Threat Intel Roundup: Linux, FishEye, Jia Tan's, ZerOcon

Week in Overview[2 Apr-9 Apr] - 2024

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

1. **CVE-2024-1086**: This is a critical vulnerability affecting Linux kernels 5.14 to v6.6, allowing local privilege escalation. An exploit has been disclosed and made available on GitHub, posing a significant threat to Linux systems.
2. **UCPD Driver and Default Browser Lockdown**: Microsoft introduced a new Windows driver, UCPD.sys, targeting Registry keys associated with default browser settings for HTTP and HTTPS URL associations. This driver restricts users from modifying these keys, affecting Windows 10 and Windows 11 devices.
3. **CVE-2024-26331 and CVE-2024-28269**: These vulnerabilities were discovered in ReCrystallize Server software. CVE-2024-26331 is an authentication bypass, while CVE-2024-28269 enables remote code execution. These vulnerabilities pose risks to systems utilizing ReCrystallize Server and require immediate attention and patching.
4. **Malicious WORD File Evasion**: A malicious Word file evaded detection by nearly all antivirus solutions, highlighting weaknesses in existing security measures. The file contained embedded URLs and files, demonstrating the evolving sophistication of cyber threats.
5. **Dopamine Jailbreak at Zer0con 2024**: The developer behind the Dopamine jailbreak fulfilled his promise by presenting at Zer0con 2024, discussing technical insights into jailbreaking iOS 16. This event underscores advancements in jailbreaking techniques and their implications for iOS security.

6. FishEye: Specific details about FishEye are not provided. FishEye could refer to Atlassian's FishEye, a tool for viewing and analyzing code changes. Further context is needed to provide a technical summary.

7. **Jia Tan's SSH Agent**: Jia Tan's SSH Agent is a simple SSH Agent implementation that facilitates exploration of the XZ sshd backdoor functionality. It allows users to interact with SSH clients more easily, providing insights into potential security vulnerabilities.

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:

- A critical vulnerability, CVE-2024-1086
- UCPD driver specifically targeted Registry keys related to HTTP and HTTPS URL associations
- CVE-2024-26331 and CVE-2024-28269, in the ReCrystallize Server software
- Malicious WORD File Evaded Nearly All the AV Solutions
- Dopamine jailbreak, fulfilled his promise by presenting at Zer0con 2024
- FishEye
- Jia Tan's SSH Agent

🚨 Vulnerability of the Week

Linux CVE-2024-1086

A critical vulnerability, CVE-2024-1086, has surfaced, posing a significant threat to Linux systems by enabling local privilege escalation. This exploit has emerged amidst the commotion surrounding the xz backdoor, presenting a stealthy but potent danger.

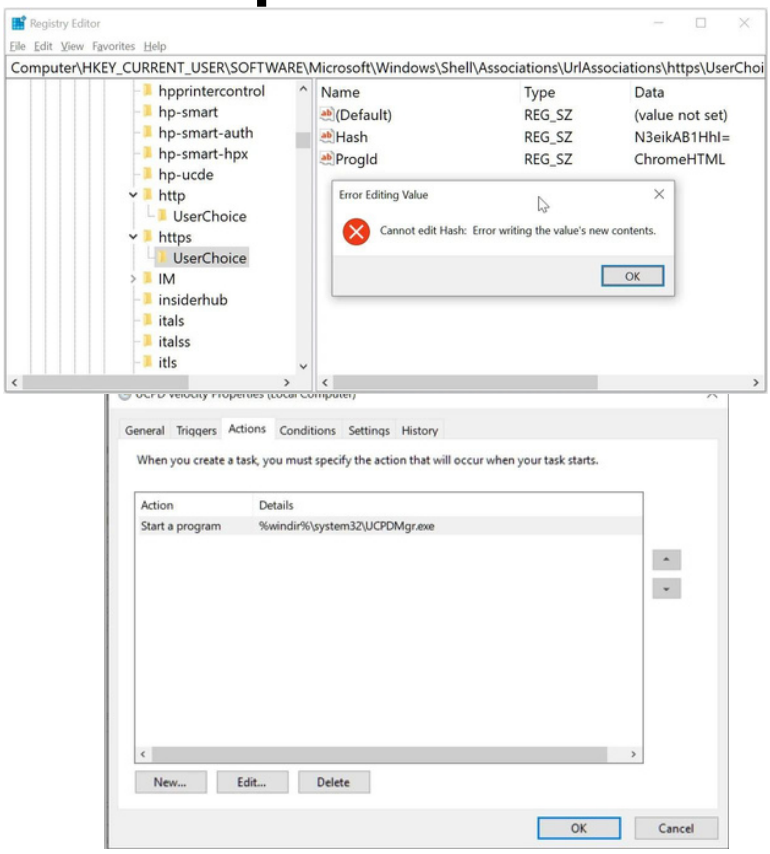
Key points about this exploit:

