Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

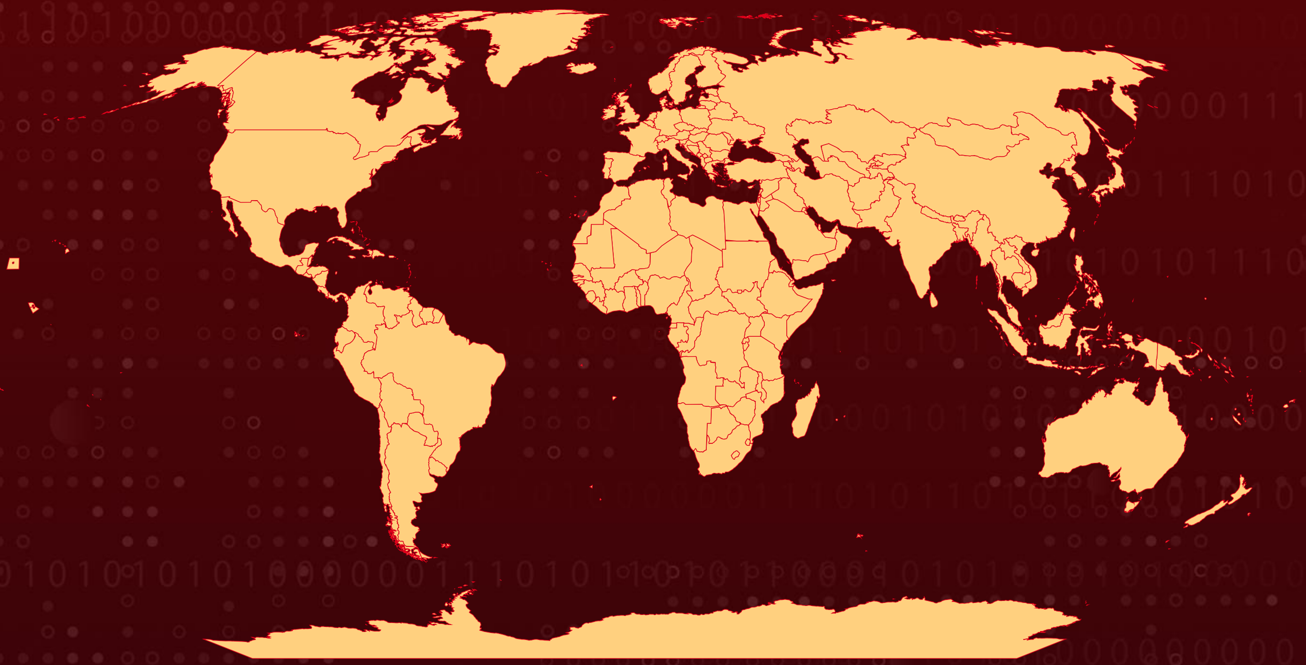
New Remcos RAT Variant Targets Windows Users

Date of Publication	Admiralty Code	TA Number
November 13, 2024	A1	TA2024427

Summary

Attack Began: September 2024
Malware: Remcos RAT
Targeted Region: Worldwide
Affected Platform: Windows
Attack: A new phishing campaign is targeting Windows users with malicious Excel documents. Once opened, these documents exploit a vulnerability to download and install the Remcos RAT. This powerful malware can steal sensitive information, control the infected device, and carry out other malicious activities, posing a significant threat to users and organizations.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2017-0199	Microsoft Office and WordPad Remote Code Execution Vulnerability	Microsoft Office and WordPad	✓	✓	✓

Attack Details

#1

A new phishing campaign leverages a variant of the Remcos RAT (Remote Access Trojan) to target Microsoft Windows users. The attack typically begins with phishing emails containing a malicious Excel document, which exploits the CVE-2017-0199 vulnerability. This vulnerability allows attackers to gain unauthorized control over victims' computers when the malicious document is opened.

#2

Victims receive deceptive phishing emails that appear to contain legitimate order documents in Excel format. However, upon opening the file, the CVE-2017-0199 vulnerability is triggered, leading to the download and execution of a malicious HTA (HTML Application) file on the victim's device. This file executes various scripts such as JavaScript, VBScript, and PowerShell to fetch an executable named dllhost.exe from a remote server. Once downloaded, this executable is run to extract and execute additional malicious components hidden within the user's AppData folder.

#3

The Remcos variant used in this campaign is equipped with advanced anti-analysis techniques designed to evade detection and complicate reverse engineering efforts. For instance, it employs vectored exception handlers to manage exceptions and avoid debugging. Additionally, it utilizes dynamic API calls with hashed names instead of constant strings, making static analysis more challenging. One of its more sophisticated methods includes process hollowing, which allows it to inject malicious code into a new process without leaving obvious traces.

#4

Once installed on a victim's machine, this variant of Remcos RAT can execute a wide range of malicious activities. It can collect sensitive information, execute commands received from its command and control (C&C) server, log keystrokes, capture screenshots, record audio, and manipulate browser credentials. The versatility of this malware poses significant risks to individuals and organizations alike.

Recommendations

Enhance Email Security: Use solutions that incorporate machine learning to detect and block phishing emails before they reach users' inboxes. Conduct regular training sessions to raise awareness about phishing tactics, including how to recognize suspicious emails and attachments.

