sirar
by stc

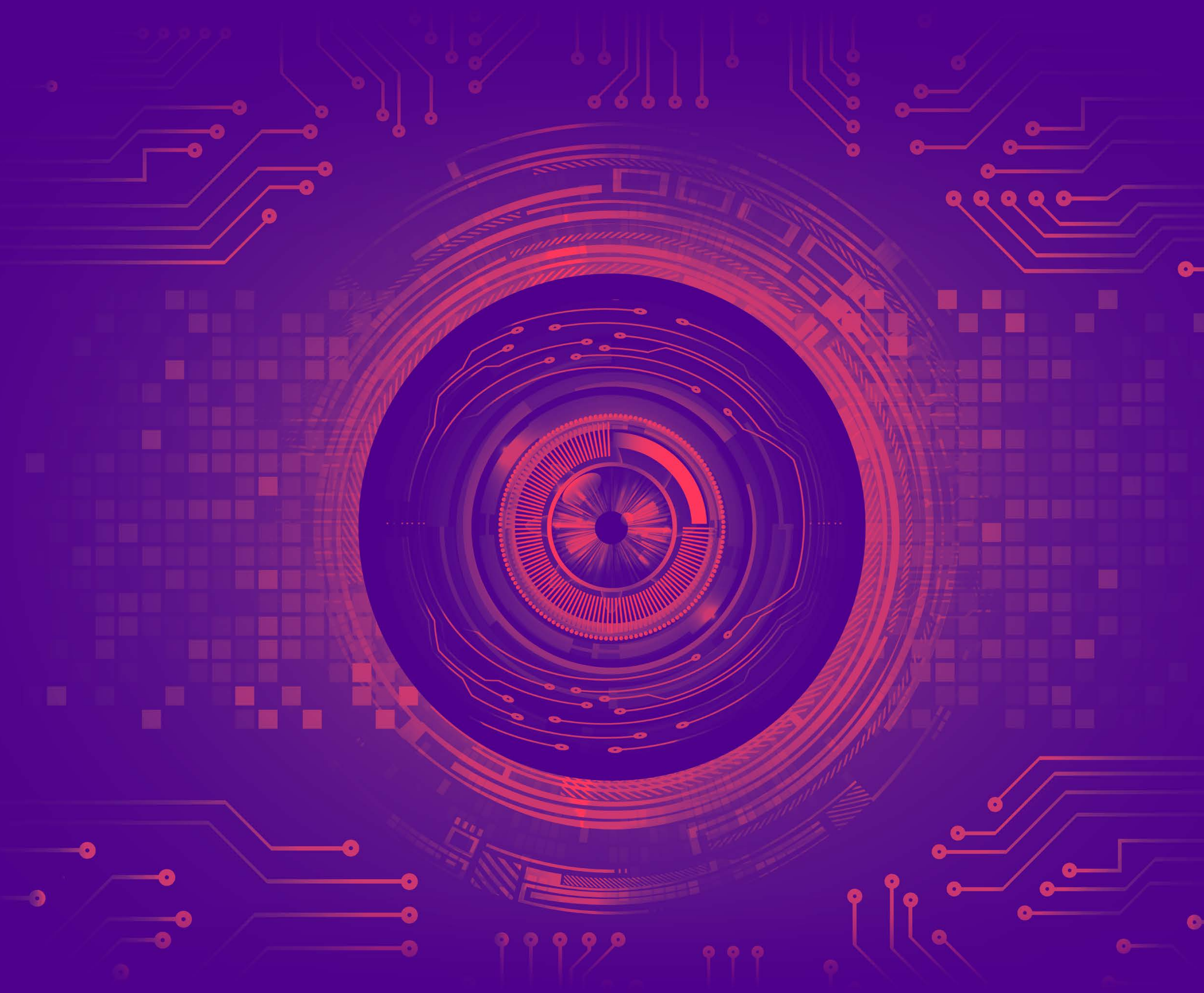
Threat Landscape

Report in 2022

Agenda

Introduction

01



sirar
by stc

Introduction

The Trusted platform for the data economy

Saudi Company

As a 100% Saudi company, we are not affected by the restrictions impacting foreign-owned consultancy companies.

Strong Partner Ecosystem

An ecosystem of top tier partners that we can leverage to compliment our offerings and fulfill all your needs.

Highly Qualified Team

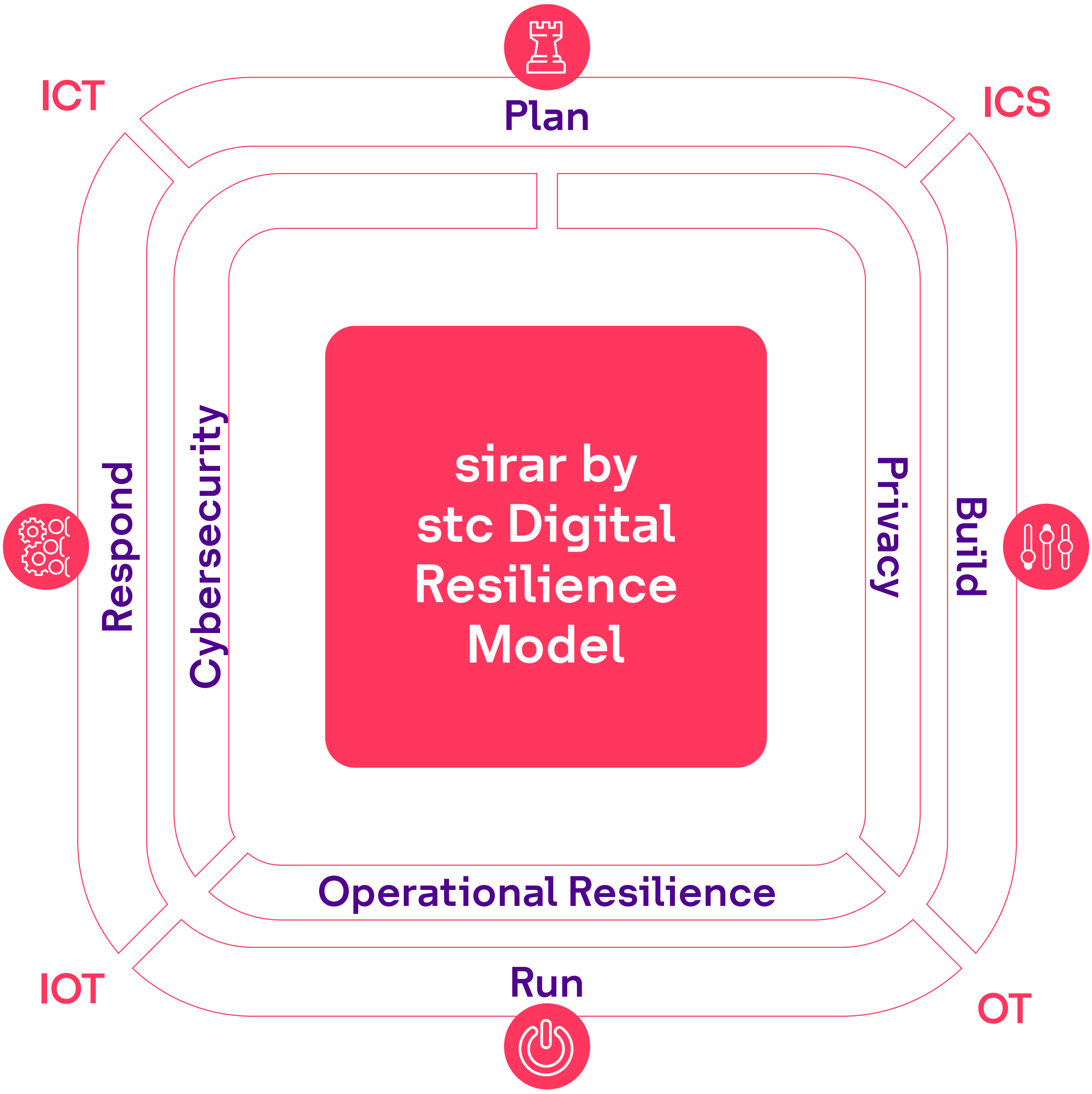
A team with an average of 15 years of experience; previously worked for international companies, large entities, and big 4

One Stop Shop

We provide all your privacy, cybersecurity, & resilience needs; save the time spent coordinating between many vendors.

Data Driven Protection

Offering Superior Threat Intelligence as we have great visibility on the threat landscape locally and regionally

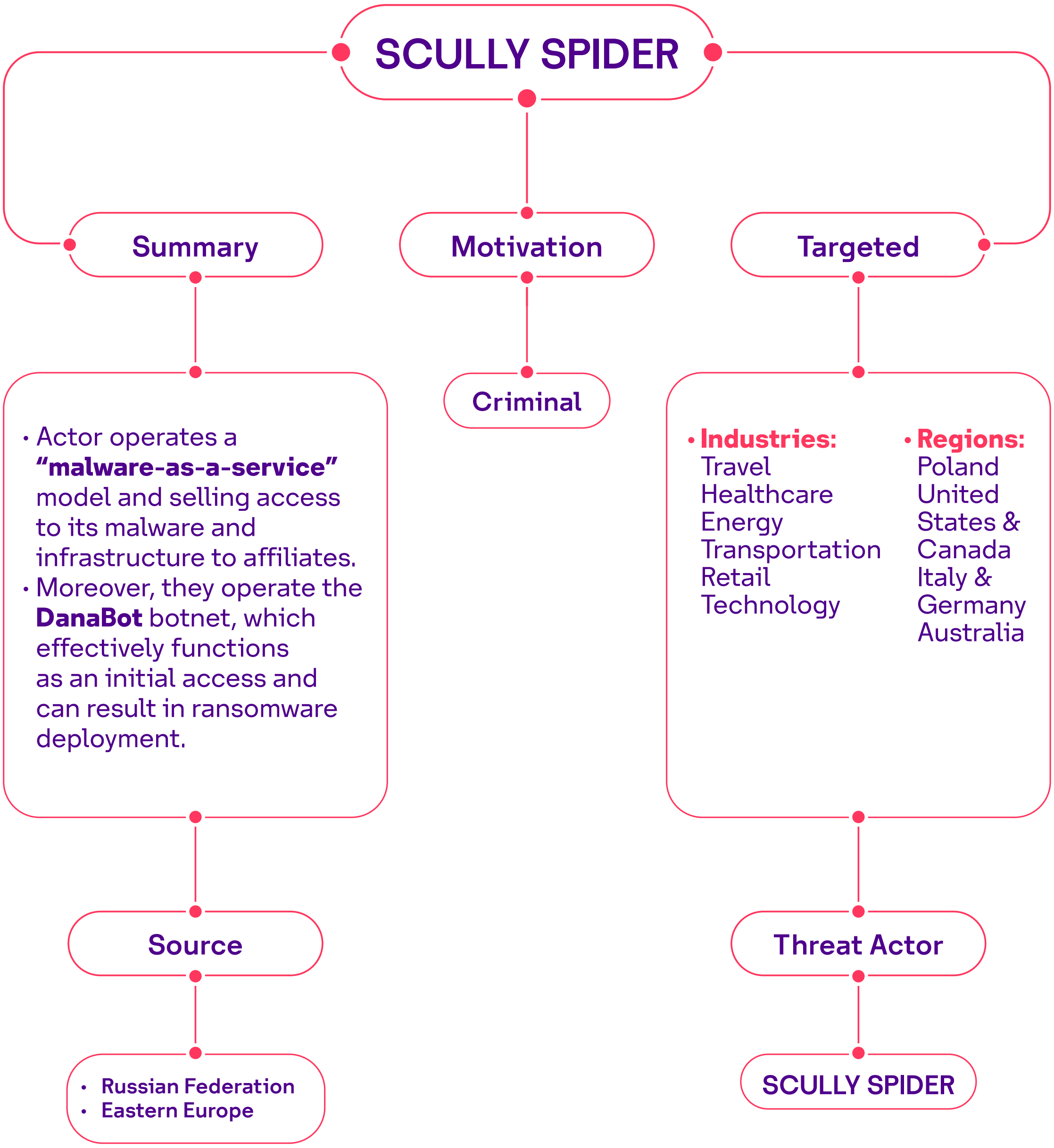


Global Attack Trends

02

sirar
by stc

Most Global Active APTs



SCULLY SPIDER

Summary

- Actor operates a **“malware-as-a-service”** model and selling access to its malware and infrastructure to affiliates.
- Moreover, they operate the **DanaBot** botnet, which effectively functions as an initial access and can result in ransomware deployment.