1. **Affected Systems**: The exploit targets Linux kernels ranging from version 5.14 to v6.6, encompassing a broad spectrum of Linux distributions.
2. **GitHub Repository**: The exploit's details and code have been made available on GitHub at http://github.com/Notselwyn/CVE-2024-1086. This repository serves as a resource for security professionals and Linux administrators to understand and mitigate the vulnerability.
3. **Exploit Details**: The exploit has been unveiled through a blog post, shedding light on its universal applicability across various Linux kernel versions (v5.14 - v6.7). Notably, it is capable of compromising systems running Debian, Ubuntu, and KernelCTF Mitigation instances.
4. **Novel Techniques**: The exploit incorporates novel techniques, including the utilization of Dirty Pagedirectory, to achieve local privilege escalation. These techniques demonstrate the evolving sophistication of cyber threats targeting Linux environments.

Given the severity of CVE-2024-1086 and its potential impact on Linux systems, it is imperative for administrators and security professionals to take immediate action. This includes patching affected systems, monitoring for any signs of exploitation, and implementing additional security measures to mitigate the risk posed by this vulnerability.

https://twitter.com/notselwyn/status/1772621383329001941

Art of Exploitation



https://twitter.com/vinopaljiri/status/1777279818070966556

A recent development in the Windows ecosystem has caught the attention of cybersecurity experts and Windows users alike. Microsoft has quietly introduced a new Windows driver, named UCPD.sys, as part of the February updates for both Windows 10 (KB5034763) and Windows 11 (KB5034765). This driver, referred to as the "User Choice Protection Driver," aims to prevent users from modifying specific Registry keys associated with default browser settings.

The discovery of this driver came to light when IT consultant Christoph Kolbicz noticed that his programs, SetUserFTA and SetDefaultBrowser, suddenly stopped functioning. These command-line tools allowed Windows administrators to change file associations and default browser settings, respectively. However, with the installation of the February updates, attempts to modify the Registry keys associated with default browser settings resulted in errors, indicating that these keys had been locked down.

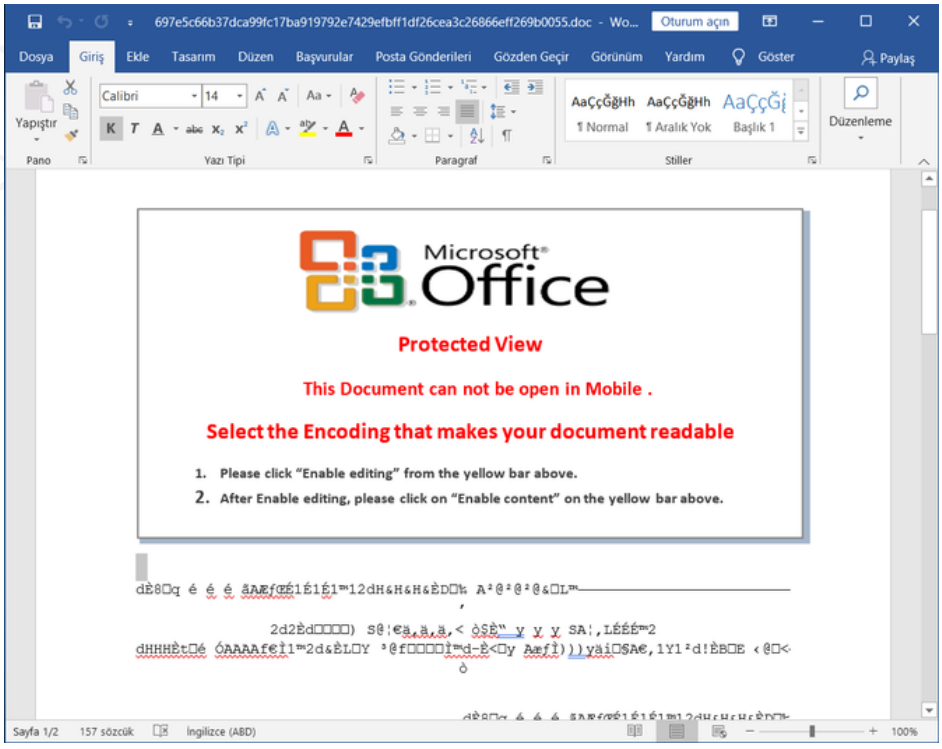
Further investigation revealed that the UCPD driver specifically targeted Registry keys related to HTTP and HTTPS URL associations, as well as the .PDF file association. Attempting to edit these Registry keys outside of the Windows Settings interface resulted in errors, indicating that modifications were not permitted.

