Threat Landscape

Report in 2023

sirar
by stc

Table of content

01- Introduction 02
Summary of the report 03
Our Mission, Vision, Values 04
02- Global Top Trends 05
MOVEit Exploitation 06
ALPHV Ransomware Group 07
QakBot. 08
03- Regional Statistics 09
Top 10 Actors Observed in Middle East 10
Top 10 Malwares Observed in Middle East 11
Top 10 MITRE Techniques Used in Middle East 12
Threat Types Observed Middle East 13
04- KSA Statistics 14
Top 10 Actors Observed in Saudi Arabia 15
Top 10 Malwares Observed in Saudi Arabia 16
Top 10 MITRE Techniques in Saudi Arabia 17
05- sirar Battles 18
DDoS Protection 19
VDMR 23
Email Security 25
Web Security 27
SOCaaS 29
Incident Response 31
06- General Recommendations 36
07- Sayen 41
Digitize your signature with sayen 42
Sayen Use Cases 43
08- sirar Glossary 45
09- References 51
Contact Us 55

sirar by stc

01

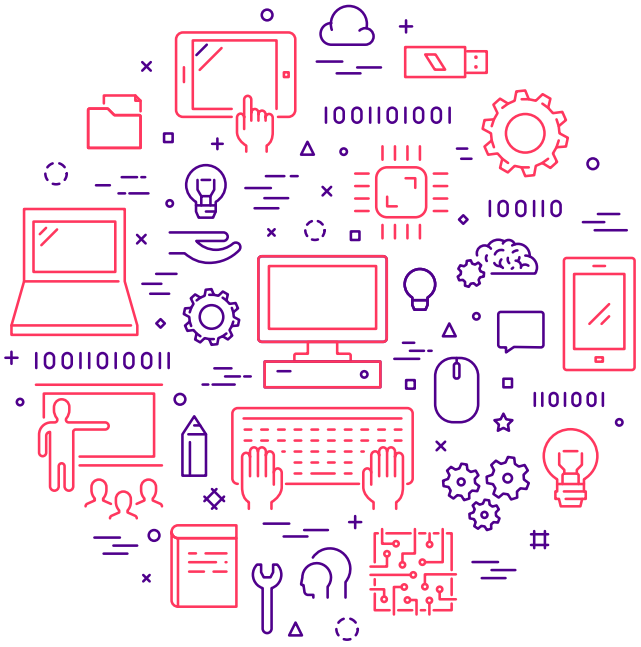
Introduction

sirar by stc

Introduction

Summary of the report

With sirar's threat landscape report as your source, you'll gain a comprehensive understanding of the ever-changing cybersecurity landscape that includes an insight of **Global threat trends, Regional statistics, and Specific vulnerabilities within the Kingdom of Saudi Arabia** for you to make informed decisions to fortify your organization's defenses. This comprehensive report delves into the ever-evolving threat landscape, shedding light on the formidable efforts of sirar's Battles. Through its innovative products and services, it provides robust protection to clients, ensuring their businesses stay secure in the face of emerging risks. Moreover, the report unveils insights on preserving business security through the implementation of **Sayen**, a product that maintains security and enhances customer experiences by providing digital signature. Designed to empower organizations with the knowledge needed to proactively protect against emerging threats, **sirar's 2023 Threat Landscape Report** is a valuable resource for preserving business security and staying ahead of evolving risks.



Introduction

Our Mission, Vision, Values

Established by stc, the region's top ICT and digital services provider. sirar by stc is a cutting-edge cybersecurity provider that empowers organizations to take control of their cyber and digital capabilities.

As experts in cybersecurity, privacy, and resilience, sirar offer a comprehensive range of solutions that help you manage your digital risks effectively, achieve compliance with relevant laws and regulations, and enable a safe digital transformation journey.

Mission

sirar develop world-class cyber solutions and capabilities to enable secure customers' digitization journeys in the kingdom and beyond.

Vision

The #1 cybersecurity enabler for the digital economy.

Values

Dynamism
Devotion
Drive

02

Global Top Trends

sirar
by stc

Global Top Trends

MOVEit Vulnerability

Summary

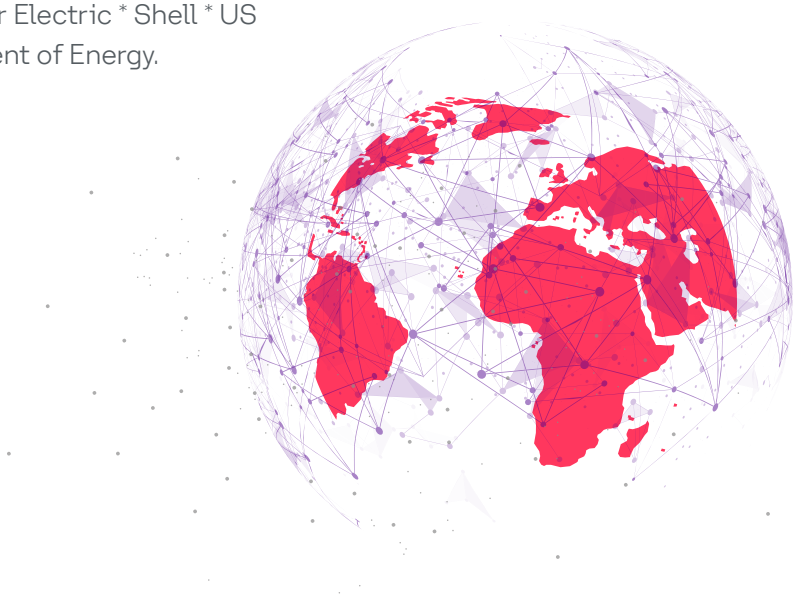
- MOVEit Transfer vulnerabilities were publicly disclosed in May-June 2023. It was wildly exploited and impacted many sectors such as energy, critical national infrastructure, and government sectors.
- Over 2300 organizations overall, with Cl0p ransomware claiming over 400 organizations and over 60 million individuals as victims while leveraging the MOVEit zero-day.
- CCleaner "Siemens Energy" Schneider Electric * Shell * US Department of Energy.

Investigation

- A critical SQL injection zero-day vulnerability has been exploited since March 2023. The vulnerability allows attackers to have backdoor access by leveraging LemurLoot then steal data by exfiltrating it through MOVEit Transfer.

Breached Data

- Sectors impacted: Education (39%); Health (21%); Finance (14%); Public (3.8%); Legal (0.2%); Unspecified (22%). Education and Health more severly impacted due to their exposure to third-party services.
- Depending on sector multiple data types in transit were breached: Date of Birth; Email address; Financial Information; Personal Health Information (PHI); Personally Identifiable Information (PII); Phone numbers; Postal addresses; Social Security ID and Government ID numbers.



source:

statistics drawn from the last 6 months of regional intelligence of attacks (malware, actors) from the Anomali Intelligence Channels (Malware, Adversary) powered by Anomali's partners Polyswarm and Bitdefender.

Global Top Trends

ALPHV Ransomware Group

Summary

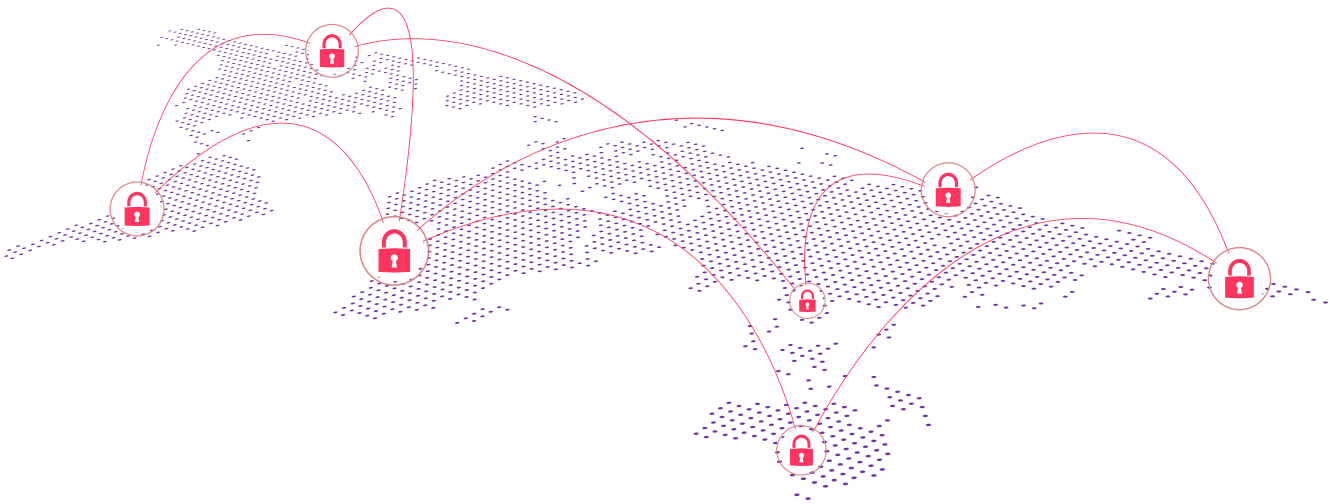
- Proficient in social engineering tactics and human-operated ransomware attacks.
- The ALPHV/BlackCat ransomware group stood out due to its growing popularity and tendency to be used to compromise high-value targets.

Investigation

- Multiple ransomware variants with similar code, including ALPHV, BlackCat, Sphynx, and Noberus.
- Rust language base makes it customizable and extensible.
- Double and triple extortion tactics, charging a ransom to decrypt files and threatening to disclose files or engage in DDoS attacks and even complaining to regulators.

Actors

- Works alone and with affiliates such as FIN8 group.



source:

statistics drawn from the last 6 months of regional intelligence of attacks (malware, actors) from the Anomali Intelligence Channels (Malware, Adversary) powered by Anomali's partners Polyswarm and Bitdefender.

Global Top Trends

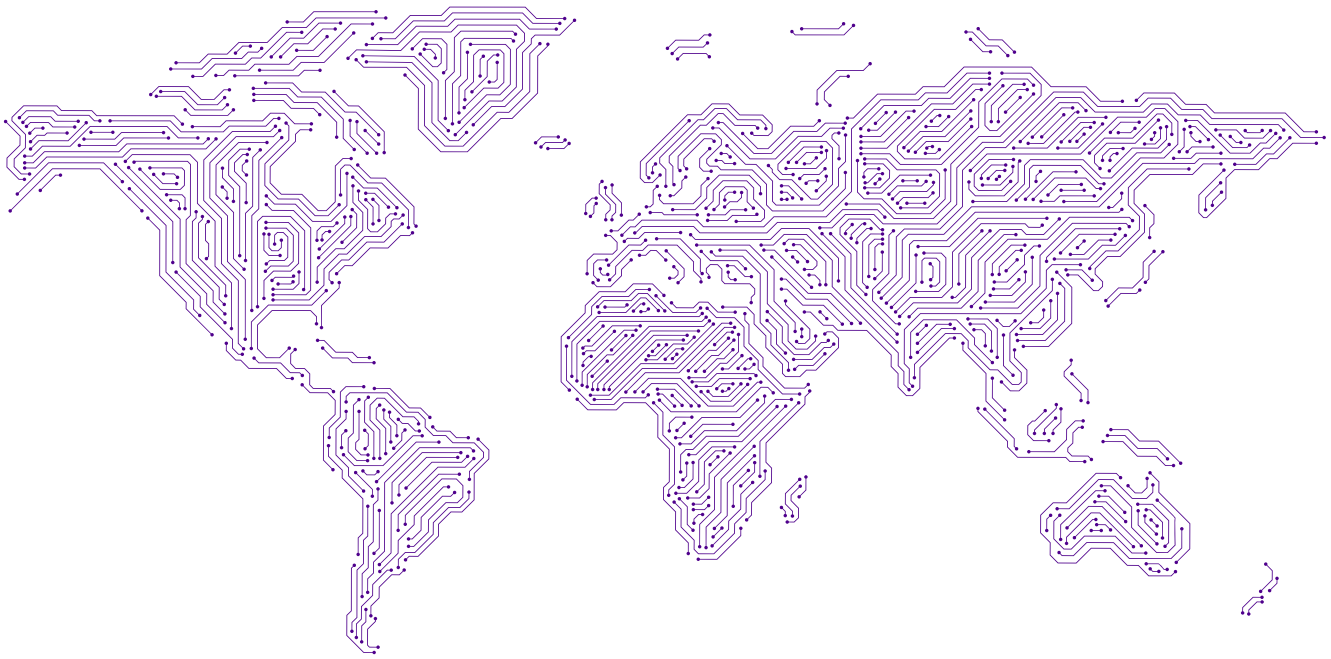
QakBot Trojan

Summary

- QakBot (Pinkslipbot, Qbot) is a long-standing banking trojan that has evolved into a major malware delivery service, and was disrupted by law enforcement in August 2023. In December 2023, Qakbot started to come-back with the unseen version (0x500).

