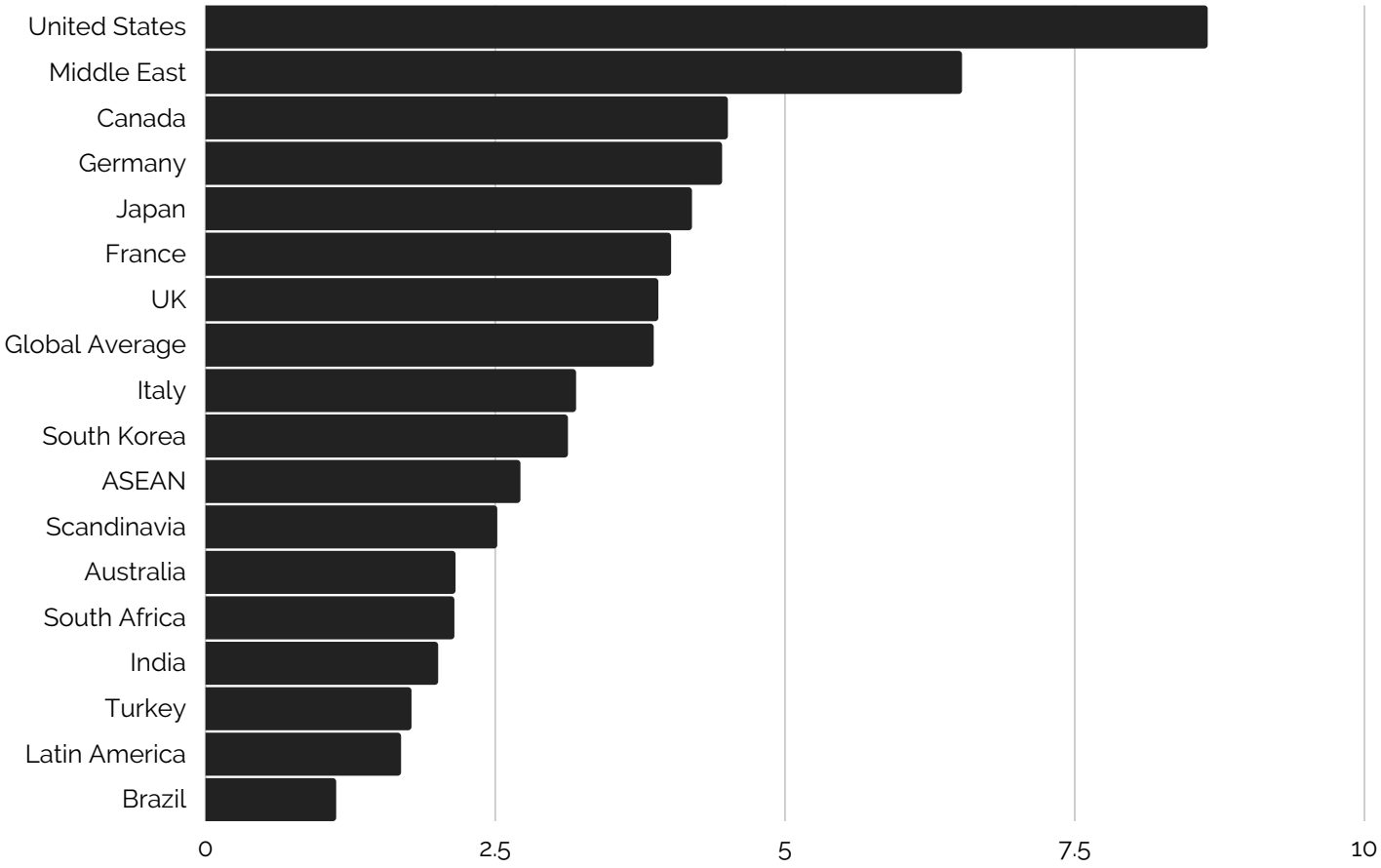
22% of all folders were available to every employee.

On average, every employee had access to 17 million files.

$3.9 million is the average cost of a data breach.