Motivation

Criminal

Targeted

- **Industries:** Travel, Healthcare, Energy, Transportation, Retail, Technology
- **Regions:** Poland, United States & Canada, Italy & Germany, Australia

Source

- Russian Federation
- Eastern Europe

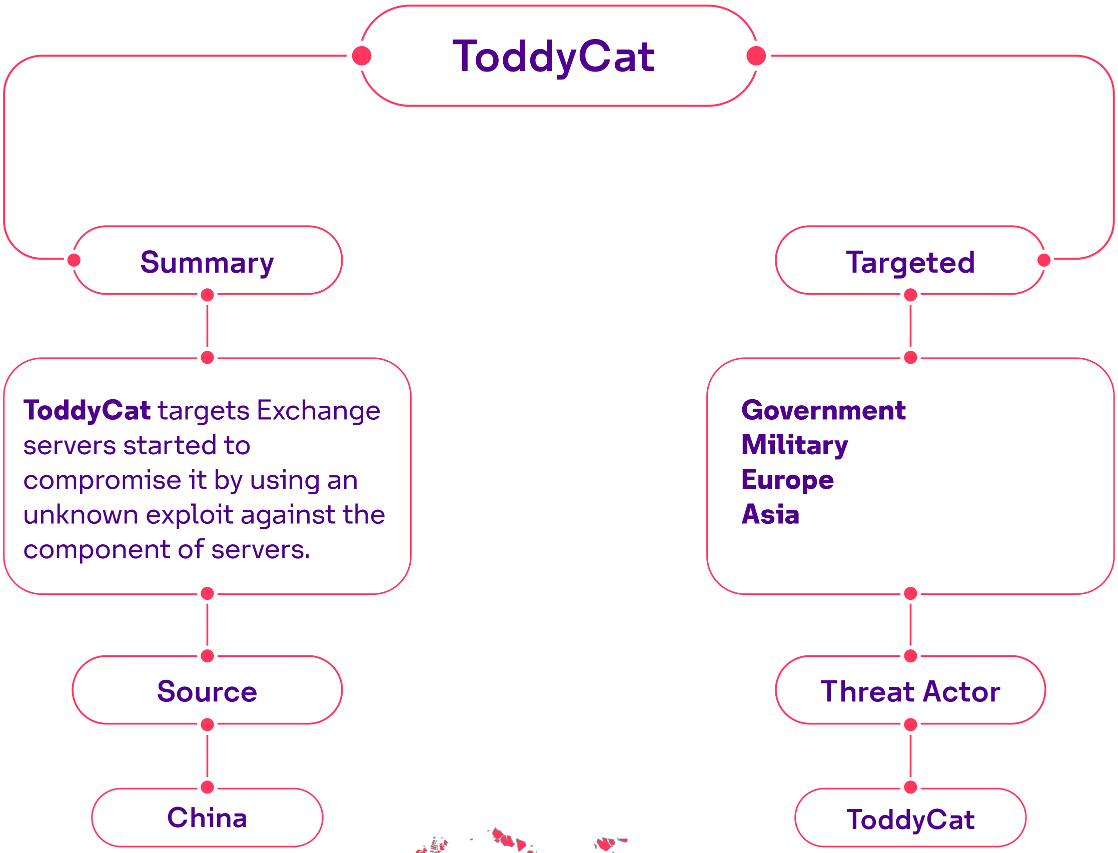
Threat Actor

SCULLY SPIDER

Russian & Europe based threat actor

APT Stands for advanced persistent threat (Attack Group).

Most Global Active APTs



ToddyCat

Summary

ToddyCat targets Exchange servers started to compromise it by using an unknown exploit against the component of servers.

Source

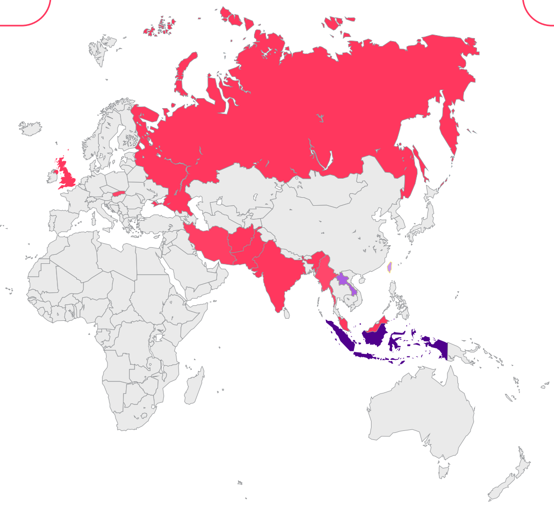
China

Targeted

Government
Military
Europe
Asia

Threat Actor

ToddyCat



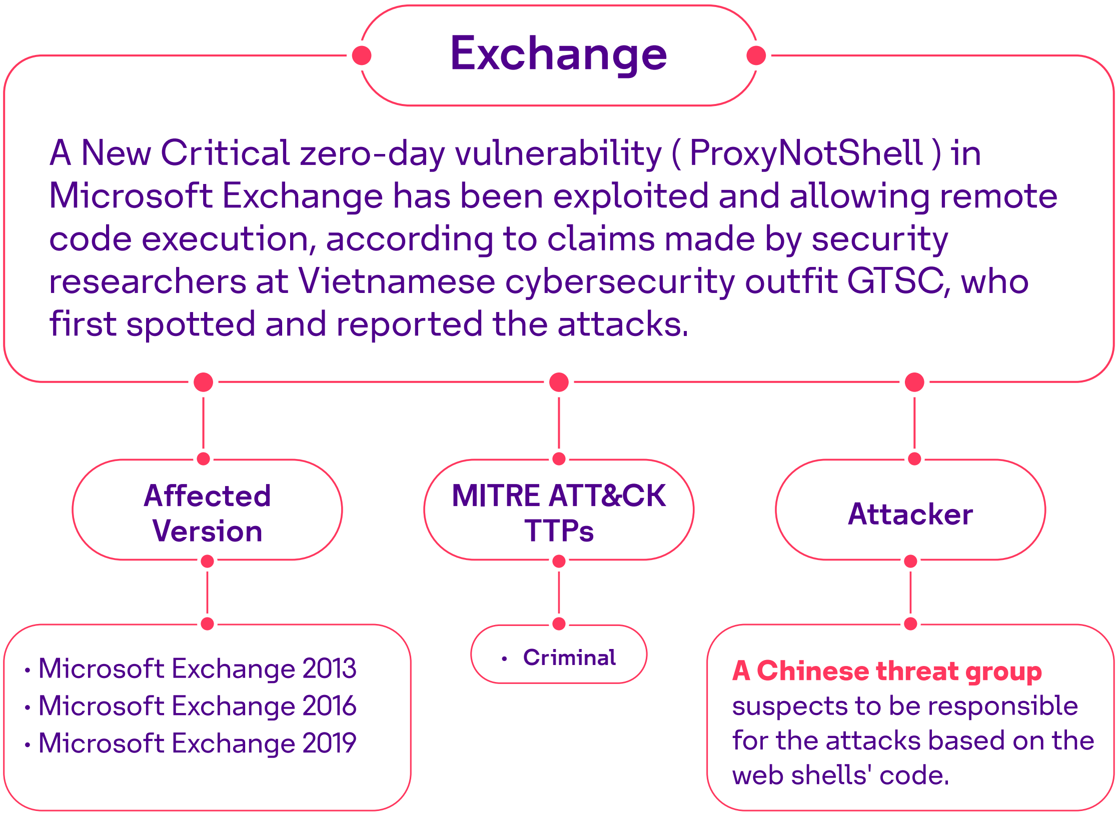
● The First wave ● The Second wave ● The Third wave

China based threat actor

APT Stands for advanced persistent threat (Attack Group).

Microsoft Exchange Zero-Day vulnerability

(ProxyNotShell)



Exchange

A New Critical zero-day vulnerability (ProxyNotShell) in Microsoft Exchange has been exploited and allowing remote code execution, according to claims made by security researchers at Vietnamese cybersecurity outfit GTSC, who first spotted and reported the attacks.

Affected Version

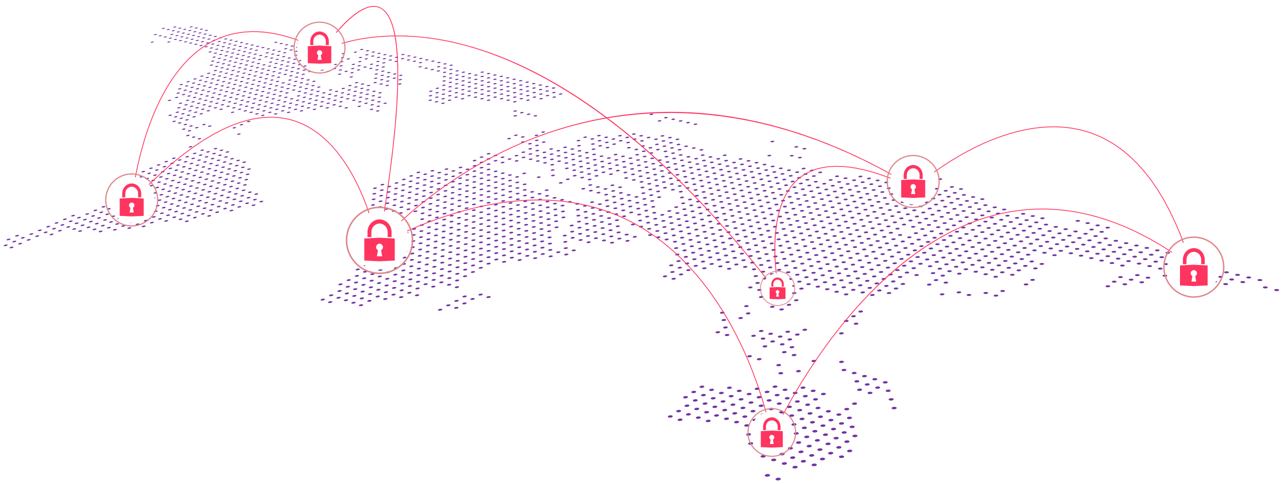
- Microsoft Exchange 2013
- Microsoft Exchange 2016
- Microsoft Exchange 2019

MITRE ATT&CK TTPs

- Criminal

Attacker

A Chinese threat group suspects to be responsible for the attacks based on the web shells' code.



Source: PaloAlto

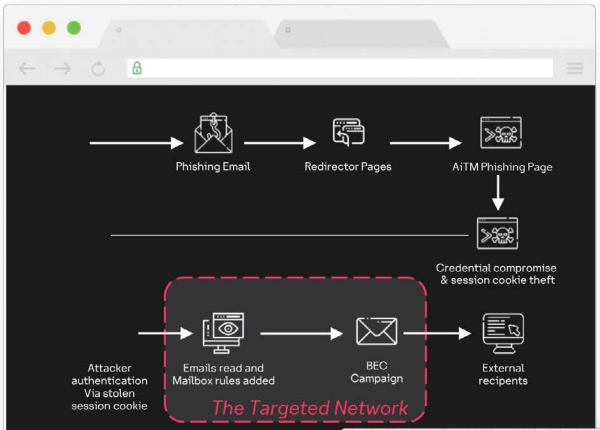
Microsoft Warns AiTM Phishing Attacksand Payment Frauds

Microsoft

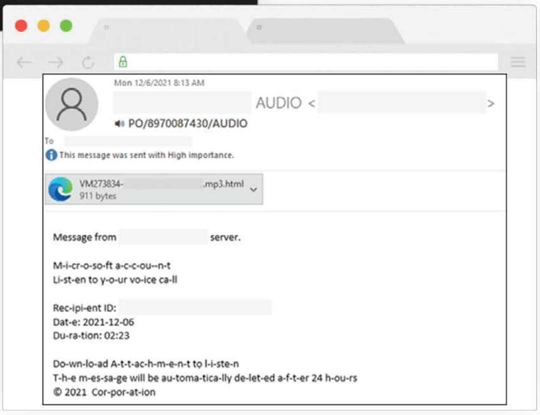
Microsoft disclosed a large-scale phishing campaign targeting over 10,000 organizations by hijacking Office 365's authentication process. It uses stolen credentials and session cookies to access affected users' mailboxes to perform payment fraud by using a technique called Email Thread Hijacking to dupe parties.

