

# Threat Landscape

Report in **2022**

# Agenda

- 01 Introduction
- 02 Global Attack Trends
- 03 KSA Statistics
- 04 sirar Battles
- 05 Key takeaways
- 06 sirar Glossary
- 07 References



# Introduction

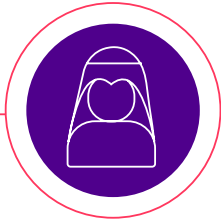
01





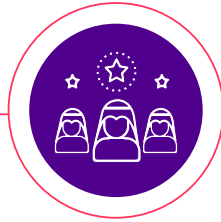
# Introduction

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



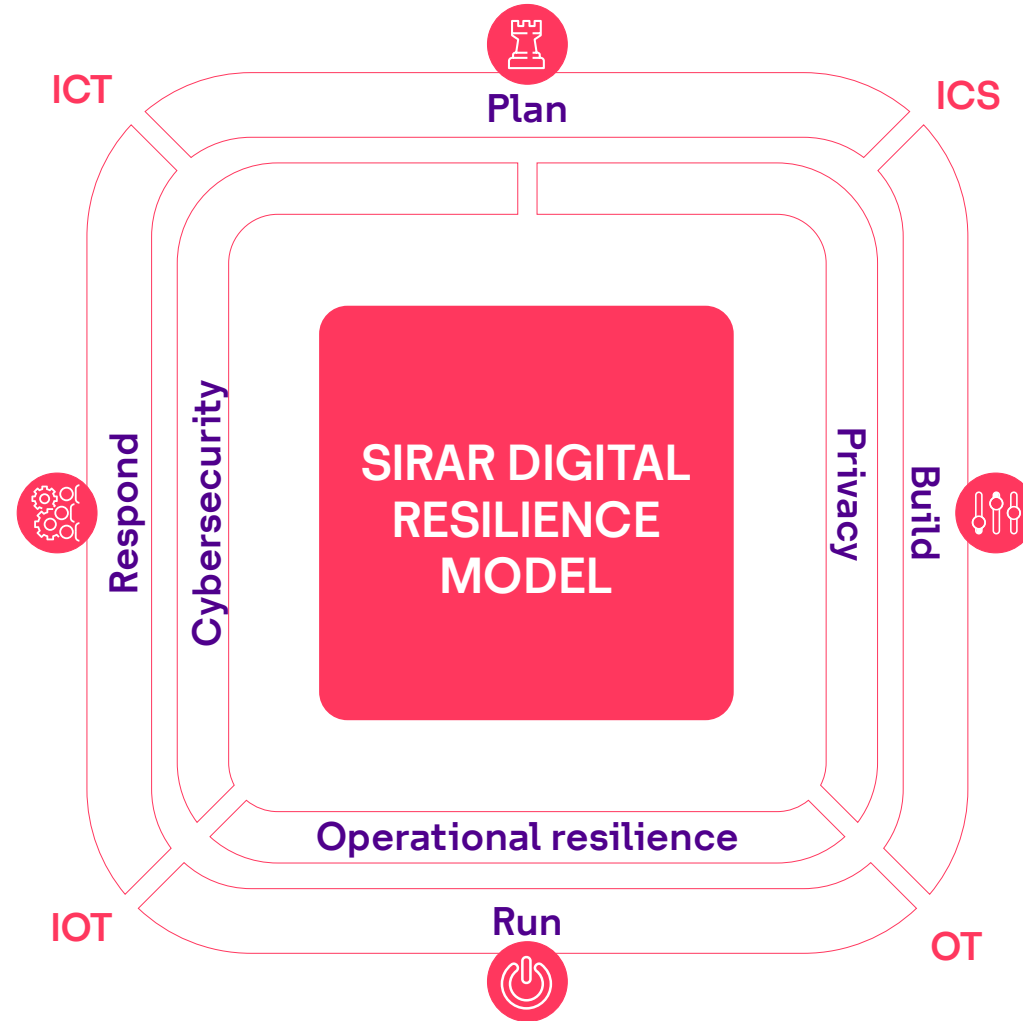
## One Stop Shop

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.

