Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

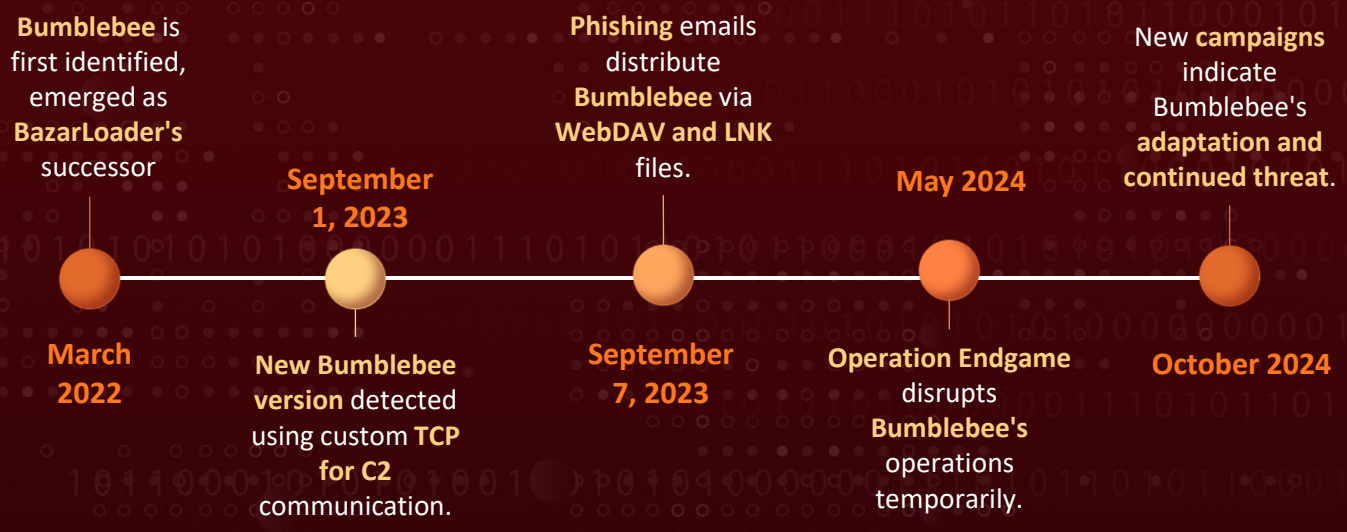
Bumblebee Bites Back with New Infection Chain