Investigation

- Often delivered through phishing, email hijacking and social engineering.
- In 2023, Qakbot employed various tactics, including the use of **malicious OneNote is benign by nature (a Windows Application)** and signed Windows Installer (MSI) files, Mark of the Web evasion, and HTML smuggling.
- QakBot has been operated by Mallard Spider also involved in the Ransom Knight ransomware delivery by the Remcos backdoor.



source:

statistics drawn from the last 6 months of regional intelligence of attacks (malware, actors) from the Anomali Intelligence Channels (Malware, Adversary) powered by Anomali's partners Polyswarm and Bitdefender.

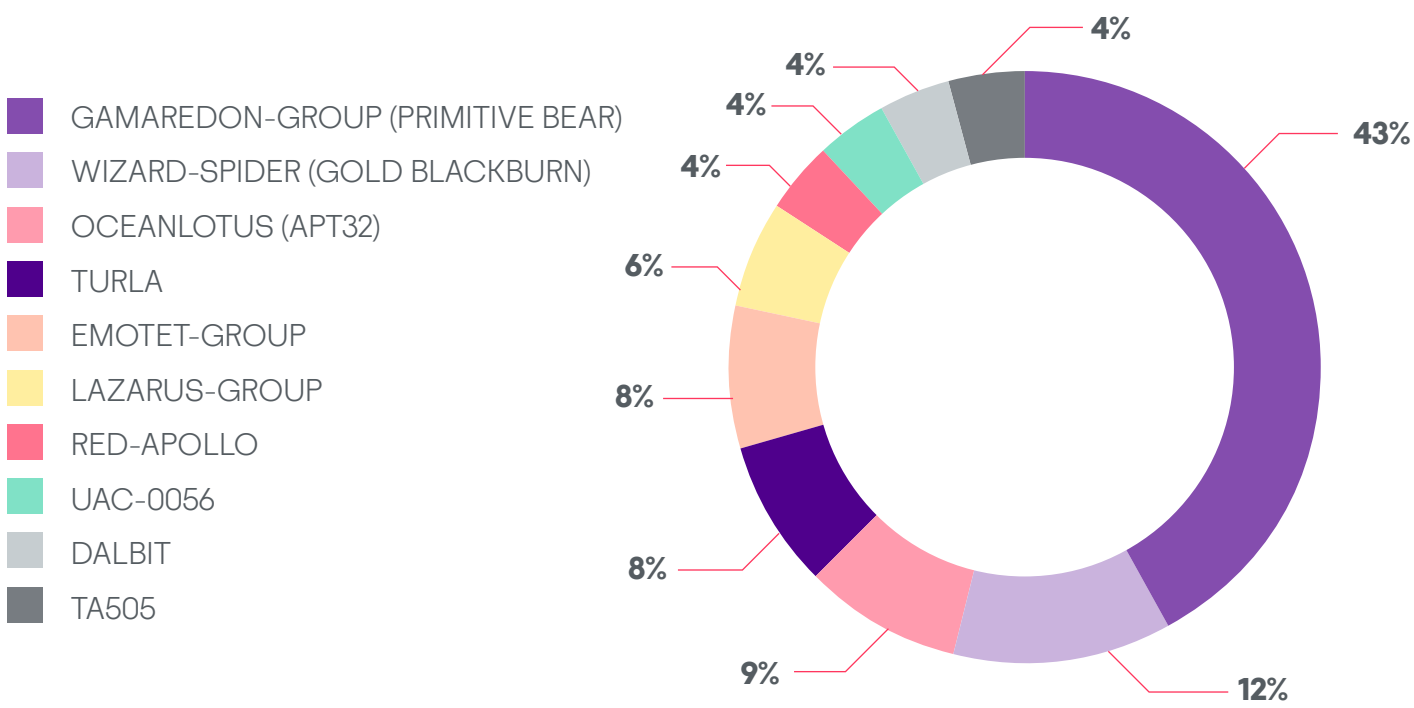
03

Regional Statistics

sirar by stc

Top 10 Threat Actors

Observed in Middle East



Summary :

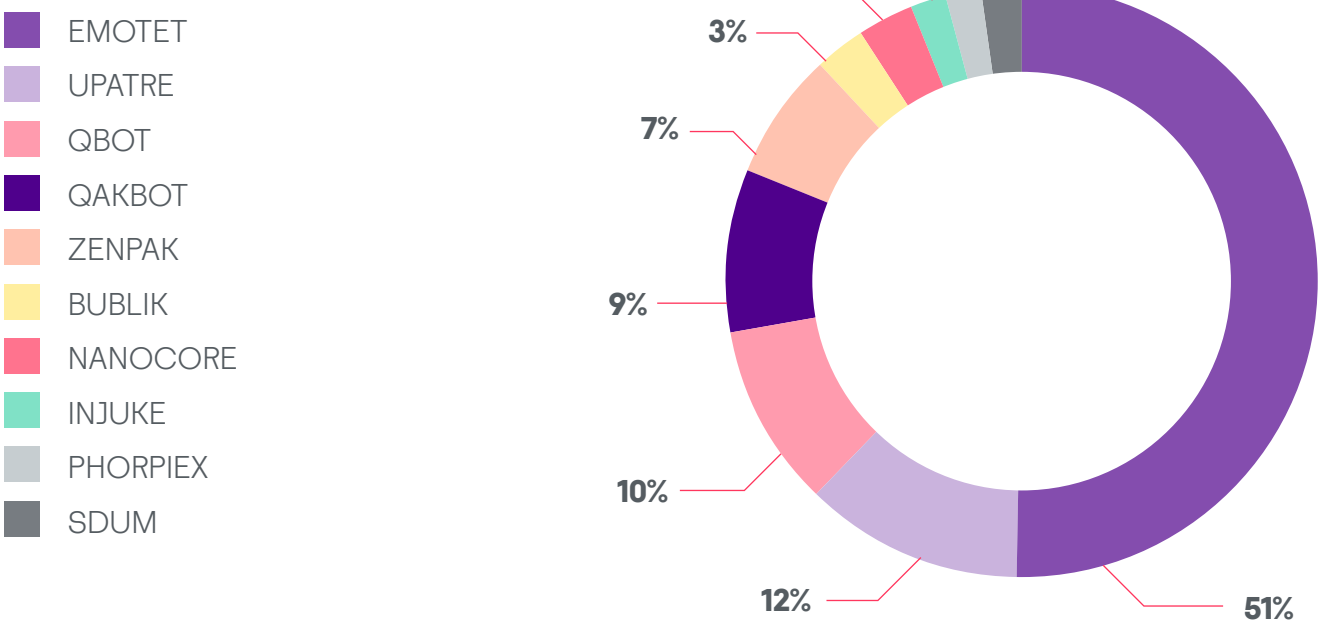
The top threat actors targeting the Middle East can be split into two primary categories. Cybercrime, which are the financially motivated threat actors, and cyberespionage, which are threat actors motivated by information. Out of the 10 actors, seven of them are cyberespionage groups (Dalbit, Gamaredon Group (Primitive Bear), Lazarus Group, Turla, OceanLotus (APT32), Red Apollo (APT10), Turla, and UAC-0056 (Ember Bear), while the remaining three are cybercrime groups (Emotet Group, TA505, and Wizard Spider). This report implies that over the last six months, the majority of attributed threat actor activity targeting the Middle East was conducted to steal sensitive information. Information supporting these insights was gathered from the Anomali Intelligence Channels for Adversary and Malware correlated with the Threat Actor Profiles, news, advisory and research sources maintained by Anomali Threat Research on the ThreatStream platform.

source:

statistics drawn from the last 6 months of regional intelligence of attacks (actors, malware) from the Anomali Intelligence Channels (Malware, Adversary, ...) powered by Anomali's partners Polyswarm and Bitdefender.

Top 10 Malwares

Observed in Middle East



Summary :

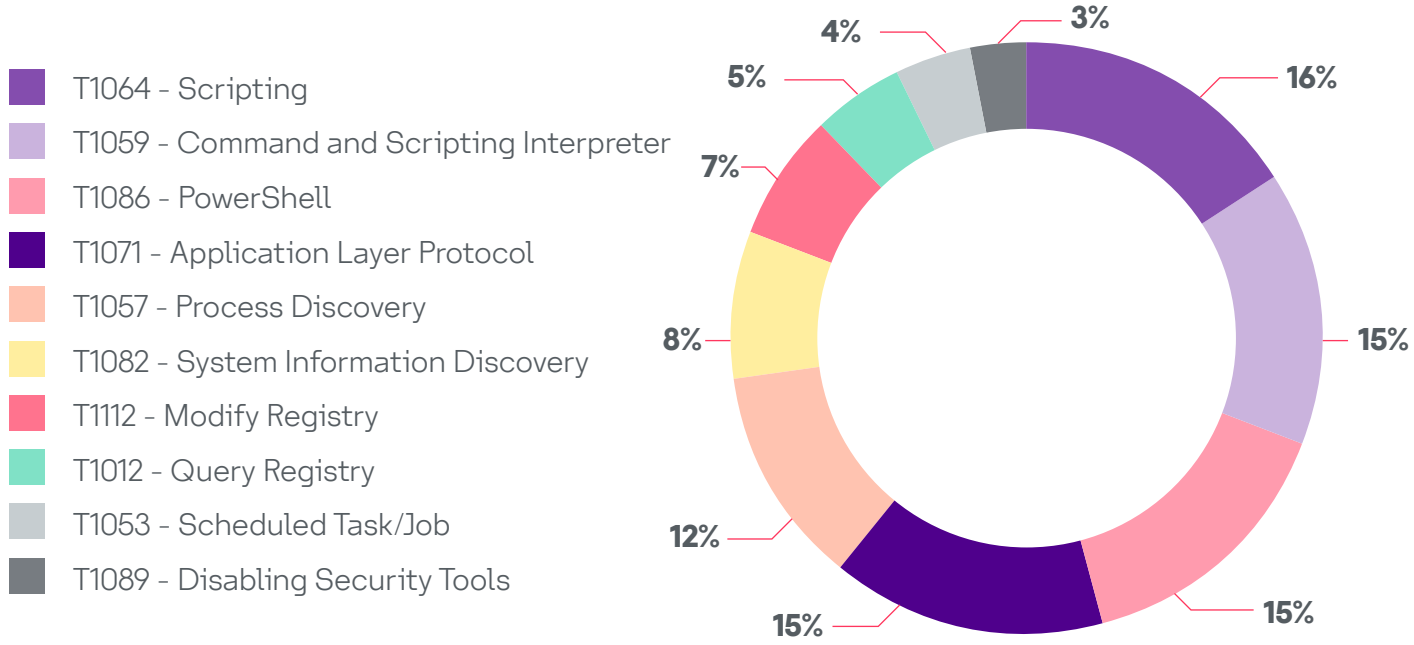
These top three malware families (Emotet, Qbot, and Upatre), representing **73%** of the attributed attacks on the Middle East, all have been in the wild for nearly or over **10 years**. These malware families show the longevity and persistence of their developers and operators, while also highlighting threat actor's perceived value in modular malware. The ability of modular malware to do things "on the fly" allows actors to test multiple ways to achieve their objective instead of always relying hardcoded instructions.

source:

statistics drawn from the last 6 months of regional intelligence of attacks (actors, malware) from the Anomali Intelligence Channels (Malware, Adversary, ...) powered by Anomali's partners Polyswarm and Bitdefender.