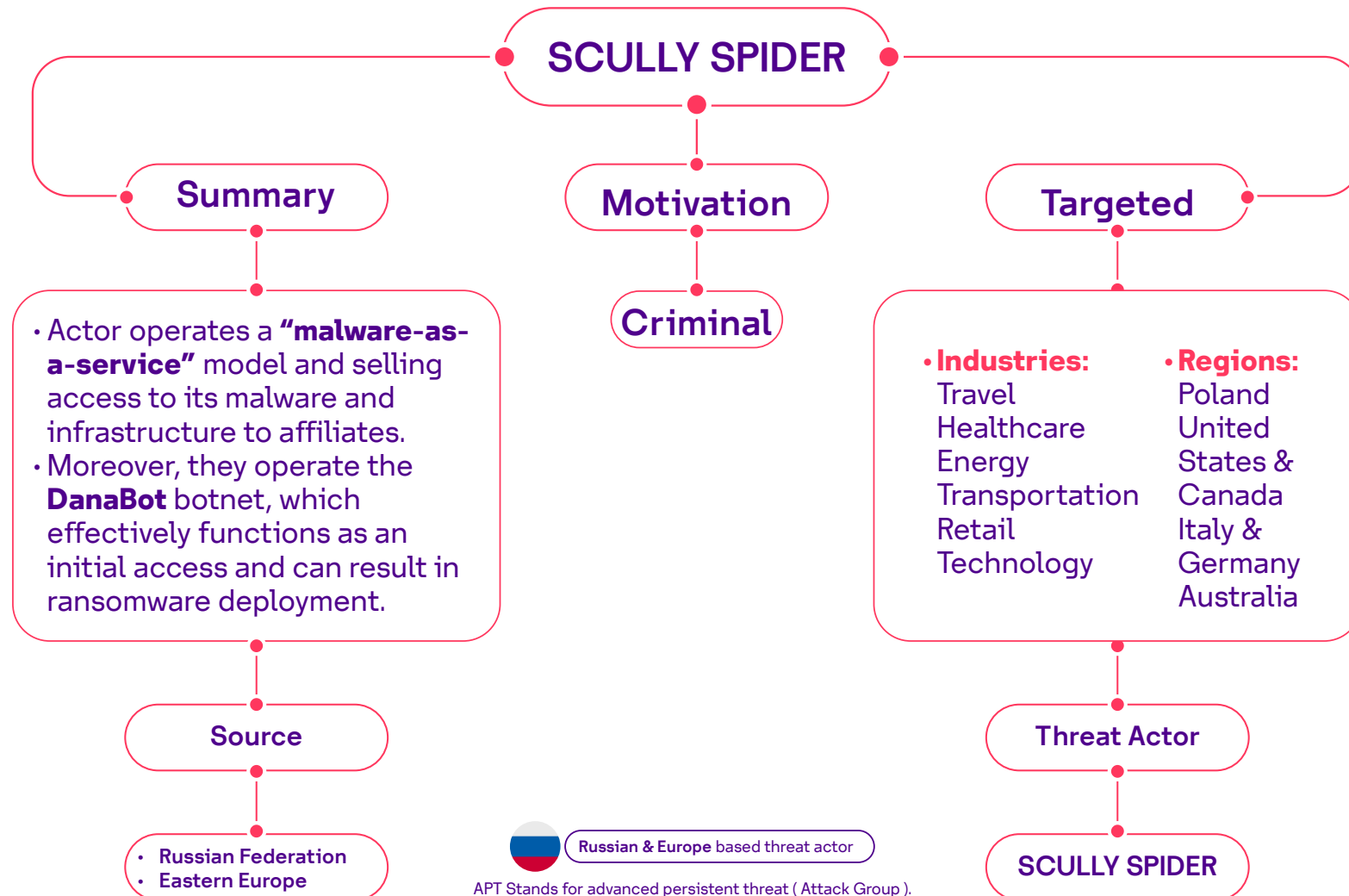




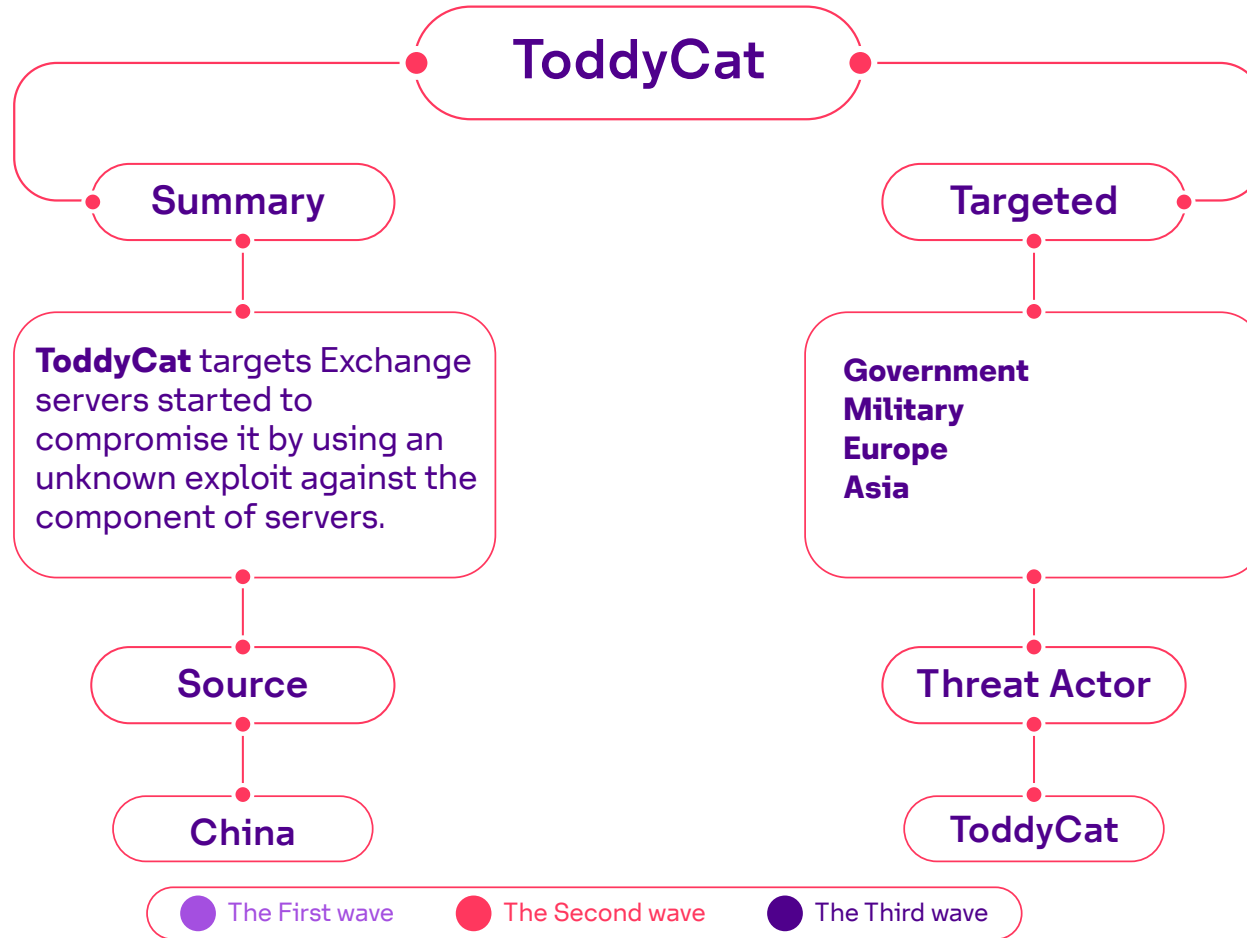
# Global Attack Trends

02

# Most Global Active APTs



# Most Global Active APTs



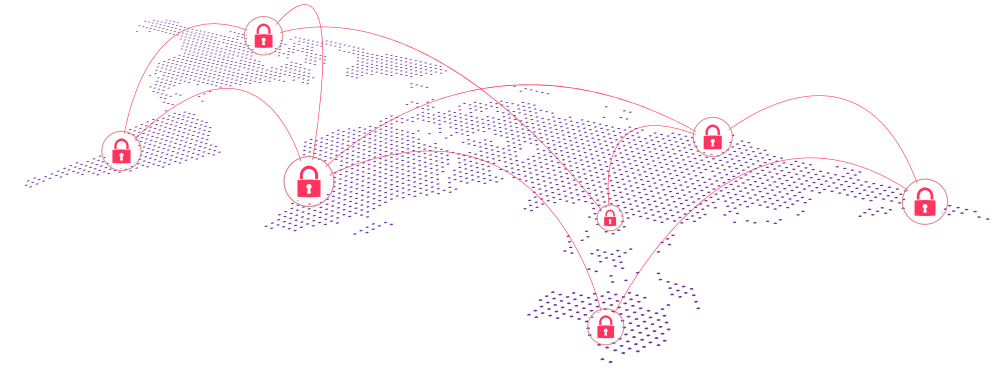
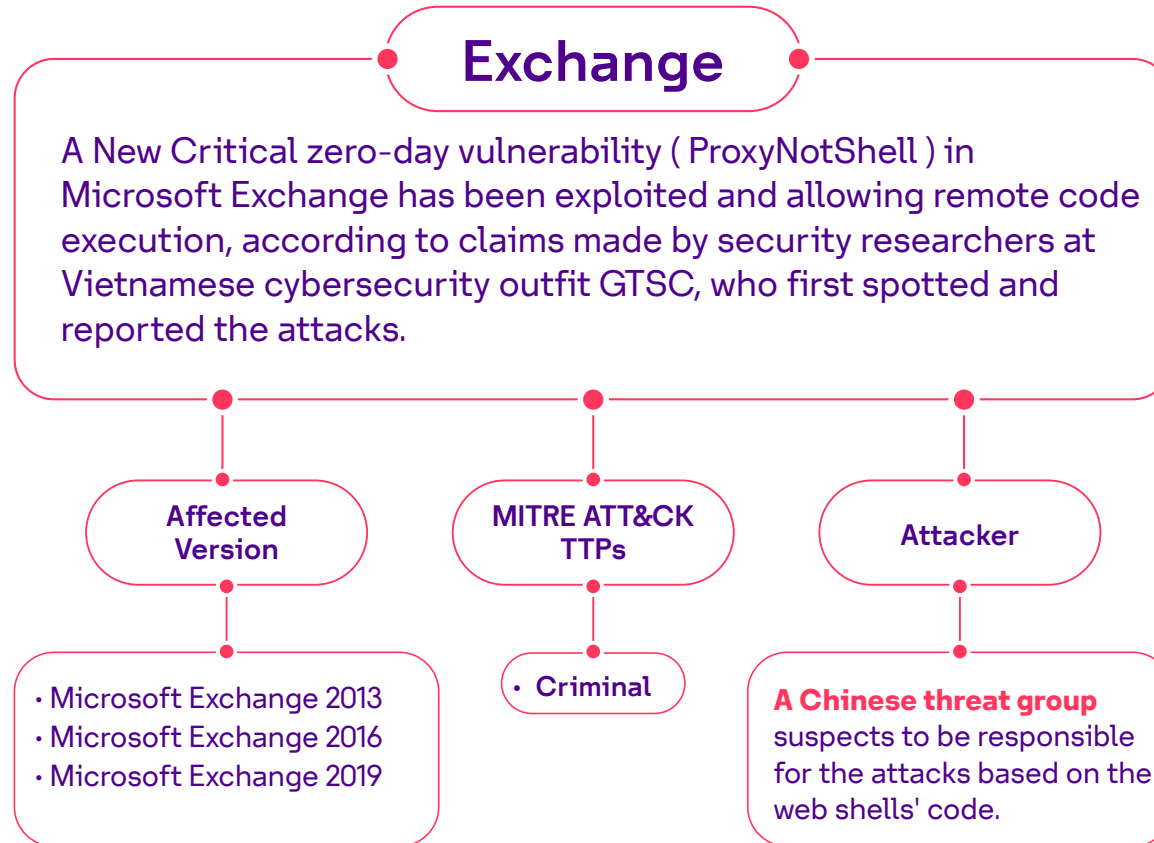
China based threat actor

APT Stands for advanced persistent threat ( Attack Group ).