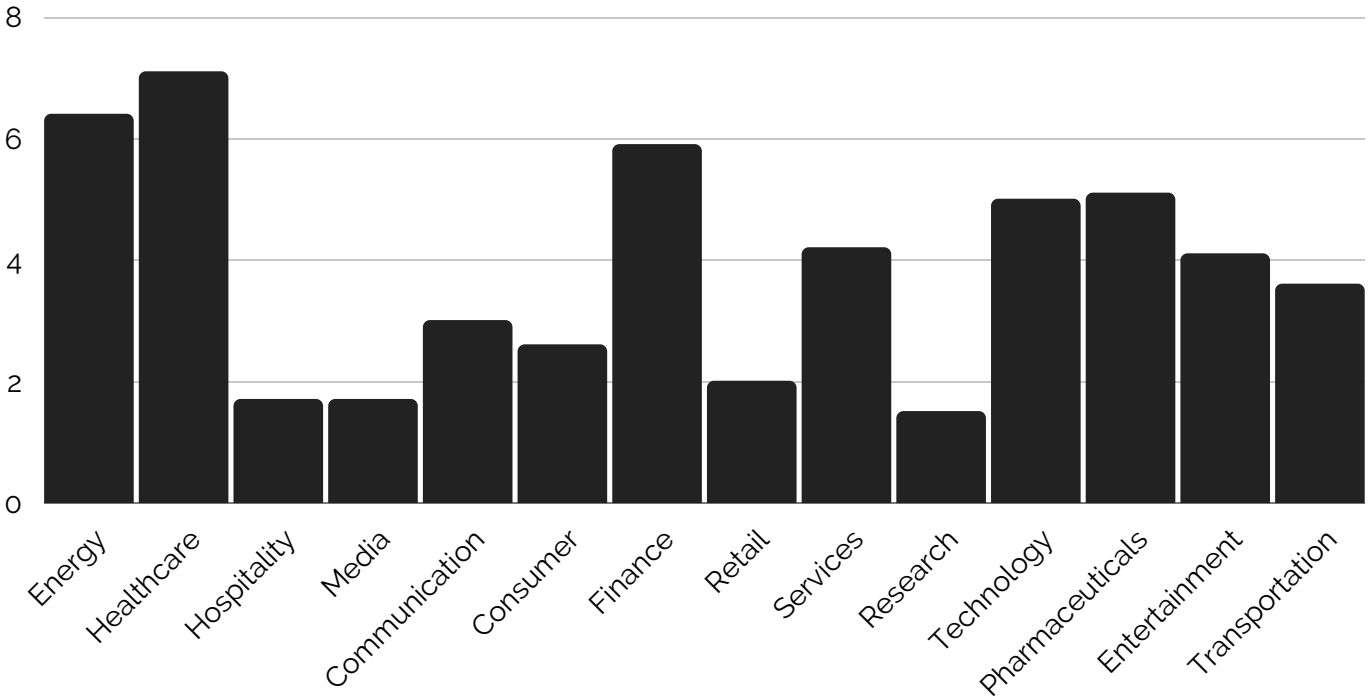
The average cost per record stolen is $150. [5]

AVERAGE COST OF DATA BREACHES WORLDWIDE ($ MILLIONS)



As of 2020, the average cost of a data breach in the United States amounted to 8.64 million U.S. dollars. The global average cost of a data breach in the measured period was 3.86 million U.S. dollars.[6]

AVERAGE COST OF DATA BREACHES BY INDUSTRY ($ MILLIONS)



Healthcare organizations have had the highest costs associated with a data breach. Healthcare, Pharma and Biotech had 352,771 exposed sensitive files on average which is the highest when comparing industries. 15% of breaches involved Healthcare organizations, 10% in the Financial industry.

250 MILLION RECORDS

MICROSOFT

A recent study showed that over 14 years, 250 million Microsoft consumer data without password protection have been revealed online.There is the Internet Explorer zero-day vulnerability that Microsoft hasn't issued a patch for, despite it being actively exploited. The organization launched an internal investigation and claimed there were no signs of malicious use nor data breach with personal identifiable information (PII). Microsoft says everyone whose email address was exposed notified personally.

271 MILLION RECORDS

WATTPAD

Over the 270 million records of over 268 million unique email addresses and password combinations are used in the leaked folder.The breached SQL database contains one large user table, consisting of 270,784,079 email addresses. After removing the duplicates,268,830,266 email addresses remained. Stolen data was given away for free on Dark Web where claims that 145 million passwords are hashed with bcrypt, and the other 44 million are hashed with SHA256. The same database was previously on sale for 10 Bitcoins (~$100,000).

Screenshot of the threat actor's database dump post on a Deep Web Forum called RaidForums

440 MILLION RECORDS

ESTÉE LAUDER

As Security Discovery and other media sources first noted, the privacy breach revealed domestic emails without evidence that consumer accounts or payment details were compromised. There were 440,336,852 documents in this hacked database, including internal emails. Security researchers observed that stolen data linked to middleware could provide another access for cybercriminals to get access to more relevant information. However, Estée Lauder's clients and its large-scale subsidiary products, such as the Clinique and MAC, did not run a direct risk. According to the official statement; "On 30 January, 2020, we were made aware that a limited number of non-consumer email addresses from an education platform were temporarily accessible via the internet. This education platform was not consumer facing, nor did it contain consumer data. We have found no evidence of unauthorized use of the temporarily accessible data."