Technical Details:

Threat Actor : Unknown
Threat Vector: Phishing site
Impact : Credentials & Session Cookies Theft, Payment fraud
Severity : High


Phishing Email
Redirector Pages
AiTM Phishing Page
Credential compromise & session cookie theft
Attacker authentication Via stolen session cookie
Emails read and Mailbox rules added
BEC Campaign
External recipents
The Targeted Network

Attacker Action Flow.



Mon 12/6/2021 8:13 AM
AUDIO < >
PO/8970087430/AUDIO
To
This message was sent with High importance.

VM273834- .mp3.html
911 bytes

Message from server.

M-i-cr-o-so-ft a-c-c-ou--n-t
Li-st-en to y-o-ur vo-ice ca-ll

Rec-ipi-ent ID:
Dat-e: 2021-12-06
Du-ra-tion: 02:23

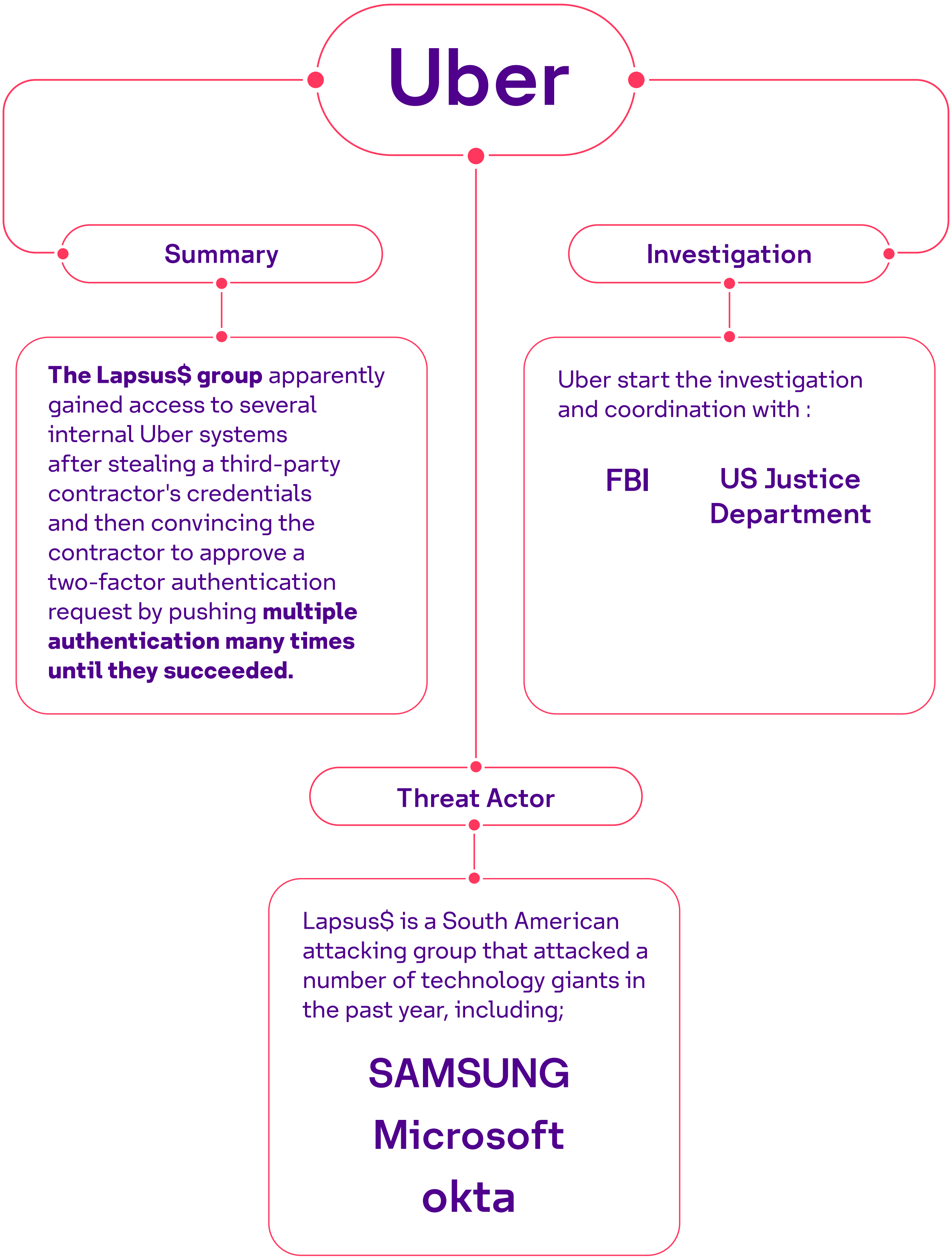
Do-wn-lo-ad A-t-t-ac-h-m-e-n-t to l-i-ste-n
T-h-e m-es-sa-ge will be au-toma-tica-lly de-let-ed a-f-t-er 24 h-ou-rs
© 2021 Cor-por-at-ion

Figure 2: Phishing sample.

Source: Microsoft

Introduction
Global Attack Trends
KSA Statistics
sirar Battles
Key takeaways
sirar Glossary
References

Uber's Internal Network Breached



Uber

Summary

The Lapsus$ group apparently gained access to several internal Uber systems after stealing a third-party contractor's credentials and then convincing the contractor to approve a two-factor authentication request by pushing **multiple authentication many times until they succeeded.**

Investigation

Uber start the investigation and coordination with :

FBI

US Justice Department

Threat Actor

Lapsus$ is a South American attacking group that attacked a number of technology giants in the past year, including;

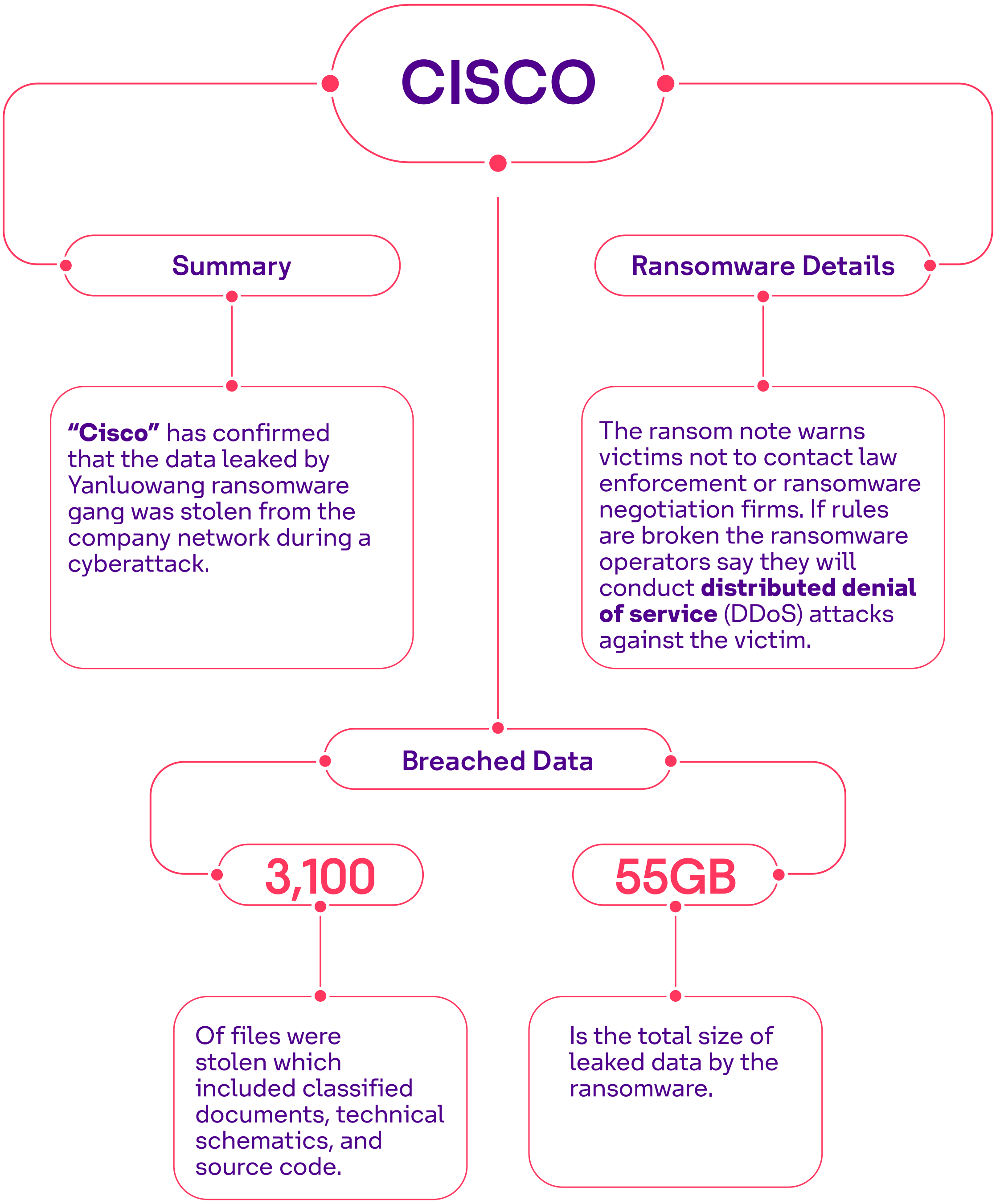
SAMSUNG

Microsoft

okta

Source: The Newyork times

Cisco Hit By Ransomware That Leaked Its Data



CISCO

Summary

"Cisco" has confirmed that the data leaked by Yanluowang ransomware gang was stolen from the company network during a cyberattack.

Ransomware Details

The ransom note warns victims not to contact law enforcement or ransomware negotiation firms. If rules are broken the ransomware operators say they will conduct **distributed denial of service** (DDoS) attacks against the victim.

Breached Data

3,100

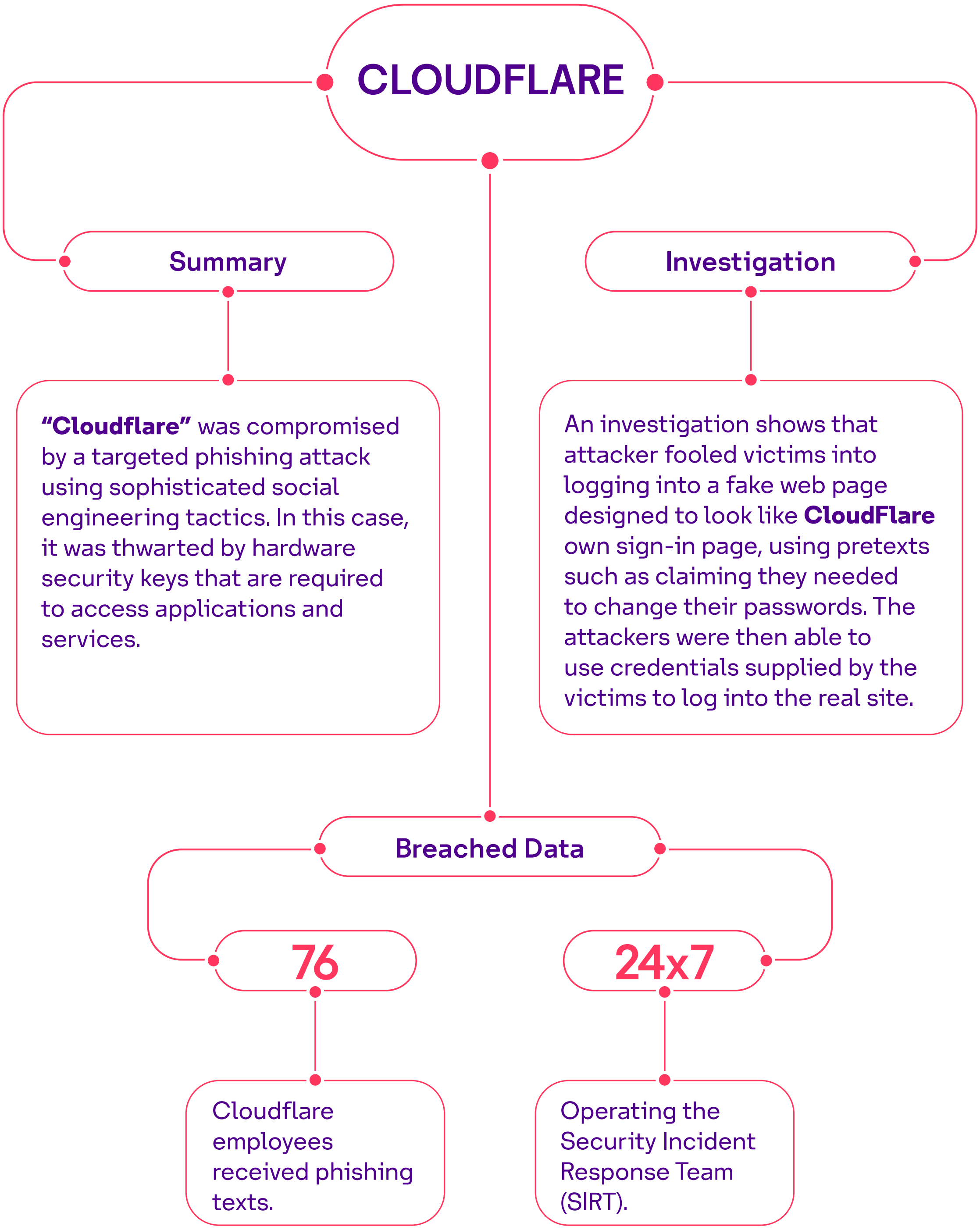
Of files were stolen which included classified documents, technical schematics, and source code.

