Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

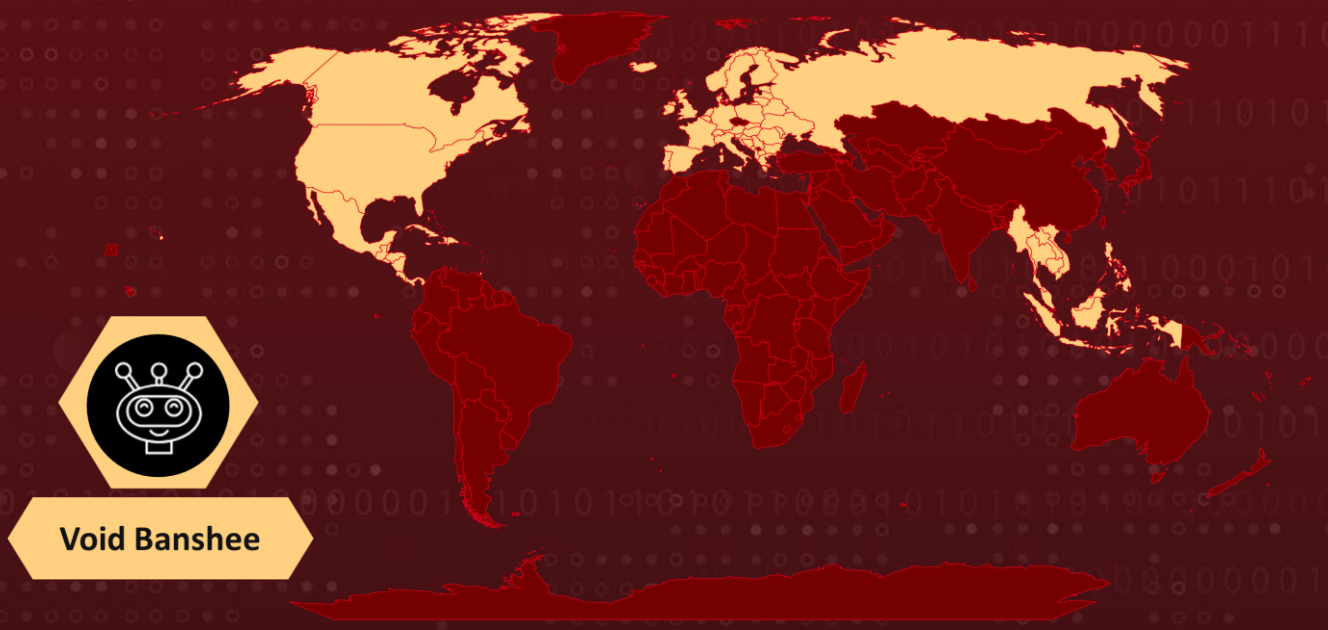
Void Banshee's Zero-Day Assault on Windows Users via Internet Explorer

Date of Publication	Admiralty Code	TA Number
July 17, 2024	A1	TA2024275

Summary

Attack Discovered: May 2024
Attack Region: North America, Europe, and Southeast Asia
Affected Industries: Education
Malware: Atlantida Stealer
Actor: Void Banshee
Attack: Threat actors are exploiting the CVE-2024-38112 vulnerability by abusing the mhtml protocol handler to lure Windows users into remote code execution. They use Windows Internet Shortcut files (.url) to trigger the retired Internet Explorer (IE) to visit attacker-controlled URLs. The APT group Void Banshee has been found capitalizing on this flaw, deploying the Atlantida stealer for information theft and financial gains.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-38112	Microsoft Windows MSHTML Platform Spoofing Vulnerability	Windows MSHTML	✓	✓	✓

Attack Details

#1 Microsoft recently addressed a critical zero-day vulnerability in Windows, designated CVE-2024-38112, which was actively exploited by attackers. This flaw allowed them to execute files through the deprecated Internet Explorer using MSHTML. They employed specially crafted Windows Internet Shortcut files (.url) that, when clicked, invoked the retired Internet Explorer to visit websites controlled by the attackers.