Regular Software Updates: Ensure that all software, especially operating systems and applications, are regularly updated to mitigate known vulnerabilities like CVE-2017-0199. Implement tools that automatically apply updates to reduce the risk of human error in the update process.

Employ Endpoint Protection: Use reputable antivirus software that offers real-time protection against malware, including RATs like Remcos. Utilize IPS to monitor network traffic for suspicious activity and prevent exploitation attempts.

Implement Multi-Factor Authentication (MFA): Require MFA for all accounts, especially those with access to sensitive information or critical systems, to add an additional layer of protection.

Monitor Network Activity: Conduct Regular Security Audits: Perform audits of network traffic and user behavior to identify any unusual activities that may indicate a breach. Implement tools that can analyze network traffic for signs of malware communication with command and control servers.

Potential MITRE ATT&CK TTPs

TA0011 Command and Control	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0001 Initial Access	**TA0042** Resource Development	**TA0002** Execution	**T1218** System Binary Proxy Execution
T1059 Command and Scripting Interpreter	**T1588.006** Vulnerabilities	**T1588** Obtain Capabilities	**T1588.005** Exploits
T1068 Exploitation for Privilege Escalation	**T1078** Valid Accounts	**T1566.001** Spearphishing Attachment	**T1566** Phishing

T1059.007 JavaScript	**T1059.001** PowerShell	**T1059.005** Visual Basic	**T1036** Masquerading
T1140 Deobfuscate/Decode Files or Information	**T1027** Obfuscated Files or Information	**T1106** Native API	**T1055.012** Process Hollowing
T1055 Process Injection	**T1112** Modify Registry	**T1056.001** Keylogging	**T1056** Input Capture
T1218.005 Mshta			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4:PORT	107[.]173[.]4[.]16[:]2404
URLs	hxxps://og1[.]in/2Rxzb3, hxxp://192[.]3[.]220[.]22/xampp/en/cookienetbookinetcahce.hta, hxxp://192[.]3[.]220[.]22/hFXELFSwRHRwqbE214.bin, hxxp://192[.]3[.]220[.]22/430/dllhost.exe,
SHA256	4A670E3D4B8481CED88C74458FEC448A0FE40064AB2B1B00A289AB504015E944, F99757C98007DA241258AE12EC0FD5083F0475A993CA6309811263AAD17D4661, 9124D7696D2B94E7959933C3F7A8F68E61A5CE29CD5934A4D0379C2193B126BE, D4D98FDBE306D61986BED62340744554E0A288C5A804ED5C924F66885CBF3514, F9B744D0223EFE3C01C94D526881A95523C2F5E457F03774DD1D661944E60852, 24A4EBF1DE71F332F38DE69BAF2DA3019A87D45129411AD4F7D3EA48F506119D

Patch Link

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0199

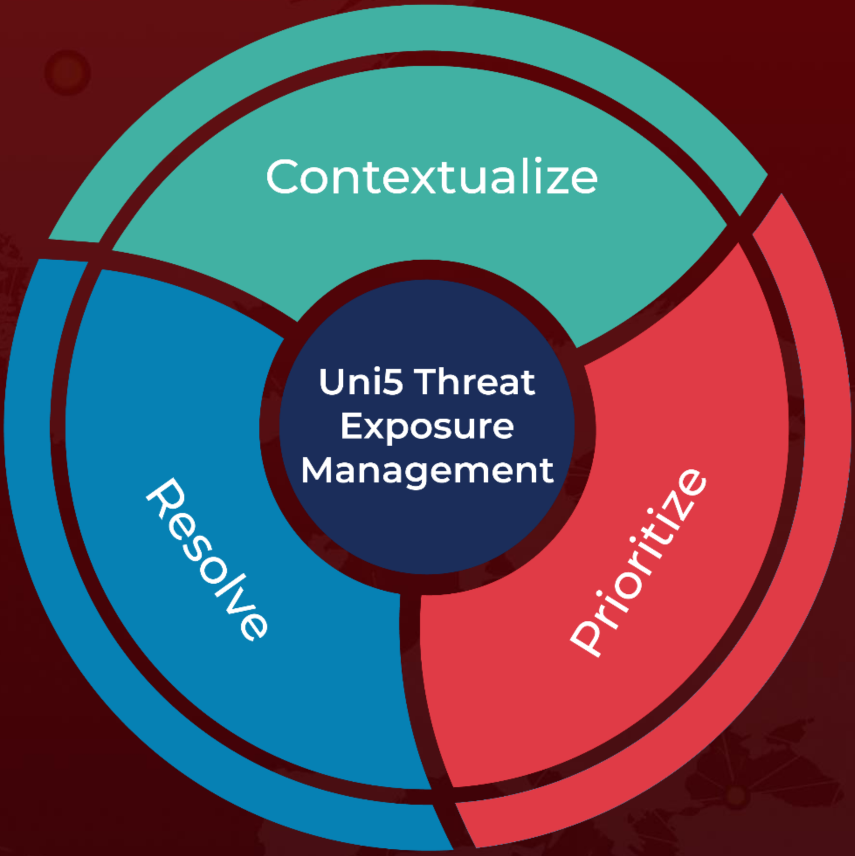
References

https://www.fortinet.com/blog/threat-research/new-campaign-uses-remcos-rat-to-exploit-victims

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 13, 2024 • 6:30 AM

More at www.hivepro.com