Date of Publication	Admiralty Code	TA Number
October 24, 2024	A1	TA2024408

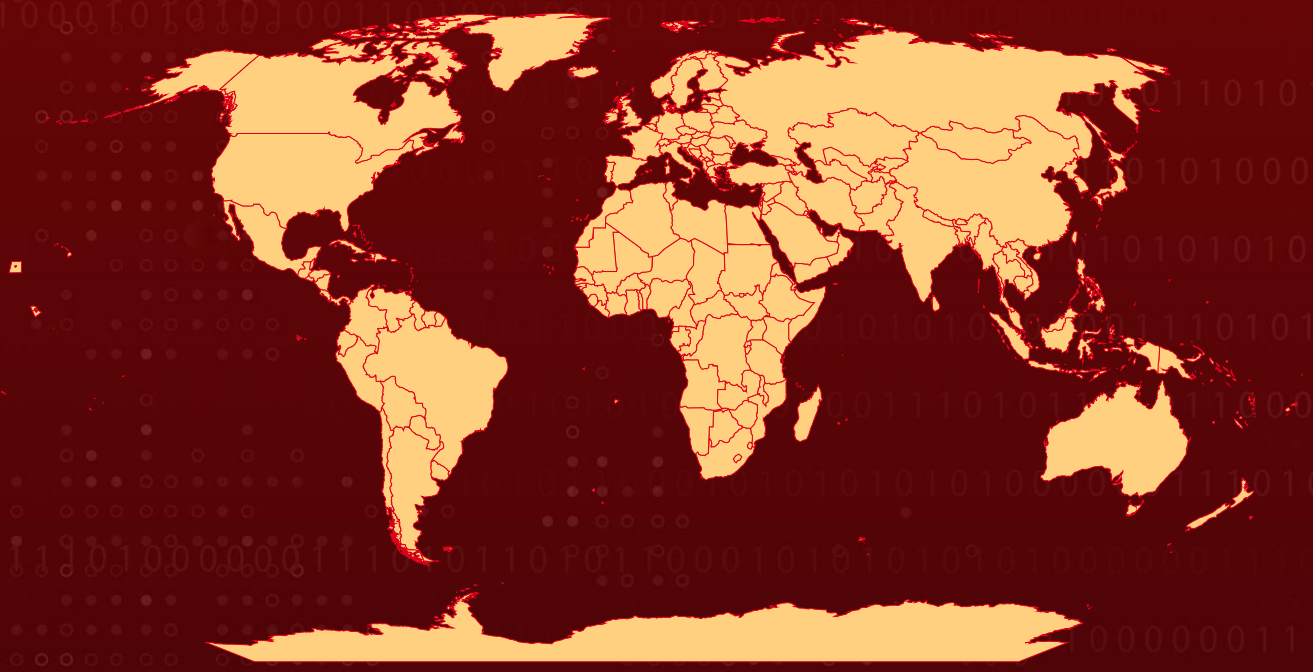
Summary

Active Since: October 2024
Campaign Name: Operation Endgame
Malware: Bumblebee
Affected Platform: Windows
Targeted Region: Worldwide
Attack: Bumblebee is a sophisticated malware loader first discovered in March 2022, primarily used by ransomware groups to deliver malicious payloads. Written in C++, it employs advanced evasion techniques, such as leveraging Windows shortcut (.LNK) files and PowerShell commands for stealth and persistence. Despite efforts to disrupt its operations during Europol's May 2024 Operation Endgame, Bumblebee has resurfaced with updated tactics, continuing to evade detection. Its infection chain focuses on minimizing process creation to avoid triggering security alerts.

Attack Timeline



Attack Regions



Attack Details

#1

Bumblebee is a sophisticated malware loader that has gained prominence in the cybercrime landscape, particularly among ransomware groups. Initially discovered in March 2022, it has evolved significantly, demonstrating advanced evasion techniques and a flexible infection chain. As a loader, Bumblebee's primary role is to establish a foothold in compromised systems and facilitate the download and execution of additional malicious payloads, including ransomware and information-stealing malware.

#2

The loader is written in C++ and employs various advanced techniques for stealth and persistence. Recent findings indicate that this is the first Bumblebee campaign observed since Operation Endgame, conducted by Europol in May 2024, which aimed to disrupt major malware botnets, including Bumblebee, IcedID, and Pikabot. While the infection chain used to deliver the final payload is not entirely new, its application in this context represents a significant development in Bumblebee's operational tactics.

#3 Bumblebee typically gains initial access through phishing campaigns that distribute ZIP files containing Windows shortcut (.LNK) files. When executed, these LNK files run commands designed to download the actual malware payload. The infection process generally involves the LNK file executing a PowerShell command to download an MSI file from a remote server. The MSI file is then renamed and executed using msiexec.exe, allowing the malware to run without writing to disk.

#4 In prior versions of Bumblebee and other malware families, the CustomAction table within MSI files was commonly employed to dictate execution steps during installation. However, Bumblebee has adopted a more discreet approach by leveraging the SelfReg table to execute the DllRegisterServer function from a DLL contained within a CAB file named "disk1." This technique minimizes process creation and reduces the likelihood of detection by security systems.

#5 The resurgence of the Bumblebee loader highlights an ongoing trend in cybercrime, where threat actors continuously adapt their strategies to evade detection and enhance operational effectiveness. The loader's architecture has also been updated to improve stealthiness by avoiding the creation of additional processes that could trigger security alerts.

