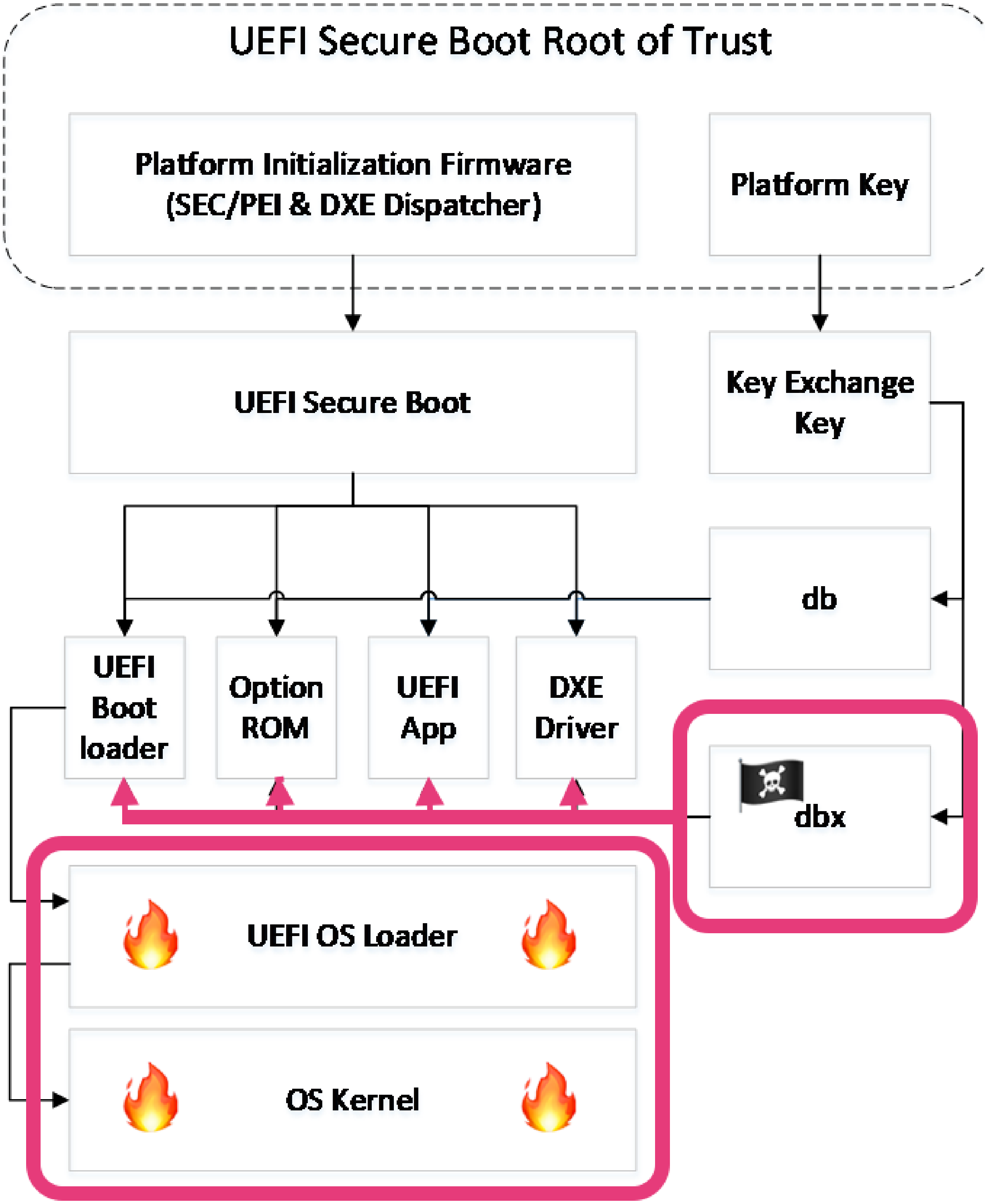
The Untold Story of the BlackLotus UEFI Bootkit

binarly.io/posts/The_Untold_Story_of_the_BlackLotus_UEFI_Bootkit/index.html



My experience with the analysis and detection of rootkits and bootkits goes back more than 20 years. In the early 2000s, the main challenge was dealing with infected machines when rootkits and bootkits modified the operating system kernel to conceal malicious components. It was such a fun time reverse engineering advanced threats in the good old days that I co-wrote "Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats," a book full of the most interesting stories of our time going down the rabbit hole of advanced malware.

When the major operating systems moved to UEFI support and Secure Boot was widely implemented, I really believed the golden age of bootkits had ended and the natural evolution would lead in the direction of firmware implants. I was wrong. Last week, researchers at ESET published "BlackLotus UEFI Bootkit: Myth Confirmed," confirming the existence of UEFI bootkits all over again. UEFI bootkits like BlackLotus are not new and have been publicly seen since 2013 or even earlier. Modified or replaced bootloaders create very visible and noisy Indicators of Compromise (IOCs) that attackers who are focused on persistence want to avoid.

