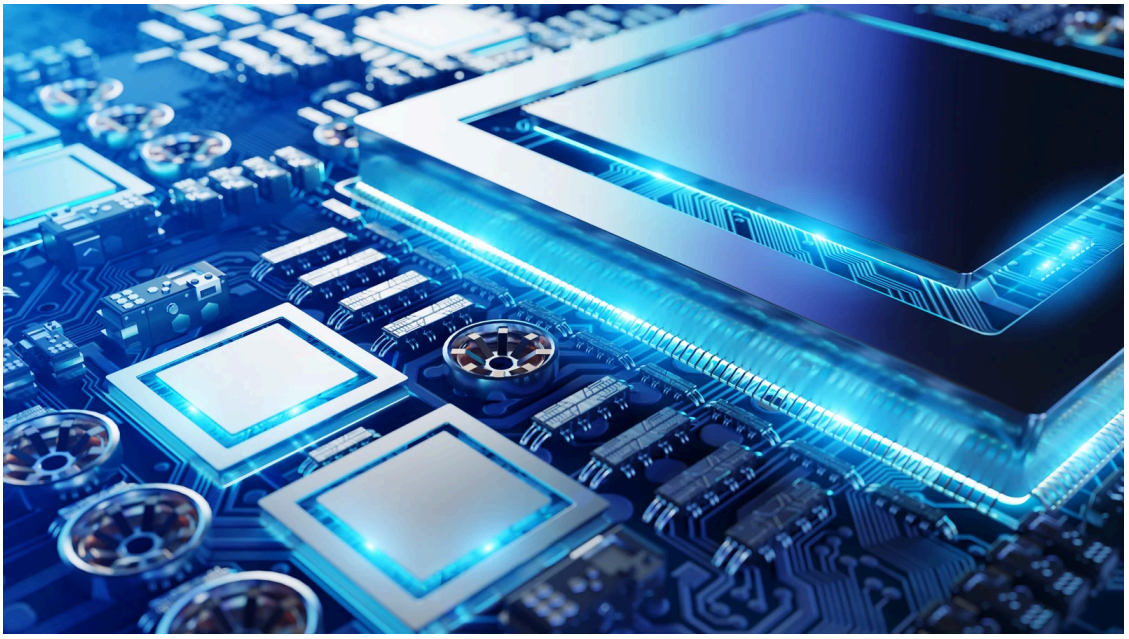
Source code for BlackLotus Windows UEFI malware leaked on GitHub

By Bill Toulas

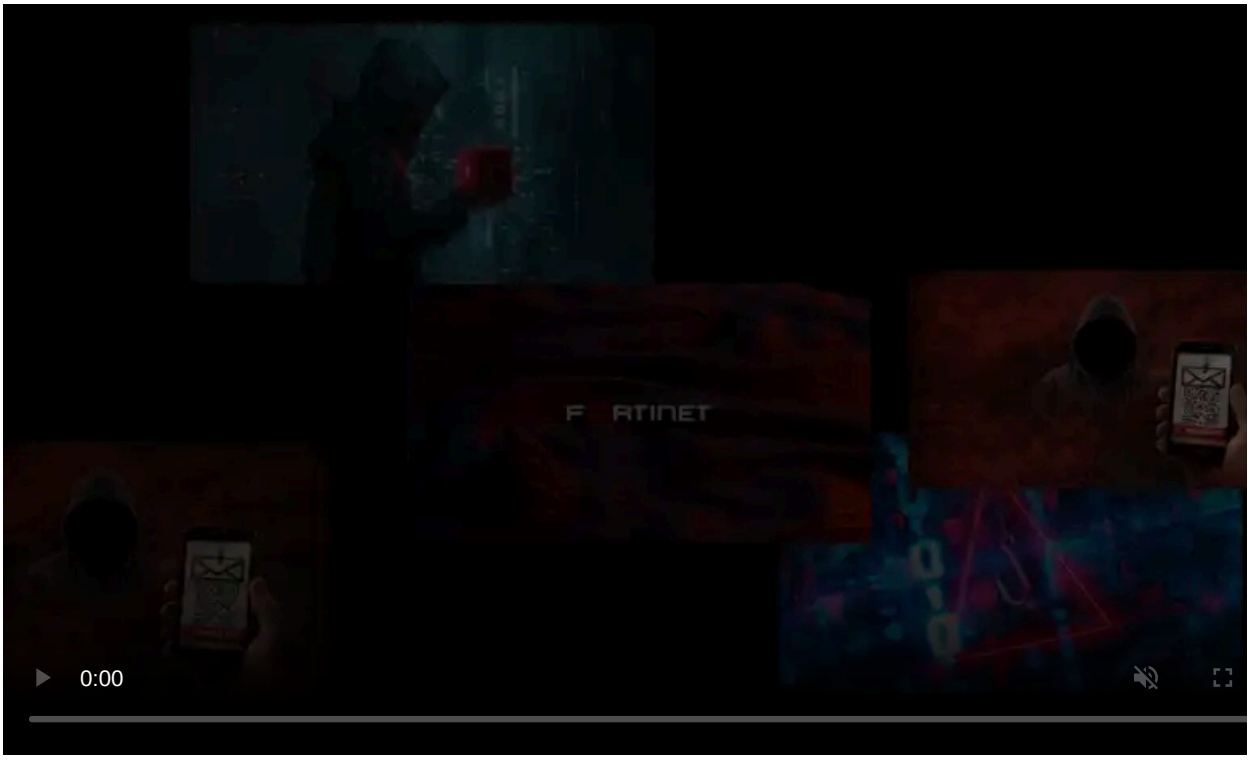
Published: 2023-07-13 · Archived: 2026-04-05 23:51:20 UTC