# Microsoft Exchange Zero-Day vulnerability (ProxyNotShell)



Source: PaloAlto

# Microsoft Warns AiTM Phishing Attacks and 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

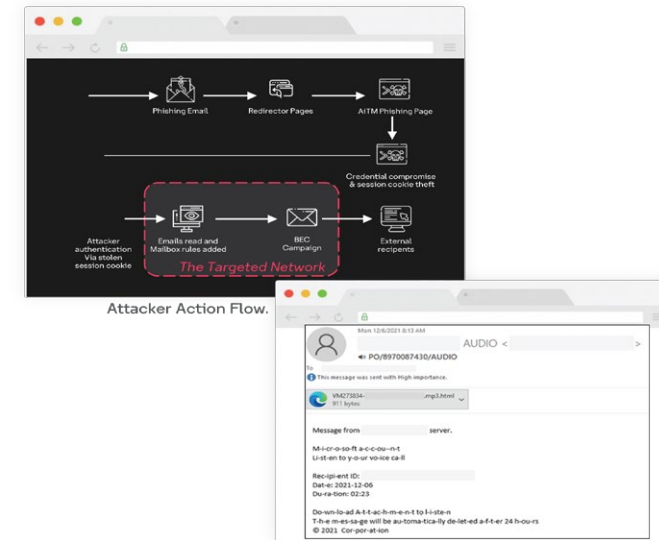
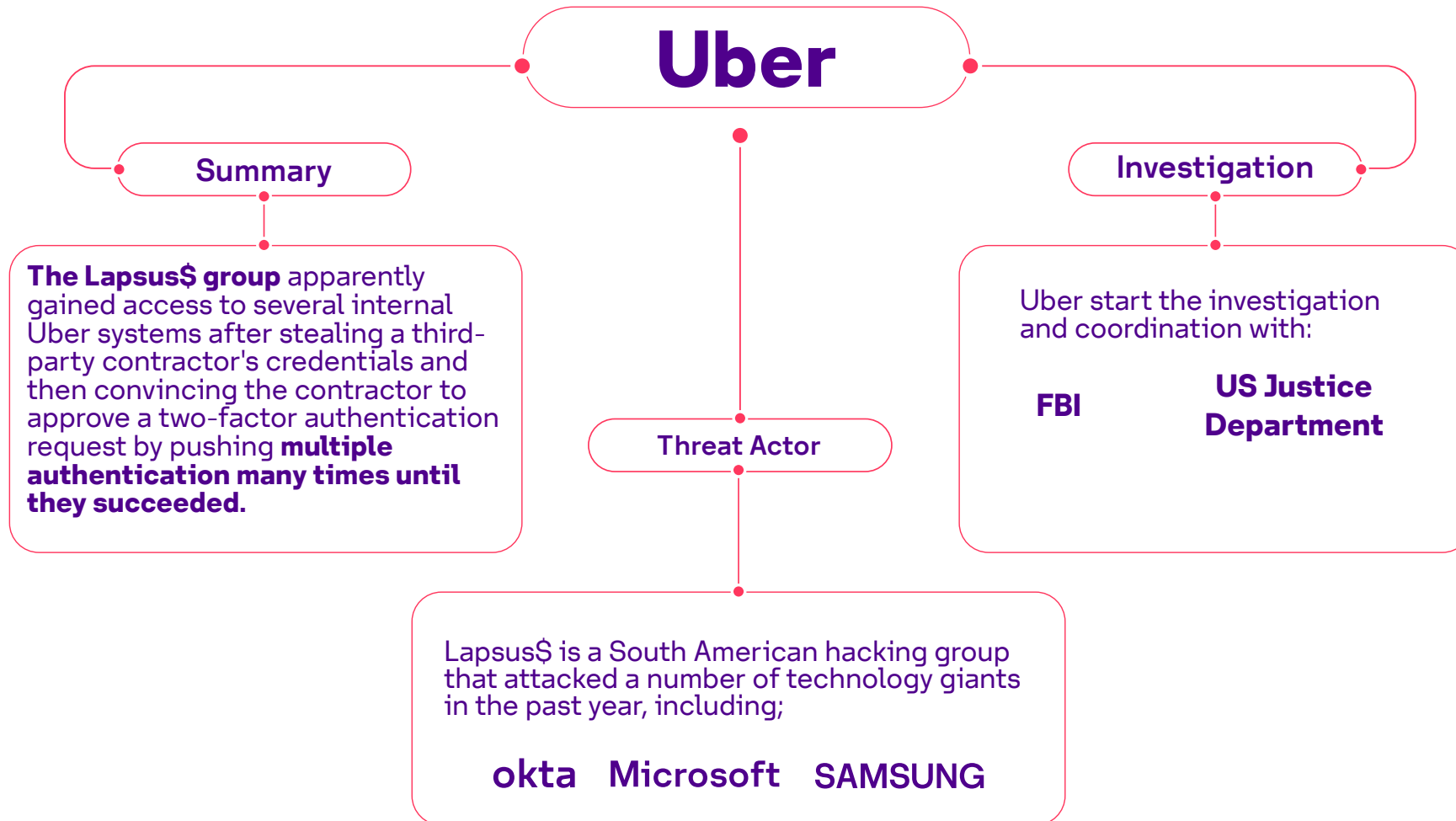


Figure 2: Phishing sample.

