Hive Pro

THREAT ADVISORY

New Threat Actor Exotic Lily acting as Initial Access Broker for Conti and Diavol ransomware group	TA2022068
Threat Level RED	**Publish Date –** Mar 18, 2022

Exotic Lily was first discovered exploiting a zero-day vulnerability in Microsoft MSHTML (CVE-2021-40444), which piqued the curiosity of researchers as a potentially sophisticated threat actor. Following additional analysis, it was revealed that the group is an initial access broker that utilizes large-scale phishing operations to infiltrate specific corporate networks and subsequently sells access to those networks to ransomware groups such as Conti and Diavol gangs.

The group starts by producing fake social media profiles, including LinkedIn profiles, by exploiting readily available employee data to make the illicit clones look genuine using advanced A.I. imaging technology. When it was originally discovered, the malware was in the form of a document file that attempted to attack the CVE-2021-40444 vulnerability. Subsequently, the threat actor switched to ISO archives having BazarLoader DLLs with LNK shortcuts.

Currently, the group continued to utilize ISO files but added a DLL containing a new loader, an enhanced form of the prior first-stage loader. The loader injects a malware strain known as "Bumblebee," which uses WMI to capture system information and exfiltrate it to the C2. Bumblebee may also receive remote actors such as Conti and Diavol orders and download and perform extra payloads.

The Mitre TTPs used by Exotic Lily are:

TA0001 - Initial Access
TA0002 - Execution
TA0004 - Privilege Escalation
TA0010 – Exfiltration
T1566: Phishing
T1566.001: Phishing: Spearphishing Attachment
T1204.002: User Execution: Malicious File
T1047: Windows Management Instrumentation
T1068: Exploitation for Privilege Escalation
T1041: Exfiltration Over C2 Channel

Hive Pro

THREAT ADVISORY

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-40444	Microsoft Windows 10. 7. 8.1, Windows Server 2008, 2012, 2016, 2019, 2022	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_7:-:sp1:*:*:-:*:-:*, cpe:2.3:o:microsoft:windows_8.1:-:*:*:*:-:*:-:*, cpe:2.3:o:microsoft:windows_rt_8.1:-:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:x64:*, 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_2016:20h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2016:2004:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2019:-:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2022:-:*:*:*:*:*:*:*	Windows Print Spooler Remote Code Execution	CWE-94

Indicators of Compromise (IoCs)

Type	Value
SHA-256	5ceb28316f29c3912332065eeaaebf59f10d79cd9388ef2a7802b9bb80d797be, 9fdec91231fe3a709c8d4ec39e25ce8c55282167c561b14917b52701494ac269, c896ee848586dd0c61c2a821a03192a5efef1b4b4e03b48aba18eedab1b864f7, 9eacade8174f008c48ea57d43068dbce3d91093603db0511467c18252f60de32, 6214e19836c0c3c4bc94e23d6391c45ad87fdd890f6cbd3ab078650455c31dc8, 201c4d0070552d9dc06b76ee55479fc0a9dfacb6dbec6bbec5265e04644eebc9, 1fd5326034792c0f0fb00be77629a10ac9162b2f473f96072397a5d639da45dd, 01cc151149b5bf974449b00de08ce7dbf5eca77f55edd00982a959e48d017225
IPs	23.81.246[.]187
Domain	3conlfex[.]com, avrobio[.]co, elemblo[.]com, phxmfg[.]co, modernmeadow[.]co, lsoplexis[.]com, craneveyor[.]us, faustel[.]us, lagauge[.]us, missionbio[.]us, richllndmetals[.]com, kvnational[.]us, prmflltration[.]com, brightlnsight[.]co, belcolnd[.]com, awsblopharma[.]com, amevida[.]us, revergy[.]us, al-ghurair[.]us, opontia[.]us

Patch

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444

References

https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/