

HiveForce Labs

THREAT ADVISORY



ATTACK REPORT

BlackLotus UEFI Bootkit Exploits Windows 11 vulnerability

Date of Publication

March 14, 2023

Admiralty Code

A1

TA Number

TA2023133

Summary

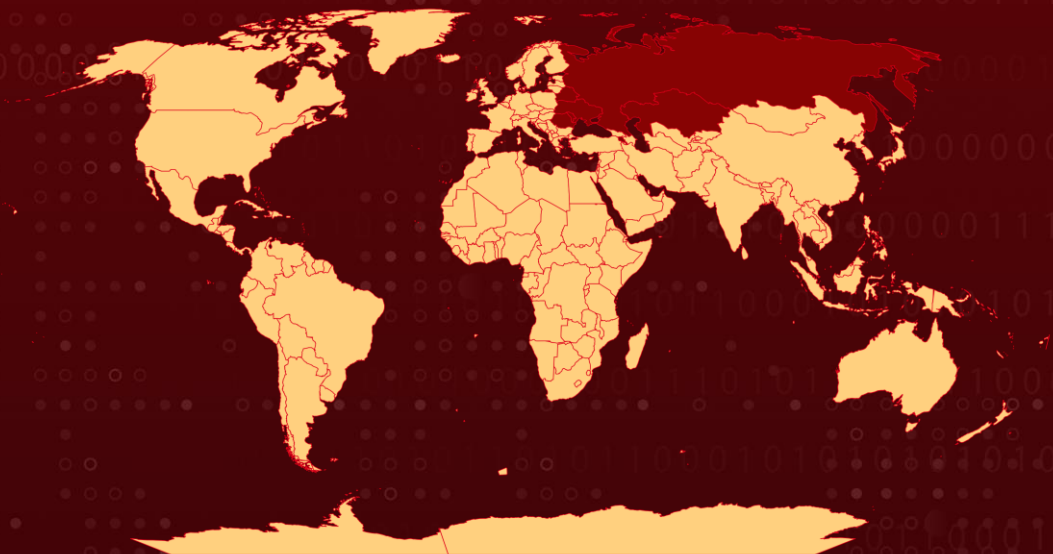
Attack Begin: October 2022

Attack Countries: Worldwide except Romania, Moldova, Russia, Ukraine, Armenia, Belarus, Kazakhstan

Malware: BlackLotus bootkit

Attack: BlackLotus is a dangerous UEFI bootkit that can take full control of the operating system boot process, allowing it to disable security measures and deploy its own payloads; it exploits a known vulnerability in UEFI Secure Boot and is capable of running on up-to-date Windows 11 systems, and is advertised and sold on underground forums for \$5,000 to unknown threat actors.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, NavInfo, OpenStreetMap, TomTom, Zenrin

CVE

CVE	NAME	PATCH
CVE-2022-21894	Secure Boot Security Feature Bypass Vulnerability (Baton Drop)	

Attack Details

#1

BlackLotus is a type of UEFI bootkit, which is a powerful threat that has full control over the operating system boot process. It can disable various security mechanisms of the OS and deploy its own payloads in the early stages of startup. The BlackLotus bootkit is capable of running on fully-up-to-date Windows 11 systems with UEFI Secure Boot enabled.

#2

The bootkit exploits the Baton Drop vulnerability(CVE-2022-21894) that allows it to bypass UEFI Secure Boot and set up persistence on the system. This vulnerability was fixed by Microsoft in January 2022, but its exploitation is still possible as the affected, validly signed binaries have not been added to the UEFI revocation list. BlackLotus takes advantage of this and brings its own copies of legitimate but vulnerable binaries to the system in order to exploit the vulnerability.

#3

Once installed, the bootkit's main goal is to deploy a kernel driver and an HTTP downloader responsible for communication with the command-and-control server and capable of loading additional payloads. BlackLotus is advertised and sold on underground forums since at least October 6th, 2022, for \$5,000. It has been sold to unknown threat actors, and the distribution channel used to deploy the bootkit to victims is unknown. There are claims made by the BlackLotus developer on underground hacking forums about its capabilities, including a built-in Secure Boot bypass and kernel protection against removal.