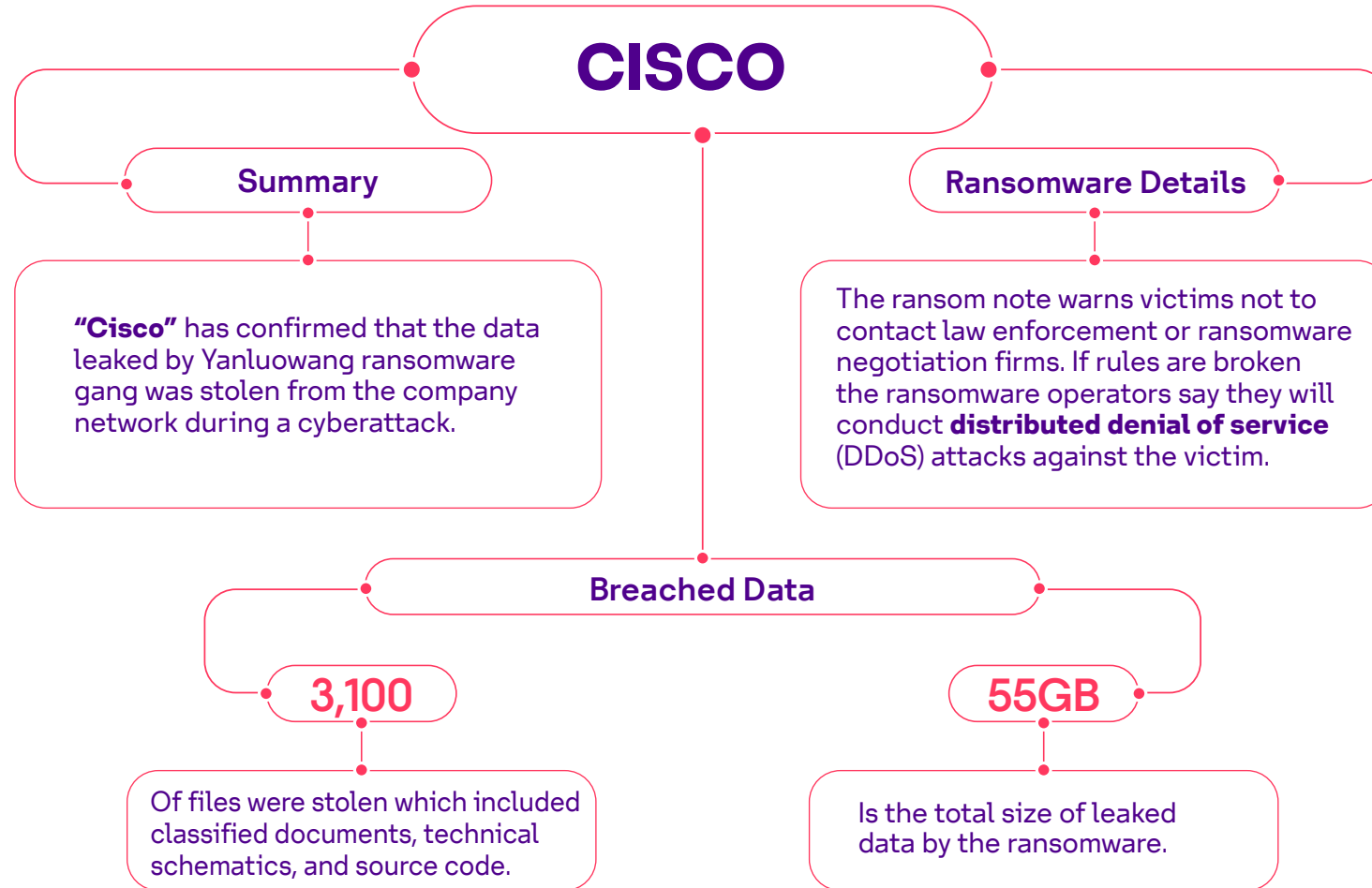
Source: Microsoft

# Uber's Internal Network Breached



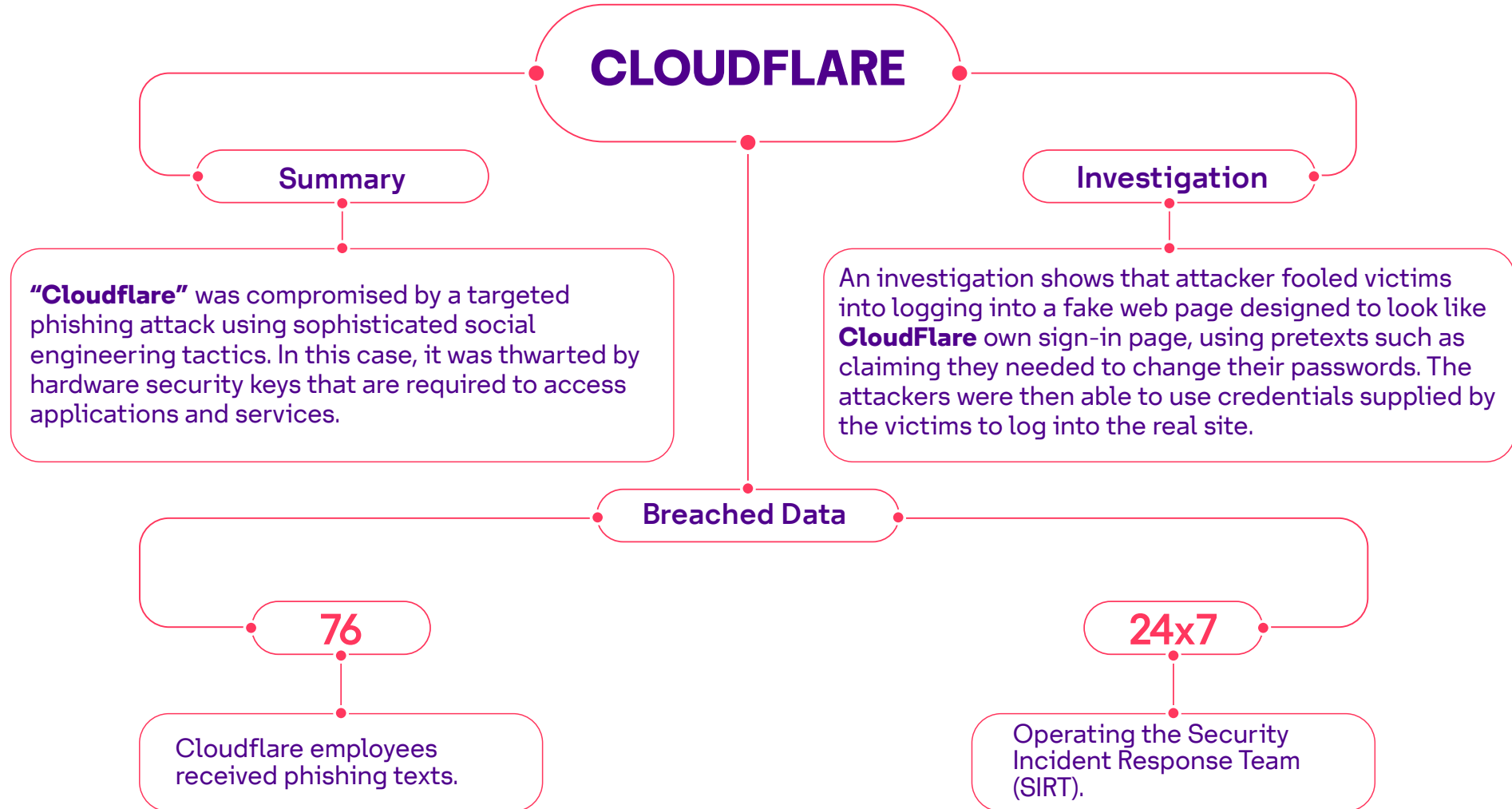
Source: The New York Times

# Cisco Hit By Ransomware That Leaked Its Data



Source: Cisco talos

# Phishing Campaign Reported On Twilio & Cloudflare

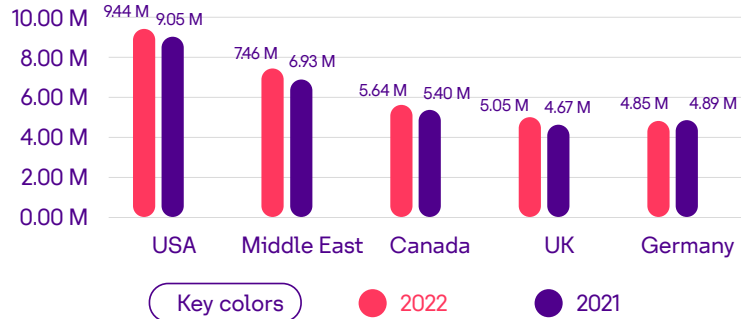


Source: Cloudflare

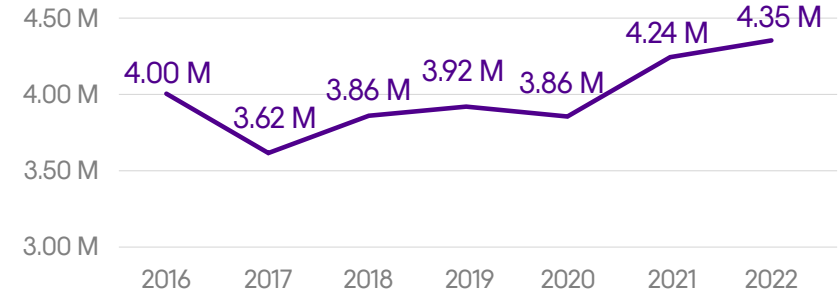


# Cyber Data Breach Statistics 2022

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



Average Total Cost Of Data Breach



Breaches Cost And Causes

• **\$4.24M** •

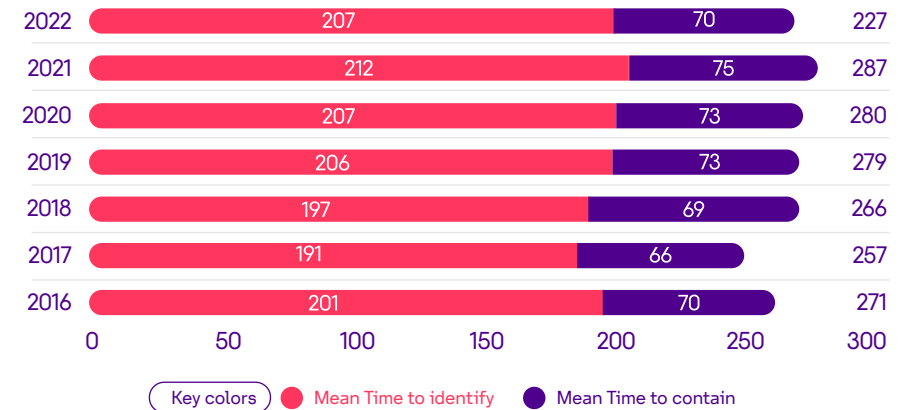
Is the cost of data breach of **private** clouds in 2022.