Top 10 MITRE

Techniques Used in Middle East



Summary :

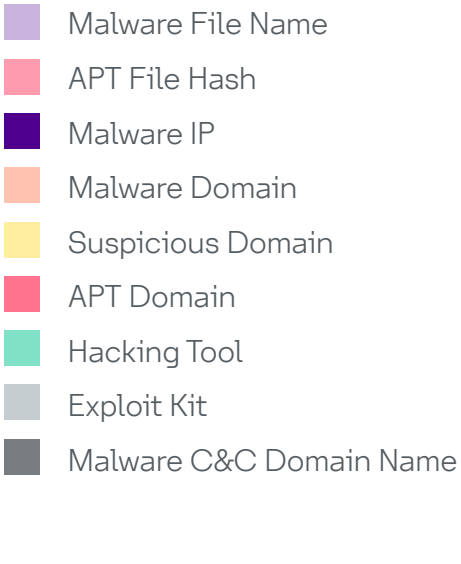
The most-frequently used Tactics, Techniques and Procedures (TTPs) in attacks targeting the Middle East are themed, from most to least from TTPs that involve using scripts and scripting interpreters, to communication and discovery, to maintaining persistence. Threat actors and malware used scripts (T1064) and scripting interpreters (T1059) to execute commands, files, or other scripts (like PowerShell (T1086)) in attempts to abuse system functionality to conduct arbitrary actions on a target machine. For communication, attackers and their tools utilized application layer protocols (T1071) that can be used for various actions like DNS, email, and web browsing. In the discovery phase, identifying system information (T1082), and modifying (T1112) and querying registry (T1012) components. In the final phase, actors and malware used scheduled tasks/jobs (T1053) and disabling security tools (T1089) to maintain persistence and avoid discovery.

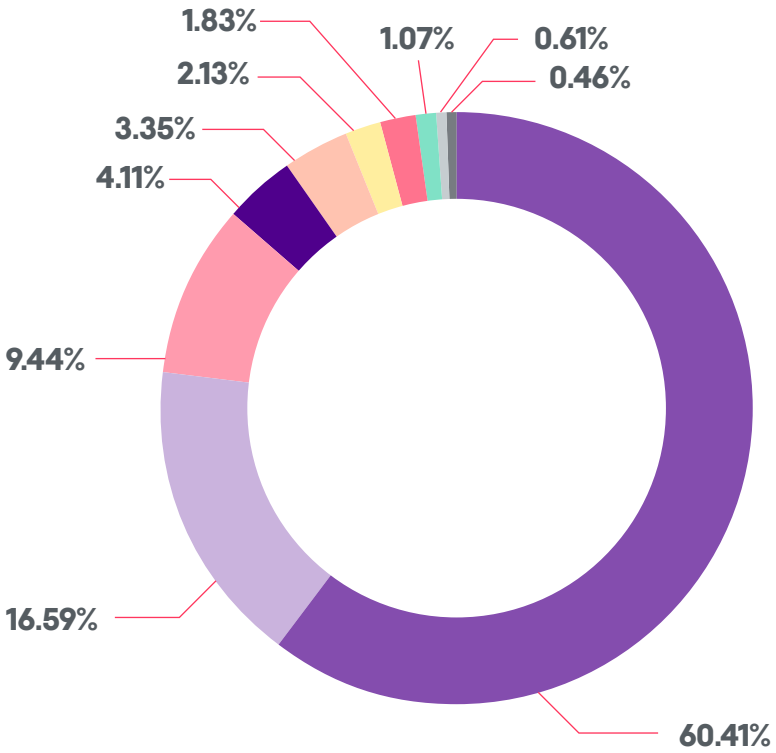
source:

statistics drawn from the last 6 months of regional intelligence of attacks (actors, malware) from the Anomali Intelligence Channels (Malware, Adversary, ...) powered by Anomali's partners Polyswarm and Bitdefender.

Threat Types

Observed in Middle East





Summary :

The Middle East region continues its rapid growth in economic prosperity well beyond the origins in oil and gas. Many parts of the region have established themselves as leading technology innovation hubs and exploit the latest innovations in new digital cities. Alongside this the region has expanded its influence on the world stage both economically and into the challenges facing the globe. There is much to celebrate and take pride in but all of this attracts greater cyber attacks. Motivation shows a mix of cyberespionage (data and IP theft) and financially motivated (enterprise extortion (ransomware, denial of service), fraud) attacks and phishing. Beyond this, as has been witnessed in other regions, disruption and leverage of persistence also rises. The graphic highlights the technical indicators threatening the region - the dominance of Malware and its associated Command and Control and Botnet infrastructures underlines the methods of operation for the attacks. All of this underlines the critical importance of comprehensive security monitoring and response led by relevant threat intelligence that allows organizations to dynamically minimize their attack surface and act swiftly with precision to protect their business, customers and employees as new threats emerge, and attacks affect operations.

source:

statistics drawn from the last 90 days of regional intelligence from OSINT and the Anomali Intelligence Channels (Malware, Adversary, ...) powered by Anomali's partners Polyswarm and Bitdefender.

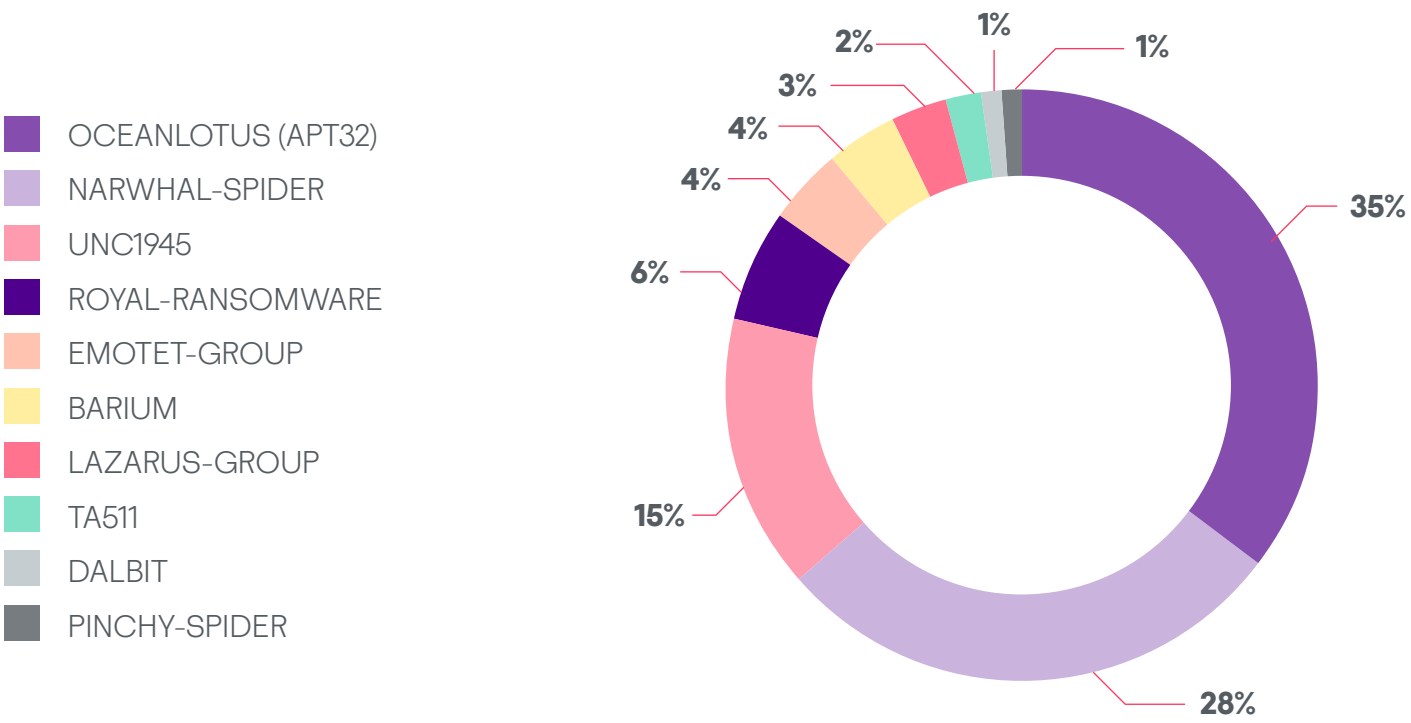
04

KSA Key Statistics

sirar by stc

Top 10 Threat Actors

Observed in Saudi Arabia



Summary :

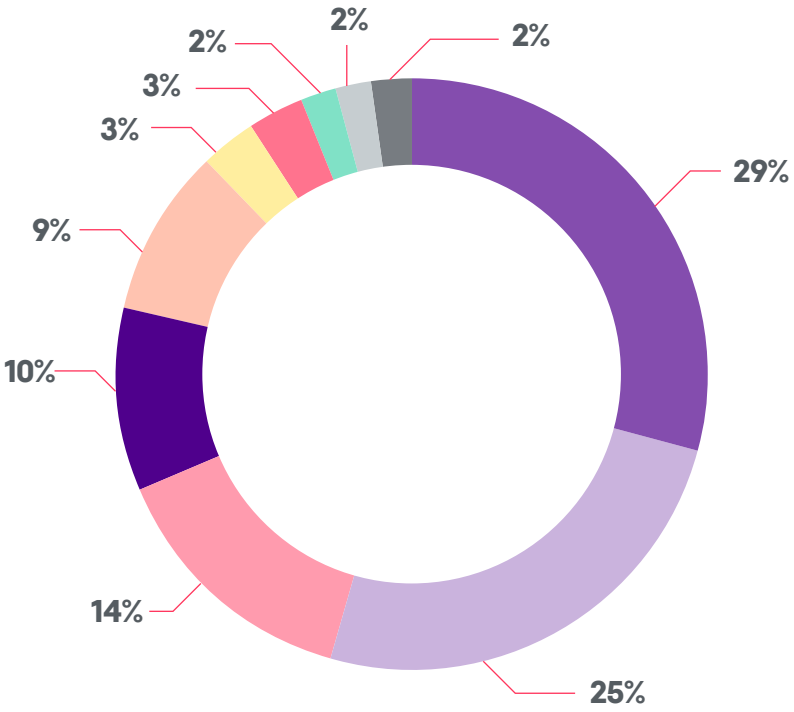
The top threat actors targeting Saudi Arabia can be split into two primary categories. Cybercrime, which are the financially motivated threat actors, and cyberespionage, which are threat actors motivated by information. Out of the **10 threat** groups, seven of them are cybercrime groups (Dalbit, Emotet (Mealybug), Narwhal Spider, Pinchy Spider (Gold Southfield), Royal Ransomware, TA511, and UNC1945), while the remaining three are cyberespionage groups (Barium, OceanLotus (APT32), and Lazarus). This report shows that over the last six months, the majority of threat actors targeting the Kingdom of Saudi Arabia had financial motivations.

source:

statistics drawn from the last 6 months of regional intelligence of attacks (actors, malware) from the Anomali Intelligence Channels (Malware, Adversary, ...) powered by Anomali's partners Polyswarm and Bitdefender.

