Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

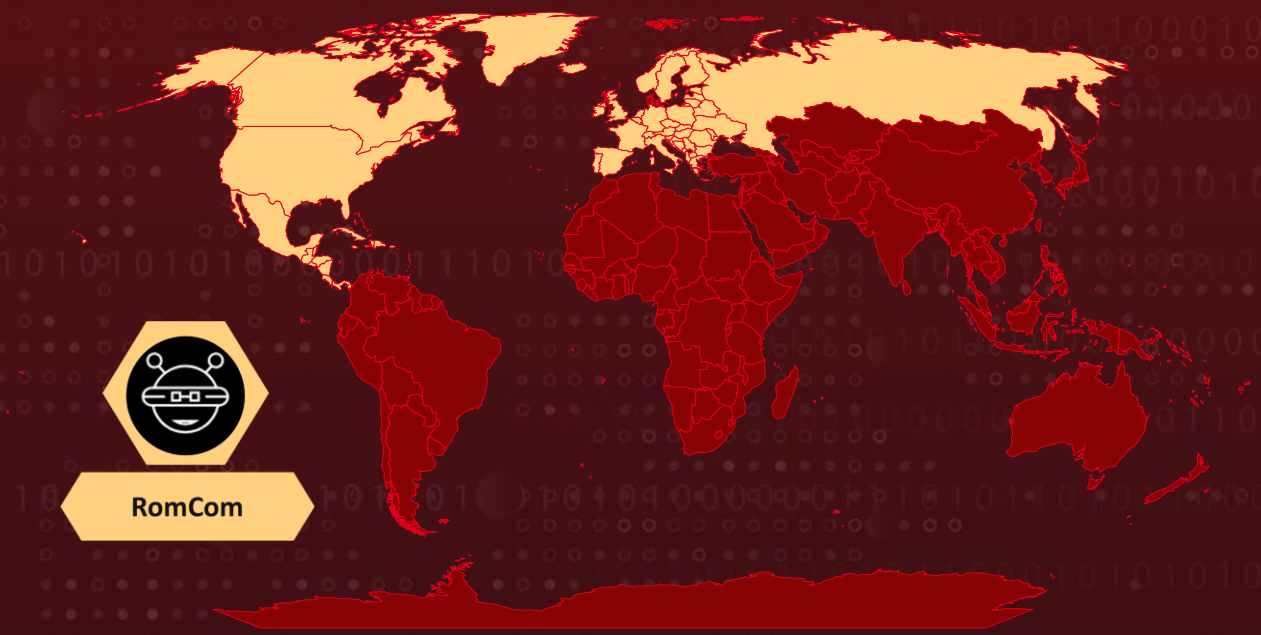
RomCom Leverages Dual Zero-Day Exploits in Widespread Campaign

Date of Publication	Last Update Date	Admiralty Code	TA Number
November 27, 2024	December 6, 2024	A1	TA2024445

Summary

Attack Discovered: October 10th, 2024
Targeted Countries: Europe and North America
Malware: RomCom backdoor
Actor: RomCom (aka Storm-0978, Tropical Scorpius, UNC2596, Void Rabisu, DEV-0978)
Attack: The Russia-based RomCom cybercrime group has been observed leveraging two zero-day vulnerabilities in a sophisticated attack chain targeting Firefox and Tor Browser users across Europe and North America. These vulnerabilities were exploited to deploy their signature malware, the RomCom backdoor, onto victims' systems. By crafting a seamless zero-day exploit chain, the group achieved remote code execution without any need for user interaction. Victims were compromised simply by visiting attacker-controlled websites specifically designed to deliver the malicious payload.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-36884	Microsoft Windows Search Remote Code Execution Vulnerability	Microsoft Office and Windows	✓	✓	✓
CVE-2024-9680	Mozilla Firefox Use-After-Free Vulnerability	Mozilla Firefox and Firefox ESR	✓	✓	✓
CVE-2024-49039	Microsoft Windows Task Scheduler Privilege Escalation Vulnerability	Microsoft Windows	✓	✓	✓

Attack Details

#1 A sophisticated campaign by the Russia-aligned RomCom cybercrime group has come to light, leveraging critical zero-day vulnerabilities to infiltrate systems across Europe and North America. The attackers exploited a severe flaw in Mozilla products, identified as CVE-2024-9680, which enables code execution in the restricted context of Firefox, Thunderbird, and Tor Browser. By chaining this with a Windows vulnerability (CVE-2024-49039), RomCom executed arbitrary code in the user's context, seamlessly delivering their backdoor without requiring user interaction. Their targets included business sectors and strategically important organizations, signaling a blend of cybercrime and espionage motives.

#2 The attack begins by redirecting victims to a maliciously crafted website designed to exploit these vulnerabilities. Visiting the site triggers a use-after-free vulnerability in Firefox's animation timelines, initiating the execution of staged shellcode. This shellcode, split into two components, uses advanced techniques like Shellcode Reflective DLL Injection (RDI) to bypass sandboxing and escalate privileges. The final payload, the RomCom backdoor, is delivered through various command-and-control (C&C) servers, granting attackers the ability to execute arbitrary commands, deploy additional malware, and extract sensitive data.

#3 This campaign showcases the increasing sophistication of exploitation chains, particularly those targeting widely used software. RomCom's strategic use of dual zero-day vulnerabilities underscores the need for robust defenses and strong sandboxing mechanisms. This incident marks another instance of RomCom exploiting a major zero-day, following their abuse of CVE-2023-36884 in June 2023. Implementing these measures are critical to reducing the risks posed by highly capable threat actors like RomCom, who continue to evolve their tactics for maximum impact.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Enable Browser Sandboxing Features: Configure browsers to enforce strict sandboxing rules, reducing the risk of exploits escaping restricted environments.