55GB

Is the total size of leaked data by the ransomware.

Source: Cisco talos

Phishing Campaign Reported On Twilio & Cloudflare



CLOUDFLARE

Summary

"Cloudflare" was compromised by a targeted phishing attack using sophisticated social engineering tactics. In this case, it was thwarted by hardware security keys that are required to access applications and services.

Investigation

An investigation shows that attacker fooled victims into logging into a fake web page designed to look like **CloudFlare** own sign-in page, using pretexts such as claiming they needed to change their passwords. The attackers were then able to use credentials supplied by the victims to log into the real site.

Breached Data

76

Cloudflare employees received phishing texts.

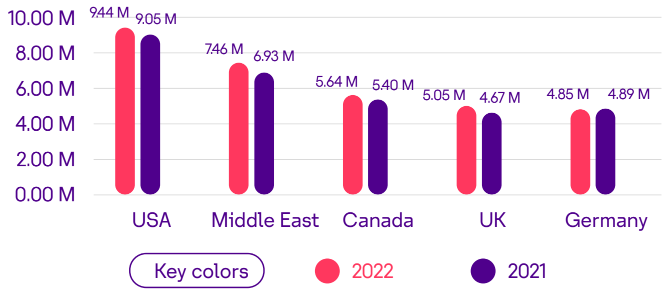
24x7

Operating the Security Incident Response Team (SIRT).

Source: Cloudflare

Cyber Data Breach Statistics 2022

Average Cost Of A Data Breach For Top 5 Country/Region



Breaches Cost And Causes

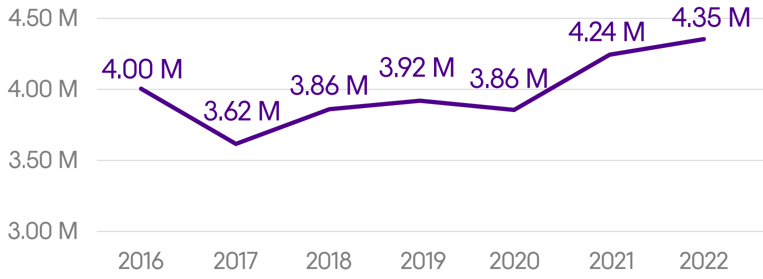
$4.24M

Is the cost of data breach of **private** clouds in 2022.

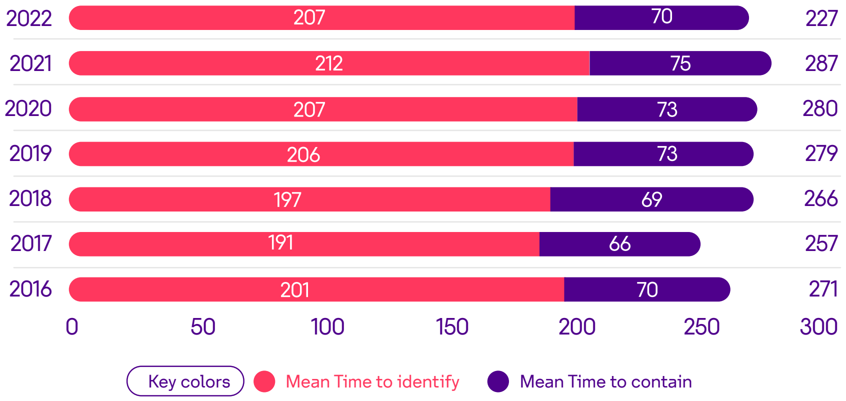
$5.02M

Is the cost of data breach of **public** clouds in 2022.

Average Total Cost Of Data Breach



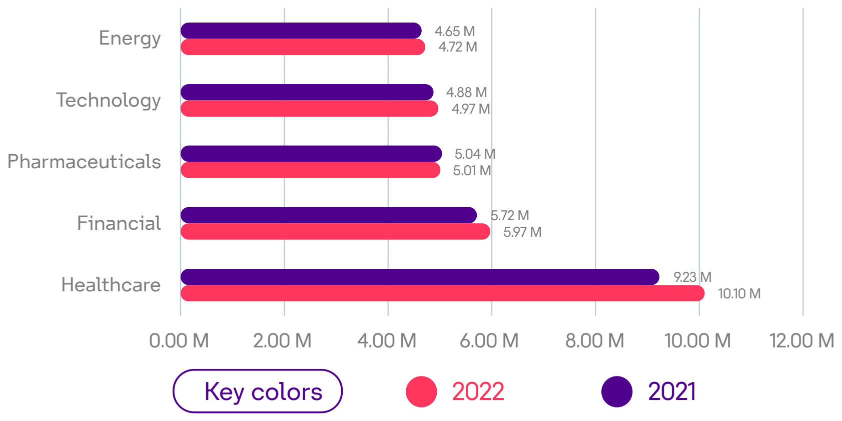
Average Time To Identify And Contain A Data Breach



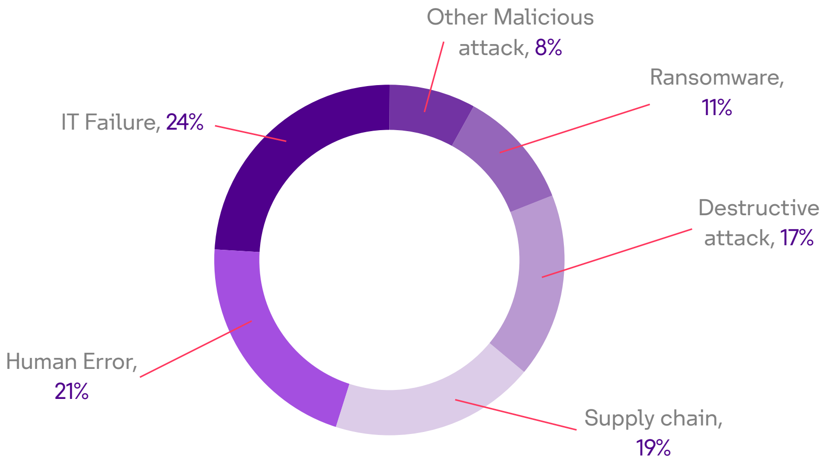
Source: IBM

Cyber Data Breach Statistics 2022

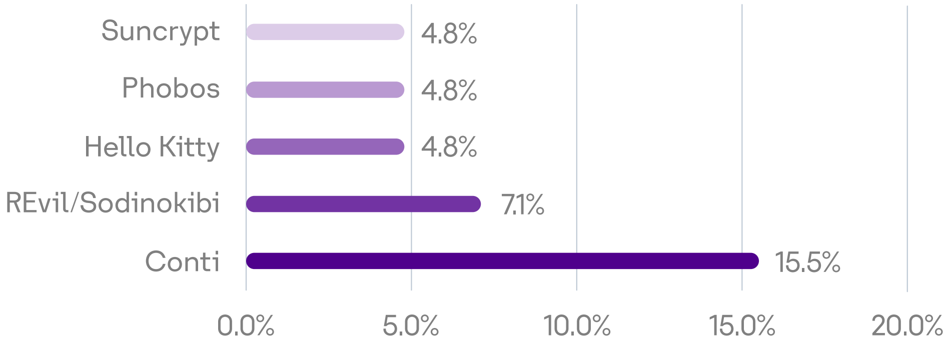
Average Cost Of A Data Breach By Top 5 Industry



Types of breaches experienced by organizations



Most Active Ransomware Group



Source: IBM

Cyber Sector Attacks

Sector	List of Actors	List of Malware & Tools
HealthCare	TEMP.Hex UNC2633 UNC2420 UNC2500 UNC3840 APT29 UNC2835 UNC3810	NIGHTROPE BITPAYMER FAKEUPDATES FLASHBANG HANDYAXE SNOWFIRE CASUMARZU CHIPSEAL MIXDOOR SUCCESSFLY
Logistics and Industry	UNC1543 UNC2975 UNC2165 FIN11 UNC2824	TOUGHQUIZ OLDFLAT ROOMMATE DRABCUBE
Metaverse	UNC3524	QUIETEXIT
Smart Cities	FIN11	CLOP FLOWERPIPE QUICKPEEK SIXFINGERS
Space	GhostSec Gonjeshke Darande UNC4368 Gaza Cybergang	CLOP INCONTROLLER METEORLIGHT METEOR

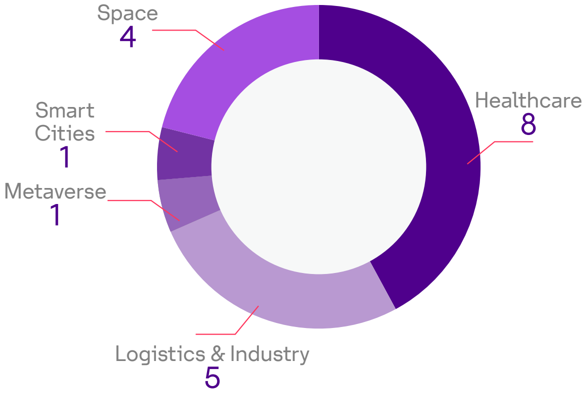
Source: Anamoli
Source: Mandiant

Cyber Sector Attacks

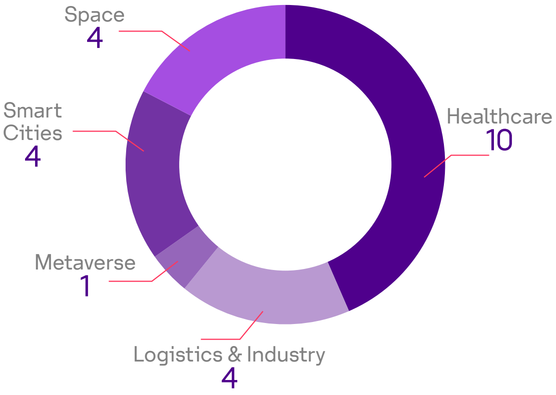
Indicator Of Compromised By Sector

Total Indicators	Sector
1,726	Healthcare
238	Logistics and Industry
1,899	Space
323	Smart Cities
7	Metaverse