300,000 RECORDS

NINTENDO

The Japanese gaming giant reported that 160,000 Nintendo accounts were hacked by disclosing personal details such as the name of the account holders, email address, dates of birth, and country. Another 140,000 Nintendo accounts were hacked in an amended statement.A Nintendo Network ID is a unique username and password used mainly for older Nintendo 3DS and Wii U consoles. Some customers began complaining about missing funds from their Nintendo accounts. Nintendo informed its consumers to check their purchase history for any unauthorized transactions and request for refund. Based on the company's statement no credit card information exposed.

8,3 BILLION RECORDS

AIS THAILAND

More than 8 billion records of Thai users in the country's largest AIS network have been leaked. A total of 4.7 TB of information was available online without any password requirement.

The breach was uncovered on May 7 by security researcher Justin Paine, who discovered an open ElasticSearch database online which appeared to be controlled by AWN, a subsidiary of Thailand's largest GSM mobile phone operator, Advanced Info Service (AIS). The database contained DNS queries and Netflow data, using which it would be all too easy to map a user's internet activity.

According to the company's spokesperson; "We can confirm that a small amount of non-personal, non-critical information was exposed for a limited period in May during a scheduled test. All of the data related to Internet usage patterns and did not contain personal information that could be used to identify any customer or cause them financial or any other harm.

THIRD PARTY ATTACKS

Cyber criminals are still seeking the easiest, safest, and cheapest route to the weakest link. Third party suppliers in your supply-chain are attractive targets because many small and medium-sized enterprises have a shortage of proper security resources, facilities, and secure protocols.

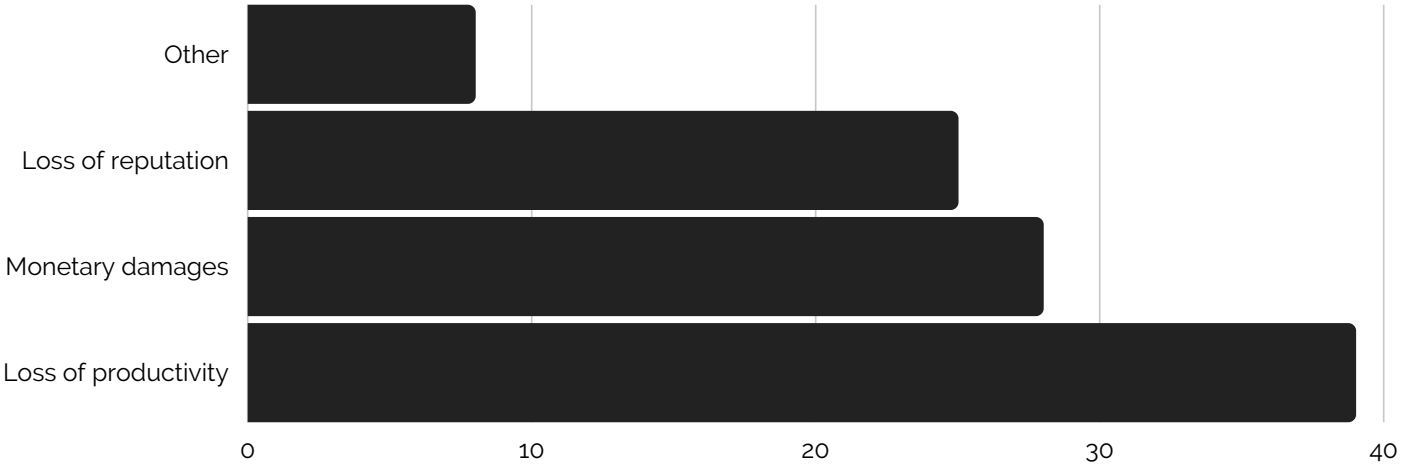
Most of the time-sensitive and personal information can also be used by SMEs (Small and medium enterprises).

The target of a small vendor is much more cost-effective than a big organization with rigorous security protocols. Third-parties are companies that support your organization and often have access to, share, or maintain data critical to your operations. Third-parties include a broad range of companies such as data management companies, law firms, email providers, web hosting companies, subsidiaries, vendors, service providers, subcontractors. Essentially any company whose employees or systems have access to your systems or your data is considered a third party. However, third-party cyber risk is not limited to these entities.

