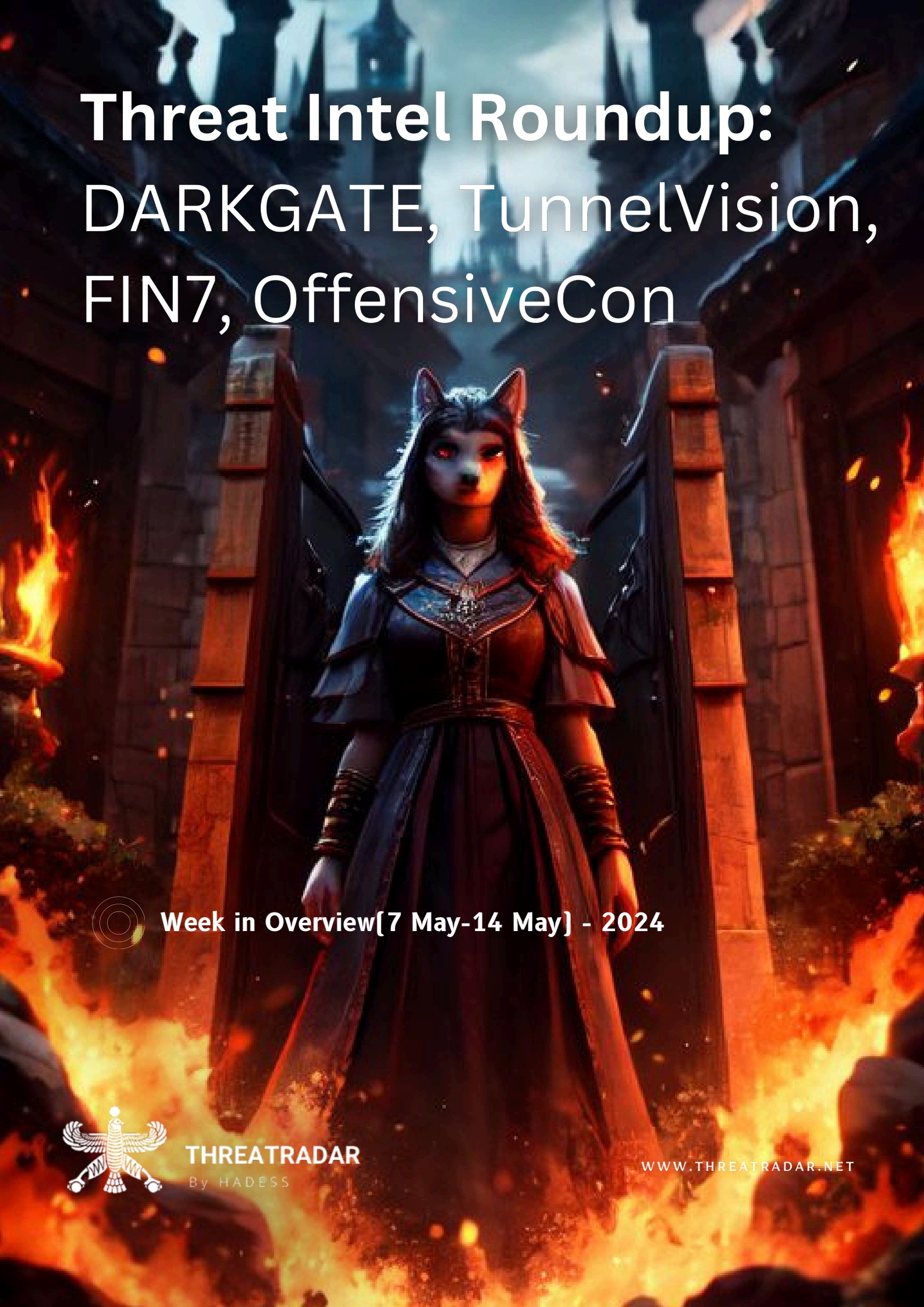
Threat Intel Roundup: DARKGATE, TunnelVision, FIN7, OffensiveCon



Week in Overview[7 May-14 May] - 2024

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

- DARKGATE:
  - Overview: DARKGATE is a sophisticated Malware-as-a-Service (MaaS) platform known for its continuous evolution and strategic targeting.
  - Key Features: Utilizes deceptive lures, such as exploiting the end of the US tax reporting season. Notable features include complex infection chains involving Adobe Creative Cloud, ZIP files, Delphi EXE, and C2 Beaconing. Persistence via registry, video adapter mismatch checks, and encrypted network traffic.
  - Recommendations: Employ network traffic decryption tools like provided Python scripts, utilize Threat Intelligence (TI) Lookups, and maintain a proactive defense posture.
- OffensiveCon:
  - Overview: OffensiveCon is a prominent cybersecurity conference focusing on offensive techniques, penetration testing, exploit development, and red team operations.
  - Key Themes: Explores penetration testing, red teaming, exploit development, and offensive security tools. Emphasizes ethical considerations, responsible disclosure, and community engagement.
  - Takeaways: Attendees gain insights into cutting-edge offensive techniques, network with industry experts, and enhance offensive cybersecurity skills.