Top 10 Malwares

Observed in Saudi Arabia



Summary :

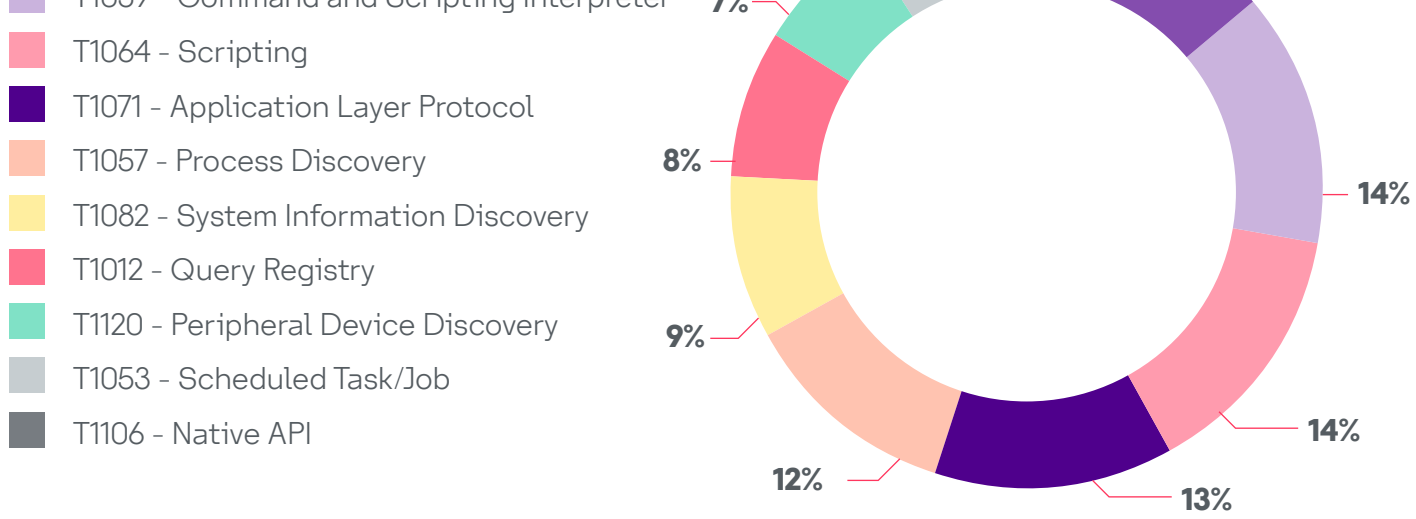
The top four malware families (Emotet, Upatre, Qakbot, and Qbot) represent **68%** of the attributed attacks on the Kingdom of Saudi Arabia. This report shows that the same trends for malware targeting the Middle East can also be applied to malware only targeting the KSA. These malware families are commodity and often widely distributed in an indiscriminate nature. The modular functionality of the malware allows them to function as multiple malware in one, particularly with the ability to function as a downloader for other malicious payloads while also having information stealing and/or worm capabilities themselves.

source:

statistics drawn from the last 6 months of regional intelligence of attacks (actors, malware) from the Anomali Intelligence Channels (Malware, Adversary, ...) powered by Anomali's partners Polyswarm and Bitdefender.

Top 10 MITRE

Techniques in Saudi Arabia



Summary :

The most-frequently used TTPs in attacks targeting the Kingdom of Saudi Arabia are themed, from most to least from TTPs that involve using scripts and scripting interpreters, to communication and discovery, to maintaining persistence. Threat actors and malware used PowerShell (T1086) scripts and interacted with command and scripting interpreters (T1059) in attempts to execute scripts (T1064), and less frequently the native API (T1106) to launch commands and open applications or files. For communication, attackers and their tools utilized application layer protocols (T1071) that can be used for various actions like DNS, email, and web browsing. Discovery actions were conducted to identify processes (T1057), system information (T1082), query registries (T1012), and discovering peripheral devices (T1120). In the maintaining persistence phase, actors and malware most heavily-relied on scheduled tasks/jobs (T1106).

source:

statistics drawn from the last 6 months of regional intelligence of attacks (actors, malware) from the Anomali Intelligence Channels (Malware, Adversary, ...) powered by Anomali's partners Polyswarm and Bitdefender.

05

sirar Battles

sirar
by stc

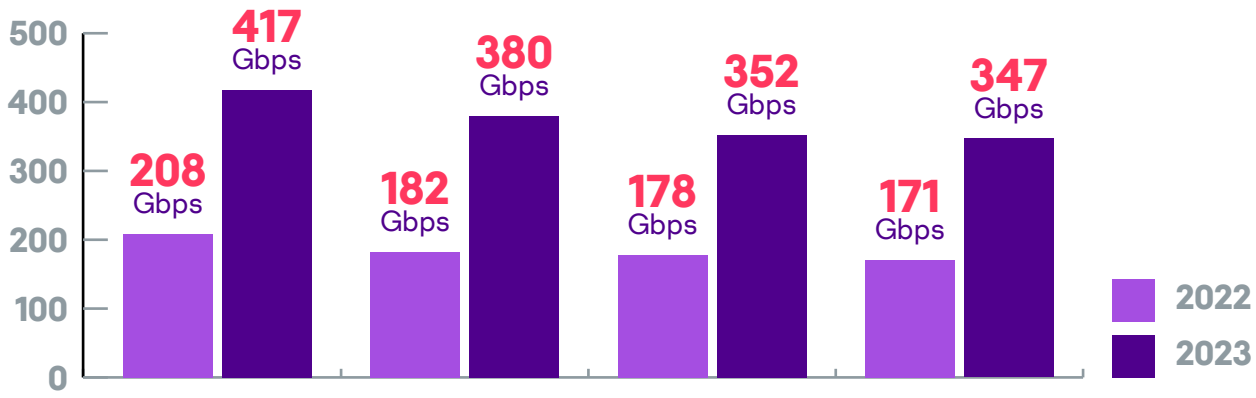
sirar Battles

DDoS Protection

sirar
by stc

Top DDoS

KSA Attacks in 2023 in comparison to 2022



Average Attack Volume Increased by **121%**

Top **4** attacks volume

The size of the largest **DDoS** attack mitigated **2022-2023**

Total Prevented Downtimes

2022
5,560 Hours

2023
6,639 Hours

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

4 Tbps

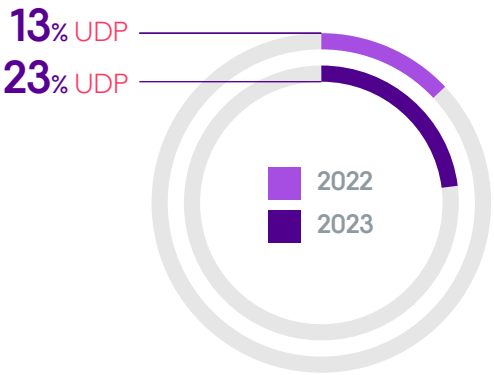
sirar local scrubbing centers can mitigate national & international DDoS attacks up to **4Tbps** (locally within KSA), which is the largest in the region.

DDoS

Attacks In Details

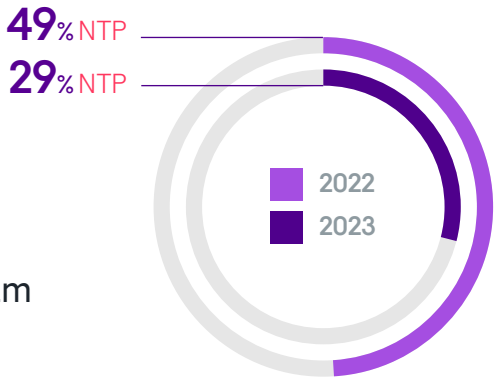
UDP Flood

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



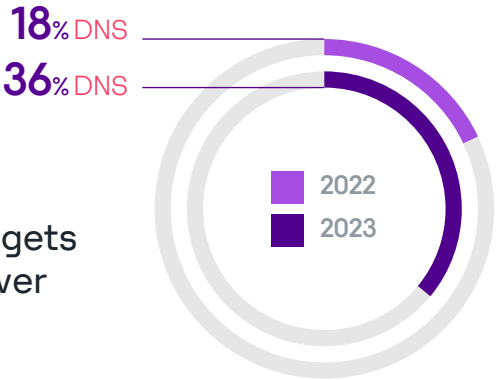
NTP Amplification

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



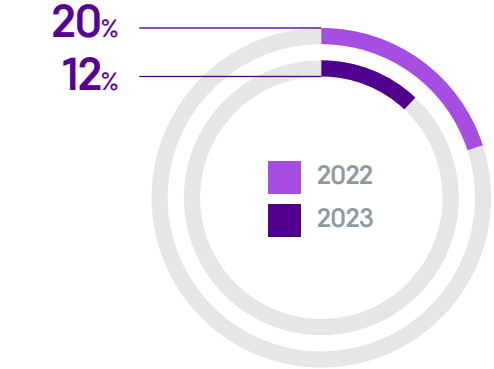
DNS Amplification

DNS Amplification attack is when an attacker targets open recursive DNS servers for the purpose of over consuming the bandwidth.