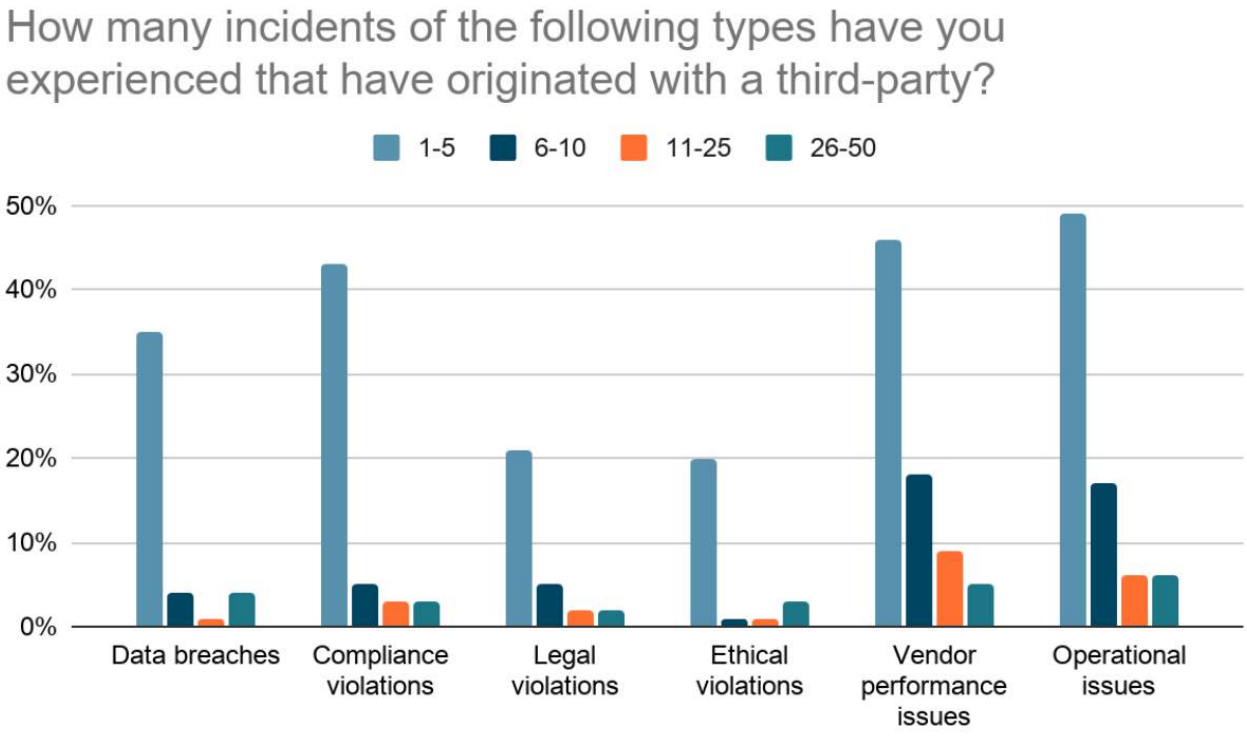
Any external software, hardware or firmware that you use for your business can also pose a cyber risk. A successful third-party risk program, which includes the various third-party sectors, ought to provide threat information. Detailed vulnerability information will then be used for defined attack scenarios to map hacker workflows. A recent survey conducted by the Ponemon Institute revealed that 59% of organizations have experienced one or more data breaches caused by a third party, costing an average of $7.5 million to remediate. [7]

STUDY ON THE RESULTS OF THIRD PARTY ATTACKS

In February 2020, Prevalent and Shared Assessments partnered together to study current trends, challenges, and initiatives impacting third-party risk practitioners. Third-party attacks mostly cause loss of productivity followed by monetary damages as it can be seen below.[7]

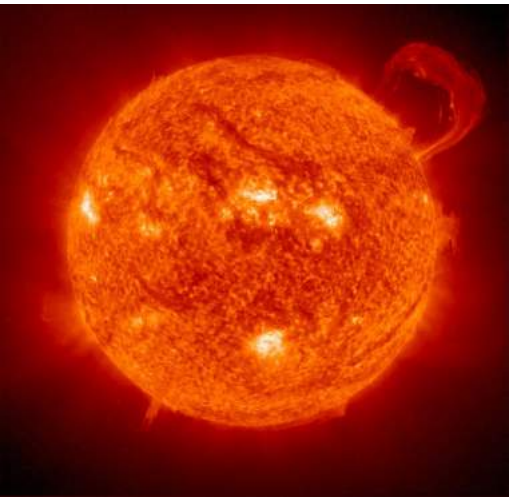


Below graphics shows 76% of those who replied to the question whether events that originated in a third party in the past two years had an effect on the vendor's results, followed by operational problems with 74%, 55%, on the other hand, indicating a breach.



DECEMBER 2020

SOLARWINDS



At the end of 2020, malicious SolarWinds update package was found to have infected more than a dozen critical infrastructure companies in the electric, oil, and manufacturing industries who were also running the software.Original Equipment Manufacturers (OEMs) have remote access to critical parts of customer networks, as well as privileges that let them make changes to those networks, install new software, or even control critical operations. This means that hackers who breached the OEMs could potentially use their credentials to control critical customer processes.