FIN7 Campaign:

- Overview: FIN7 is a financially motivated threat group originating from Russia, known for targeting financial institutions and retail sectors.
- Recent Activity: Notable April 2024 campaigns involved impersonating trusted brands to distribute malware via fake browser extensions and MSIX app installer files.
- Tactics: Leveraged PowerShell scripts, NetSupport RAT, and DiceLoader for data exfiltration and persistence. Utilized C2 infrastructure, URL structures, and payload signatures for continuity.
- Mitigation: Maintain awareness of social engineering tactics, scrutinize unexpected download prompts, and leverage Threat Intelligence (TI) Lookups for sample hunting.

CVE-2023-46012:

- Overview: CVE-2023-46012 is a critical vulnerability discovered in Linksys EA7500 routers, scored at 9.8 on CVSS, allowing remote code execution with root privileges.
- Exploitation: Attackers can exploit the flaw in the Internet Gateway Device (IGD) UPnP service, leading to buffer overflow conditions and arbitrary code execution.
- Mitigation: Currently, there's no official patch available. Users can mitigate the risk by disabling UPnP service, implementing firewalls, and monitoring for updates from Linksys.

TunnelVision Attack:

- Overview: TunnelVision is a network attack similar to TunnelCrack, exploiting DHCP option 121 to reroute traffic through an attacker-controlled server.
- Vulnerability: Primarily affects Mullvad VPN app on iOS devices due to DHCP option 121 implementation. Attackers can intercept plaintext traffic when on the same local network as the victim.
- Mitigation: Requires patch integration and production deployment, similar to fixes for TunnelCrack. Mullvad VPN app desktop versions remain protected via firewall rules.

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:

- DARKGATE
- OffensiveCon
- FIN7 Campaign
- CVE-2023-46012
- TunnelVision attack

🚨 Vulnerability of the Week

TunnelVision CVE-2024-0024

CVE-2024-3661, known as the TunnelVision attack, has emerged as a significant concern in the realm of cybersecurity, particularly for users of the Mullvad VPN app. This exploit shares striking similarities with its predecessor, TunnelCrack LocalNet (CVE-2023-36672 and CVE-2023-35838), underscoring the persistent challenges posed by network vulnerabilities.

At its core, TunnelVision hinges on the attacker's ability to infiltrate the victim's local network and assume the role of a DHCP server. By manipulating DHCP option 121, the attacker can coerce the victim into routing certain public IP ranges through the attacker's system instead of the intended VPN tunnel. This clandestine rerouting opens avenues for potential interception and compromise of sensitive information.

Fortunately, users of Mullvad's VPN app on desktop platforms (Windows, macOS, and Linux) benefit from robust firewall measures. These firewall rules are designed to thwart any attempts by attackers to siphon off plaintext traffic from the victim. Consequently, both LocalNet and TunnelVision encounters are effectively neutralized on these platforms, safeguarding user privacy and security.