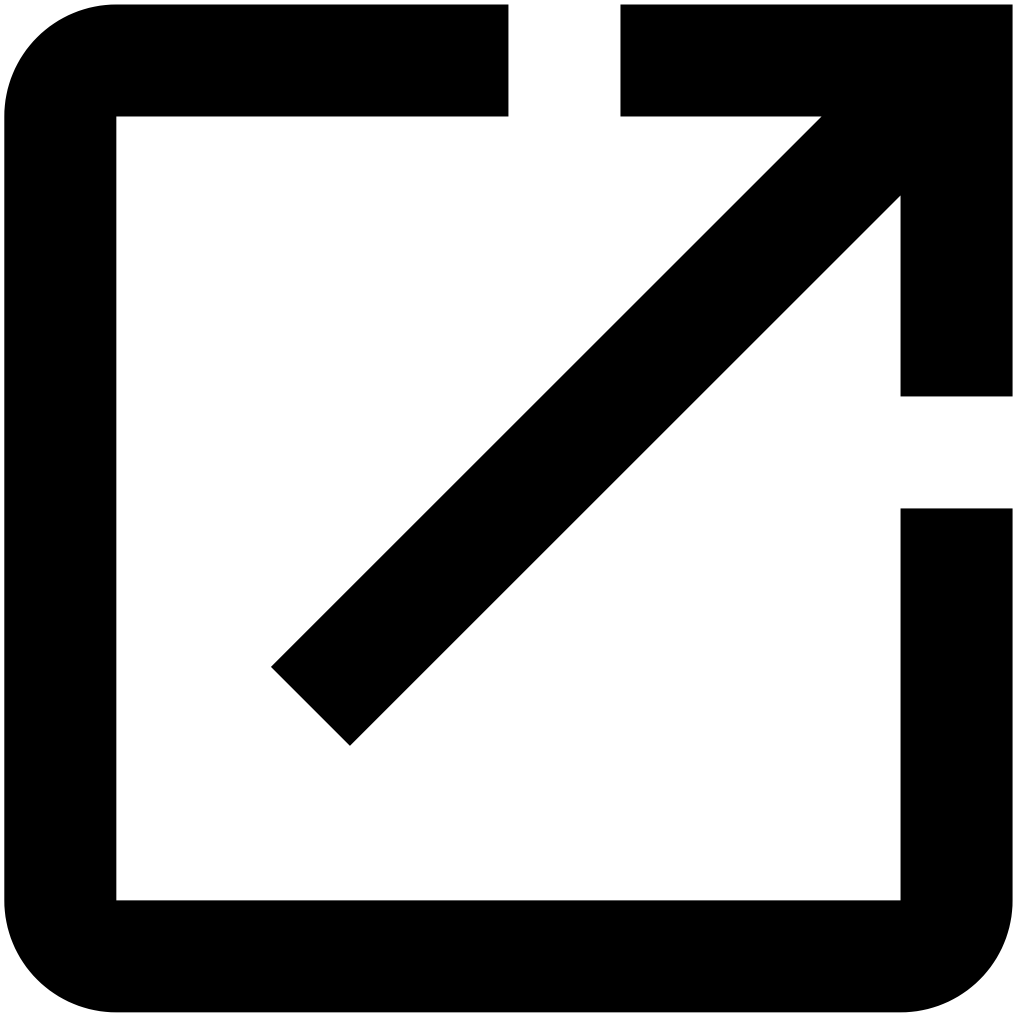


The source code for the BlackLotus UEFI bootkit has leaked online, allowing greater insight into a malware that has caused great concern among the enterprise, governments, and the cybersecurity community.

BlackLotus is a Windows-targeting UEFI bootkit that bypasses Secure Boot on fully patched Windows 11 installs, evades security software, persists on an infected system, and executes payloads with the highest level of privileges in the operating system.

Its features include impairing the BitLocker data protection feature, the Microsoft Defender Antivirus, and the Hypervisor-protected Code Integrity (HVCI) - also known as the Memory Integrity feature that protects against attempts to exploit the Windows Kernel.