REPORTED VICTIMS OF SOLARWINDS SUPPLY CHAIN ATTACK

US Department of Defense | US Department of Energy | US Department of Commerce | US Department of Health and Human Services | US Department of Homeland Security | US Department of State | US Department of Treasury | Belkin International | California Department of State Hospitals | CiscoCox Communications | Deloitte | Digital Sense | FireEye | Intel | ITPS | Kent State University | Microsoft | Netdecisions | Nvidia | Pima County, State of Arizona | SolarWinds | Stratus Networks | VMware

NOVEMBER 2020

EXPEDIA AND HOTELS.COM

Expedia and Hotels.com suffered data breach by a third-party named Prestige Software that is a Spanish software company. The software company left over 10 million records from their clients in an exposed AWS S3 data bucket due to a simple software configuration.

Breached data includes; NamesCredit card details, Driver's license or passport numbers, Reservation details

How many people are impacted by this event is impossible to tell since several leaked logs contained many details for one reservation. Investigators were unable to confirm whether the data would be collected until the open bucket was discovered. On the other hand, Hotels.com and Expedia sued over data breach since data breach exposed information that is protected by the California Consumer Privacy Act (CCPA).

MARCH 2020

GENERAL ELECTRIC

Announced in late March, a data-breach hit Fortune 500 company GE. According to the announcement made by General Electric, one of its third-party service providers, Canon, experienced a data-leak through unauthorized access to an employee email account. Canon Business Process Services revealed that the breach window took place from approximately February 3 – 14, 2020, and the data exposed include: passports, birth certificates, marriage certificates, death certificates, direct deposit forms, driver's licenses, medical child support orders, tax withholding forms, beneficiary designation forms, applications for retirement, severance, death benefits with related forms and documents relating to GE employees as well as other beneficiaries.

GE systems were not directly impacted by the breach. However, the information harvested might be used by criminals and fraudsters in scams and phishing campaigns. Canon promised to provide financial assistance to those affected by the breach if they notify the company by June 30, 2020. It's unclear how many people were affected by the data breach.

MARCH 2020

AMAZON

Over 8 million sales records of Amazon UK, eBay and Shopify customers were recently exposed due to a security vulnerability in a third-party app.The third-party app was used by small retailers in the EU for calculating value-added taxes for different EU countries. The exposed data included sales records, customer names, email addresses, customer shipping addresses, the types and values of purchases, the final four digits of credit card numbers. The majority of the personal records exposed were related to the customers in the UK.

MARCH 2020

SPACEX, TESLA, BOEING, LOCKHEED MARTIN

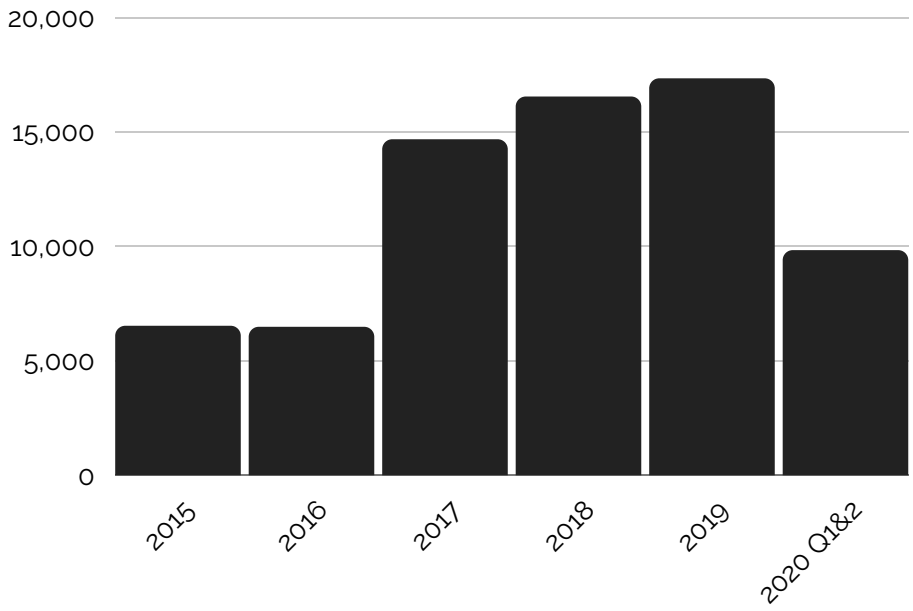
Visser, a third-party vendor providing precision parts to space and defense contractors, announced a "cybersecurity incident," in early March. Although the third party revealed it is "continuing its comprehensive investigation of the attack, and business is operating normally," initial findings indicate the attack was likely caused by DoppelPaymer ransomware.DoppelPaymer, the latest data-stealing ransomware, is a file-encrypting malware that first exfiltrates the company's data and threatens to publish the stolen files if the ransom is not paid.The ransomware's website lists the stolen files from its beneficiaries including Tesla, SpaceX, aircraft maker Boeing, and defense contractor Lockheed Martin.

