Hive Pro

THREAT ADVISORY

Are you a victim of the Conti Ransomware?

TA202137

Threat Level RED

Publish Date – Sept 23, 2021

Conti Ransomware targets enterprises who have not patched their systems by exploiting old vulnerabilities. Conti Ransomware steals sensitive information from businesses and demands a ransom in exchange. CISA has issued a warning about the rise in Conti ransomware attacks. To avoid becoming a victim of Conti ransomware, the Hive Pro Threat Research team suggested you patch these vulnerabilities.

The Techniques used by the Conti includes:

- T1078 - Valid Accounts
- T1133 - External Remote Services
- T1566.001 - Phishing: Spearphishing Attachment
- T1566.002 - Phishing: Spearphishing Link
- T1059.003 - Command and Scripting Interpreter: Windows Command Shell
- T1106 - Native API
- T1055.001 - Process Injection: Dynamic-link Library Injection
- T1027 - Obfuscated Files or Information
- T1140 - Deobfuscate/Decode Files or Information
- T1110 - Brute Force
- T1558.003 - Steal or Forge Kerberos Tickets: Kerberoasting
- T1016 - System Network Configuration Discovery
- T1049 - System Network Connections Discovery
- T1057 - Process Discovery
- T1083 - File and Directory Discovery
- T1135 - Network Share Discovery
- T1021.002 - Remote Services: SMB/Windows Admin Shares
- T1080 - Taint Shared Content
- T1486 - Data Encrypted for Impact
- T1489 - Service Stop
- T1490 - Inhibit System Recovery

Actor Details

Name	Known as	Origin	Target Locations	Target sectors
Conti Ransomware	Wizard Spider, TrickBot, TrickLoader, TheTrick, TotBrick, Ryuk, UNC1878, Anchor DNS, BazarLoader, Kegtap, TrickBoot, Grim Spider, TEMP.MixMaster, Gold Blackburn	Russia	Worldwide	Defense, Financial, Government, Healthcare, Telecommunications.

Hive Pro

THREAT ADVISORY

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0148	Microsoft Windows 7 SP1, 8.1, 10, RT 8.1, Server 2008 R2 SP1, Server 2008 SP2, Server 2012, Server 2012 R2, Server 2016, Vista SP2, XP SP3	cpe:2.3:o:microsoft:windows_7:sp1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_8.1:*:*:*:*:*:*:*:*,cpe:2.3:o:microsoft:windows_10:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_rt_8.1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:sp2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2016:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_vista:sp2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_xp:sp3:*:*:*:*:*:*:*	Microsoft Server Message Block version 1 code execution	CWE-20
CVE-2017-0147			Microsoft Server Message Block version 1 information disclosure	CWE-200
CVE-2020-1472	Microsoft Windows Server 1903, Server 1909, Server 2004, Server 2008 R2, Server 2012, Server 2012 R2, Server 2016, Server 2019	cpe:2.3:o:microsoft:windows_server:1903:*:*:*:*:*:*:*,cpe:2.3:o:microsoft:windows_server:1909:*:*:*:*:*:*:*,cpe:2.3:o:microsoft:windows_server:2004:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:r2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:*:*,cpe:2.3:o:microsoft:windows_server_2016:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:*	Microsoft Window Netlogon privilege escalation	CWE-330
CVE-2021-34527	Microsoft Windows version 7 SP1, 8.1, 10, 10 20H2, 10 21H1, 10 1607, 10 1809, 10 1909, 10 2004, RT 8.1, Server 20H2, Server 1909, Server 2004, Server 2008 R2 SP1, Server 2008 SP2, Server 2012, Server 2012 R2, Server 2016, Server 2019	cpe:2.3:o:microsoft:windows_7:sp1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_8.1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:2004:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_rt_8.1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:1909:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:2004:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:sp2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2016:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:*	Microsoft Windows code execution	CWE-269

Indicators of Compromise (IoCs)

Type	Value
IPV4	162.244.80[.]235 85.93.88[.]165 185.141.63[.]120 82.118.21[.]1

Patch Link

https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

References

https://us-cert.cisa.gov/ncas/alerts/aa21-265a