Total Actors



Total Malware & Tools



Source: Anamoli
Source: Mandiant

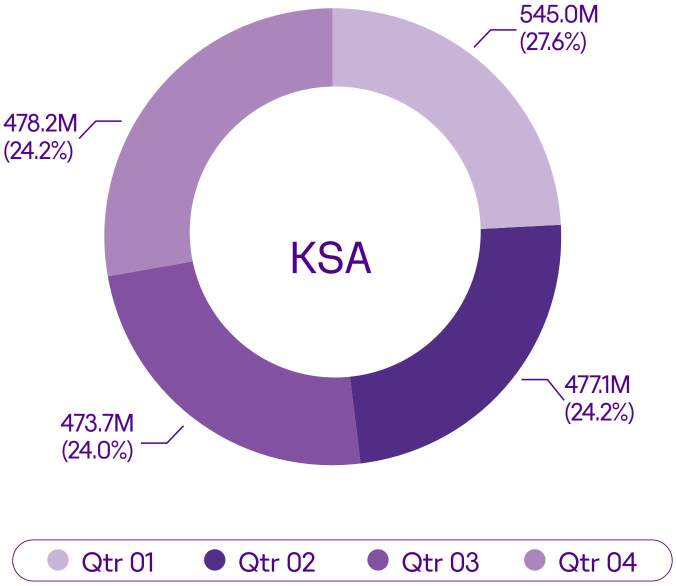
KSA Key Statistics

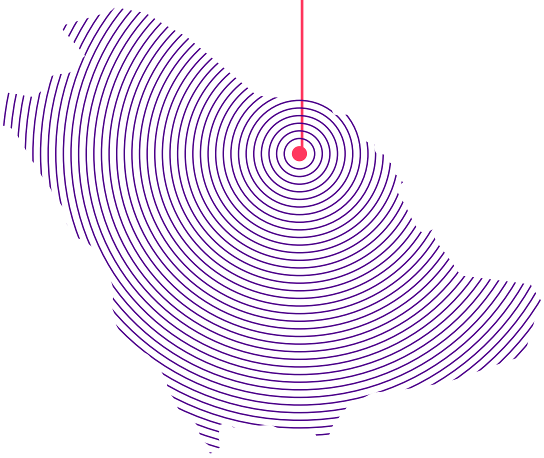
03

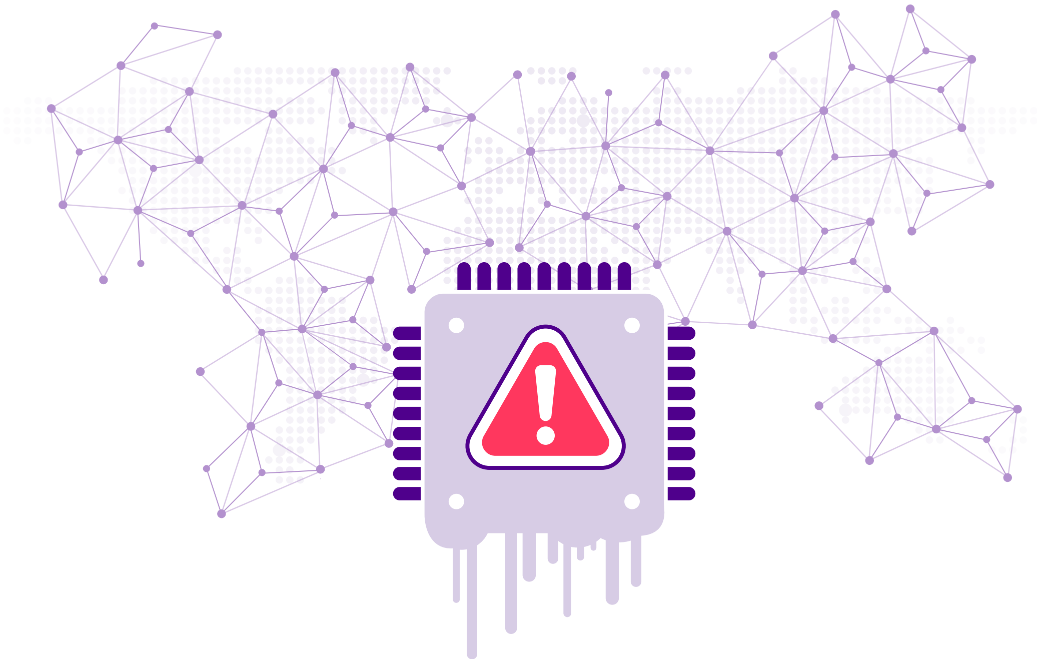
sirar
by stc

Malicious Activity Distribution by Country

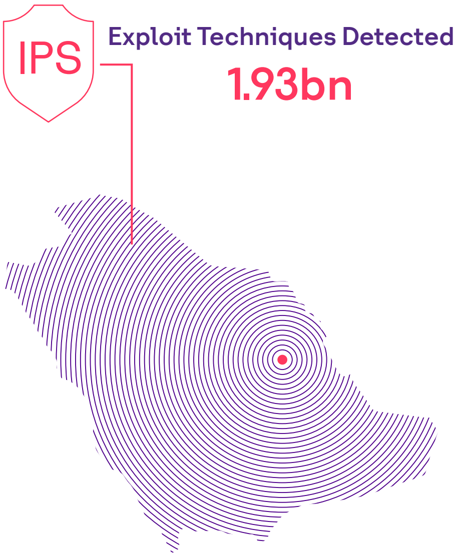
Saudi Arabia







Exploit Attempts



Exploit Techniques Detected

1.93bn

Log4Shell

53 M

DoublePulsar

624 M

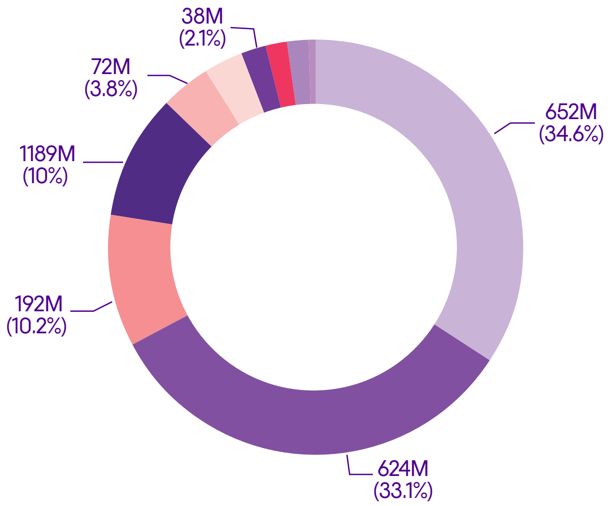
Cross Site Scripting

3 M

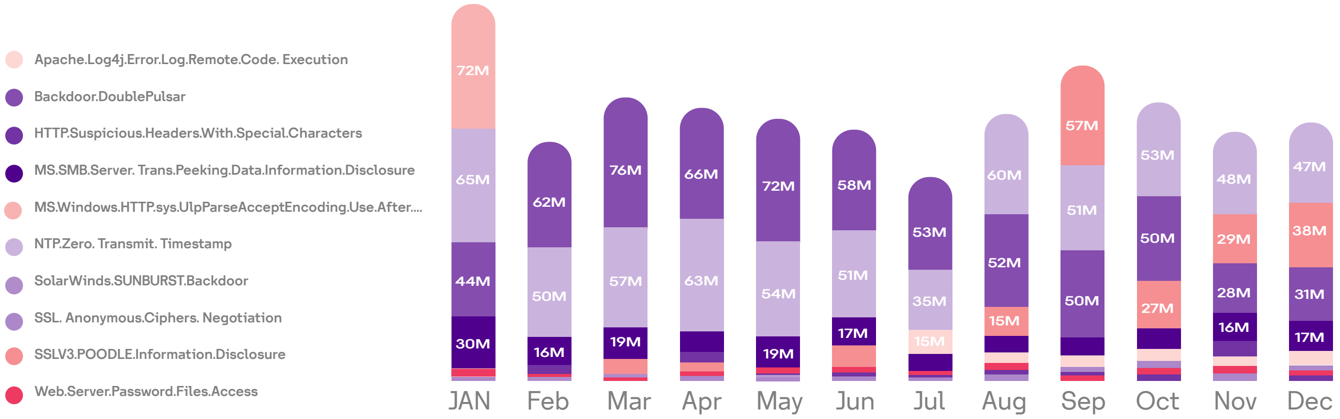
SUNBURTS

10 M

Exploit Attempts Distribution by Signature



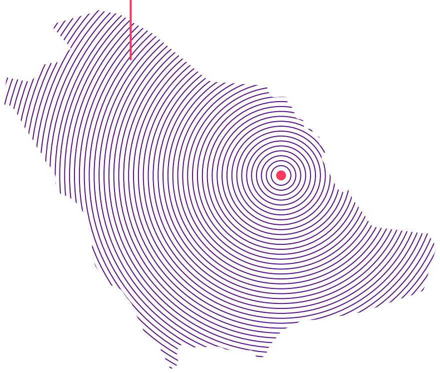
Behavioral Trend Analysis by Signature



Malware Detections

AV Malware Distribution Detected

10.53M



CryptoMiner

956K

Trojans

8M

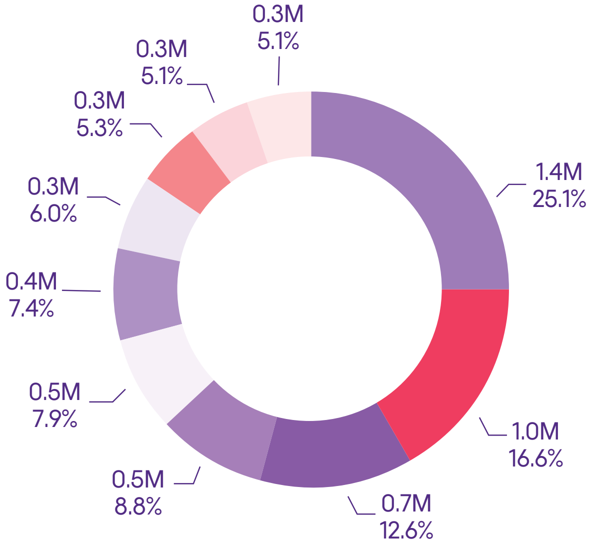
Mal Office Docs

3M

Drive by Download

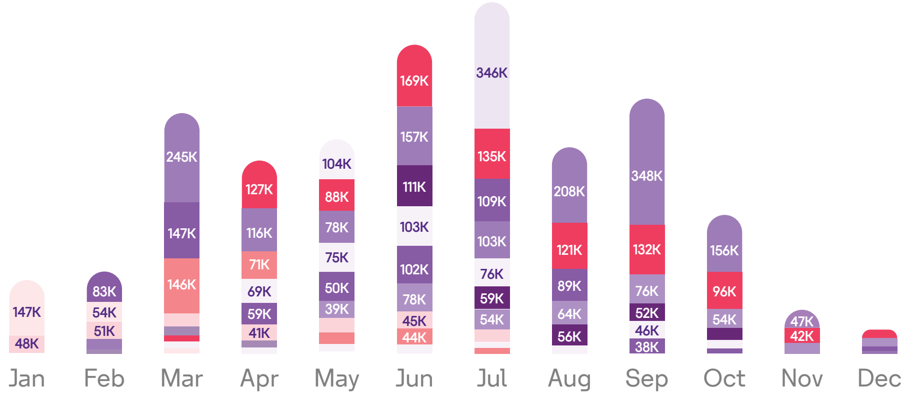
1 M

Malware Distribution by Signature



Behavioral Trend Analysis by Signature

- ● LNK/Phishing.B166!tr
- ● MSExcel/Agent.DKF!tr.dldr
- ● MSExcel/Agent.DVP!tr.dldr
- ● MSExcel/CVE 2017_11882.F!exploit
- ● MSExcel/CVE 2018 0798.F!exploit
- ● MSIL/Injector.VLV!tr
- ● MSOffice/CVE_2017_11882.C!exploit
- ● VBS/Rbik.5BDA!tr
- ● W32/CVE 2017_11882.F!exploit
- ● 1XF/Coin Miner.Z!tr