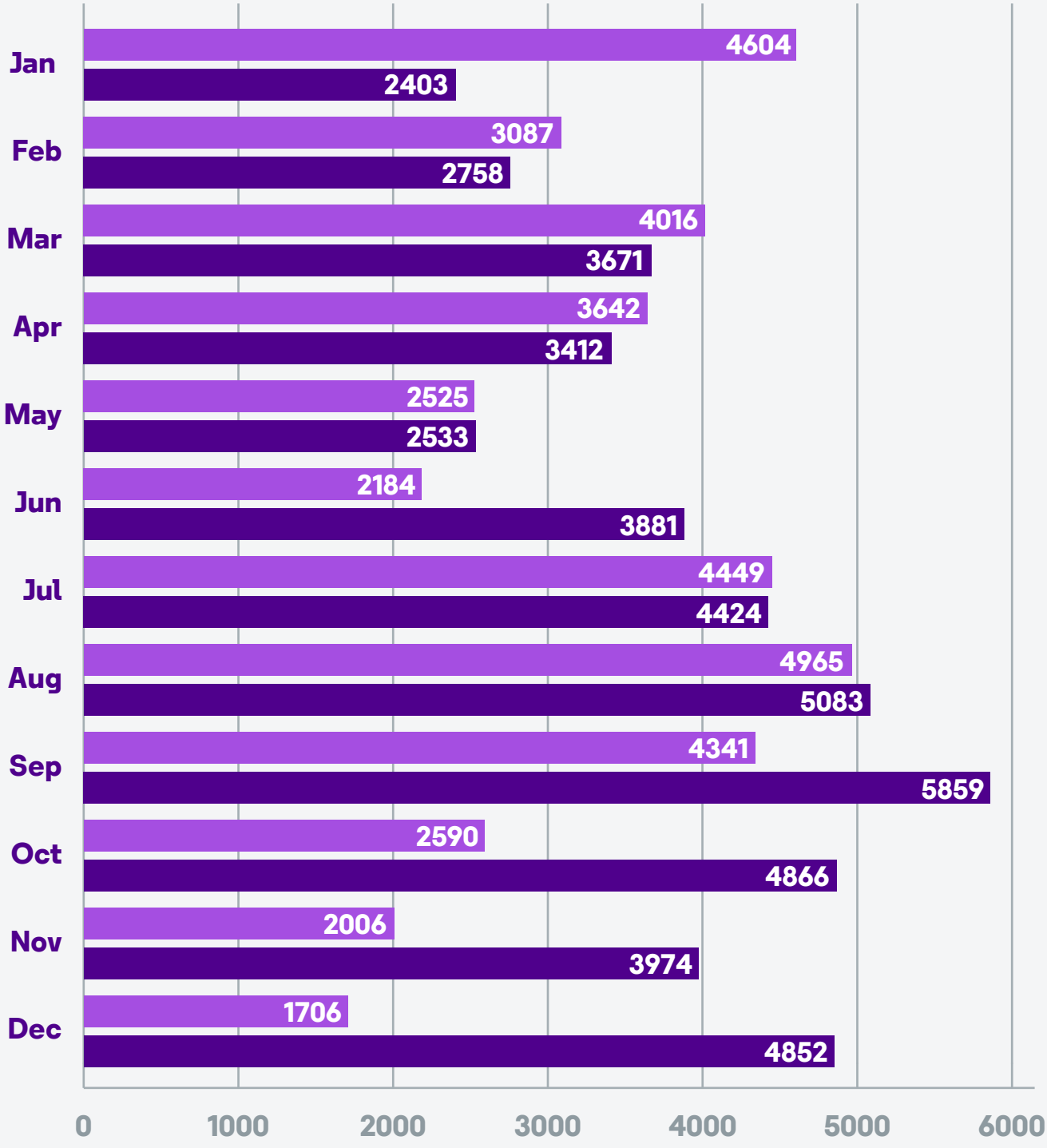
Others

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



Top DDoS

Number of DDoS attacks per month



Number of attacks increased by **19%** compared to last year.

2022 2023

sirar Battles

Vulnerability Management, Detection and Response

sirar
by stc

Vulnerability Management, Detection and Response (VMDR)

sirar by stc vulnerability management detection and response services offers continuous assessments of your infrastructure's cybersecurity vulnerabilities and compliance posture. Gain comprehensive visibility across all IT assets, automate threat prioritization, patching, and other responses. Stay ahead of evolving threats, enhance your cybersecurity posture, and protect critical assets by leveraging these proactive services.

	2022	2023
CLOSED VULNERABILITIES	402K	604K
VULNERABILITIES DETECTED	785K	701K

Protecting our customers by continuously scanning and detecting vulnerabilities based on the sirar vulnerability database according to the newly discovered vulnerabilities in the public.

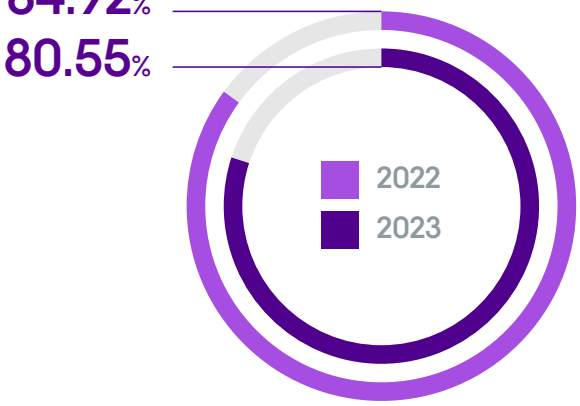
sirar Battles

Email Security

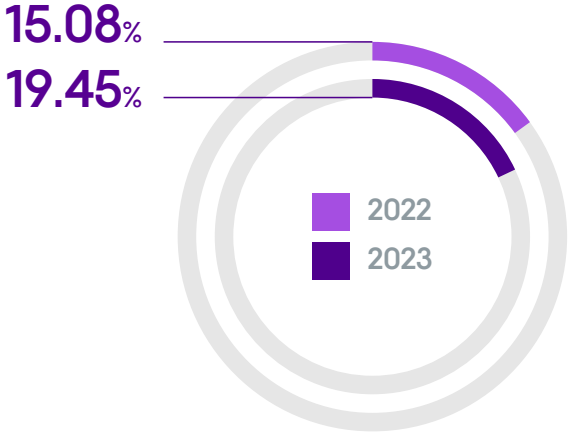
sirar
by stc

Email Security

sirar by stc Cloud-based Email Security service offers robust protection against diverse email threats. With advanced defense mechanisms, it prevents, detects, and it detects and prevents spam, phishing, malware, zero-day threats, impersonation attacks, and BEC incidents. This globally recognized service covers the entire email lifecycle without requiring onsite hardware or software installation, reducing complexity and resource needs.



PERCENTAGE OF CLEAN EMAILS



PERCENTAGE OF MALICIOUS EMAILS

sirar Battles

Web Security

sirar
by stc

Web Security

sirar by stc Web Security service is a highly secure and comprehensive solution that protects organizations from a wide range of web-based threats. It simplifies the security landscape, reduces costs, and enhances web browsing experiences through a locally distributed cloud infrastructure. With scalable protection for all users, it eliminates the need for extensive network infrastructure, reducing costs and simplifying maintenance.

	2022	2023
Total number of threats blocked in sirar	2.4 M	7.3 M

More than **200%** increase in the total number of threats blocked.

Advanced threats blocked by transactions 2023:

Adware/Spyware Sites	44%
Phishing	28%
Malicious Content	24%
Others	4%

sirar Battles

SOCaaS

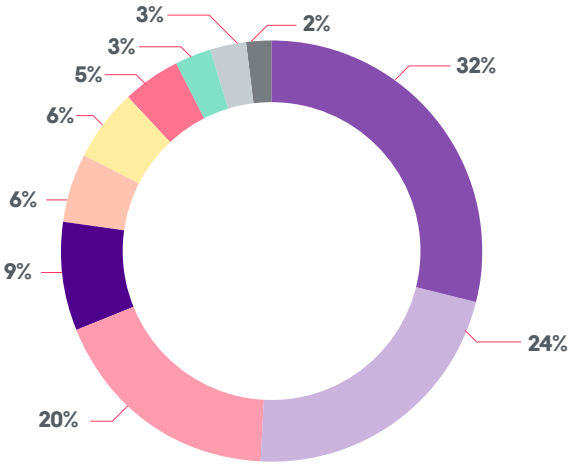
sirar
by stc

Security Operation Center as a service (SOCaaS)

sirar by stc security Operations center (SOC) is a premier 24/7 monitoring and detection service. Our comprehensive solution integrates skilled experts, advanced technologies, and adherence to regulatory standards. Based in Saudi Arabia, and we help organizations to proactively identify and address cyber threats.

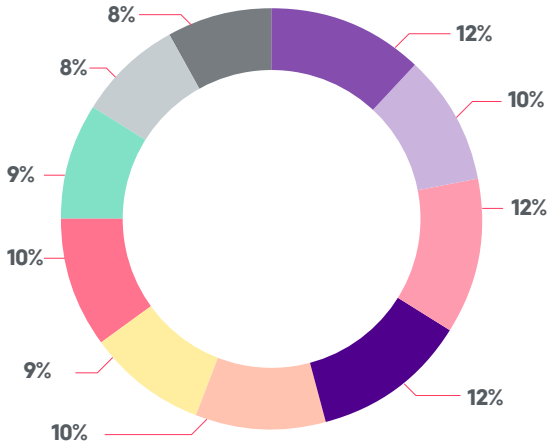
Top 10 Types of Attacks :

- Brute Force
- Malicious/Suspicious connection
- Suspicious/Malicious file
- Unauthorized access
- Account Access Manipulation
- Web application attack
- Suspicious/Malicious process
- System Network Discovery
- Network Scanning
- Phishing Email



Top Targeted Industries:

- Government and Military
- Financial Services
- Telecommunication
- Manufacturing
- Education
- Information Technology
- Transportation
- Real Estate
- Energy
- Hospitality



sirar Battles

Incident Response

sirar
by stc

Incident Response

This section provides insights into the Incident Response (IR) cases handled by sirar throughout 2023.

Dwell Time

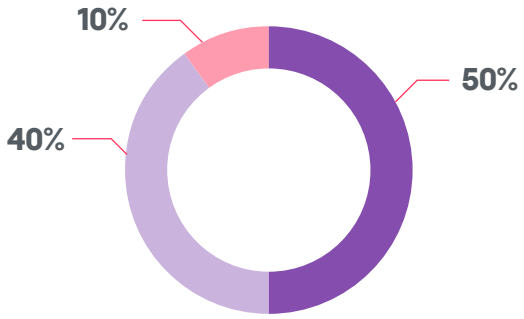
Dwell time is defined as the duration that a cyber threat remains undetected within an environment, measuring the period from the initial compromise until its discovery.

	Number of days
Median Dwell Time	13

Initial Attack Vector

The initial attack vector is the specific method by which a cyber attacker first gains unauthorized access to a system or network.

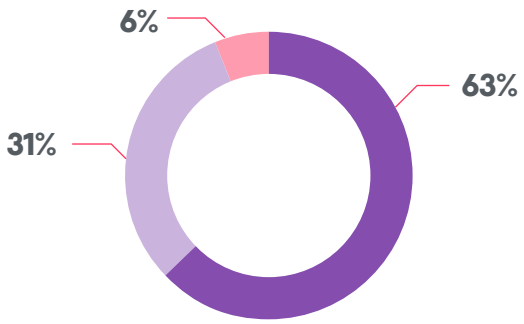
- Exploit Public-Facing Application
- Valid Accounts
- Phishing



Detection Source

A metric to showcase how the attack was detected, either by self-detection, third party, or an attacker email/note.

- Third Party
- Self-Detection
- Attacker Email/Note

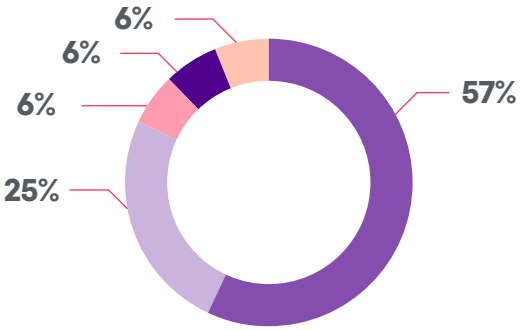


Incident Response

Attack Type

Attack type refers to the categorization or classification of a cyber threat based on its methods, techniques, and objectives.