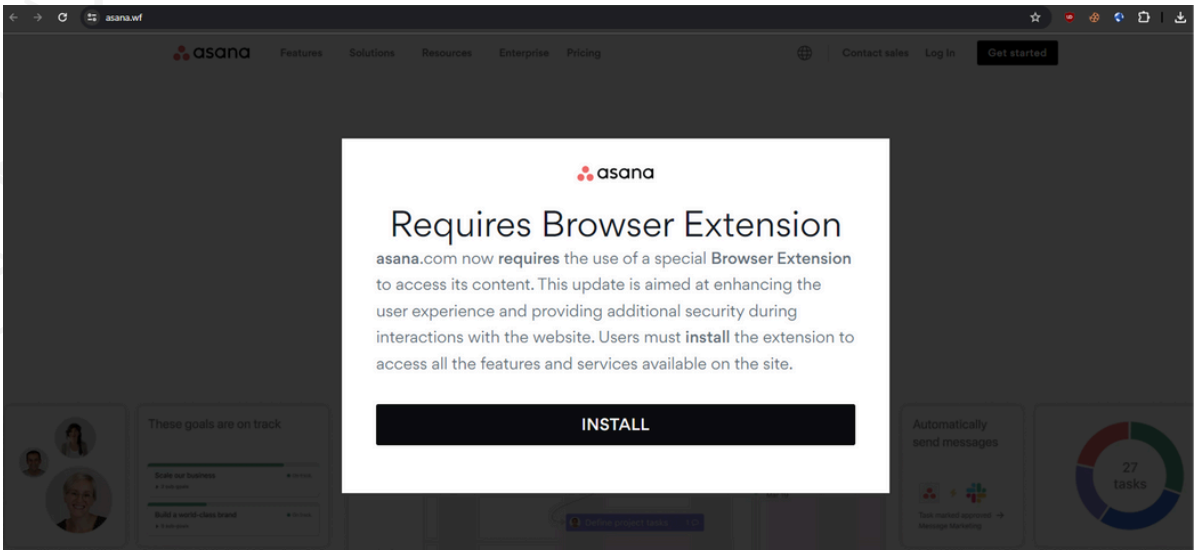
However, the scenario is less reassuring for users of the Mullvad VPN app on mobile platforms. While Android remains immune to TunnelVision due to the absence of DHCP option 121 implementation, iOS users find themselves vulnerable to this exploit, echoing the susceptibility observed with LocalNet.

Addressing this vulnerability demands a concerted effort to implement and deploy effective fixes. The solution likely mirrors that devised for LocalNet, necessitating rigorous integration and deployment procedures before it can be rolled out to production environments. Until then, users are urged to exercise vigilance and employ additional safeguards to mitigate the risks posed by TunnelVision and similar threats.

In essence, CVE-2024-3661 underscores the persistent cat-and-mouse game between cybersecurity practitioners and threat actors, highlighting the imperative of proactive defense measures and swift response to emerging vulnerabilities.

https://twitter.com/mullvadnet/status/1787877221652111663

Art of Detection



https://twitter.com/BushidoToken/status/1789976792339489150

At eSentire, our commitment to cybersecurity knows no bounds, evident in our round-the-clock Security Operations Centers (SOCs) staffed with Elite Threat Hunters and Cyber Analysts. We are relentless in our pursuit to detect, investigate, and neutralize threats promptly. Recently, our vigilance led us to uncover concerning activities orchestrated by the financially motivated threat group FIN7, originating from Russia and operational since 2013.

Overview of Threat: Throughout April 2024, eSentire's Threat Response Unit (TRU) diligently monitored multiple incidents involving FIN7. The threat actors employed sophisticated tactics, leveraging malicious websites to impersonate renowned brands like AnyDesk, WinSCP, BlackRock, and others, as part of their nefarious schemes.
This TRU Positive sheds light on our observations of FIN7's distribution of NetSupport RAT via MSIX app installer files. These incidents echo previously reported FIN7 activities by industry giants like Microsoft and Red Canary.

Incident Analysis:

1. Malicious Payload Distribution: Users visiting sponsored Google Ads encountered fake pop-ups prompting them to download a purported browser extension. These extensions were packaged as MSIX files, ostensibly legitimate Windows app packaging formats.
2. Payload Characteristics:
   - The observed MSIX files were signed with "SOFTWARE SP Z O O" and "SOFTWARE BYTES LTD," indicating deceptive authenticity.
   - Upon extraction, the MSIX files revealed malicious PowerShell scripts designed to collect system information and establish communication with a Command and Control (C2) server.
3. Infection Case Studies:
   - In one instance, the PowerShell script facilitated the download and execution of NetSupport RAT, granting threat actors remote access to compromised systems.
   - Another case involved the distribution of NetSupport RAT followed by DiceLoader payload execution, enabling data exfiltration and persistent access.