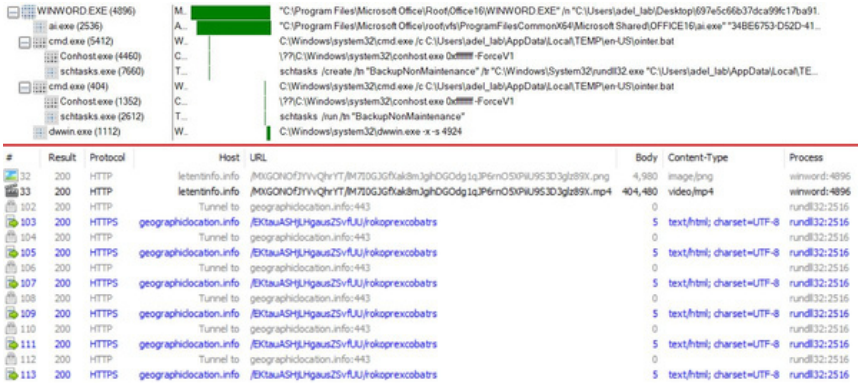
Christoph Kolbicz found a workaround to disable the UCPD driver by modifying the Windows Registry. However, Gunnar Haslinger discovered that a scheduled task, named 'UCPD velocity,' would automatically re-enable the service if disabled. This finding implies that fully disabling the driver requires not only modifying the Registry but also deleting or disabling the associated scheduled task.

The introduction of this driver has sparked speculation about its purpose and implications. Some experts believe that it may be related to compliance with Europe's Digital Markets Act (DMA), which aims to ensure fair competition among large technology companies, including Microsoft. However, the rollout of the driver to devices outside the European Economic Area (EEA), such as those in the USA, casts doubt on this theory.

Additionally, questions have arisen regarding the impact of this driver on user choice and security. While Microsoft has stated that Windows will honor users' configured default browser settings, some users have reported instances where default browser settings are ignored for operating system links, leading to concerns about user autonomy and security vulnerabilities.
Despite inquiries made to Microsoft regarding the purpose and implications of the UCPD driver, the company has not provided further information at this time.

Art of Detection





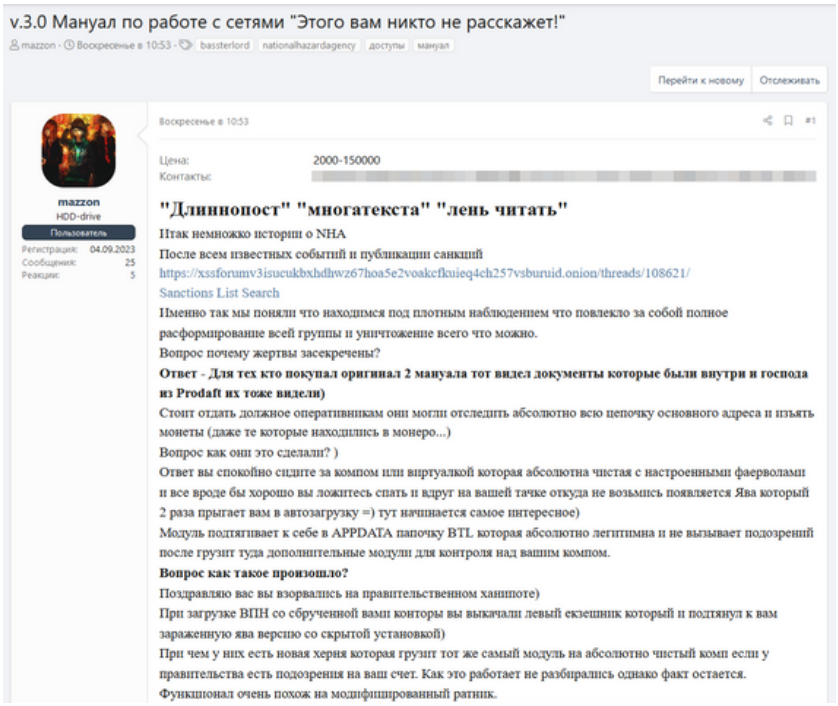
https://twitter.com/doc_guard/status/1777328001073471710