#2 CVE-2024-38112, was part of an attack chain orchestrated by a group known as Void Banshee. Targeting regions in North America, Europe, and Southeast Asia, Void Banshee aimed to steal information and generate financial gains. The APT group appears to target professionals and students who frequently use online libraries and cloud services. The final stage of their attack involved deploying the Atlantida stealer.

#3 Despite Internet Explorer being officially retired since June 15, 2022, and disabled in Windows 10 and 11, remnants of its functionality persist on modern systems. To exploit CVE-2024-38112, attackers disguise internet shortcut files as PDFs, utilizing the mhtml protocol handler along with the x-usc directive for invoking web calls. When opened, this method triggers Internet Explorer, running within the Edge sandbox, to connect to a remote website hosting malicious HTML Applications (HTAs).

#4 The default behavior of Internet Explorer to execute HTA files leads to the next stage of the infection. To conceal their malicious activity, attackers manipulate the size of the IE window and create long filenames padded with spaces to obscure the .hta extension. Inside the HTA file, a VBScript decrypts and executes malicious code using PowerShell. This script then downloads additional malicious scripts from compromised servers and runs them using PowerShell commands.

#5 The malware employs advanced techniques such as the Donut Loader, derived from open-source tools, to execute the Atlantida stealer within Windows processes. Atlantida targets sensitive information from various applications, stealing passwords, cookies, and specific files from victims' desktops. It captures screenshots and gathers detailed system information, compressing all stolen data into ZIP files sent over TCP to the attacker.

#6 This campaign underscores that despite the inaccessibility of Internet Explorer, attackers can exploit its remnants in Windows systems. Groups like Void Banshee pose significant threats by leveraging unsupported services to evade modern security measures, highlighting ongoing cybersecurity risks.

Recommendations

Apply Security Patches: Immediately update your Windows OS to the latest version to protect your system from being exploited by the CVE-2024-38112 vulnerability. These patches address the zero-day vulnerability and safeguard your system from exploitation.

Remain Vigilant: Avoid clicking on suspicious links or visiting untrusted websites, as they may harbor malicious content. Be cautious when opening emails or messages from unknown sources, as they could be part of phishing attempts. Refrain from clicking on internet shortcut files (.url), particularly if they promise eBooks or other tempting content.

Trusted Installers: Always download software from the official website of the software vendor. Avoid third-party websites as they may host tampered versions of the software.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0010 Exfiltration	T1566 Phishing	T1566.002 Spearphishing Link	T1204 User Execution
T1204.002 Malicious File	T1218 System Binary Proxy Execution	T1218.009 Regsvcs/Regasm	T1584 Compromise Infrastructure

T1584.004 Server	T1059 Command and Scripting Interpreter	T1059.005 Visual Basic	T1059.001 PowerShell
T1027 Obfuscated Files or Information	T1055 Process Injection	T1560 Archive Collected Data	T1560.001 Archive via Utility
T1005 Data from Local System	T1082 System Information Discovery	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers
T1113 Screen Capture	T1041 Exfiltration Over C2 Channel		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	c9f58d96ec809a75679ec3c7a61eaaf3adbbeb6613d667257517bdc41ecca9ae, d8824f643127c1d8f73028be01363fd77b2ecb050ebe8c17793633b9879d20eb, 87480b151e465b73151220533c965f3a77046138f079ca3ceb961a7d5fee9a33, c85eedd51dced48b3764c2d5bdb8febefe4210a2d9611e0fb14ffc937b80e302, 13907caae48ea741942bce60fa32087328475bd14f5a81a6d04d82286bd28b4d, 119b0994bcf9c9494ce44f896b7ff4a489b62f31706be2cb6e4a9338b63cdfdb, 6f1f3415c3e52dcdbb012f412aef7b9744786b2d4a1b850f1f4561048716c750, b371fbdce6935039218d4b4272db3521881c9cec48ef82dec1e9e0188a32d3ad, bd710ee53ef3ad872f3f0678117050608a8e073c87045a06a86fb4a7f0e4eff0, b16aee58b7dfaf2a612144e2c993e29dcbd59d8c20e0fd0ab75b76dd9170e104, 65142c8f490839a60f4907ab8f28dd9db4258e1cfab2d48e89437ef2188a6e94, bfd59ed369057c325e517b22be505f42d60916a47e8bdcbe690210a3087d466d, 22e2d84c2a9525e8c6a825fb53f2f30621c5e6c68b1051432b1c5c625ae46f8c