FortiGaurd labs

Botnet Activity

C2

Botnet Activity Detected

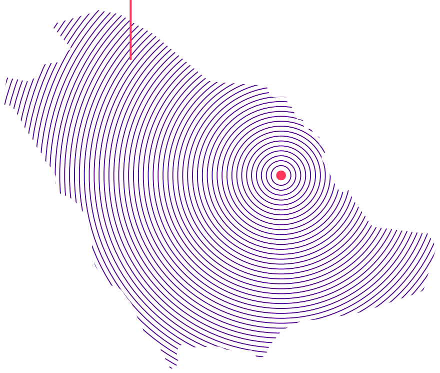
41.67M

IoT- MIRAI
1 M

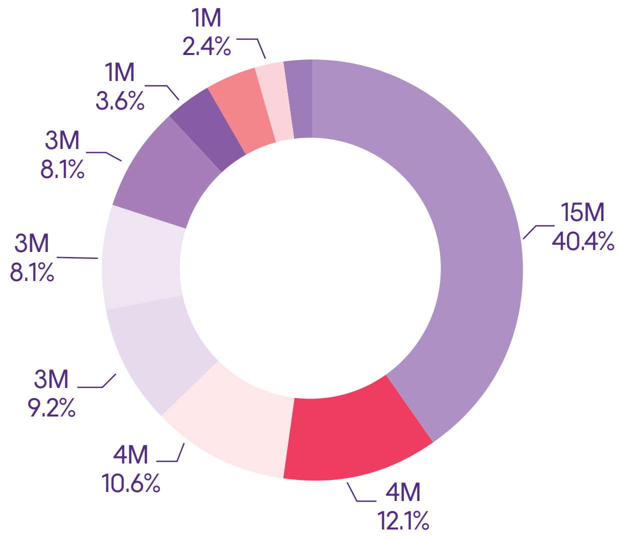
GhOst RAT
120K

H-Worm
1 M

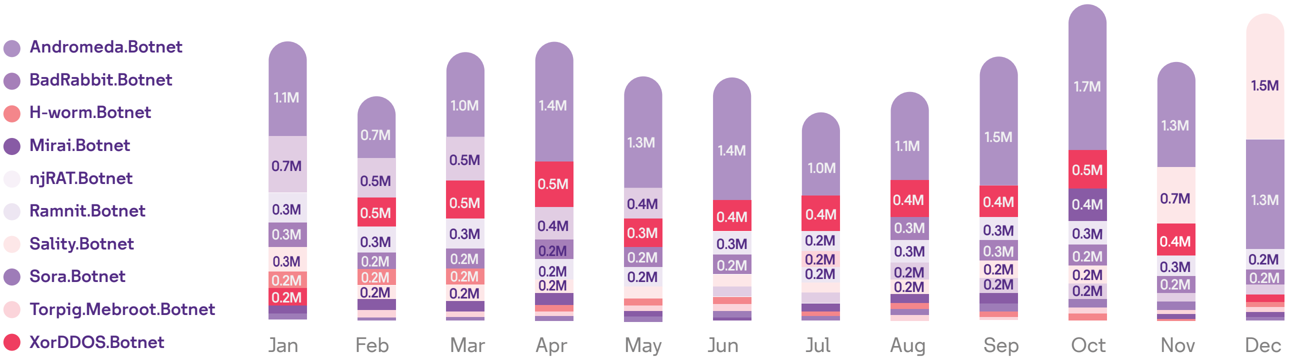
Bad Rabbit
3 M



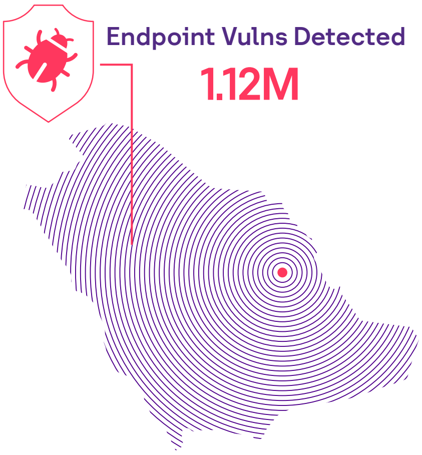
Botnet Activity Distribution by Signature



Behavioral Trend Analysis by Signature



Endpoint Vulnerabilities



Endpoint Vulns Detected

1.12M

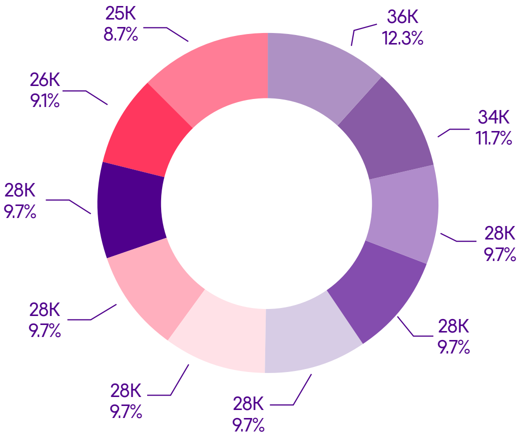
Oracle Vulns

675K

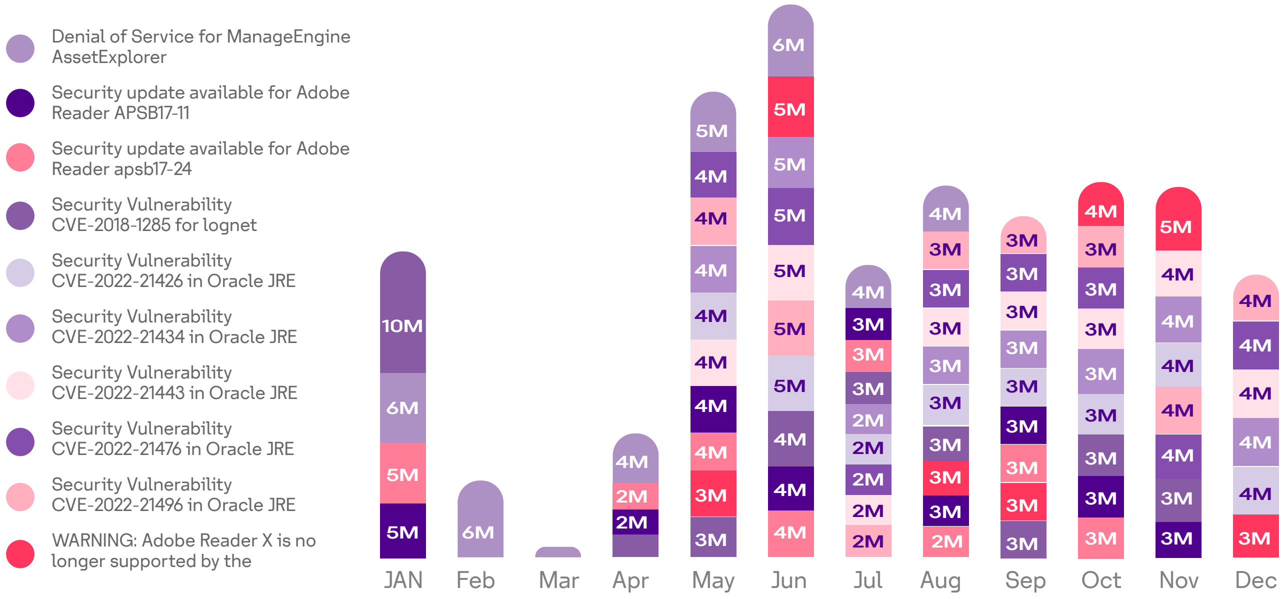
Log4Net

34K

Vulnerabilities Distribution by Signature



Behavioral Trend Analysis by Signature



KSA Breaches On The Dark Web

5
Underground forums selling or sharing the leaked data.

256
The number of Actors behind the breaches.

111
Corporation infected by the breaches.

1057
Total number of breaches on the dark web.

sirar Battles

04

sirar
by stc

sirar Battles

DDoS

sirar
by stc

Top DDoS Attacks In KSA In 2022

208 Gbps

Top 4 attacks by volume
The size of the largest DDoS attack mitigated 2022

182 Gbps

178 Gbps

171 Gbps

Total Prevented Downtimes

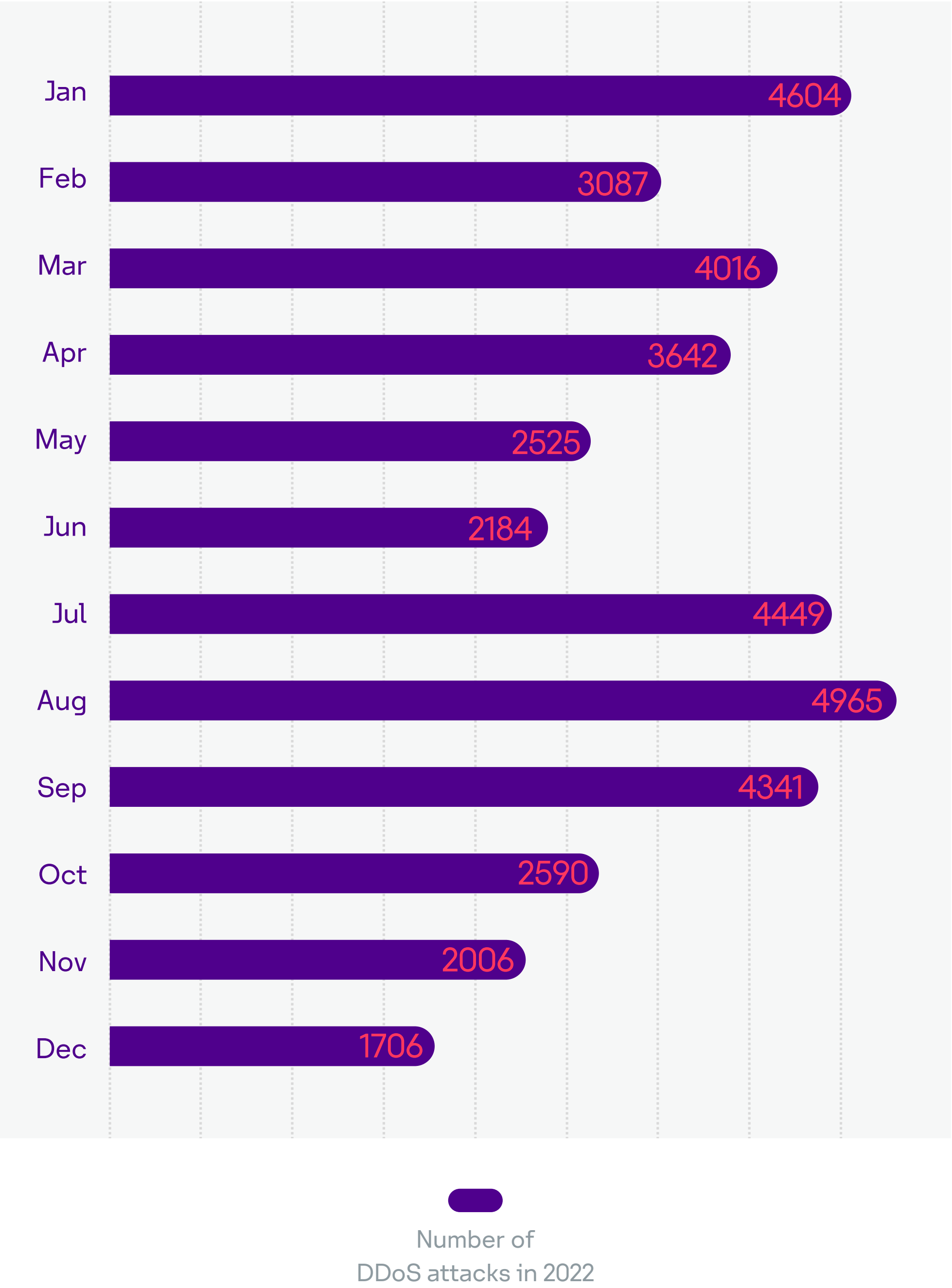
5,560 Hours

The period of time a DDoS attack could have taken services / network / applications down if not mitigated properly .

4 TB

Our local scrubbing unit (which is the largest in the region) can mitigate up to 8tps on cloud level.

Top DDoS Attacks In 2022:



Source : **sirar** Anti - DDoS service

DDoS Attacks In Details

49% NTP Amplification

DDoS attacks that exploit publicly- accessibile Network Time Protocol (NTP) servers to overwhelm the targeted with UDP traffic.

18% DNS Amplification

DDoS attacks that massively exploit open recursive DNS servers mainly for performing bandwidth consumption DDoS attacks.

20% Others

Other vectors i.e., TCP SYN, CLDAP, Memcache.. etc.

13% UDP

DDoS attacks that can be initiated when an attacker sends a large number of UDP packets to random ports on a remote host.

sirar Battles

VMDR

Vulnerability Management, Detection and Response

sirar
by stc

Vulnerability Management, Detection And Response (VMDR)

In **2022**

402K

CLOSED VULNERABILITIES

This represents A **172%** increase in closed vulnerabilities vs last year.