Apply Security Updates Promptly: Ensure all systems are running the latest versions of Mozilla products (Firefox, Thunderbird, Tor Browser) and Windows. These updates address CVE-2024-9680 and CVE-2024-49039, closing the vulnerabilities exploited in this campaign.

Harden RPC Interfaces: Apply security policies that enforce restrictions on RPC interfaces, preventing exploitation of undocumented endpoints for privilege escalation.

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	TA0003 Persistence
TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery
TA0008 Lateral Movement	TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control
TA0040 Impact	T1583 Acquire Infrastructure	T1587 Develop Capabilities	T1587.001 Malware

T1587.004 Exploits	T1588 Obtain Capabilities	T1588.003 Code Signing Certificates	T1588.005 Exploits
T1588.006 Vulnerabilities	T1608 Stage Capabilities	T1189 Drive-by Compromise	T1053 Scheduled Task/Job
T1053.005 Scheduled Task	T1546 Event Triggered Execution	T1546.015 Component Object Model Hijacking	T1068 Exploitation for Privilege Escalation
T1622 Debugger Evasion	T1480 Execution Guardrails	T1027 Obfuscated Files or Information	T1027.011 Fileless Storage
T1553 Subvert Trust Controls	T1553.002 Code Signing	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers
T1552 Unsecured Credentials	T1552.001 Credentials In Files	T1087 Account Discovery	T1518 Software Discovery
T1614 System Location Discovery	T1021 Remote Services	T1560 Archive Collected Data	T1185 Browser Session Hijacking
T1005 Data from Local System	T1114 Email Collection	T1114.001 Local Email Collection	T1113 Screen Capture
T1071 Application Layer Protocol	T1071.001 Web Protocols	T1573 Encrypted Channel	T1573.002 Asymmetric Cryptography
T1041 Exfiltration Over C2 Channel	T1565 Data Manipulation	T1657 Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	A4AAD0E2AC1EE0C8DD25968FA4631805689757B6, CA6F8966A3B2640F49B19434BA8C21832E77A031, 21918CFD17B378EB4152910F1246D2446F9B5B11, 703A25F053E356EB6ECE4D16A048344C55DC89FD, ABB54C4751F97A9FC1C9598FED1EC9FB9E6B1DB6, A9D445B77F6F4E90C29E385264D4B1B95947ADD5

TYPE	VALUE
IPv4	194[.]87[.]189[.]171, 178[.]236[.]246[.]241, 62[.]60[.]238[.]81, 147[.]45[.]78[.]102, 46[.]226[.]163[.]67, 62[.]60[.]237[.]116, 62[.]60[.]237[.]38, 194[.]87[.]189[.]19, 45[.]138[.]74[.]238, 176[.]124[.]206[.]88

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884

https://www.mozilla.org/en-US/firefox/new/

https://www.mozilla.org/en-US/firefox/enterprise/#download

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49039

References

https://www.welivesecurity.com/en/eset-research/romcom-exploits-firefox-and-windows-zero-days-in-the-wild/

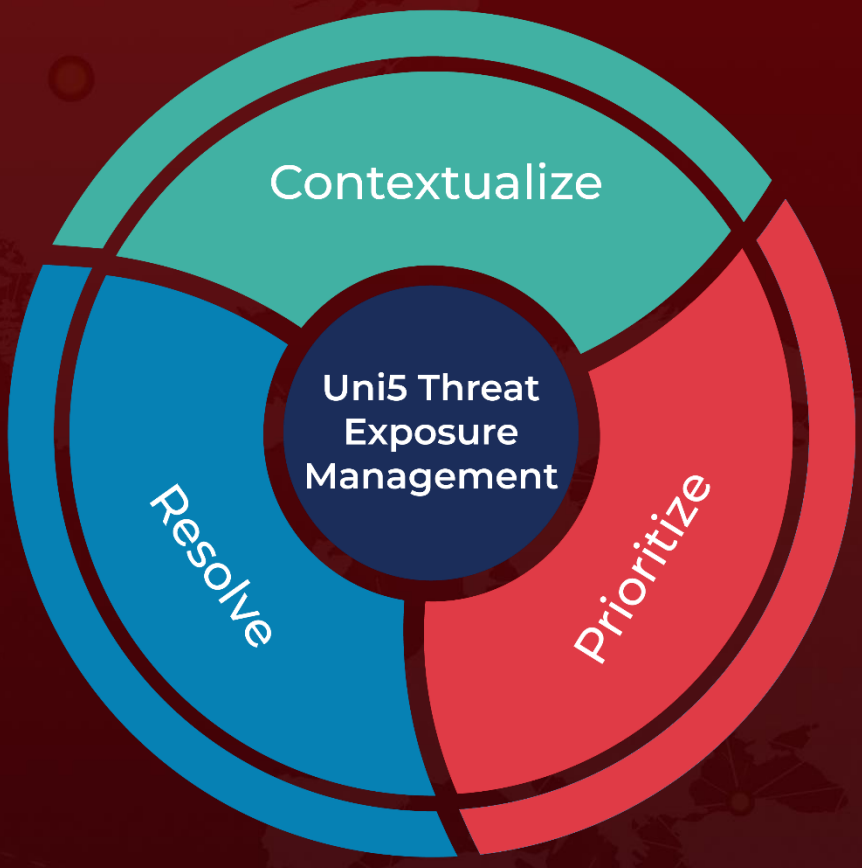
https://hivepro.com/threat-advisory/firefox-zero-day-alert-critical-animation-timeline-flaw-exploited-in-the-wild/

https://hivepro.com/threat-advisory/microsofts-august-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

November 27, 2024 • 4:15 AM

More at www.hivepro.com