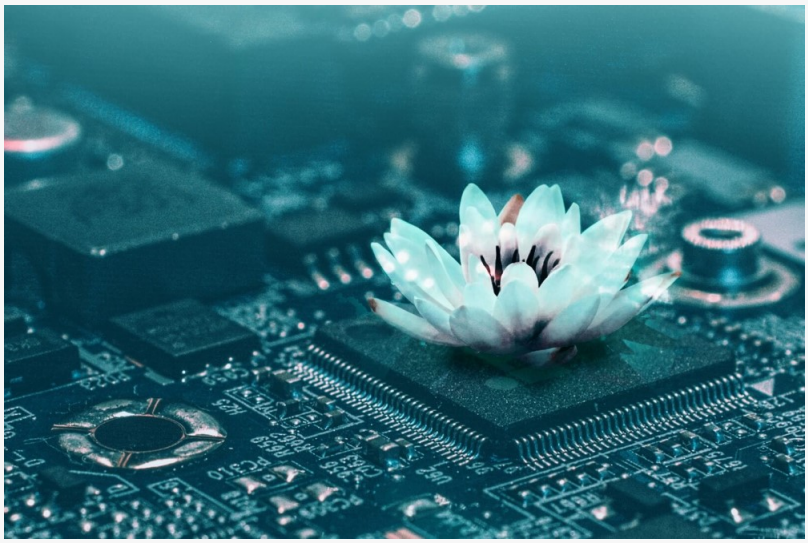
ESET Research analyzes BlackLotus: A UEFI bootkit that can bypass UEFI Secure Boot on fully patched systems



DUBAI, UNITED ARAB EMIRATES, March 6, 2023 /EINPresswire.com/ -- ESET researchers are the first to publish an analysis of a UEFI bootkit that is capable of bypassing an essential platform security feature – UEFI Secure Boot. The functionality of the bootkit and its individual features make ESET Research believe that it is a threat known as BlackLotus, a UEFI bootkit that has been sold on hacking forums for USD$5,000 since at least October 2022. This bootkit can run even on fully up-to-date Windows 11 systems with UEFI Secure Boot enabled.

“Our investigation started with a few hits on what turned out to be (with a high level of confidence) the BlackLotus user-mode component — an HTTP downloader — in our telemetry late in 2022. After an initial assessment, code patterns found in the samples brought us to the discovery of six BlackLotus installers. This allowed us to explore the whole execution chain and to realize that what we were dealing with here is not just regular malware,” says Martin Smolár, the ESET researcher who led the investigation into the bootkit.

The bootkit exploits a more than one-year-old vulnerability (CVE-2022-21894) to bypass UEFI Secure Boot and set up persistence for the bootkit. This is the first publicly known, in-the-wild abuse of this vulnerability. Although the vulnerability was fixed in Microsoft’s January 2022 update, its exploitation is still possible as the affected, validly signed binaries have still not been added to the UEFI revocation list. BlackLotus takes advantage of this, bringing its own copies of legitimate — but vulnerable — binaries to the system in order to exploit the vulnerability.

BlackLotus is capable of disabling operating system security mechanisms such as BitLocker, HVCI, and Windows Defender. Once installed, the bootkit’s main goal is to deploy a kernel driver (which, among other things, protects the bootkit from removal) and an HTTP downloader

responsible for communication with the Command and Control server and capable of loading additional user-mode or kernel-mode payloads. Interestingly, some of the BlackLotus installers ESET has analyzed do not proceed with bootkit installation if the compromised host uses locales from Armenia, Belarus, Kazakhstan, Moldova, Russia, or Ukraine.

BlackLotus has been advertised and sold on underground forums since at least early October 2022. “We can now present evidence that the bootkit is real, and the advertisement is not merely a scam,” says Smolár. “The low number of BlackLotus samples we have been able to obtain, both from public sources and our telemetry, leads us to believe that not many threat actors have started using it yet. We are concerned that things will change rapidly should this bootkit get into the hands of crimeware groups, based on the bootkit’s easy deployment and crimeware groups’ capabilities for spreading malware using their botnets.”

Many critical vulnerabilities affecting the security of UEFI systems have been discovered in the past few years. Unfortunately, due to the complexity of the whole UEFI ecosystem and related supply-chain problems, many of these vulnerabilities have left systems vulnerable even a long time after the vulnerabilities have been fixed … or at least since we were told they had been fixed.

UEFI bootkits are very powerful threats, having full control over the operating system boot process and thus being capable of disabling various operating system security mechanisms and deploying their own kernel-mode or user-mode payloads in early boot stages. This allows them to operate very stealthily and with high privileges. So far, only a few have been discovered in the wild and publicly described. UEFI bootkits may lose on stealthiness when compared to firmware implants — such as LoJax, the first in-the-wild UEFI firmware implant, discovered by ESET Research in 2018 — as bootkits are located on an easily accessible FAT32 disk partition. However, running as a bootloader gives them almost the same capabilities, without having to overcome multiple layers of security features protecting against firmware implants.

“The best advice, of course, is to keep your system and its security product up to date to raise the chance that a threat will be stopped right at the beginning, before it’s able to achieve pre-OS persistence,” concludes Smolár

For more technical information about BlackLotus, along with mitigation and remediation advice, check out the blog post “BlackLotus UEFI Bootkit: Myth confirmed” on WeLiveSecurity. Make sure to follow ESET Research on Twitter for the latest news from ESET Research.

About ESET
For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure, and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET’s high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in

real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter.

Sanjeev Kant
Vistar Communications
email us here