785K

VULNERABILITIES DETECTED

This Represents A **192%** increase in vulnerabilities detected vs last year.

sirar by stc vulnerability management detection and response services gives your organization a continuous, always-on , assessment of your infrastructure Cybersecurity vulnerabilities and compliance posture.

sirar Battles

Email Security

sirar
by stc

Email Security

In 2022

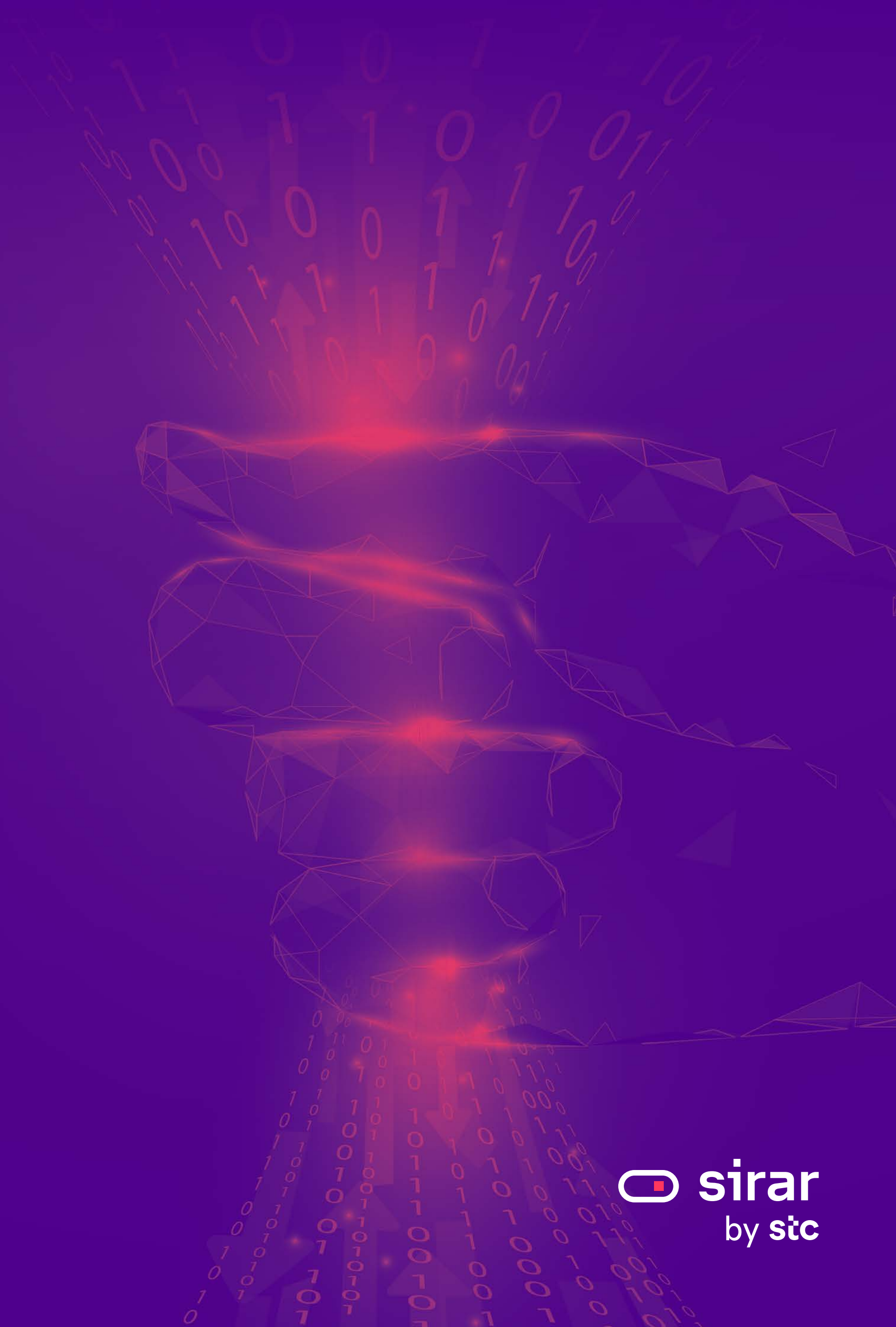
84.92%
PERCENTAGE OF CLEAN EMAILS

15.08%
PERCENTAGE OF BLOCKED EMAILS

The email security is helping customers to prevent, detect and respond to the latest email-borne threats including spam, phishing, malware, zero-day threats, impersonation, and Business Email Compromise (BEC) attacks.

sirar Battles

Web Security



sirar
by stc

Web Security

In 2022

Total Number of **transactions** proceed in sirar:

251.7 M

Total Number of **threats** blocked in sirar:

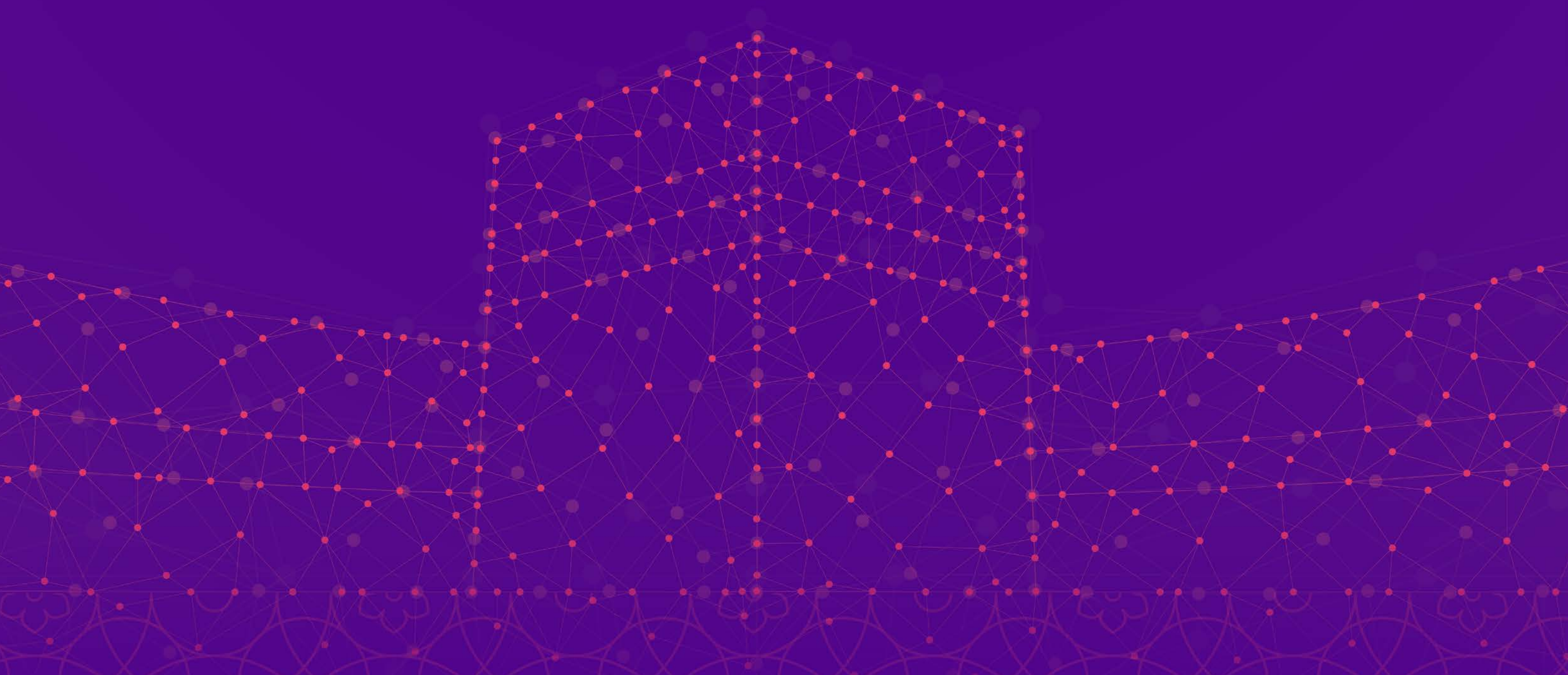
2.398 M

Total Number of **policy traffic** Volume:

266.6 GB

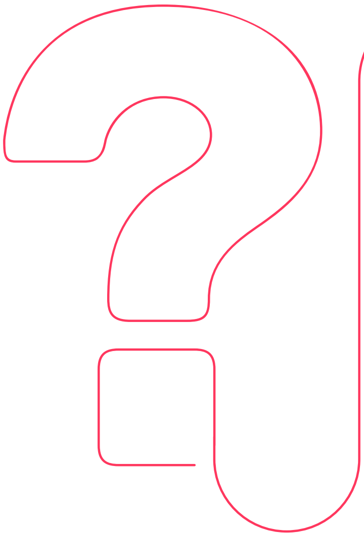
sirar Battles

Hajj & National Day



sirar
by stc

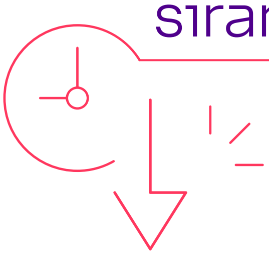
Our Contributions To Keep Our Home And Country Safe



What Happened During Hajj?

1 **sirar's contribution**

sirar monitoring services



600 Million Inbound Malicious traffic

Blocked Malware: **39**

Our Contributions To Keep Our Home And Country Safe

2 sirar’s contribution

Prevented Attacks
(29th of June – 11th of July)

DDoS

Total Attacks: **1266**

The largest mitigated **DDoS attack** **66** Gbps

Total
Prevented Downtime

167:12:38
Hour

Our Contributions To Keep Our Home And Country Safe

What Happened During National Day?

sirar's contribution

During national day, sirar was able to protect the Kingdom against multiple attacks

Most targeted entities were government and critical infrastructure

74 phishing URL's addressed

111 phishing domains addressed

10 ATP's and
9 Malwares Adressed

Our Contributions To Keep Our Home And Country Safe

What Happened During Jeddah summit?

sirar's contribution

sirar by stc was defending Jeddah Security and Development Summit from Cyber Attacks