VULNERABILITY ATTACKS

In the first half of 2020, new vulnerability reports increased significantly (9,799 in 2020, up from 7,318 in 2019, a rise of 34%). This number further beats the previous high for the first six months of 2018 (8,485) and suggests a record-breaking figure for 2020. [8]

- 20,000+ New Vulnerability Reports Likely in 2020
- 50% Increase in Mobile Vulnerabilities Highlights Dangers of Blurring Line Between Corporate and Personal Networks
- Attacks on Critical Infrastructure Adding to the Chaos

NEW VULNERABILITIES BY YEAR

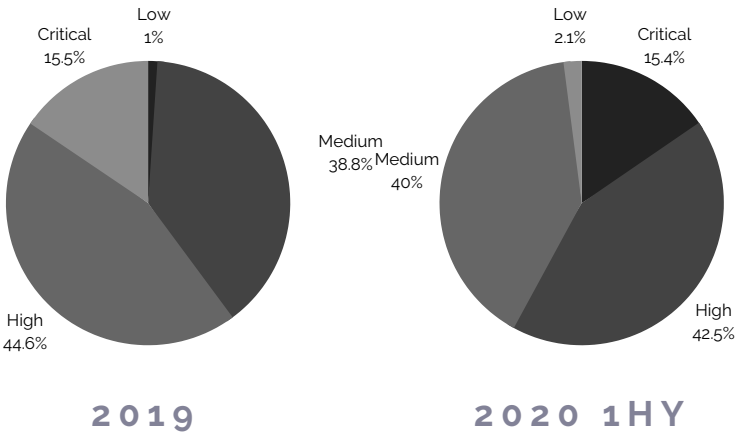


The number of vulnerabilities registered to the CVE database annually fluctuated within a narrow range between 2005 and 2016 – before jumping 128% from 6,447 in 2016 to 14,714 in 2017. That number seems to be climbing again considering the numbers for Q1 and Q2 of 2020.

VULNERABILITY STATISTICS 2020

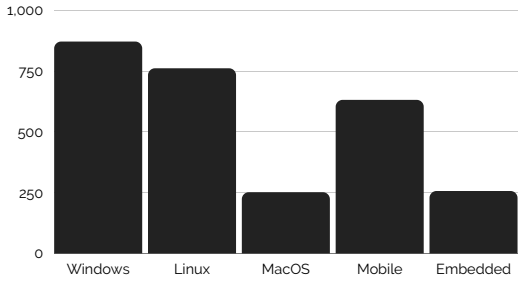
The severity distribution in the first six months of 2020 for current vulnerabilities looks very close to the 2019. High-severity vulnerabilities constitute 42.5% of the overall vulnerability list, medium-sized vulnerabilities are 40% of the total. 15% of the new disclosures contain critical extreme vulnerabilities. On average 67.8% of assets had at least one CVE with a CVSS score of 4.0 or more. From a PCI DSS standpoint, this would result in an average of 67.8% of assets failing PCI compliance. On average 27% of assets had a CVE with a CVSS score of 7.0 or more.

NEW VULNERABILITIES BY CVSS SCORE



2019 2020 1HY

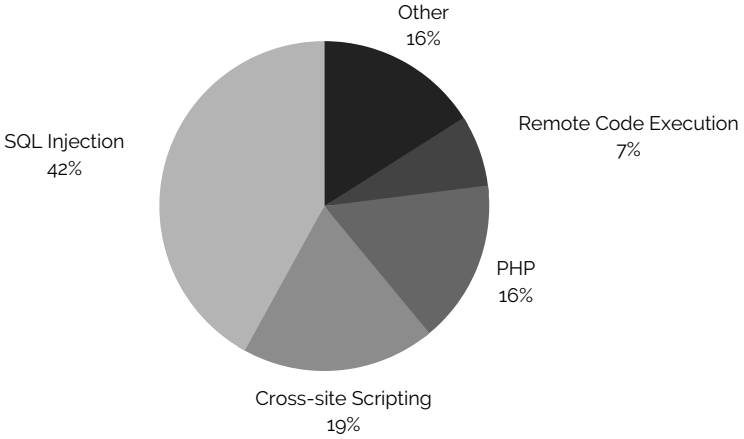
VULNERABILITIES BY OS



In the first six months of 2020, smartphone OS vulnerabilities have increased by 50%. This surge can be due solely to the spike in new bugs in Google Android, which more than doubled from the previous year's 230 average to 492.

MOST COMMON CRITICAL VULNERABILITIES

Critical Risk Vulnerabilities cause compromise of a system or a user. They are highly likely to occur with high impact. For instance, even though SQL injection was first discovered in 1998, it is still one of the most effective vulnerabilities as of today together with (Cross Site Scripting) XSS and Remote Code Execution (RCE).