F RTINET
0:00



Windows Secure Boot is a security feature that blocks untrusted bootloaders on computers with Unified Extensible Firmware Interface (UEFI) firmware and a Trusted Platform Module (TPM) chip. This security feature is meant to prevent rootkits from loading during the startup process and evade detection by applications running in Windows.

BlackLotus was the first discovered example of a UEFI bootkit that could bypass the Secure Boot mechanism and turn off OS-level security protections. This was accomplished initially by exploiting the "Baton Drop" vulnerability (CVE-2022-21894), which Microsoft patched in January 2022.

Bypasses were found for the security update, allowing BlackLotus to continue to operate and forcing Microsoft to play catchup by revoking additional Windows Boot Managers.

This led to another security update for CVE-2023-24932 (another Secure Boot Security Feature Bypass) that revoked further malicious boot managers.

However, Microsoft disabled the security update for CVE-2023-24932 by default, requiring Windows users to perform a lengthy and somewhat complicated manual installation to patch their systems.

As Microsoft warned that incorrectly installing the security fix could cause your system not to start or be recoverable from Windows installation media, many decided not to install the update, leaving devices vulnerable to Secure Boot bypass attacks.

"If you use Secure Boot and incorrectly perform the steps on this article, you might be unable to start or recover your device from media," explained Microsoft in a support bulletin.

"This can prevent you from using recovery media, such as discs or external drives, or network boot recovery, if the media has not been correctly updated."

Due to the concern and stealthiness of the BlackLotus malware, both Microsoft and the NSA shared guidance on detecting and removing the bootkit from Windows.

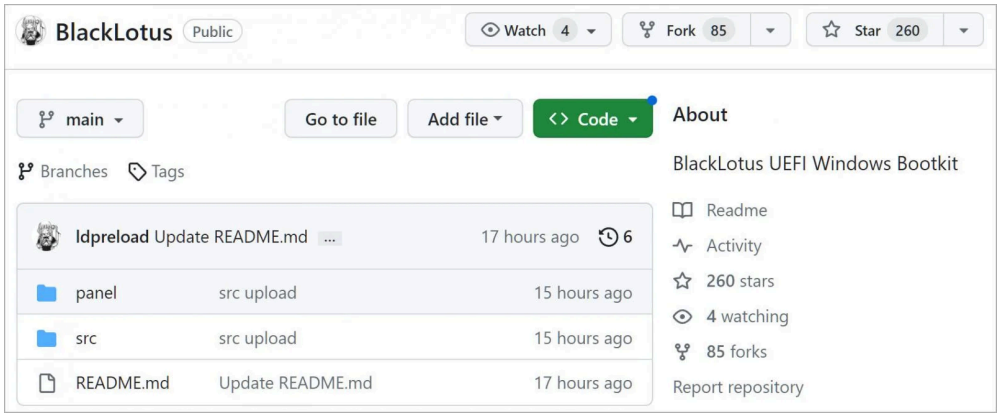
The BlackLotus source code leak

BlackLotus was initially sold on hacker forums for as little as $5,000, allowing threat actors of all skills to gain access to malware usually associated with state-sponsored hacking groups.

However, the threat actor kept the source code private, offering rebuilds for $200 to customers who wanted to customize the bootkit.

Today, security firm Binarly told BleepingComputer that the source code of the BlackLotus UEFI bootkit was leaked on GitHub by the user 'Yukari.' making the tool widely available to anyone.

Yukari says that the source code has been modified to remove the Baton Drop vulnerability and instead uses the bootlicker UEFI rootkit, which is based on the CosmicStrand, MoonBounce, and ESPECTRE UEFI APT rootkits.



Leaked BlackLotus source code on GitHub
Source: BleepingComputer

"The leaked source code isn't complete and contains mainly the rootkit part and bootkit code to bypass Secure Boot," stated Binarly's co-founder and CEO Alex Matrosov.

Matrosov explains that the bootkit's techniques are no longer new, but the source code leak makes it trivial for threat actors to combine the bootkit with new bootloader vulnerabilities, either known or unknown.

"Most of these tricks and techniques are previously known for years and don't present significant impact," Matrosov told BleepingComputer in a conversation about the leak.

"However, the fact that it's possible to combine them with new exploits like the BlackLotus campaign did was something unexpected to the industry and shows the real limitations of the current mitigations below the operating system."

It is important to stress that even though Microsoft addressed the Secure Boot bypasses in CVE-2022-21894 and CVE-2023-24932, the security update is optional, and the fixes are disabled by default.

To secure systems against the BlackLotus UEFI bootkit threat, make sure to follow the comprehensive mitigation advice that NSA published last month.

With the bootkit's source code now widely available, it is also possible that competent malware authors might create more potent variants that can bypass existing and future countermeasures.

Matrosov told BleepingComputer that this particular attack vector has significant benefits for attackers and will only get more sophisticated and complex.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