Recommendations



Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.



Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0002</u> Execution	<u>TA0003</u> Persistence	<u>TA0004</u> Privilege Escalation
<u>TA0005</u> Defense Evasion	<u>TA0007</u> Discovery	<u>TA0011</u> Command and Control	<u>T1587</u> Develop Capabilities
<u>T1587.002</u> Code Signing Certificates	<u>T1588</u> Obtain Capabilities	<u>T1588.005</u> Exploits	<u>T1203</u> Exploitation for Client Execution
<u>T1559</u> Inter-Process Communication	<u>T1106</u> Native API	<u>T1129</u> Shared Modules	<u>T1542</u> Pre-OS Boot
<u>T1542.003</u> Bootkit	<u>T1548</u> Abuse Elevation Control Mechanism	<u>T1548.002</u> Bypass User Account Control	<u>T1134</u> Access Token Manipulation
<u>T1134.002</u> Create Process with Token	<u>T1622</u> Debugger Evasion	<u>T1574</u> Hijack Execution Flow	<u>T1562</u> Impair Defenses
<u>T1070</u> Indicator Removal	<u>T1070.004</u> File Deletion	<u>T1070.009</u> Clear Persistence	<u>T1036</u> Masquerading
<u>T1036.005</u> Match Legitimate Name or Location	<u>T1112</u> Modify Registry	<u>T1027</u> Obfuscated Files or Information	<u>T1027.007</u> Dynamic API Resolution
<u>T1027.009</u> Embedded Payloads	<u>T1055</u> Process Injection	<u>T1055.002</u> Portable Executable Injection	<u>T1055.012</u> Process Hollowing
<u>T1014</u> Rootkit	<u>T1497</u> Virtualization/Sandbox Evasion	<u>T1497.001</u> System Checks	<u>T1082</u> System Information Discovery
<u>T1614</u> System Location Discovery	<u>T1016</u> System Network Configuration Discovery	<u>T1016.001</u> Internet Connection Discovery	<u>T1071</u> Application Layer Protocol
<u>T1071.001</u> Web Protocols	<u>T1132</u> Data Encoding	<u>T1132.001</u> Standard Encoding	<u>T1573</u> Encrypted Channel
<u>T1573.001</u> Symmetric Cryptography	<u>T1573.002</u> Asymmetric Cryptography		

🔗 Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	05846D5B1D37EE2D716140DE4F4F984CF1E631D1 A5A530A91100ED5F07A5D74698B15C646DD44E16 D82539BFC2CC7CB504BE74AC74DF696B13DB486A 16B12CEA54360AA42E1120E82C1E9BC0371CB635 DAE7E7C4EEC2AC0DC7963C44A5A4F47D930C5508 45701A83DEC1DC71A48268C9D6D205F31D9E7FFB 2CE056AE323B0380B0E87225EA0AE087A33CD316 5A0074203ABD5DEB464BA0A79E14B7541A033216 5DC9CBD75ABD830E83641A0265BFFDDDD2F602815 97AEC21042DF47D39AC212761729C6BE484D064D ADCEEC18FF009BED635D168E0B116E72096F18D2 DBC064F757C69EC43517EFF496146B43CBA949D1 06AF3016ACCD83DFE1C23657BF1BF91C13BAA757 0C0E78BF97116E781DDE0E00A1CD0C29E68D623D 6D8CEE28DA8BCF25A4D232FEB0810452ACADA11D 74FF58FCE8F19083D16DF0109DC91D78C94342FA ACC74217CBE3F2E727A826B34BDE482DCAE15BE6 111C4998F3264617A7A9D9BF662D4B1577445B20 17FA047C1F979B180644906FE9265F21AF5B0509 1F3799FED3CF43254FE30DCDFDB8DC02D82E662B 4B882748FAF2C6C360884C6812DD5BCBCE75EBFF 91F832F46E4C38ECC9335460D46F6F71352CFFED 994DC79255AEB662A672A1814280DE73D405617A FFF4F28287677CAABC60C8AB36786C370226588D 71559C3E2F3950D4EE016F24CA54DA17D28B9D82 D6D3F3151B188A9DA62DEB95EA1D1ABEFF257914 547FAA2D64B85BF883955B723B07635C0A09326B D1BBAA3D408E944C70B3815471EED7FA9AEE6425 0E6DD7110C38464ECAA55EE4E2FA303ADA0EDEFB D6BB89D8734B3E49725362DAE9A868AE681E8BD6 164BB587109CFB20824303AD1609A65ABB36C3E9
Domains	xrepositoryx[.]name myrepositoryx[.]com erdjknfweklsgwfmewfgref[.]com harrysucksdick[.]com heickickgn[.]com frassirishiproc[.]com myrepository[.]name egscorp[.]net