Nevertheless, BlackLotus has been detected in-the-wild by the end of 2022, which is surprising for a malware class that has been around for 10+ years.

Dive into (in)secure boot and the CVSS scoring problem

This story also has a supply chain twist. A critical aspect of the BlackLotus story lies in supply chain problems relating to modern operating systems, their bootloaders, and UEFI firmware. In order to bypass Secure Boot at scale, BlackLotus exploits CVE-2022-21894, a vulnerability patched by Microsoft in January 2022. A proof-of-concept exploit was released in August 2022, seven months after Microsoft’s public disclosure.

The CVE-2022-21894 vulnerability’s CVSS score (4.4 medium) doesn't seem to indicate a serious vulnerability, does it?

The problem with most of the Secure Boot bypass vulnerabilities is that they require local or physical access to the target. This significantly affects CVSS scoring in terms of the impact. Since Secure Boot bypass attacks cross security boundaries or allow the disabling of security features, we need to treat them as privilege escalation vulnerabilities to more accurately reflect the CVSS impact score.

As the operating system bootloader becomes the middle layer between the firmware and operating system during the boot process, the bootloader provides a significant attack surface that can impact a lot of security features like disk encryption and secure boot. Currently, there is little documentation on attacks against bootloaders and a lot of inconsistency in the published existing knowledge. Here are some Microsoft advisories related to Secure Boot bypasses and other bootloader vulnerabilities.

Vulnerability	CVSS Score	Impact
CVE-2023-21560	6.6 Medium	BitLocker Encryption Bypass
CVE-2022-21894	4.4. Medium	Secure Boot Security Bypass
BootHole (ADV200011)	5.7 Medium	Secure Boot Security Bypass
CVE-2020-0689	6.7 Medium	Secure Boot Security Bypass
CVE-2019-1368	4.6 Medium	Secure Boot Security Bypass
CVE-2019-1294	4.6 Medium	Secure Boot Security Bypass
CVE-2016-7247	5.0 Medium	Secure Boot Security Bypass
CVE-2016-3287	4.4 Medium	Secure Boot Security Bypass
CVE-2016-3320	4.9 Medium	Secure Boot Security Bypass
CVE-2015-6095	4.9 Medium	BitLocker Encryption Bypass

As an aside, the navigation on the Microsoft Security Response Center (MSRC) website is a complete disaster from the perspective of tracking retrospective vulnerabilities and attacks. According to CVSS scores, all of these issues fall under ‘medium-severity’ impact. Despite this, many of them allow bypassing Secure Boot and attacking the bootloader with serious consequences.

Even after the vendor fixes the secure boot bypass vulnerabilities shown in the figure above, the vulnerabilities can present long-term, industry-wide supply chain impact. Using CVE-2022-21894 as an example shows how such vulnerabilities can be exploited in the wild after one year, even with a vendor fix available.

Interestingly, CVE-2022-21894 reminds me of previous findings MS16-094/CVE-2016-3287 and MS16-100/CVE-2016-3320 (also known as Golden Key vulnerabilities) discovered by the same researcher Clark Zammis. The complexity of the modern Microsoft Windows Boot Manager (bootmgfw) grows with every new release of Windows, simultaneously expanding the attack surface. Modern UEFI-based Secure Boot schemes are extremely complicated to configure correctly and/or to reduce their attack surfaces meaningfully. That being said, bootloader attacks are not likely to disappear anytime soon.

A record number of high-impact vulnerabilities (228) were disclosed by the Binarly REsearch team in UEFI system firmware within one year. By design, most of these vulnerabilities bypass Secure Boot and allow attackers to persist at the firmware level.

The example of BlackLotus shows how old tricks with less complicated malware can be used to gain persistence below the operating system via exploitation of a known secure boot bypass vulnerability. Still, it is quite difficult to mitigate the BlackLotus/CVE-2022-21894 secure boot bypass across the industry. The UEFI Forum is usually responsible for coordinating and supporting the major vendor-independent mitigation of UEFI Revocation List Files (DBX). This list contains the hashes of signed bootloaders or firmware components that were blacklisted.

The problem with every blacklist technology is that it will always miss known problems if it is not updated or well maintained. In the history of UEFI Revocation List Files (DBX), Microsoft pushed mandatory updates only a handful of times. Other than OS vendors, who else should be responsible for these updates? Device vendors with firmware updates? As we all know, firmware updates typically occur only a few times a year, so any blacklist will be near useless with such minimal update frequency, but it is better than nothing.