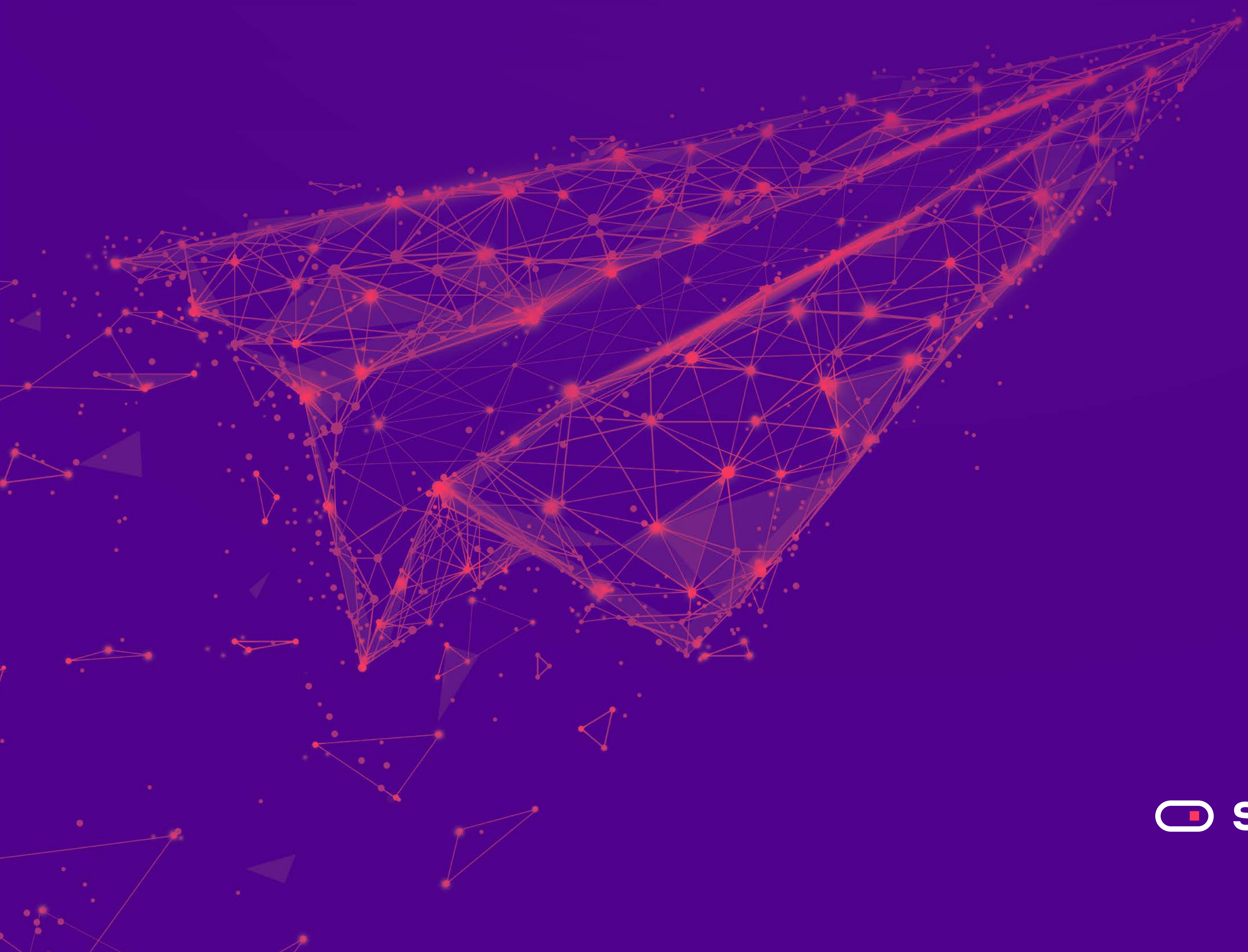
+33
Number of blocked attacks

5.5 Gbps
Largest attack size

+8 Hours
Total prevented downtime

Key takeaways

04



sirar
by stc

Main Takeaways

Proactive Security , Data Backups and Relevant additional security controls are necessary to prevent **Ransomware**

Software Code security is essential to prevent **Supply Chain Attacks**

Effective Information Security Governance **Policies**

User Awareness is paramount to prevent infection through **Phishing**

Build your outbound countermeasures to detect data exfiltration with **Web Security** solution

Adoption of **AI** / **ML** in security to stop sophisticated Attacks

Security First kind of cultural shift should be instilled to prevent intrusions

Make the service available and stable with **Anti-DDoS Service**

sirar Glossary

05

sirar
by stc

sirar **Glossary**

Cybersecurity

Cybersecurity is a process through which people and organizations lower their risk of being attacked online. The main goal of cyber security is to prevent theft or damage to the electronic devices that we all use (which include computers, laptops, tablets, and smartphones) along with the services we use both at work and at home.

SOCaaS

The Security Operations Center performs 24/7 comprehensive monitoring for advanced cyber threats across client on-premise networks, cloud environments, SaaS applications, endpoints, and event logs encriched with threat intelligence. The SOC has senior analysts that conduct threat hunting in logs to improve detection capabilities and find anomalies that are not automatically detected in addition to threat-intelligence based detection. The SOC will be monitoring for the tactics and techniques based on leading Cybersecurity frameworks.

Ransomware Attack

is a type of malware actively used by cybercriminals to disrupt a victim's organization by encrypting an organization's important files into an unreadable form and demands a ransom payment to decrypt them.

DDoS

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) is a framework, set of data metrics, and assessment tool developed by MITRE Corporation to help organizations understand their security readiness and uncover vulnerabilities in their defenses.

Malware

Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for “malicious software.” Examples of common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransomware.

Phishing Attacks

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually performed through email. The goal is to steal sensitive data like credit card , login information or to install malware on the victim's machine. Phishing is a common type of cyber attack that exploits the weakest link of cybersecurity, the human element.

Cybersecurity Architecture

A cyber security architecture is the foundation of an organization's defense against cyber threats, and ensures that all components of its IT infrastructure are protected.

sirar Glossary

Zero Trust Security

Zero Trust is a framework for securing infrastructure and data for today's modern digital transformation. It uniquely addresses the modern challenges of today's business, including securing remote workers, hybrid cloud environments, and ransomware threats. While many vendors have tried to create their own definitions of Zero Trust, there are a number of standards from recognized organizations that can help you align Zero Trust with your organization.

Dark web

The dark web is the hidden collective of internet sites only accessible by a specialized web browser. It is used for keeping internet activity anonymous and private, which can be helpful in both legal and illegal applications. While some use it to evade government censorship, it has also been known to be utilized for highly illegal activity including but not limited to selling victim credentials, credit card info or even providing cyber-attack services for a fee.

Network Time Protocol (NTP)

Is a protocol that helps the computers clock times to be synchronized in a network. This protocol is an application protocol that is responsible for the synchronization of hosts on a TCP/IP network. NTP was developed by David Mills in 1981 at the University of Delaware. This is required in a communication mechanism so that a seamless connection is present between the computers.

User Datagram Protocol (UDP)

Is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as UDP/IP suite. Unlike TCP, it is an unreliable and connectionless protocol. So, there is no need to establish a connection prior to data transfer. The UDP helps to establish low-latency and loss-tolerating connections establish over the network.The UDP enables process to process communication.

DNS Servers

Domain Name System (DNS) Server: is when users type domain names into the URL bar in their browser, DNS servers are responsible for translating those domain names to numeric IP addresses, leading them to the correct website.

Vulnerability Management, Detection & Response (VMDR)

Identify Your Cybersecurity Vulnerabilities Proactively.
Cybersecurity is changing constantly, and new threats are emerging daily. Vulnerability management detection and response services gives your organization a continuous, always-on , assessment of your infrastructure Cybersecurity vulnerabilities and compliance posture.
A comprehensive visibility across your entire IT assets, wherever they reside, with automated built-in threat prioritization, patching, and other response capabilities.

Log4Net

Log4Shell, an internet vulnerability that affects millions of computers, involves an obscure but nearly ubiquitous piece of software, Log4j. The software is used to record all manner of activities that go on under the hood in a wide range of computer systems.

sirar **Glossary**

Scrubbing

is a common DDoS mitigation technique. The live traffic destined for a particular IP address range is re-directed where any malicious traffic is "scrubbed" or cleaned and the clean traffic is then forwarded to delivery. Keeping you online without losing service.

Brute force attack

A brute force attack is a method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks. The Attacker tries multiple usernames and passwords, often using a computer to test a wide range of combinations, until they find the correct login information.

Log4Shell

Apache Log4j 2, a well-known Java library for logging error messages in applications, has a software vulnerability called Log4Shell. If a device is using a specific version of Log4j 2, the vulnerability, identified as CVE-2021-44228, allows a remote attacker to take control of the device over the internet.

DoublePulsar

DOUBLEPULSAR is a loading dock for extra malware whose purpose is to provide a covert channel by which to load other malware or executables. All the SMB and RDP exploits in FuzzBunch exploitation framework uses DoublePulsar as the primary payload.

Cryptominer

Cryptomining malware, or 'cryptojacking,' is a malware attack that co-opts the target's computing resources in order to mine cryptocurrencies like bitcoin. This malware uses a systems CPU and sometimes GPU to perform complex mathematical calculations that result in long alphanumeric strings called hashes.

Trojan

Is malware that appears to be legitimate software disguised as native operating system programs or harmless files like free downloads. Trojans are installed through social engineering techniques such as phishing or bait websites.

Bad Rabbit

Is a strain of ransomware that first appeared in 2017 and is a suspected variant of Petya. Like other strains of ransomware, Bad Rabbit virus infections lock up victims' computers, servers, or files preventing them from regaining access until a ransom — usually in Bitcoin — is paid.

References

06

* References

"California, Security Operations Center as a service (SOCaaS). CDT Services.
From https://cdt.ca.gov/services/security-operations-center-as-a-service-socaas/ "

"Threatlabz Ransomware Review: The advent of double extortion.
From https://info.zscaler.com/resources-white-papers-threatlabz-ransomware-review"

"What is a distributed denial-of-service (ddos) attack? - cloudflare.
From https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ "

"Cisco. (2022, June 6). What is malware? - definition and examples. Cisco.
From https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html "

"Cisco. (2022, December 21). What is phishing? Cisco.
From https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html "

"Chkadmin. (2022, May 11). What is a cyber security architecture? Check Point Software.
From https://www.checkpoint.com/cyber-hub/cyber-security/what-is-a-cyber-security-architecture/"

"What is Zero trust security? principles of the zero trust model (2022, November10).
From https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/"

"Kaspersky. (2022, October 21). What is the deep and dark web?.
From https://www.kaspersky.com/resource-center/threats/deep-web "

"Network time protocol (NTP). GeeksforGeeks.
From https://www.geeksforgeeks.org/network-time-protocol-ntp/ "

"User datagram protocol (UDP). GeeksforGeeks. (2022, November 1).
From https://www.geeksforgeeks.org/user-datagram-protocol-udp/ "

"What is a DNS server? | cloudflare.
From https://www.cloudflare.com/learning/dns/what-is-a-dns-server/"

" (2022, September 13). What is Log4j? A cybersecurity expert explains the latest internet vulnerability, how bad it is and what's at stake. The Conversation.
From https://theconversation.com/what-is-log4j-a-cybersecurity-expert-explains-the-latest-internet-vulnerability-how-bad-it-is-and-whats-at-stake-173896 "

* References

"What is a brute force attack?: Definition, Types & How It Works. Fortinet.
From https://www.fortinet.com/resources/cyberglossary/brute-force-attack"

"Bhat, S. (2022, March 16). Doublepulsar – a very sophisticated payload for windows. SecPod Blog.
From https://www.secpod.com/blog/doublepulsar-a-very-sophisticated-payload-for-windows/ "

"Cryptomining malware - definition, examples, &amp; detection - extrahop. ExtraHop.
From https://www.extrahop.com/resources/attacks/cryptomining/"

"What is malware? detection &amp; removal methods: CrowdStrike.
From https://www.crowdstrike.com/cybersecurity-101/malware/ "

"What is bad rabbit ransomware?: Proofpoint us. Proofpoint. (2022, November30).
From https://www.proofpoint.com/us/threat-reference/"

Paganini, P. (2022, May 3). UNC3524 APT uses IP cameras to deploy backdoors and Target Exchange. Security Affairs.
Retrieved from https://securityaffairs.com/130838/apt/unc3524-apt-ip-cameras.html

Mandiant.UNC3524: Eye spy on your email. Mandiant.
Retrieved from https://www.mandiant.com/resources/blog/unc3524-eye-spy-email

Ransomware spotlight: Clop. Security News.
Retrieved from https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-clop

Hacktivist attacks show ease of hacking industrial control systems. SecurityWeek.
Retrieved from https://www.securityweek.com/hacktivist-attacks-show-ease-hacking-industrial-control-sys

Microsoft 365 Defender Research Team, M. T. I. C. (M. S. T. I. C. (2022, July 12). From cookie theft to BEC: Attackers use AITM phishing sites as entry point to further financial fraud. Microsoft Security Blog.
Retrieved from https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

* References

Westfall, S. (2022, November 3). Threat brief: CVE-2022-41040 and CVE-2022-41082: Microsoft Exchange Server (ProxyNotShell). Unit 42.
Retrieved from https://unit42.paloaltonetworks.com/proxynotshell-cve-2022-41040-cve-2022-41082/

Conger, K., & Roose, K. (2022, September 16). Uber investigating breach of its computer systems. The New York Times.
Retrieved from https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html

Biasini, N. (2022, November 2). Cisco Talos shares insights related to recent cyber-attack on Cisco. Cisco Talos Blog.
Retrieved from https://blog.talosintelligence.com/recent-cyber-attack/

Prince, M. (2023, January 13). The mechanics of a sophisticated phishing scam and how we stopped it. The Cloudflare Blog.
Retrieved from https://blog.cloudflare.com/2022-07-sms-phishing-attacks/

IBM - United States.
Retrieved from https://www.ibm.com/downloads/cas/3R8N1DZJ

Westfall, S. (2022, November 3). Threat brief: CVE-2022-41040 and CVE-2022-41082: Microsoft Exchange Server (ProxyNotShell). Unit 42.
Retrieved from https://unit42.paloaltonetworks.com/proxynotshell-cve-2022-41040-cve-2022-41082/

sirar

by stc

Cybersecurity in

excellence