TYPE	VALUE
IPV4	104.21.22[.]185 164.90.172[.]211 185.145.245[.]123 185.150.24[.]114 190.147.189[.]122
URLs	hxxps[:]//xrepositoryx[.]name/network/API/hpb_gate.php hxxps[:]//myrepositoryx[.]com/network/API/hpb_gate.php hxxps[:]//erdjknfweklsgwfmewfgref[.]com/API/hpb_gate.php hxxps[:]//harrysucksdick[.]com/API/hpb_gate.php hxxps[:]//heickickgn[.]com/API/hpb_gate.php hxxps[:]//frassirishiproc[.]com/API/hpb_gate.php hxxps[:]//egscorp[.]net/API/hpb_gate.php

🔗 Patch Link

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21894>

🔗 References

<https://www.welivesecurity.com/2023/03/01/blacklotus-uefi-bootkit-myth-confirmed/>

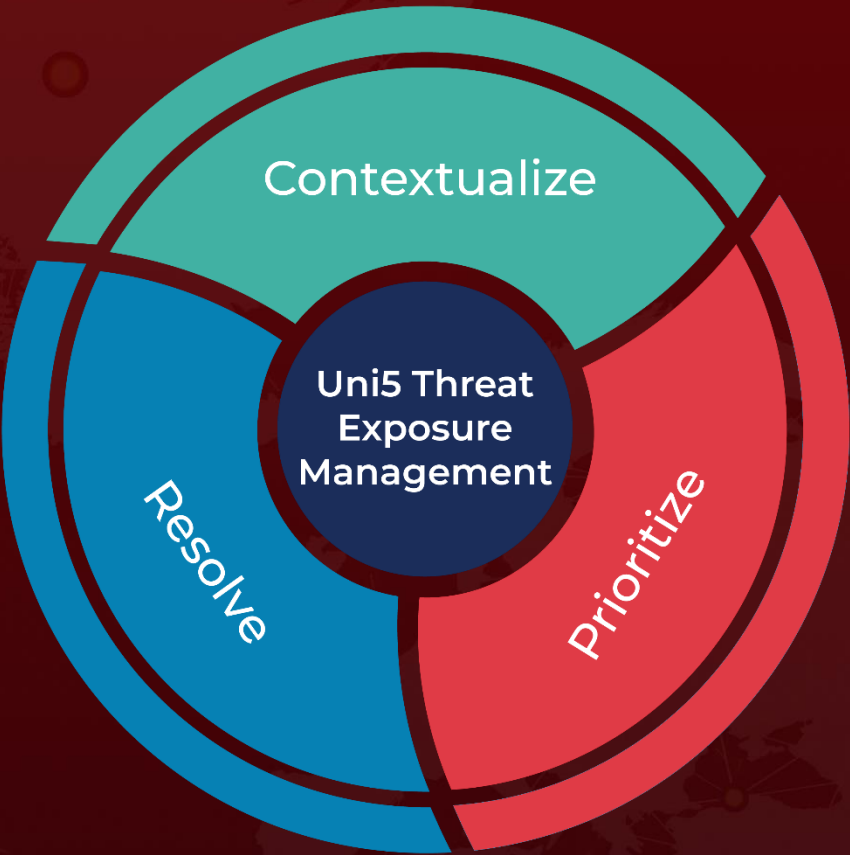
<https://www.darkreading.com/threat-intelligence/blacklotus-secure-boot-bypass-malware-set-to-ramp-up>

<https://eclypsium.com/2023/03/09/blacklotus-a-threat-coming-to-a-system-near-you/>

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
March 14, 2023 • 2:30 AM