Recommendations

- **Enhance Email Security:** Implement robust email filtering solutions to detect and block phishing campaigns, particularly those distributing ZIP or LNK files. Educate employees on phishing recognition and avoidance strategies.
- **Limit Macros and LNK Execution:** Configure systems to block the execution of Windows shortcuts (.LNK files) and disable macros in email attachments by default, reducing attack vectors commonly exploited by Bumblebee.
- **Use Advanced Threat Detection Tools:** Deploy endpoint detection and response (EDR) systems and behavior-based monitoring to detect unusual activity, such as PowerShell scripts, and MSI file downloads that could indicate Bumblebee activity.
- **Regular Software Updates:** Ensure all software, including operating systems and applications, is kept up to date with the latest security patches to minimize vulnerabilities that attackers can exploit.
- **Network Segmentation:** Implement network segmentation to limit lateral movement within your organization. This can help contain any potential infections and protect sensitive data.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0042 Resource Development	TA0002 Execution	TA0005 Defense Evasion
TA0003 Persistence	TA0011 Command and Control	T1573 Encrypted Channel	T1573.001 Symmetric Cryptography
T1566 Phishing	T1204.001 Malicious Link	T1059.001 PowerShell	T1059 Command and Scripting Interpreter
T1041 Exfiltration Over C2 Channel	T1588.002 Tool	T1588 Obtain Capabilities	T1566.001 Spearphishing Attachment
T1204 User Execution	T1218.007 Msiexec	T1218 System Binary Proxy Execution	T1036 Masquerading
T1204.002 Malicious File	T1218.011 Rundll32		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	2bca5abfac168454ce4e97a10ccf8ffc068e1428fa655286210006b298de42fb, 106c81f547cfe8332110520c968062004ca58bcfd2dbb0accd51616dd694721f, c26344bfd07b871dd9f6bd7c71275216e18be265e91e5d0800348e8aa06543f9, 0ab5b3e9790aa8ada1bbadd5d22908b5ba7b9f078e8f5b4e8fcc27cc0011cce7, d3f551d1fb2c307edfceb65793e527d94d76eba1cd8ab0a5d1f86db11c9474c3, d1cabe0d6a2f3cef5da04e35220e2431ef627470dd2801b4ed22a8ed9a918768, 7df703625ee06db2786650b48ffefb13fa1f0dae41e521b861a16772e800c115

TYPE	VALUE
URLs	hxxp[://]193.242.145.138/mid/w1/Midjourney[.]msi, hxxp[://]193.176.190.41/down1/nvinstall[.]msi
IPv4	193[.]242[.]145[.]138, 193[.]176[.]190[.]41

References

https://www.netskope.com/blog/new-bumblebee-loader-infection-chain-signals-possible-resurgence

https://github.com/netskopeoss/NetskopeThreatLabsIOCs/tree/main/Malware/Bumblebee/IOCs

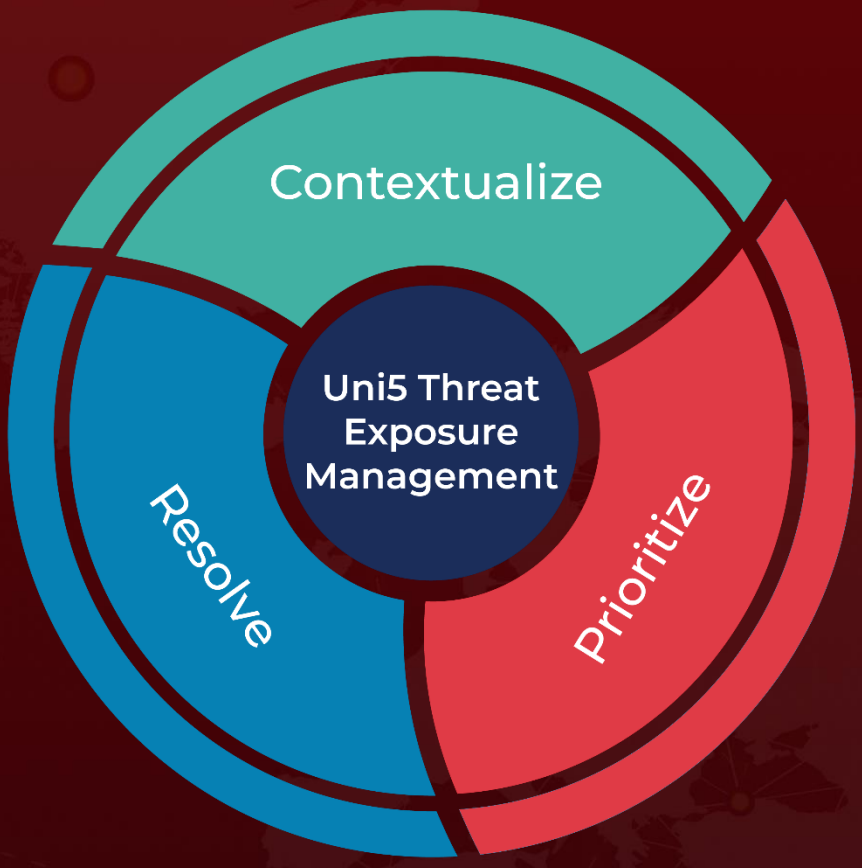
https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem

https://hivepro.com/threat-advisory/a-fresh-look-at-the-bumblebees-comeback-strategies/

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

October 24, 2024 . 4:30 AM

More at www.hivepro.com