Recently, a malicious Word document managed to evade the detection of the majority of antivirus (AV) solutions, marking a concerning development in cybersecurity. With only 10 out of 65 AV solutions detecting the threat, this incident underscores the increasing sophistication of cyber attacks.

The malicious Word file, identified by its MD5 hash as 3d98b4c649408c7021b1e01dc72f2ae4, contained embedded URLs leading to letentinfo[.]info and geographiclocation[.]info, as well as several files with MD5 hashes 1386effe1ff6b2609a88d5d07d21242c, 64b3ab7e26010ff160fc80c12d76dfab, and 4b2af85af66efdb86402614c5a9ced20.

The low detection rate on VirusTotal raises concerns about the effectiveness of current security measures in detecting and mitigating such threats. It emphasizes the need for continuous improvement in threat detection and response capabilities.
To provide further insight into the threat, a DOCGuard report has been made available, detailing the analysis of the malicious Word file and its associated indicators of compromise (IOCs). This report serves as a valuable resource for security professionals and organizations seeking to enhance their defenses against similar threats.

😡 Malware or Ransomware

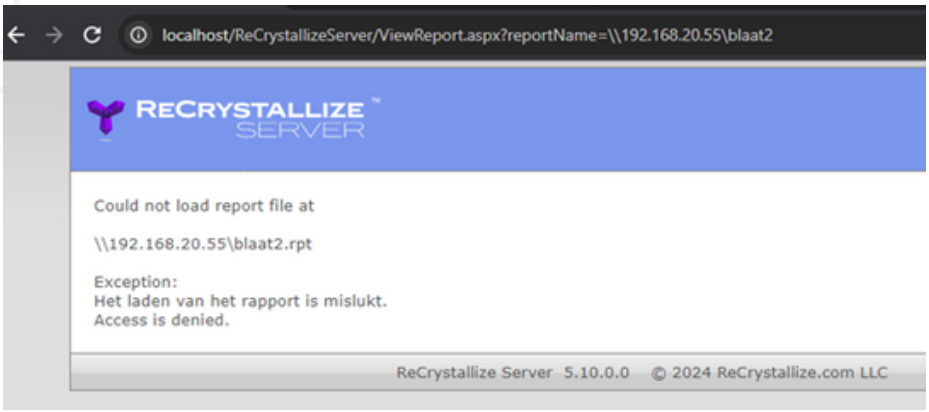


https://twitter.com/3xp0rtblog/status/1777508040972931085

Bassterlord, also known as FishEye, has resurfaced with new revelations following Operation Cronos. Here's a breakdown of the statements he made:

- **Cryptocurrency Seizure**: Law enforcement successfully tracked down and seized Bassterlord's cryptocurrency assets, including Monero, utilizing a government "honeypot" strategy.
- **Prosecution Difficulty**: The FBI faced challenges in prosecuting Bassterlord due to the random generation of usernames for LockBit accounts. It was noted that one account could be utilized by multiple individuals, potentially numbering between 10 to 15 people in Bassterlord's case.
- **Fake Voice Interview**: Bassterlord alleges that the voice interview conducted by @TheRecord_Media was orchestrated by a fake person. Evidence supporting this claim includes a delay in the meeting due to the installation of the fake voice. The stories shared during the interview with @Jon_DiMaggio were also purportedly fabricated.
- **False Identity Creation**: Bassterlord admits to fabricating a false identity to deceive others. The individual who received illicit funds, as revealed in Operation Cronos, is described as a figurehead distinct from the person who obtained the LockBit logo tattoo, which was allegedly done by a random individual and posted on YouTube.
- **Assistance in Investigation**: Bassterlord's team allegedly provided network access to hospitals and emergency services to @AShukuhi and @Jon_DiMaggio as part of the investigation. Additionally, @AShukuhi was granted access to a Cisco test server to address a vulnerability, which was used to gain access to the aforementioned networks.
- **Non-Targeting of Hospitals**: Bassterlord claims that his team never intentionally targeted hospitals.
- **Secrecy of Real Name**: Bassterlord asserts that only LockBit knows his real name.
- **Sale of Manual**: Due to financial constraints resulting from the cryptocurrency seizure, Bassterlord is selling the third version of his manual. He seeks a buyer willing to purchase it in its entirety for $150,000, but is open to selling partial copies for $2,000 if a complete sale cannot be achieved.
- **Creation of New Tox Profiles**: Concerned about potential FBI access to their Tox profiles, Bassterlord and his team have created new ones to maintain anonymity.

1Day



https://twitter.com/sensepost/status/1777292706483458262

In his latest post, @PvdH shares his discovery of two vulnerabilities, CVE-2024-26331 and CVE-2024-28269, in the ReCrystallize Server software. He begins by recounting his experience during a routine web application assessment, where he encountered an instance of ReCrystallize Server while attempting to print a report. Intrigued by this third-party software, he decided to explore its functionality further.

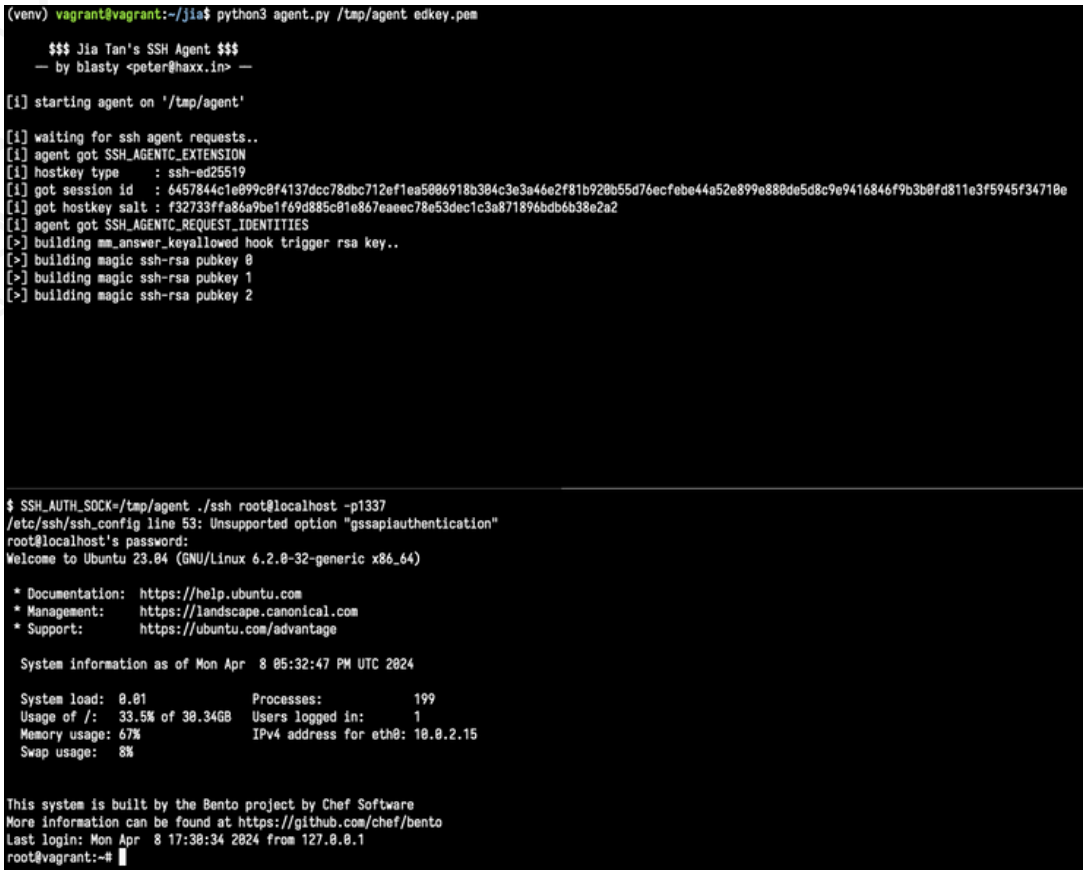
Despite initial attempts to log in with common default credentials proving unsuccessful, @PvdH decided to investigate known vulnerabilities associated with the software. However, his search yielded no relevant CVEs. Undeterred, he continued his exploration and discovered that the application's settings allowed for the use of absolute paths, potentially leading to local file inclusion vulnerabilities.