• **\$5.02M** •

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

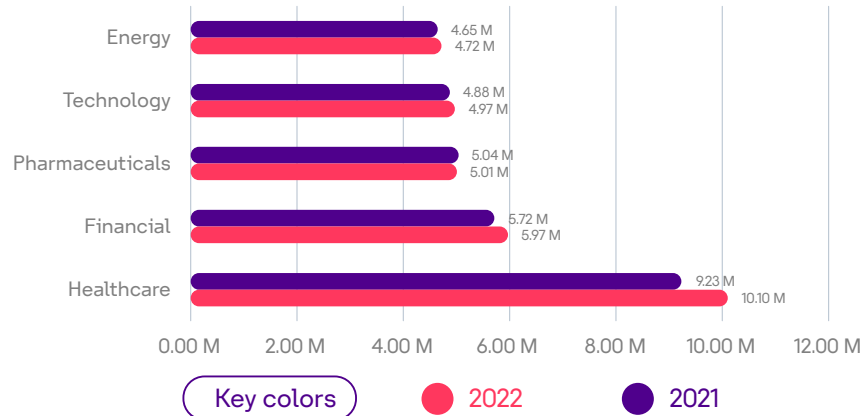
Source: IBM

Average Time To Identify And Contain A Data Breach

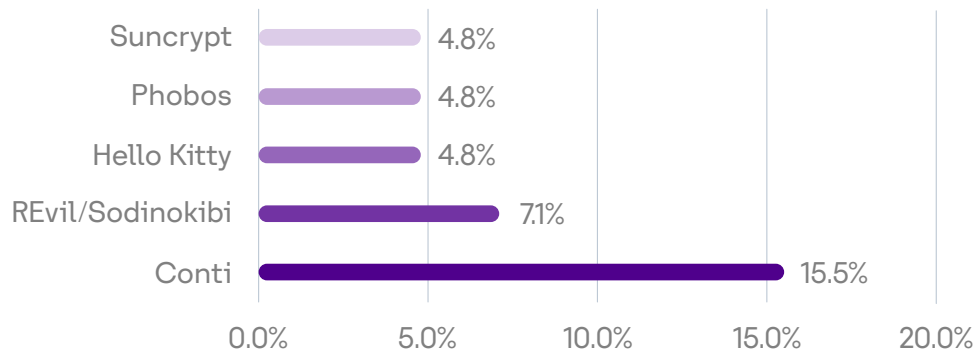


# Cyber Data Breach Statistics 2022

Average Cost Of A Data Breach By Top 5 Industry

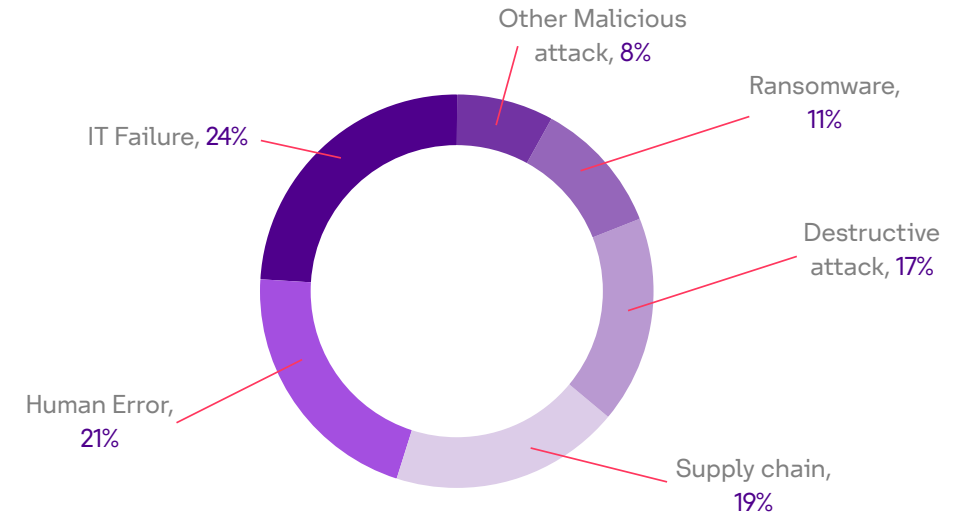


Most Active Ransomware Group








Source: IBM

Types of breaches experienced by organizations



# Cyber Sector Attacks

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

Source: Anamoli  
Source: Mandiant

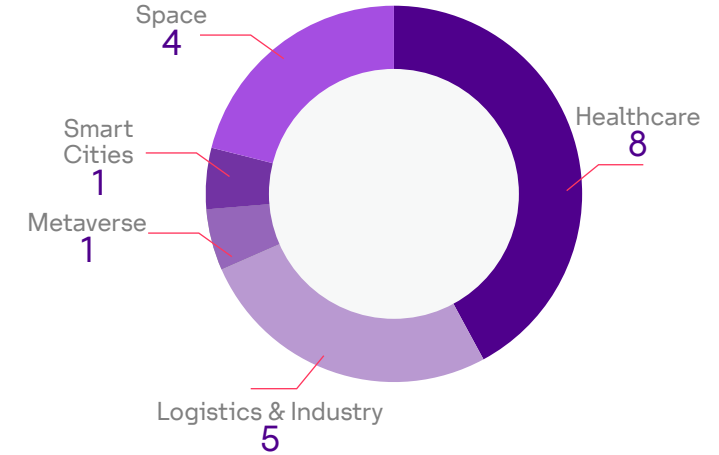
# Cyber Sector Attacks

## Indicator Of Compromised By Sector

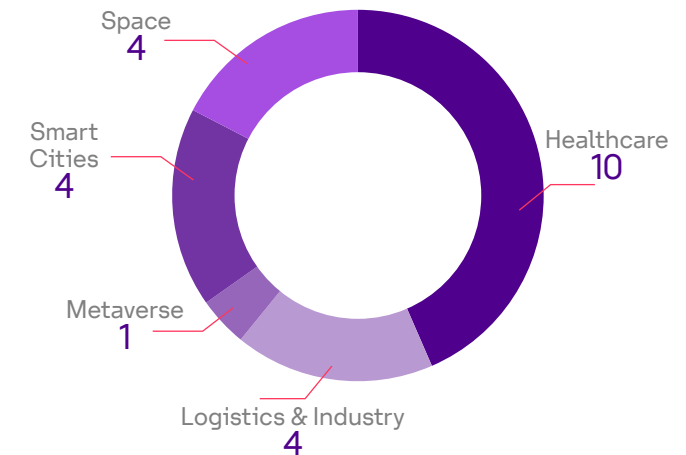
Total Indicators	Sector
1,726	Healthcare
238	Logistics and Industry
1,899	Space
323	Smart Cities
7	Metaverse