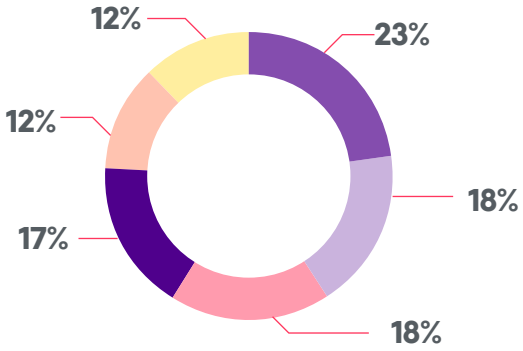
- Web Attack
- Malware
- Unauthorized Access
- Cyber Extortion
- Phishing



Attacker Motivation

Attacker motivation refers to the underlying reasons or goals driving an individual or group to engage in cyber attacks.

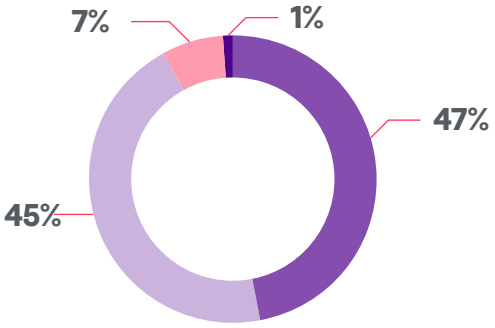
- Knowledge Gaining
- Financial Gain
- Access Gaining
- Data Theft
- Sabotage and Disruption
- Thrill-Seeking and Recognition



Indicator of Compromise (IoCs) based on categories

Identified Indicators of Compromise (IoCs) are clues and evidence of a data breach found in engagements by their categories.

- File Hash
- IP Address
- Domain Name
- Email ID



Incident Response

Common Vulnerability Exploits

Vulnerability exploitation involves taking advantage of weaknesses or flaws in a system's security to gain unauthorized access, manipulate, or compromise the system, often carried out by cyber attackers to exploit vulnerabilities for malicious purposes.

Oracle Enterprise Resources Planning (ERP)

CVE-2022-21587 Critical 9.8
Remote Code Execution Vulnerability:
A vulnerability in the Oracle Web Applications Desktop Integrator product of Oracle E-Business Suite (component: Upload), when exploited can lead to unauthenticated Remote Code Execution.

Apache Log4j2

CVE-2021-44228 Critical 10.0
Remote Code Execution Vulnerability:
A critical vulnerability has been identified on versions 2.0.0 and below of Apache Log4j. An attacker can run arbitrary code remotely by targeting the JNDI lookup plugin in an LDAP server.

Microsoft Exchange Server

A group of vulnerabilities known as ProxyShell targeting Microsoft exchange server, allowing an attacker to get around authentication and run code as a privileged user. The following three vulnerabilities are combined and can be utilized in producing a ProxyShell single attack chain:

CVE-2021-34473 Critical 9.8
Remote Code Execution Vulnerability:
Pre-Authentication Microsoft Exchange vulnerability when exploited can lead the attacker to bypass access control.

CVE-2021- 34523 Critical 9.8
Privilege Escalation Vulnerability:
This zero-day vulnerability can be exploited by the attacker to escalate their privileges and obtain unauthorized access to the Exchange Server.

CVE-2021-31207 High 7.2
Security Feature Bypass Vulnerability:
Post-Authentication Microsoft Exchange vulnerability that uses arbitrary file-writing that can lead to Remote Code Execution (RCE).

Microsoft SharePoint

CVE-2019-0604 Critical 9.8
Remote Code Execution Vulnerability:
Inadequate input validation while examining the source markup of an application package has resulted in a vulnerability in Microsoft SharePoint. An attacker who is successful in exploiting the vulnerability would be able to execute arbitrary code.

NetScaler ADC and NetScaler Gateway

CVE-2023-3519 Critical 9.8
Remote Code Execution Vulnerability:
A Code Injection vulnerability affecting NetScaler ADC and NetScaler Gateway that can be exploited by attackers by uploading malicious webshells and scripts, which enables them to search networks and retrieve private data.

The base score is based on Common Vulnerability Scoring System (CVSS) Version 3.X measured by NIST National Vulnerability Database (NVD).
Please refer to references page for sources.

Incident Response

MITRE ATT&CK Mapping

Mapping the attackers Tactics, Techniques, and Procedures (TTPs) with MITRE framework using a heatmap to showcase most used TTPs.

Percentage of the most used MITRE ATT&CK Tactics and Techniques

1-3% 4-6% >7%

Reconnaissance
Technique
Active Scanning
Gather Victim Network Information

Resource Development
Technique
Stage Capabilities

Initial Access
Technique
Exploit Public-Facing Application
External Remote Services
Valid Accounts
Phishing

Execution
Technique
Command and Scripting Interpreter
System Services

Persistence
Technique
Boot or Logon Autostart Execution
Create Account
External Remote Services
Server Software Component (WebShell)
Valid Accounts
Create or Modify System Process

Privilege Escalation
Technique
Abuse Elevation Control Mechanism
Valid Accounts

Defense Evasion
Technique
Subvert Trust Controls
Impair Defenses

Credential Access
Technique
OS Credential Dumping
Brute Force
Unsecured Credentials
Adversary-in-the-Middle

Discovery
Technique
Account Discovery
File and Directory Discovery
Network Service Discovery
Network Share Discovery
Remote System Discovery
Software Discovery
System Information Discovery
System Network Configuration Discovery

Lateral movement
Technique
Remote Services

Collection
Technique
Data from Local System
Data from Network Shared Drive

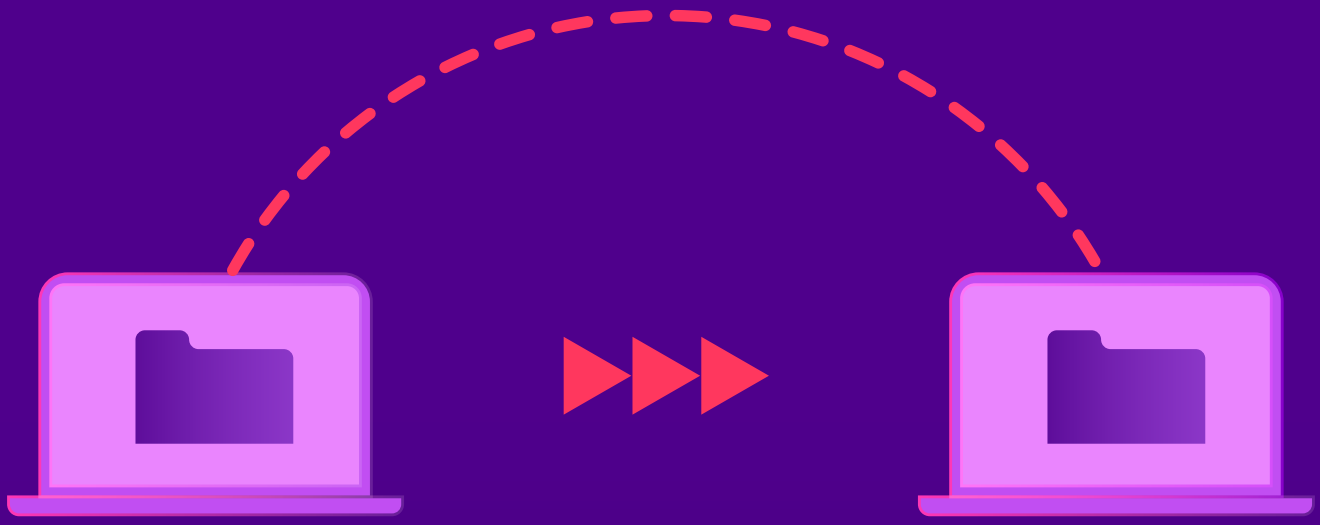
Command and Control
Technique
Ingress Tool Transfer
Application Layer Protocol

Exfiltration
Technique
Automated Exfiltration
Exfiltration Over C2 Channel

Impact
Technique
Data Encrypted for Impact
Inhibit System Recovery
Defacement

06

General Recommendations



sirar by stc

General Recommendations

The predominant cybersecurity vulnerabilities, coupled with suggested recommendations to strengthen organizations' security posture.

Access and Account Management

1- Access Control:

- Enforce Multi-Factor Authentication (MFA), where applicable, on all externally exposed enterprise or third-party applications.
- Secure external remote access to enterprise resources with virtual private network (VPN).
- Prevent unmanaged and non-compliant devices from accessing and connecting to the internal environment.

2- Corporate Account Management and Awareness:

- Develop, document, and enforce account management policy, process, and procedure.
- Maintain an inventory of all privileged accounts and perform a periodic review and updates for privileged accounts to prevent unauthorized access.
- Apply least privileges principle for privileged accounts and implement role-based access controls (RBAC) to ensure employees have access only to the resources necessary for their roles.
- Provide regular employee training and awareness programs to educate employees about the acceptable account usage and activities.

3- Multi-Factor Authentication:

- Enforce implementing Multi-Factor Authentication (MFA), where applicable for all users and services.
- Integrate MFA with identity management systems, where applicable, for centralized control and monitoring.
- Conduct a regular security audit to identify and address potential vulnerabilities in the MFA implementation.

4- Password Management:

- Develop, document, and enforce a password management policy, process, and procedure.
- Adopt the use of password manager solutions, which will improve the overall password security by generating random and strong passwords.
- Educate employees about the risks associated with default credentials and the importance of changing them.

Infrastructure Security

1. **Remote Administrator and Execution Tools:**

- Define, document, and enforce access control policies to ensure that only authorized personnel can use remote administration tools.
- Regularly review and update access permissions based on roles and responsibilities.
- Provide employees with training on the appropriate utilization of remote administration tools, ensure they are informed about potential security risks, and emphasize the importance of promptly reporting any suspicious activities.

General Recommendations

2. **External Email Hosting:**

- Develop, document, and enforce comprehensive email security policies, processes, and procedures encompassing access controls, user and password management, encryption, backup and recovery, and secure configuration.
- Adhere to the relevant regulations related to the external email infrastructure.

3. **Endpoint Security:**

- Deploy robust endpoint protection solutions on all endpoints to foster the detection and response of threats.
- Develop, document, and enforce a regular patch management process to address endpoints vulnerabilities promptly.
- Develop, document, and enforce proper logging mechanisms by leveraging a centralized log management solution.

4. **Network Security:**

- Implement and deploy network security tools for comprehensive network visibility.
- Establish network segmentation utilizing either physical separation, logical separation, or a combination of both which can be achieved through the use of firewalls, access control lists (ACLs), and virtual LANs (VLANs).
- Implement network security measures such as firewalls, intrusion detection/prevention systems (IDS/IPS), and Network Access Control (NAC) solutions to monitor and control traffic passing through network segments.

5. **Secure Configuration:**

- Implement Minimum Baseline Security Standard (MBSS) and best practices for all assets to enhance the overall security posture.
- Develop, document, and enforce a systematic process for regularly reviewing and updating default configurations on software, hardware, and network devices.
- Adhere to security guidelines provided by hardware and software vendors and follow their recommendations for secure configurations to minimize potential risks.

6. **Security Defense Controls:**

- Implement strong and diverse defense controls to oversee both the network segments and all endpoints.
- Develop and enforce a process to build, audit, and regularly review the detection and response capabilities.
- Adhere to a well-defined log management policy, process, and procedure to promptly detect and respond to emerging threats.