Figure1

We can see from the figure above that any compromised signed UEFI component can break secure boot integrity and bypass it. My mind immediately goes to the Binarly REsearch team's discovery of BRLY-2021-003/CVE-2021-39297 (stack buffer overflow) vulnerability on HP devices last year (almost 8 months under disclosure process). Based on the demo below, an attacker can execute arbitrary code over HP Hardware Diagnostics UEFI application.

Figure2

During its analysis of BlackLotus, the ESET research team discovered that the MokList NVRAM variable was modified. The MokList variable contains a list of authorized Machine Owner Keys (MOKs) and hashes (EFI_SIGNATURE_LIST according to the UEFI specification). But it's another example of a supply chain issue with broad secure boot implications in the field as the MokList variable can be modified in runtime. With the modified MokList variable, an attacker can easily load any self-signed shim bootloader, which is actually another vulnerability in the chain used to keep secure boot active.

In the modern secure boot, there are many inconsistencies due to many factors, including legacy compatibility issues. The Binarly REsearch Team has discussed these weaknesses for years at multiple public conferences, but the complexity of modern secure boot continues to increase.

Enterprise defenders and CISOs need to understand that threats below the operating system are clear and present dangers to their environments. Since this attack vector has significant benefits for the attacker, it is only going to get more sophisticated and complex. Vendor claims about security features can be completely opposite to the

reality. Binarly's small research team was able to discover and disclose 228 high-impact vulnerabilities across all major enterprise vendors in a year, which we believe only scratches the surface. This research continues, on both sides of the fence (defense and offense).

A new name for old tricks

Are there any new techniques in the BlackLotus bootkit? My opinion is that BlackLotus is a good combination of well-known techniques. Proof of concept code for CVE-2022-21894 (public since August 2022) was taken from the GitHub repository of the researcher who found the vulnerability.

Binarly REsearch discovered new interesting data points about the nature of the bootkit code. It appears the author of the BlackLotus bootkit based their development on code from the Umap GitHub project (Windows UEFI bootkit that loads a generic driver manual mapper without using a UEFI runtime driver) or coincidently arrived at the same ideas. According to the first commit, Umap was released in April 2020.

This picture shows a comparison of the logic of the main function from BlackLotus and Umap. Both look very similar and contain exactly the same steps with a few minor changes.

Figure3

The routines responsible for installing the hook chain (start with *ImgArchStartBootApplication*) are very similar as shown in the figure.

Figure4

BlackLotus trampoline code modification logic to setup hooks is identical to Umap code on GitHub.

Figure5

With these new data points, we can see how UEFI bootkit code reused from 2020 can be combined with publicly available proofs of concept for CVE-2022-1894 to lead to the creation of the BlackLotus bootkit. This relatively new secure boot bypass vulnerability (which the vendor claims is low-impact) has led to widespread distribution of old malicious UEFI bootkit code.

Zero-knowledge detection of new threats

Binarly has been focused from the beginning on developing proactive technology based on deep code inspection to detect unknown threats and vulnerabilities to help the industry recover from repeatable failures. The Binarly Platform dashboard below shows code similarity proactive detection based on machine learning models guided by code-based embeddings.

Using the BlackLotus components, we simulated infection on one of the machines available in our lab. Binarly Platform was used to compare collected snapshots of the infected and clean EFI System Partitions (ESP). Based on function similarity, we detect the replacement of bootmgfw.efi with the shim.

Figure6

The BlackLotus anomaly was proactively detected with zero knowledge about this threat, and the explained code similarity failures make it actionable for the security and incident response teams to conduct further investigation.

Let's explore the code similarity detection in more detail. The figure below shows the detailed output for the detected anomalies from the BlackLotus malicious components added to ESP partition.

Figure7

Code similarity detects anomalies based on code changes and integrity checking heuristics as shown in the figure below.

Figure8

Here is a visual explanation of the outlier (compromised ESP partition) and details of the algorithm to detect anomaly:

Figure9

Binarly's Platform is able to analyze modules and executables based on semantic similarity. The figure above shows a visualization of the program embeddings for bootmgfw and the shim. For code function signatures, we used data clustering algorithm DBSCAN with a precomputed Gower distance to detect anomalies. This is where we detect that additional suspicious modules were added. Afterwards, we visualized the results using the T-SNE algorithm.

What about detection based on FwHunt?

We continue to maintain the public FwHunt rules database and today we released a new semantic-based rule to cover malicious bootloader components from the BlackLotus bootkit.

BlackLotus rule is included in FwHunt's GitHub repository. To use these rules you will need FwHunt Community Scanner (fwhunt-scan).

Figure10

We need to increase the industry awareness to firmware related threats and build more effective threat hunting programs with cross-industry collaboration between the vendors to mutually benefit customers and provide better detection rates.

Back to overview