Source: Anamoli  
Source: Mandiant

Total Actors



Total Malware & Tools

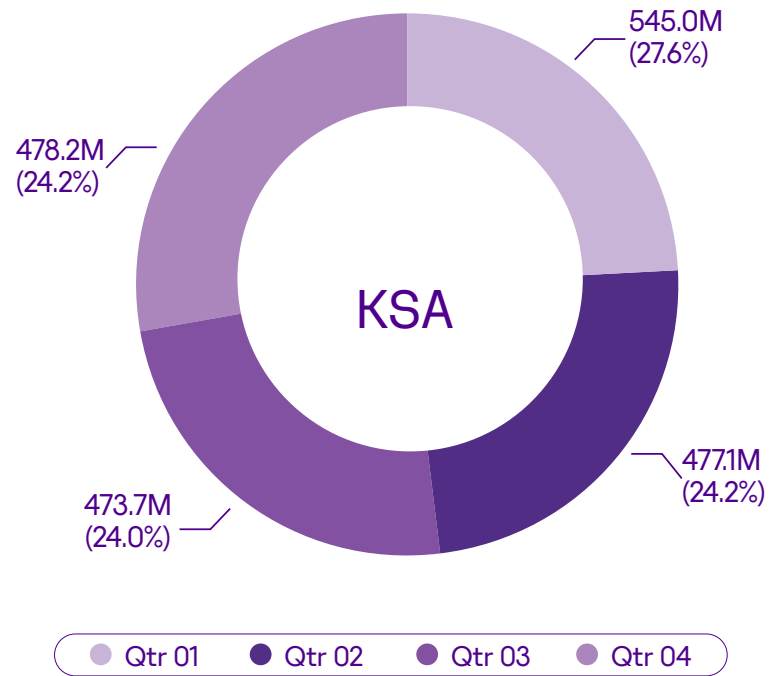


# KSA Key Statistics

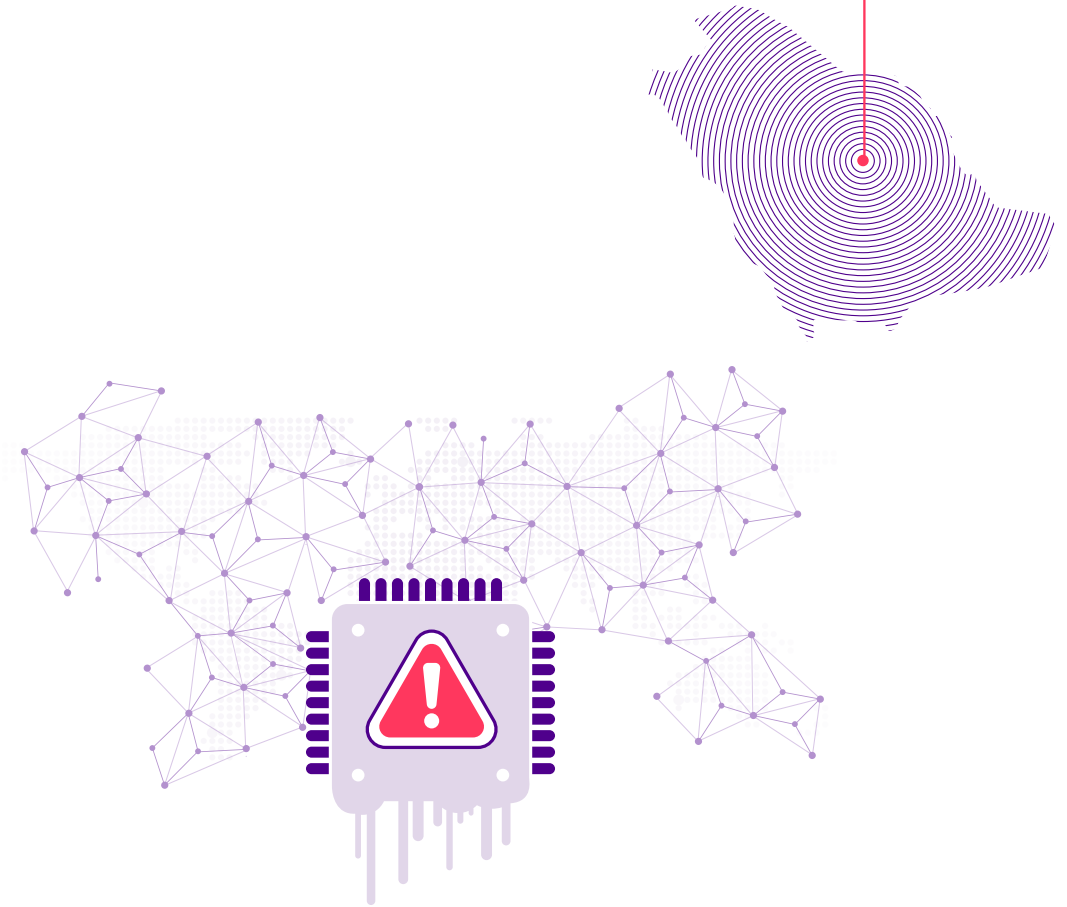
03



# Malicious Activity Distribution by Country

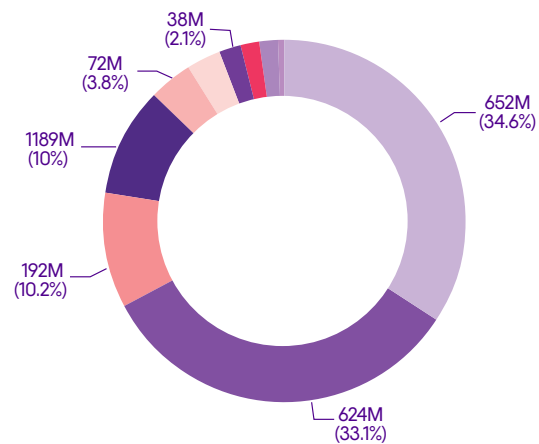


Saudi Arabia



# Exploit Attempts

Exploit Attempts Distribution by Signature



Log4Shell  
53 M



DoublePulsar  
624 M



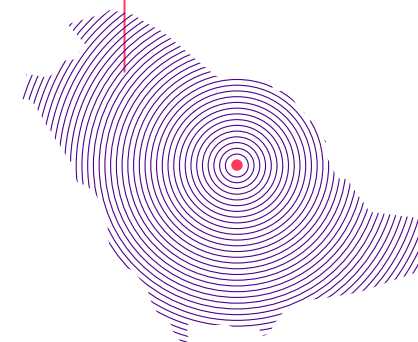
Cross Site Scripting  
3 M



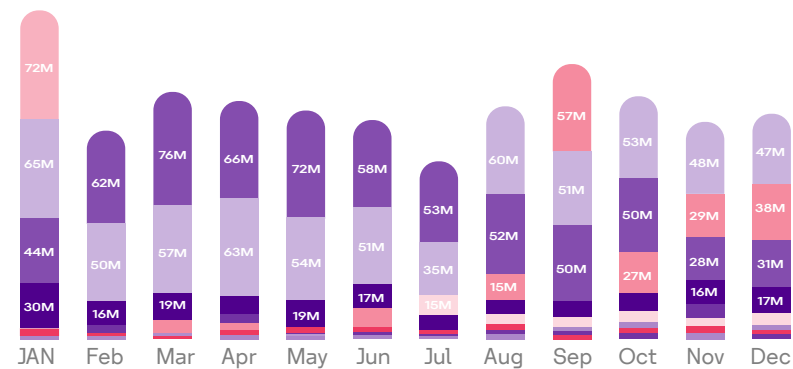
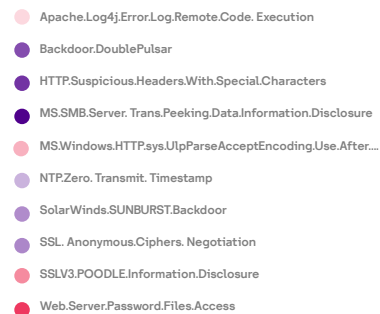
SUNBURTS  
10 M