7. **Web Services Protection:**

- Implement a multi-layered Defense-in-Depth security strategy, including a Web Application Firewall (WAF) or a host-based alternative if WAF is not applicable.
- Adhere to a well-defined vulnerability management policy, process, and procedure to detect vulnerabilities on published services.
- Adhere to a well-defined configuration management policy, process, and procedure to detect any flaws in web applications.

General Recommendations

Security Governance and Operations

1. **Asset Management:**

- Develop, document, and enforce asset management policy, process, and procedure.
- Maintain an accurate and up-to-date inventory of all assets which shall include all endpoints (physical and virtual), hardware appliances, network devices, etc.
- Utilize asset discovery tools to automatically detect and alert when unauthorized devices attempt to access the network.

2. **Backup Procedure:**

- Develop, document, and enforce a comprehensive data backup policy, process, and procedure to cover all essential information.
- Store backup copies in an offsite or geographically diverse location to mitigate risks associated with physical disasters.
- Ensure that backup management practices comply with relevant industry regulations and data protection laws governing the organization.

3. **Change Management:**

- Develop, document, and enforce change management policy, process, and procedure that outlines the steps involved in proposing, reviewing, testing, approving, and implementing changes.
- Conduct a risk assessment for each proposed change to evaluate potential impacts on the system, security, and overall business operations.
- Integrate change management with incident management processes to ensure a coordinated response in case a change leads to unexpected issues.

4. **Incident Response Plan (IRP):**

- Build a well-defined Incident Response Plan (IRP), playbooks and set of procedures to be followed by Incident response team.
- Conduct regular training sessions and simulated drills to ensure that the incident response team is familiar with their roles and the procedures outlined in the IRP.
- Regularly review and update the IRP based on changes in the IT environment, emerging threats, and lessons learned from previous incidents.

5. **Logging Management and Monitoring:**

- Develop, document, and enforce a comprehensive log management policy, process, and procedure.
- Review and enhance the existing monitoring capabilities on regular basis.
- Deploy real-time monitoring and detection mechanisms to promptly identify and address potential threats.

6. **Patch Management:**

- Develop, document and enforce patch management policy, process, and procedure.
- Utilize automated patching tools to streamline and expedite the patch deployment process.
- Establish a testing environment to evaluate patches before deploying them in the production environment.

General Recommendations

7. **Phishing Email Awareness:**

- Raise employees' awareness by providing regular training sessions and awareness programs, and conduct simulated phishing campaigns.
- Establish a user-friendly mechanism for reporting suspicious emails and encourage employees to report any emails they find suspicious.
- Regularly assess the effectiveness of phishing awareness initiatives through surveys, quizzes, or feedback sessions and use the insights gained to refine and improve the training program.

8. **Security Assessment:**

- Develop, document, and enforce security assessment policies, processes, and procedures.
- Perform periodic cybersecurity assessments, including vulnerability assessments, penetration testing, and security audits to identify and address weaknesses in the environment.
- Regularly review the implemented assessment policies to ensure they are aligned with current industry best practices, regulatory requirements, and emerging threats.

Threat Management

1. **Continuous Threat Hunting:**

- Build and implement a well-defined and thorough threat hunting program.
- Incorporate threat intelligence feeds to stay informed about the latest tactics, techniques, and procedures (TTPs) used by threat actors.
- Regularly review the outcomes of threat hunting activities, assess the effectiveness of implemented measures, and make adjustments accordingly.

2. **Threat Intelligence Program:**

- Develop threat intelligence capabilities to proactively identify any vulnerabilities or threats.
- Integrate threat intelligence feeds with security tools, such as SIEM (Security Information and Event Management) and IDS/IPS (Intrusion Detection and Prevention Systems), to automate threat detection and response.
- Correlate threat intelligence data with internal security logs and incident data to identify patterns and potential indicators of compromise (IoCs).

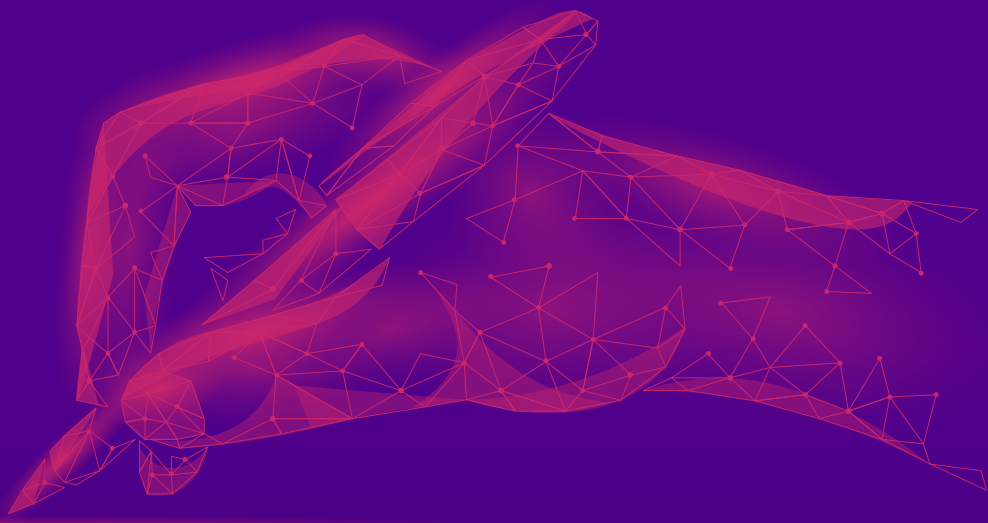
Workforce Planning

1. **Adequate Cybersecurity Staff:**

- Build a cybersecurity technical team to be able to detect and respond efficiently to threats in a timely manner.
- Invest in security automation tools to handle routine tasks, allowing existing staff to focus on more complex and strategic aspects of cybersecurity.
- Prioritize ongoing training and certifications for existing staff to ensure their skills remain up-to-date..

07

Digitize your signature with **Sayen**



sirar by stc

Digitize your signature

with Sayen

Overview

Sayen is an authorized provider of PKI and DTS services, Licensed and accredited by DGA "Digital Government Authority". Our robust **Sayen service** ensures secure document workflows with cryptographic digital signatures, ensuring authenticity, integrity, and non-repudiation. Enterprises gain a competitive advantage by confidently embracing digitalization while maintaining security and enhancing customer experiences.

Product Features

Paperless, **cost-effective** and rich workflow to share, view and sign.

You can sign from **any device, any time, any where.**

Trusted registration, **Bulk signing, 24/7** support.

Business Value

Trusted by **WebTrust, Adobe, Microsoft, Google**,..etc.

Ensures **Authenticity** , Integrity, and Non-repudiation.

Licensed by Digital Government Authority.

Sayen Use Cases

How sayen has benefited the retail and banking industries ?

Sayen's innovative product has proven to be a game-changer in the retail and banking industry, significantly enhancing the overall experience for customers, vendors, and employees alike. With an impressive track record of over **142,000** transactions and more than **1 million** paper documents saved, sayen has not only revolutionized operational efficiency but also yielded substantial time and cost savings of **300%**, equivalent to **2.1 million** SAR. By leveraging sayen's cutting-edge technology, banking and retail institutions have witnessed remarkable improvements in online applications, streamlined contract management, and optimized financial services such as credit cards and loans. This transformative solution has undeniably elevated the standards of customer service and operational excellence within the banking and retail sectors.

Sayen Use Cases

How sayen has helped the Procurement and Human resources ?

Sayen product has emerged as a transformative solution that actively enhances vendor management and boosts employee satisfaction in the realms of Human Resources and Procurement. Within these functions, sayen has achieved remarkable milestones, facilitating over **64,000** transactions and saving nearly **640,000** papers. This translates into substantial time and cost savings of **300%**, amounting to an impressive **1 million** SAR. By integrating sayen into their operations, companies have witnessed a significant improvement in their vendor purchase orders, contract management, as well as streamlining employee job offers and contracts. The impact of sayen's technology has been nothing short of remarkable, painting a picture of enhanced efficiency, improved vendor relationships, and heightened employee satisfaction within the realm of HR and Procurement.

08

sirar Glossary

sirar
by stc

sirar Glossary

Access Control Lists (ACLs):
Rules that either allow access to a computer environment or deny it.

Access Gaining:
Attacker motivated by gaining access to a victims environment.

Attacker Email/Note:
A communication, typically an email or note, sent by an attacker notifying an organization of a successful network breach, often accompanied by threats, demands, or extortion attempts.

Attack Motivation:
The underlying reasons or goals driving an individual or group to engage in cyber attacks.

Attack Surface:
The number of all possible points, or attack vectors, where an unauthorized user can access a system and extract data.

Attack Vector:
A way for attackers to enter a network or system.

Common Vulnerabilities and Exposures (CVE):
A list of publicly disclosed computer security flaws.

Cyber Extortion:
When the attacker threatens/blackmails individuals, businesses or organizations to obtain money or other valuable assets.

Cybersecurity:
The art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

Data Theft:
Attacker that aim to steal digital information stored on computers, servers, or electronic devices to obtain confidential information or compromise privacy.

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.

DNS Servers:
A DNS server is a computer server that contains a database of public IP addresses and their associated hostnames.

sirar Glossary

Dwell time:
Defined as the duration that a cyber threat remains undetected within an environment, measuring the period from the initial compromise until its discovery.

Endpoint:
Devices that connect to a network system such as mobile devices, desktop computers, virtual machines, embedded devices, and servers.

Exploits:
Is a piece of software or data that opportunistically uses a defect in an operating system or an app to provide access to unauthorized actors. The exploit may be used to install more malware or steal data.

Financial Gain:
Attacker motivated by financial gain. They seek to steal sensitive information, such as credit card data, personal information, or login credentials, which they can sell on the black market, use for fraudulent activities, or request a ransom to be paid.

Firewalls:
Network security device that monitors and filters incoming and outgoing network traffic based on an organizations previously established security policies.

Incident Response Plan (IRP):
The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information systems.

Indicators of Compromise (IoC):
Clues and evidence of a data breach.

Intrusion Detection Systems (IDS):
A network security tool that monitors network traffic for suspicious activity and alerts when such activity is discovered.

Intrusion Prevention Systems (IPS):
A network security tool that continuously monitors a network for malicious activity and takes action to prevent it.

Knowledge Gaining:
Attacker motivated by gathering data of the victims environment and infrastructure.

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.

sirar Glossary

Minimum Baseline Security Standard (MBSS):

Set of guidelines and requirements for ensuring the security of information systems and data.

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.

Multi-Factor Authentication (MFA):

Electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism.

Need-To-Know Principle:

Users should only have access to the information that their job function requires.

Network Access Control (NAC) :

A security solution that enforces policy on devices that access networks to increase network visibility and reduce risk.

Network Time Protocol (NTP):

Is a protocol that helps the computers clock times to be synchronized in a network.

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.

Principle of Least Privilege (PoLP):

Users or entities should only have access to the specific data, resources and applications needed to complete a required task.

Ransomware Attack:

organization by encrypting an organization's important files into an unreadable form and demands a ransom payment to decrypt them.

Sabotage and Disruption:

Attackers that aim to disrupt critical infrastructure, services, or operations for political or ideological reasons.

Self-Detection:

Detection was made by the organization.

sirar Glossary

Third Party:
A third party is an external entity or individual not directly related to an organization.