CVE-2020-16846 / CVE-2020-125592 / CVE-2020-17490

SALTSTACK

SaltStack is a VMware-owned company that stated critical vulnerabilities impacting Salt versions 3002 and prior.

There were 3 vulnerabilities disclosed:

- CVE-2020-16846 (High/Critical) has been described by the Salt team as a shell injection vulnerability in Salt API that was patched by removing the `shell=True` option when calling "subprocess.call" via the SSH client.
- CVE-2020-25592 (High/Critical) is an authentication bypass flaw in Salt API but the fix published for the same additionally mentions yet another mysterious identifier CVE-2020-16804.
- CVE-2020-17490 (Low) concerns a permissions issue when opening/saving cryptographic private key files.

These vulnerabilities allow remote attackers to execute arbitrary code on affected Salt installations. Shodan reports 6,138 exposed SaltStack Master nodes.

CVE-2019-0594

SHAREPOINT

Even though the SharePoint vulnerability first exploited May, nine months after it was patched by Microsoft continues to be exploited. A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0594. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account.Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected version of SharePoint.The security update addresses the vulnerability by correcting how SharePoint checks the source markup of application packages.

CVE-2020-1472

ZEROLOGON

An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC). An attacker who successfully exploited the vulnerability could run a specially crafted application on a device on the network. This vulnerability is associated with CVE-2020-1472 (updated September 28, 2020)

CVE-2019-11510

PULSE SECURE

Multiple vulnerabilities were discovered and have been resolved in Pulse Connect Secure (PCS) and Pulse Policy Secure (PPS). This includes an authentication by-pass vulnerability that can allow an unauthenticated user to perform a remote arbitrary file access on the Pulse Connect Secure gateway. Since exploitation is so easy for this vulnerability, the Common Vulnerability Scoring System (CVSS) rated it as 10.0. Bad Packets scans found a total of 14,528 Pulse Secure VPN endpoints vulnerable to CVE-2019-11510. According to their report 121 countries around the world have vulnerable hosts.[9]

CVE-2020-0688

MICROSOFT EXCHANGE

A remote code execution vulnerability exists in Microsoft Exchange Server when the server fails to properly create unique keys at install time.Knowledge of the validation key allows an authenticated user with a mailbox to pass arbitrary objects to be deserialized by the web application, which runs as SYSTEM.The security update addresses the vulnerability by correcting how Microsoft Exchange creates the keys during install. Microsoft patched this vulnerability in February 2020 as CVE-2020-0688. According to Microsoft, the issue is fixed by correcting how Microsoft Exchange creates the keys during install.

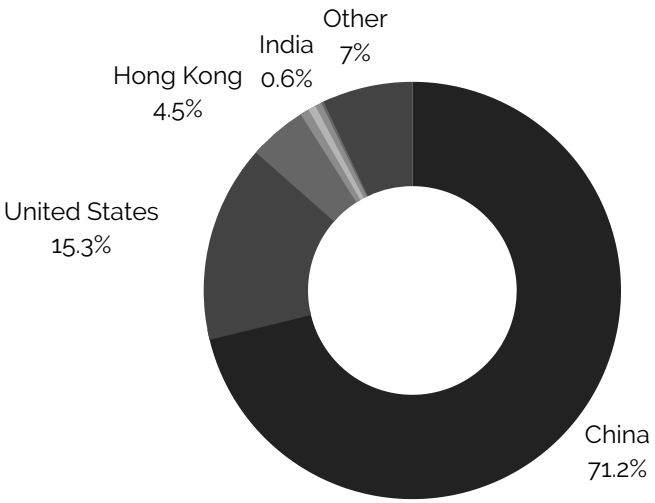
DDOS ATTACKS

DDoS attacks increased dramatically in 2020. Even though DDoS Intelligence statistics are limited to botnets detected, it can give us an idea how these kinds of attacks are still effective. [10] Ransom-driven DDoS attacks (RDDoS) are on the rise as groups claiming to be Fancy Bear, Cozy Bear and the Lazarus Group extort organizations around the world. As of this writing, the ransom campaign is still ongoing.

Stats:

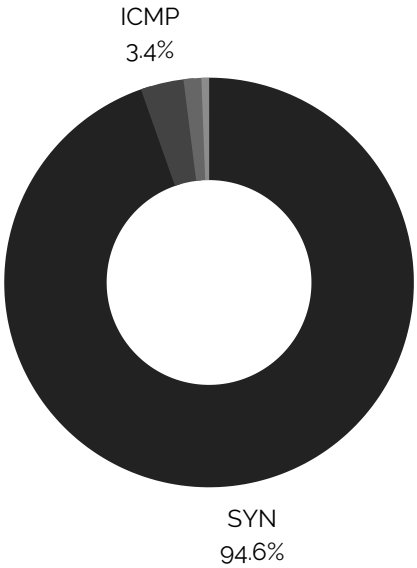
- 4.83 million DDoS attacks took place in the first half of 2020.
- 77% growth in attack size in the first half of 2020 compared to 2019.
- 92% of attacks were less than an hour.
- Linux botnets still dominate over their Windows counterparts, accounting for 95.39% of attacks