TYPE	VALUE
URLs	hxxps[://]fullgasesspa[.]cl/tet/download[.]php hxxp[://]cbmelipilla[.]cl/te/test1[.]html hxxps[://]cbmelipilla[.]cl/te/hhhh2[.]php hxxps[://]hostalaskapatagonia[.]com/tt/tedfd[.]te hxxps[://]hostalaskapatagonia[.]com/tt/become[.]txt hxxp[://]h[.]com:8000/test1[.]html
IPv4	185[.]172[.]128[.]95

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112

References

https://www.trendmicro.com/en_us/research/24/g/CVE-2024-38112-void-banshee.html

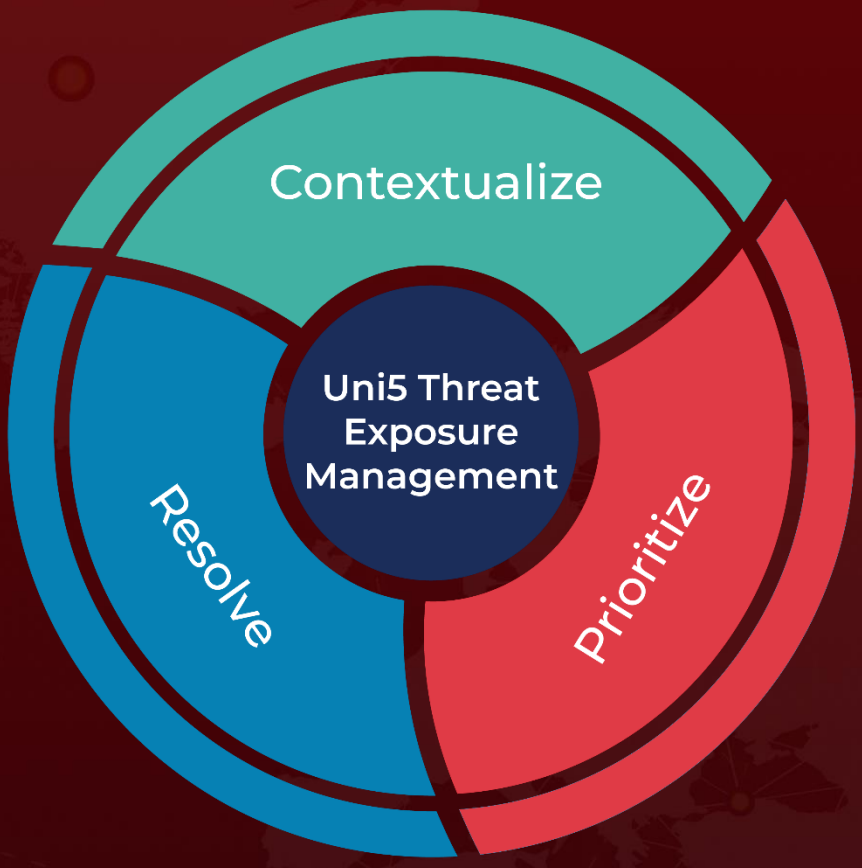
https://research.checkpoint.com/2024/resurrecting-internet-explorer-threat-actors-using-zero-day-tricks-in-internet-shortcut-file-to-lure-victims-cve-2024-38112/

https://hivepro.com/threat-advisory/microsofts-july-patch-tuesday-addresses-active-zero-day-exploits/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 17, 2024 • 6:50 AM

More at www.hivepro.com