Threat Actor:
Either a person or a group of people that take part in an action that is intended to cause harm to the cyber realm including: computers, devices, systems, or networks.

Thrill-Seeking:
Attacker motivated by the promise of fame and the challenge and excitement of hacking into systems, networks, or websites. They may seek recognition within hacker communities. In other words, some hackers just want "bragging rights."

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.

Unauthorized Access:
Is when a person who does not have permission to connect to or use a system gains entry in a manner unintended by the system owner

Unauthorized Scanning:
Unauthorized scanning involves probing or analyzing computer systems without proper authorization, typically with malicious intent to identify vulnerabilities and potential entry points for unauthorized access.

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.

Virtual LANs (VLANs):
Virtualized connection that connects multiple devices and network nodes from different LANs into one logical network.

Virtual Private Network (VPN):
A mechanism for creating a secure connection between a computing device and a computer network, or between two networks, using an insecure communication medium such as the public Internet.

Web Application Firewall (WAF):
Firewall that protects web applications by filtering and monitoring HTTP traffic between a web application and the Internet.

sirar Glossary

Web Attack:

Targets vulnerabilities in websites to gain unauthorized access, obtain confidential information, introduce malicious content, or alter the website content.

Web Defacement:

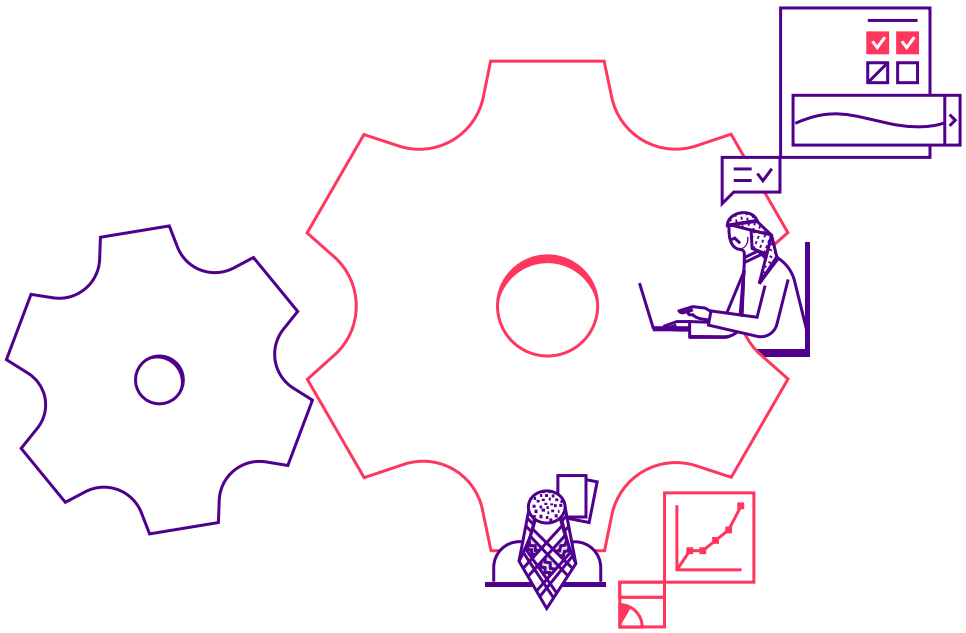
An attack on a website that changes the visual appearance of a website or a web page.

WebShells:

A web script that is placed on an openly accessible web server to allow an adversary to use the web server as a gateway into a network.

Whitelisting:

Allowing only approved and explicitly identified list (e.g., programs, users, or entities, etc.) access to a specific system, network, or service, while blocking all others.



09

References

sirar by stc

References

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

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

What is a distributed denial-of-service (ddos) attack? - cloudflare.
https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/Network time protocol (NTP). GeeksforGeeks.
https://www.geeksforgeeks.org/network-time-protocol-ntp/

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

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

What is malware? - definition and examples. Cisco. (2023, November 16).
https://www.cisco.com/site/us/en/learn/topics/security/what-is-malware.html#:~:text=Malware%2C%20short%20for%20malicious%20software,spyware%2C%20adware%2C%20and%20ransomware.

10 most common types of cyber attacks today - crowdstrike. crowdstrike.com. (2023, November 9).
https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/

Yasar, K. (2023, July 18). What is cyber extortion?: Definition from TechTarget. Security.
https://www.techtarget.com/searchsecurity/definition/cyberextortion#:~:text=Cyber%20extortion%20is%20a%20broader,money%20or%20other%20valuable%20assets.

Unauthorized access. Information Security. (2017, December 20).
https://security.tennessee.edu/unauthorized-access/#:~:text=Unauthorized%20Access%20is%20when%20a,for%20this%20is%20%E2%80%9Chacking%E2%80%9D.

Web attacks. CIS. (2021, June 15).
https://www.cisecurity.org/insights/spotlight/ei-isac-cybersecurity-spotlight-web-attack

Business advisories. Advisories || Business.
https://www.csa.gov.gh/website_defacement.php#:~:text=Website%20defacement%20is%20an%20attack,is%20a%20form%20of%20vandalism.

Server software component: Web shell. Server Software Component: Web Shell, Sub-technique T1505.003 - Enterprise | MITRE ATT&CK®.
https://attack.mitre.org/techniques/T1505/003/#:~:text=A%20web%20shell%20is%20a%20web%20script%20placed%20on%20an,the%20broader%20server%20operating%20system.

Kaspersky. (2023, April 19). What is data theft and how to prevent it. me.
https://me-en.kaspersky.com/resource-center/threats/data-theft

Threat actors explained: Motivations and capabilities. SOPHOS. (2024, January 12).
https://www.sophos.com/en-us/cybersecurity-explained/threat-actors#:~:text=Some%20common%20motivations%20for%20threat,or%20use%20for%20fraudulent%20activities.

What is a Network Access Control List (ACL)?. Fortinet.
https://www.fortinet.com/resources/cyberglossary/network-access-control-list#:~:text=An%20access%20control%20list%20(ACL)%20is%20made%20up%20of%20rules,are%20allowed%20in%20the%20doors.

What is an attack surface? definition and how to reduce it. Fortinet.
https://www.fortinet.com/resources/cyberglossary/attack-surface#:~:text=The%20attack%20surface%20is%20the,easier%20it%20is%20to%20protect.

What is an attack vector? | cloudflare.
https://www.cloudflare.com/learning/security/glossary/attack-vector/

References

Arntz, P. (2023, September 18). The mystery of the cves that are not vulnerabilities. Malwarebytes.
https://www.malwarebytes.com/blog/news/2023/09/the-mystery-of-the-cves-that-are-not-vulnerabilities#:~:text=The%20Common%20Vulnerabilities%20and%20Exposures,%2C%20databases%2C%20and%20services).

Dwell time. Plurilock. (2023, September 14).
https://plurilock.com/deep-dive/dwell-time/#:~:text=In%20the%20ever%2Devolving%20landscape,within%20a%20network%20or%20system.

What is an endpoint?: Microsoft security. What Is an Endpoint? | Microsoft Security.
://www.microsoft.com/en/security/business/security-101/what-is-an-endpoint#:~:text=Endpoints%20are%20physical%20devices%20that,%2C%20embedded%20devices%2C%20and%20servers.

Bferrite. (2023, September 7). What is a Firewall? the different types of firewalls. Check Point Software.
://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/#:~:text=A%20Firewall%20is%20a%20network,network%20and%20the%20public%20Internet.

Incident response plan - glossary: CSRC. CSRC Content Editor.
https://csrc.nist.gov/glossary/term/incident_response_plan#:~:text=Definitions%3A,organization's%20information%20systems(s).

What are indicators of compromise (IOC): Proofpoint us. Proofpoint. (2023, November 13).
://www.proofpoint.com/us/threat-reference/indicators-compromise

Lutkevich, B. (2021, October 7). What is an intrusion detection system (IDS)? definition searchsecurity. Security.
://www.techtarget.com/searchsecurity/definition/intrusion-detection-system#:~:text=An%20intrusion%20detection%20system%20(IDS)%20is%20a%20system%20that%20monitors,when%20such%20activity%20is%20discovered.

What is intrusion prevention system? | vmware glossary.
https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html

Minimum baseline security standard development. IT SECURITY C&T. (2023, April 4).
https://itsecurityct.com/services-solutions/consulting-services/technical-security-consultation/infrastructure-security/minimum-baseline-security-standard-development/#:~:text=The%20Minimum%20Baseline%20Security%20Standard,systems%20to%20protect%20sensitive%20information.

Mitre ATT&CK®. MITRE ATT&CK®.
https://attack.mitre.org/

Multi-factor authentication policy. Fordham University.
https://www.fordham.edu/information-technology/it-security--assurance/it-policies-procedures-and-guidelines/multi-factor-authentication-policy/#:~:text=Multi%2DFactor%20Authentication%20is%20an,knowledge%2C%20possession%2C%20and%20inherence.

Security: The need-to-know principle. TECHCOMMUNITY.MICROSOFT.COM. (2021, May 28).
https://techcommunity.microsoft.com/t5/azure-sql-blog/security-the-need-to-know-principle/ba-p/2112393#:~:text=This%20principle%20states%20that%20a,a%20Need%2Dto%2Dknow.

Cisco. (2023a, July 24). What is Network Access Control (NAC)?. Cisco.
https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html

What is the principle of least privilege?. Palo Alto Networks.
https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege#:~:text=The%20principle%20of%20least%20privilege%20(PoLP)%20is%20an%20information%20security,to%20complete%20a%20required%20task.

What is VLAN (virtual lan)? - it glossary. SolarWinds.
https://www.solarwinds.com/resources/it-glossary/vlan

What is a WAF? | web application firewall explained | Cloudflare.
https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

NVD.
https://nvd.nist.gov/vuln/detail/CVE-2022-21587

References

NVD.
https://nvd.nist.gov/vuln/detail/CVE-2021-44228

Mandiant. ProxyShell exploiting Microsoft Exchange Servers.
https://www.mandiant.com/resources/blog/pst-want-shell-proxyshell-exploiting-microsoft-exchange-servers

CVE-2019-0604: Critical microsoft sharepoint remote code execution flaw actively exploited. Tenable®. (2019, December 12).
https://www.tenable.com/blog/cve-2019-0604-critical-microsoft-sharepoint-remote-code-execution-flaw-actively-exploited

Sangolekar, V., Kumar, A., Gupta, N., & Sandila, V. (2024, January 5). Security advisory: Remote code execution vulnerability (CVE-2023-3519). CVE-2023-3519 | ThreatLabz.
https://www.zscaler.com/blogs/security-research/security-advisory-remote-code-execution-vulnerability-cve-2023-3519

ProxyShell vulnerabilities in Microsoft Exchange: What to do. Sophos News.(2022, September 30).
https://news.sophos.com/en-us/2021/08/23/proxyshell-vulnerabilities-in-microsoft-exchange-what-to-do/

What is cybersecurity?: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2024, January 29).
https://www.cisa.gov/news-events/news/what-cybersecurity

What you need to know about network DNS servers. Lifewire. Fisher, T. (2023, October 17).
https://www.lifewire.com/what-is-a-dns-server-2625854

Contact Us

For more information reach us on the below channels:

- www.sirar.com.sa
- info@sirar.com.sa
- @sirar_bystc
- sirarbystc

Thank You

sirar by stc