DDOS ATTACKS BY COUNTRY (2020 Q3)



The top 3 countries by number of targeted attacks remain unchanged: China (71.20), the US (15.30), and the Hong Kong Special Administrative Region (4.5)

DDOS ATTACKS BY TYPE

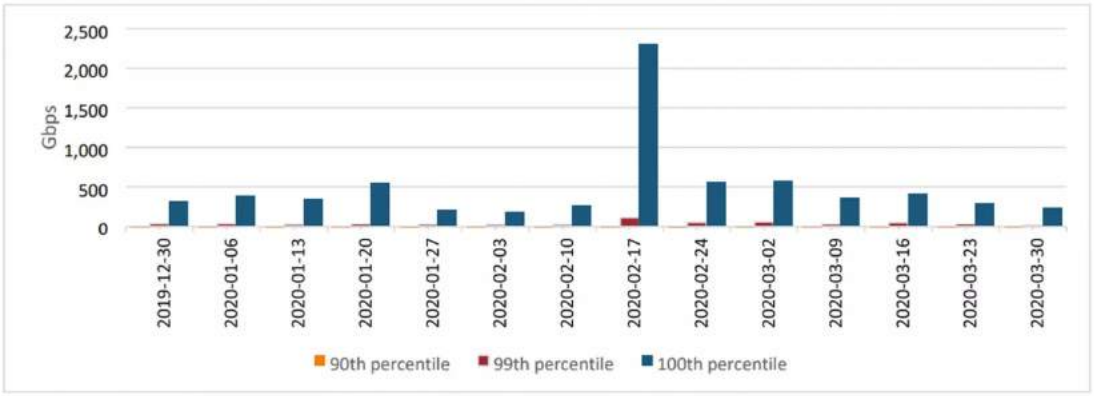


SYN flooding is still the main tool (94.6%), its share remaining virtually unchanged since the previous quarter. ICMP attacks comprised 3.4%, while HTTP flooding scored less than 0.1% of attacks.

ATTACK MAGNITUDE: 2.3 TBPS

AMAZON WEB SERVICES

In February 2020, Amazon Web Services was hit by an enormous DDoS attack. The attack lasted for three days and peaked at an 2.3 terabytes per second.This was one of the most extreme DDoS attacks ever so far. An unidentified AWS customer using a technique called Connectionless Lightweight Directory Access Protocol (CLDAP) Reflection. This technique relies on vulnerable third-party CLDAP servers request to a LDAP server with a spoofed IP address and amplifies the amount of data sent to the victim's IP address by 56 to 70 times.



The chart showing the scale of the attack. Source: Amazon

REFERENCES

[1] Ransomware Statistics, Trends and Facts for 2020 and Beyond. Cloudwards. Available on: https://www.cloudwards.net/ransomware-statistics/

[2] Global Surges in Ransomware Attacks. Check Point. Available on: https://blog.checkpoint.com/2020/10/06/study-global-rise-in-ransomware-attacks/

[3] 2020 Ransomware by Industry. Blackfog. Available on: https://www.blackfog.com/the-state-of-ransomware-in-2020/

[4] Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase. CoveWare. Available on: https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report#1

[5] 107 Must-Know Data Breach Statistics for 2020. Varonis. Available on: https://www.varonis.com/blog/data-breach-statistics/

[6] Average cost of data breaches worldwide as of 2020, by country or region. Statista. Available on: https://www.statista.com/statistics/463714/cost-data-breach-country/

[7] 2020 Third Party Risk Management Study Report. Available on: https://www.prevalent.net/assets/documents/resources/2020-third-party-risk-management-study-report.pdf

[8] 2020 Vulnerability and Threat Trends. Skybox Security. Available on: https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox_Report_2020-VT_Trends.pdf

[9] Over 14,500 Pulse Secure VPN Endpoints Vulnerable to CVE-2019-11510. Bad Packets. Available on: https://badpackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/

[10] DDoS attacks in Q3 2020. Securelist. Available on: https://securelist.com/ddos-attacks-in-q3-2020/99171/

About SOCRadar

The company is well positioned for continued success with a focus on innovation, global expansion, and feature-rich multifunctionality. Enterprises around the world are increasingly selecting SOCRadar to get proactive by understanding their attack surface and gaining automation-enabled visibility into surface, deep, and dark web. Our customers worldwide leverage our expertise and investment in scalable, innovative solutions to protect their most valuable assets: brand reputation, employees, customers and overall business operations.