Through further experimentation, @PvdH managed to exploit this feature to gain access to sensitive information, including network shares and database credentials. Despite initial resistance from the client, who attributed the vulnerabilities to misconfiguration, @PvdH successfully replicated his findings on a "hardened" version of the software.

CVE-2024-26331 was identified as an authentication bypass vulnerability, exploiting a session management flaw that granted administrative access. Meanwhile, CVE-2024-28269 allowed for remote code execution through the unrestricted file upload feature, enabling @PvdH to execute arbitrary commands on the server. Despite efforts to disclose these vulnerabilities to ReCrystallize Software and MITRE, @PvdH notes a lack of response from the vendor and the absence of a formal patch. He emphasizes the importance of isolating the server and implementing security measures such as disabling absolute paths, changing default passwords, and encrypting data.

@PvdH concludes with recommendations for securing ReCrystallize Server and underlying web servers, highlighting the necessity of maintaining up-to-date systems and employing the principle of least privilege. He also provides a disclosure timeline, acknowledging delays due to the pandemic and other work commitments.

🌶️ Trending Exploit



https://twitter.com/bl4sty/status/1777333886516613537

Blasty, a Twitter user with the handle @bl4sty, announced the release of a tool called "Jia Tan's SSH Agent" on GitHub. This tool is described as a simple SSH agent that implements functionalities similar to the XZ sshd backdoor. Blasty mentions that some people requested the code, prompting them to refactor a scrappy Paramiko script quickly and transform it into this SSH agent implementation.

The tool aims to facilitate exploration of the backdoor using a typical SSH client. It requires users to generate their own ED448 private key using OpenSSL and patch their liblzma.so with a custom ED448 public key. Additionally, users need to patch their SSH client to skip verification of the certificate by commenting out a specific section in openssh's sshkey.c file.

To use the tool, users are instructed to follow specific steps, including setting up a virtual environment, installing necessary dependencies, running the agent.py script with the generated private key, and then using the SSH client with a modified SSH_AUTH_SOCK variable.
The announcement concludes with a playful note, encouraging users to log in with any password.

The Topic of the Week

https://twitter.com/poc_crew/status/1775752185214894157?s=46&t=qqvuoLV9uFvc9wARCfQjWQ

Lars Fröder, the developer behind the Dopamine jailbreak, fulfilled his promise by presenting at Zer0con 2024, a prestigious closed conference focused on software security. The event, held at the Fairmont Ambassador Hotel in Seoul, South Korea, gathered an international assembly of esteemed security researchers to exchange knowledge and push the boundaries of security research.

Fröder's presentation delved into a technical exploration of jailbreaking iOS 16, specifically discussing the intricacies of using the Dopamine tool for this purpose. His appearance on stage marked a significant moment for the jailbreaking community, eagerly anticipating insights into the latest developments in iOS security and jailbreaking techniques.

While there were no live broadcasts of the event, an image shared by the @POC_Crew X Twitter account depicted Fröder behind the podium, poised to share his insights. Although no video feeds were available at the time, there's hope that the talk will eventually surface on YouTube, providing broader access to Fröder's expertise and insights.

The anticipation surrounding Fröder's presentation underscores the importance of events like Zer0con in fostering community engagement and knowledge sharing within the security and jailbreaking communities. By sharing their experiences and expertise, developers like Fröder not only inspire others to delve into jailbreak development but also contribute to a deeper understanding of software security among enthusiasts and professionals alike.

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.