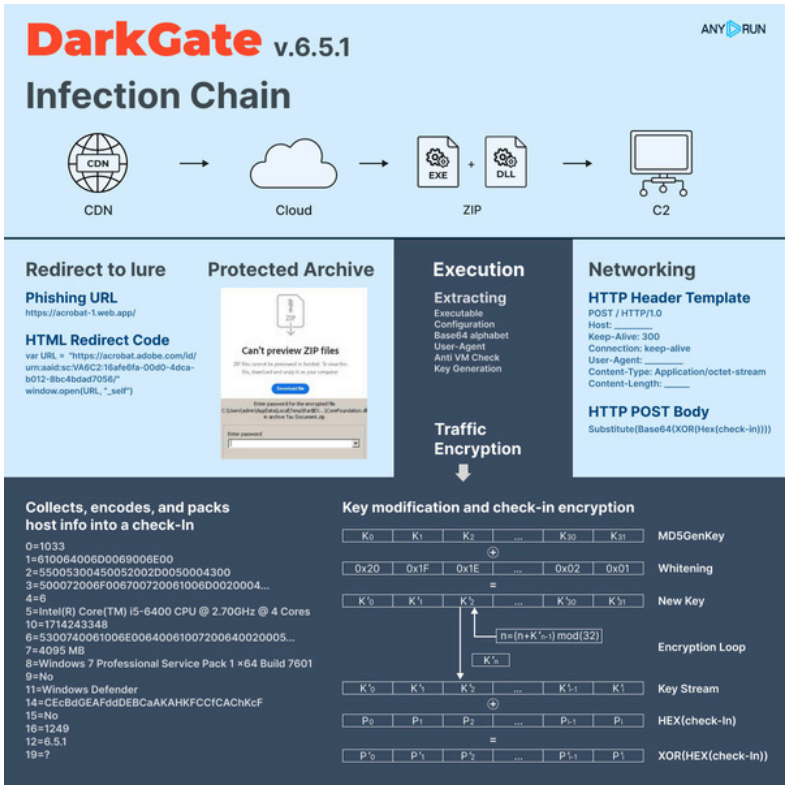
Comparative Analysis and C2 Connections:

- We compared PowerShell scripts observed in April 2024 with those from previous MSIX payloads and noted striking similarities, affirming the continuity of FIN7's tactics.
- Noteworthy overlaps were identified in C2 infrastructure, URL structures, and payload signatures, reaffirming FIN7's persistent threat landscape.

Mitigation and Recommendations:

- Users must exercise caution when encountering sponsored ads, as they can serve as entry points for malicious activities.
- Vigilance against deceptive practices, such as impersonated brand websites and unexpected download prompts, is crucial.
- Verification of file sources and scrutiny of digital certificates are imperative to mitigate risks associated with deceptive file signatures.

😈 Malware or Ransomware



https://twitter.com/anyrun_app/status/1787833295973093789

#DARKGATE – April Campaigns Overview for Version 6.5.1
⚠ DARKGATE remains a persistent and evolving Malware-as-a-Service (#MaaS) platform.
📝 April's campaigns were strategically timed to exploit the conclusion of the US tax reporting season.
Here are the notable features of DARKGATE's April "tax" campaigns distributing version 6.5.1:
🔀 **Infection Chain**: Adobe Creative Cloud -> ZIP (Protected) -> Delphi EXE (.dll / .rsrc) -> C2 Beaconing
📌 **Key Points**:
1️⃣ **Original Lure Storage Location**: [FireBase Web App CDN / Adobe Creative Cloud]
2️⃣ **No Network Requests for Additional Payload**: [AutoIT / AutoHK]
3️⃣ **Video Adapter Check for Mismatch with Strings**: [Microsoft Video / Standard VGA Graphics Adapter / Microsoft Basic Display Adapter]
4️⃣ **Persistence via Registry**: [HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
5️⃣ **Campaign IDs**: [tompang / seal001]

🔒 **Network Traffic Message Decryption**: Utilizes a combination of simple substitution cipher (custom base64) and XORing of the obtained message with a keystream generated from the original key material.
💡 **Useful Resources**:

- Decrypt HTTP POST Messages with the provided #Python script: GitHub Repository
- Employ TI Lookup to expand sample hunting area: TI Lookup Link

📎 **Sample Links**:

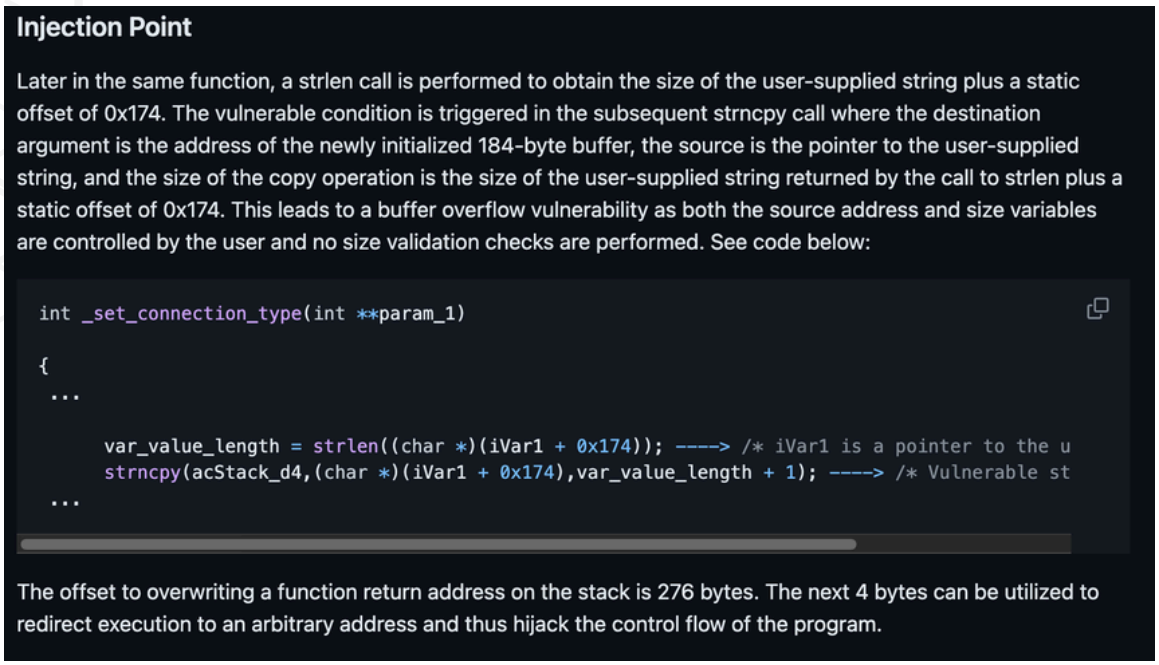
- Sample 1
- Sample 2

🔍 **Search by Tag**:

- DarkGate Submissions

DARKGATE's April campaigns underscore the evolving sophistication of cyber threats, necessitating proactive measures and vigilant defense strategies.

1Day



https://twitter.com/Dinosn/status/1790226682562978210

Cybersecurity researchers have recently unearthed a critical vulnerability, denoted as CVE-2023-46012, within Linksys EA7500 routers, casting a shadow over the security landscape of these popular devices. This flaw, assigned a perilous score of 9.8 on the Common Vulnerability Scoring System (CVSS), poses a severe risk by enabling attackers to execute code remotely with root privileges.

Vulnerability Overview: The vulnerability, CVE-2023-46012, resides in the Internet Gateway Device (IGD) Universal Plug and Play (UPnP) service of Linksys AC1900 EA7500v3 routers. Specifically, the flaw manifests within the service's handling of HTTP request data associated with UPnP SOAP Action Requests. During processing, the system inadequately validates the length of user-supplied data before copying it to a fixed-length stack buffer.

This oversight facilitates a buffer overflow scenario, granting malicious actors the capability to inject arbitrary code that executes with root-level access. Notably, exploitation of this vulnerability does not necessitate authentication from the attacker, amplifying the gravity of the threat.

Technical Breakdown: The vulnerable function, identified as _set_connection_type within the UPnP IGD service, initializes a 184-byte buffer without adequate length validation. Attackers can manipulate both the source address and the length parameter of the strncpy operation, precipitating a buffer overflow.
This overflow condition arises when the strncpy call attempts to copy data beyond the buffer's capacity, based on the attacker-controlled length derived from a strlen operation plus a static offset.

Exploitation and Impact: Discovered by security researcher Mike, the vulnerability has been accompanied by detailed technical insights and a proof-of-concept exploit, raising concerns about potential widespread exploitation. Devices running all firmware versions of the Linksys EA7500 up to and including Ver.3.0.1.207964 are susceptible to this flaw.
As of the latest update, Linksys has not released a patch to remedy this critical vulnerability, leaving affected devices vulnerable to exploitation.

https://github.com/dest-3/CVE-2023-46012

The Topic of the Week

https://twitter.com/offensive_con

OffensiveCon 2024 is a highly technical international security conference that focuses exclusively on offensive security. It took place on May 10-11th, 2024, in Berlin1. The conference is known for bringing together the hacker community to share knowledge and engage in high-quality, deep technical talks. The event featured a single track of talks over two full days, as well as technical trainings held in the days leading up to the conference.

The trainings covered a wide range of topics, including program analysis for vulnerability discovery, Windows exploit engineering, Linux kernel exploitation, security and insecurity in Apple's operating systems, attacking instant messaging applications, full stack web attack, the art of fault injection, and modern malware OPSEC & anti-reverse techniques2.

OffensiveCon prides itself on offering unique speakers and maintaining affordable ticket prices to ensure accessibility for everyone interested in offensive IT security. The talks at the conference are centered around subjects such as vulnerability discovery, advanced exploitation techniques, and reverse engineering.

For those looking to attend, it's important to note that there are limited seats available, and early registration is encouraged to secure a spot at this prestigious event3. OffensiveCon 2024 continues to be a platform where experts in the field can network, learn, and push the boundaries of IT security.

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.