Exploit Techniques Detected  
1.93bn



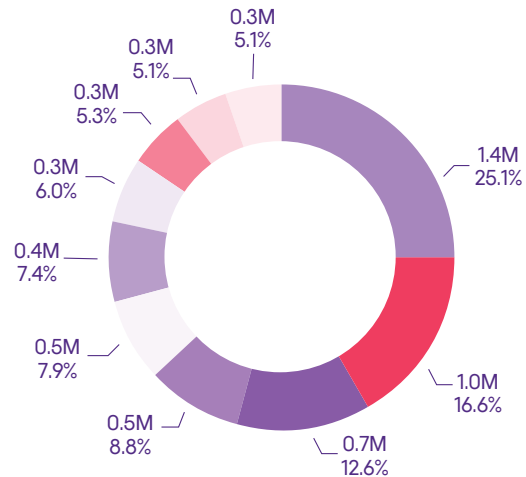
Behavioral Trend Analysis by Signature



FortiGaurd labs

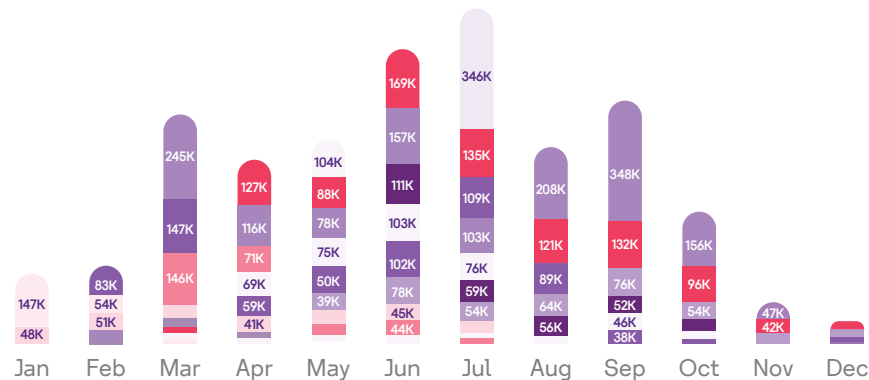
# Malware Detections

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



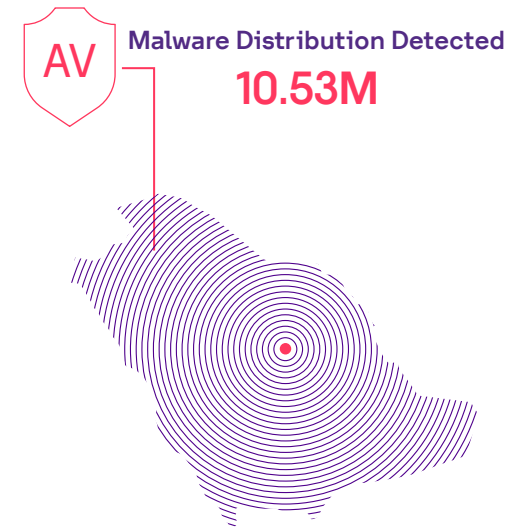
FortiGaurd labs

**CryptoMiner**  
956K

**Trojans**  
8M

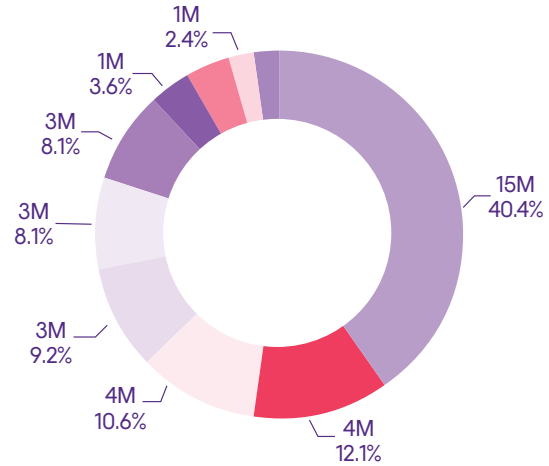
**Mal Office Docs**  
3M

**Drive by Download**  
1M



# Botnet Activity

Botnet Activity Distribution by Signature

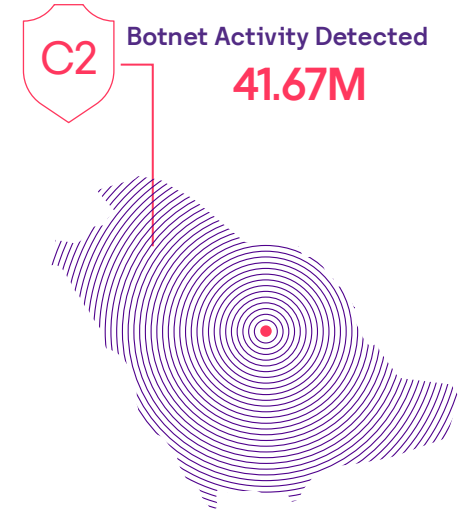


IoT- MIRAI  
1 M

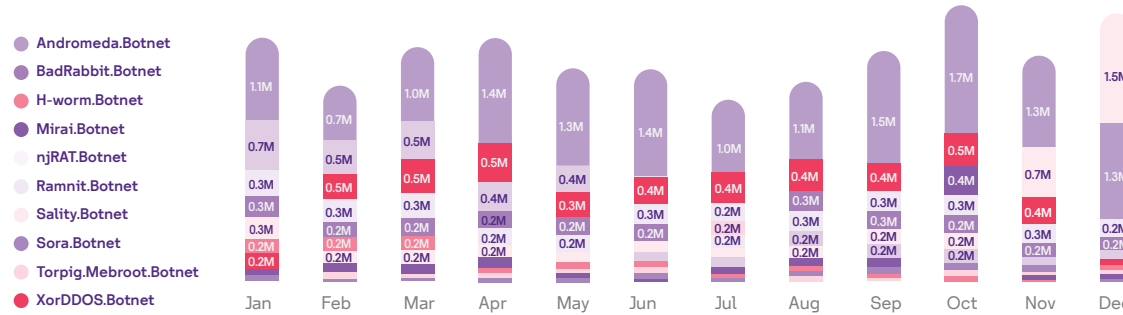
GhOst RAT  
120K

H-Worm  
1 M

Bad Rabbit  
3 M



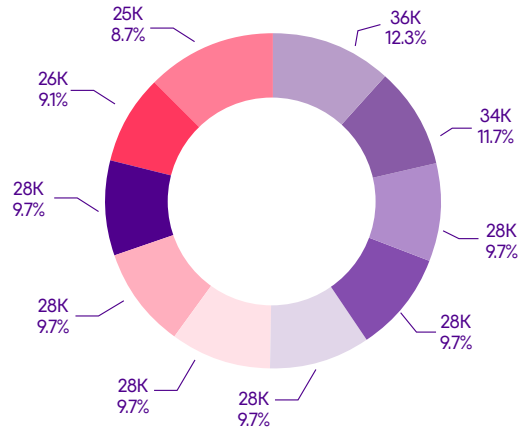
Behavioral Trend Analysis by Signature



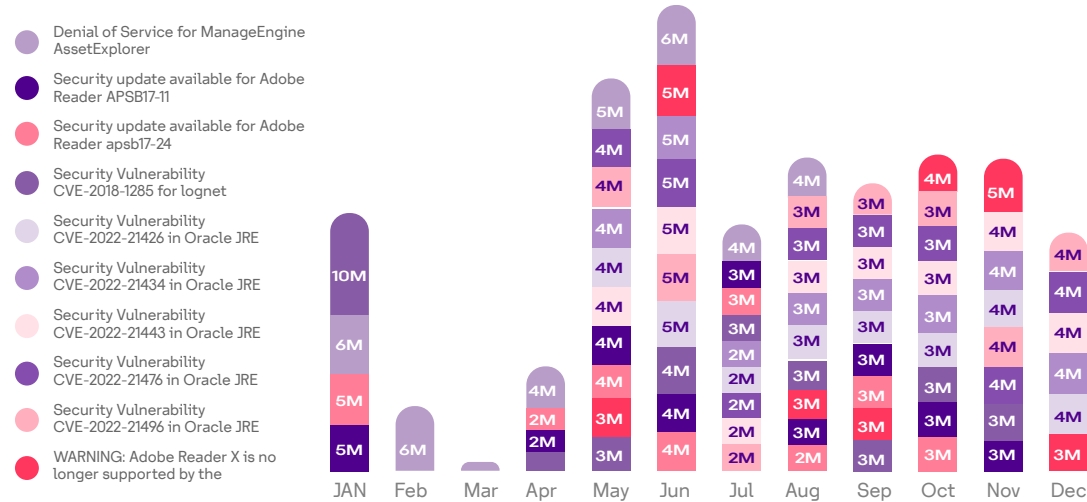
FortiGaurd labs

# Endpoint Vulnerabilities

## Vulnerabilities Distribution by Signature

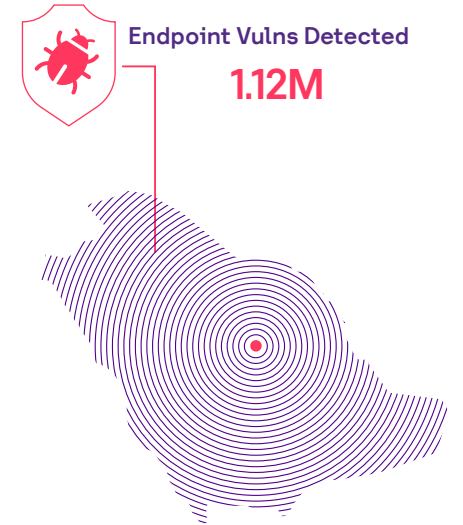


## Behavioral Trend Analysis by Signature



Oracle Vulns  
**675K**

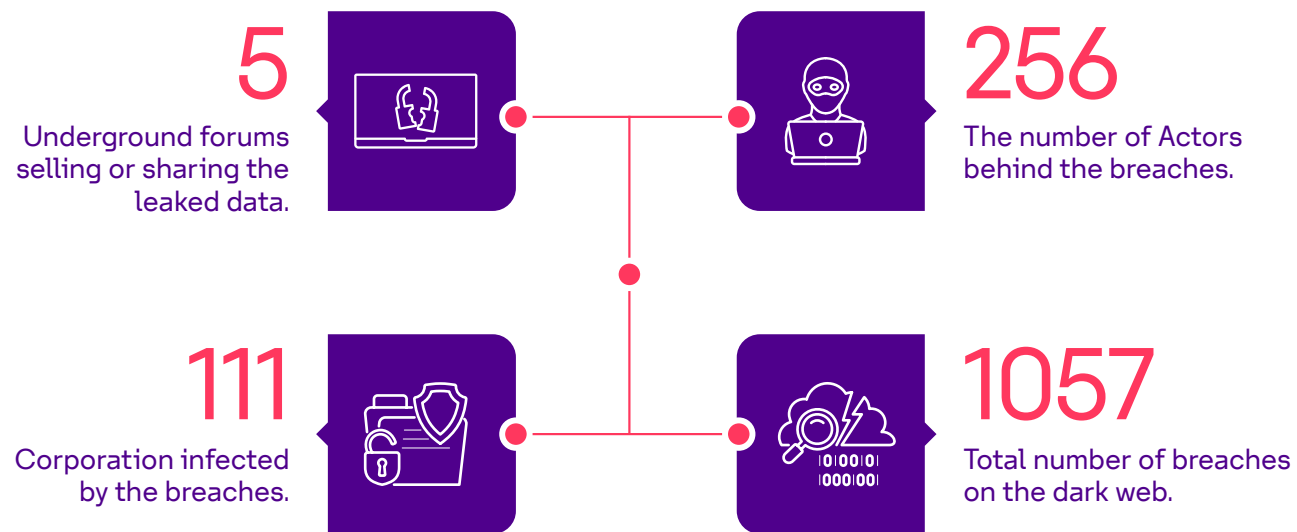
Log4Net  
**34K**



FortiGaurd labs



# KSA Breaches On The Dark Web



# sirar Battles

04



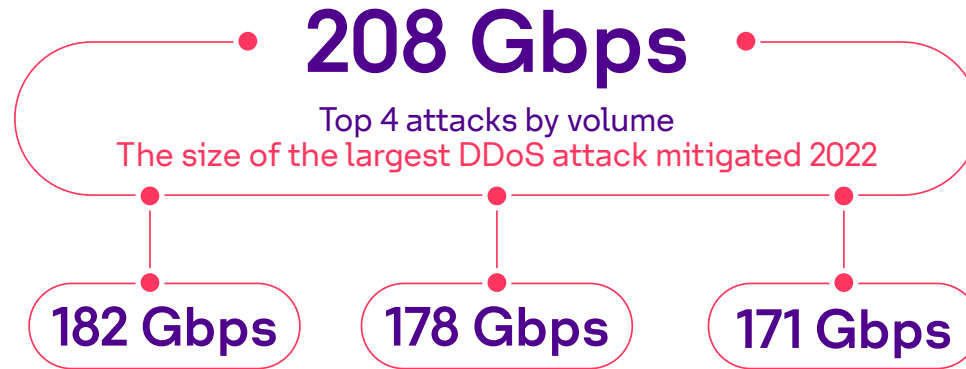
# sirar Battles

DDoS

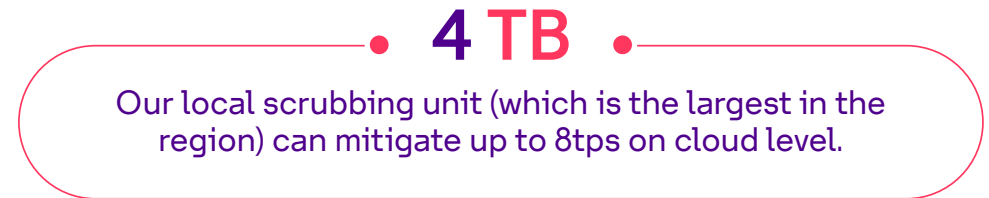


DDOS  
ATTACK

# Top DDoS Attacks In KSA In 2022



## Total Prevented Downtimes



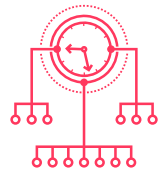
# Top DDoS Attacks In 2022:



Source : **sirar** Anti-DDoS service

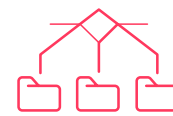
# DDoS

## Attacks In Details



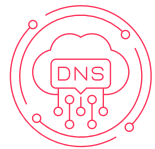
**49%** NTP  
**Amplification**

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



**20%**  
**Others**

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



**18%** DNS  
**Amplification**

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



**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.

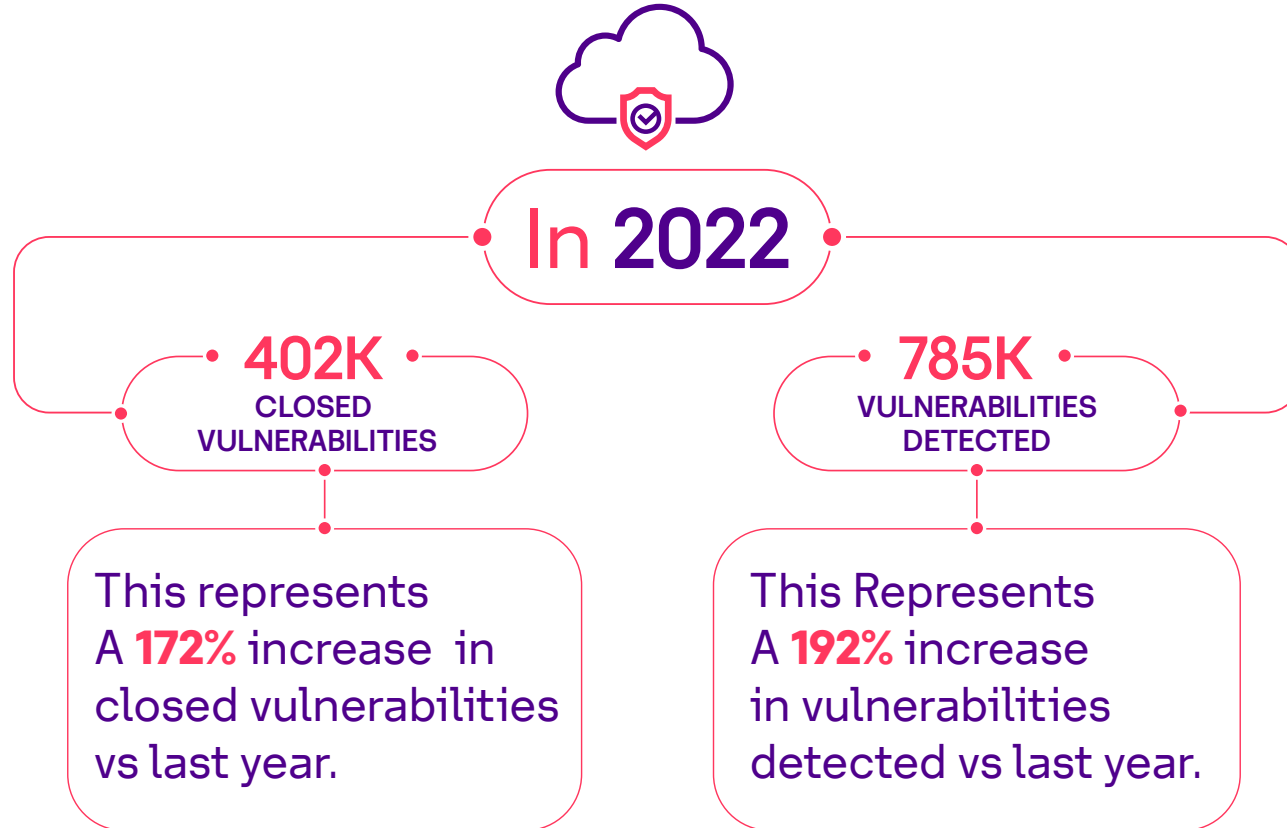


# sirar Battles

VMDR

Vulnerability Management,  
Detection and Response

# Vulnerability Management, Detection And Response (VMDR)



**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.



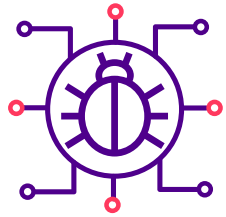
# sirar Battles

Email Security



 **sirar**  
by stc

# Email Security



In 2022

84.92%

PERCENTAGE OF  
CLEAN EMAILS

15.08%

PERCENTAGE OF  
BLOCKED EMAILS

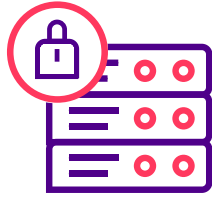
**The email security** is helping customers to prevent, detect and respond to the latest email-borne threats including spam, phishing, malware, zero-day threats, impersonation, and Business Email Compromise (BEC) attacks.



# sirar Battles

Web Security

# Web Security



In 2022

Total Number of  
**transactions**  
processed by sirar:

251.7<sub>M</sub>

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

2.398<sub>M</sub>

Total Number of  
**policy traffic**  
Volume:

266.6<sub>GB</sub>

# sirar Battles

Hajj & National Day

# Our Contributions To Keep Our Home And Country Safe

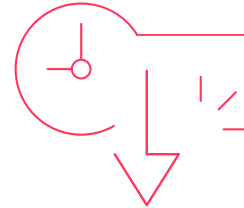


## Web Security

1

### sirar's contribution

sirar monitoring services



**600** Million Inbound  
Malicious traffic



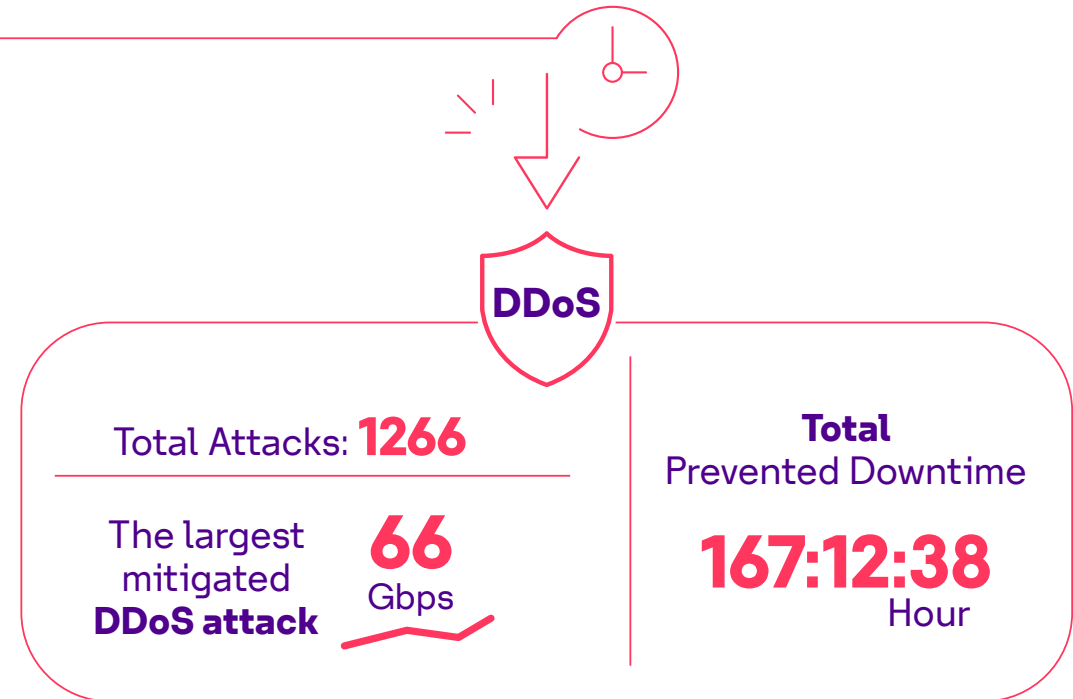
Blocked  
Malware: **39**

# Our Contributions To Keep Our Home And Country Safe

2

## sirar's contribution

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



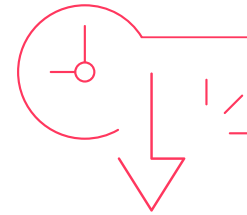


# Our Contributions To Keep Our Home And Country Safe

## 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



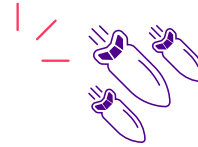
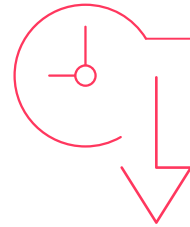
# Our Contributions To Keep Our Home And Country Safe

## What Happened During Jeddah summit?



### sirar's contribution

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



**+33**  
Number of  
blocked attacks



**5.5 Gbps**  
Largest attack size



**+8 Hours**  
Total prevented  
downtime

# Key takeaways

04

# Main Takeaways



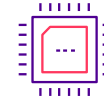
Proactive Security , Data Backups and Relevant additional security controls are necessary to prevent **Ransomware**



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



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



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



Effective Information Security Governance **Policies**



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



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



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

# sirar Glossary

05



# 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 enriched 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.

# sirar

## Glossary

### 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.

### 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 hacking 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 hacker 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, & detection - extrahop.  
ExtraHop.  
From <https://www.extrahop.com/resources/attacks/cryptomining/>"

"What is malware? detection & 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>

Hackivist attacks show ease of hacking industrial control systems.  
SecurityWeek.  
Retrieved from <https://www.securityweek.com/hackivist-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/>



Cybersecurity in  
excellence