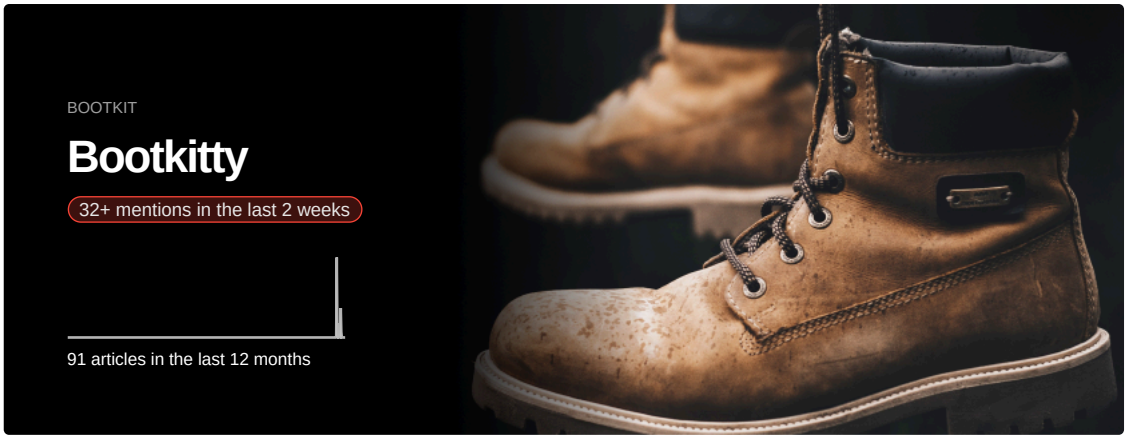

Using open-source data collected by Feedly AI.

Overview

Bootkitty is a malware targeting Linux systems, specifically recognized as the first UEFI bootkit for Linux. It utilizes self-signed certificates, which prevent it from bypassing Secure Boot on its own. However, when combined with the LogoFAIL UEFI vulnerabilities, it can execute by allowing an attacker to add a Machine Owner Key (MOK) without user interaction. Bootkitty exemplifies some new behav... See More

Article count

No article counts found. Try changing the time period.

Top targeted industries and organizations

INDUSTRIES	ORGANIZATIONS	ARTICLES	ATTACK REPORTED

No attack has been detected in the time frame selected

Top threat actors using this malware

No threat actors have been linked to this malware at the moment

Tactics, Techniques, and Procedures

Last mentioned

TECHNIQUE	MITRE ID	PROCEDURES	MITIGATION	ARTICLES
System Firmware	T1542.001	164	3	63
Bootkit	T1542.003	60	2	3
Rootkit	T1014	28	0	17
Code Signing	T1553.002	5	0	5
Software Packing	T1027.002	2	1	2
Process Injection	T1055	15	2	12
Hijack Execution Flow	T1574	3	10	3

Exploitation for Client Execution	T1203	3	2	3
Impair Defenses	T1562	1	6	1

Exploited vulnerabilities

CVE ID	CVSS SCORE	EPSS SCORE	VENDOR	PRODUCT	TREND	WEAPONIZED
CVE-2023-40238 A vulnerability known as LogoFAIL has been discovered in the BmpDecoderDxe component of Insyde InsydeH2O firmware. This issue…	CVSS 5.5	0%	Insyde	insydeh2o		Nov 30, 2024

Threat intelligence reports

Bootkitty and Linux Bootkits: We've Got You Covered

12 TTPs • Eclypsium | Supply Chain Security for th... by Chris Garland / 4d • Bootkitty first UEFI bootkit for Linux

The Threat of Linux Bootkits Recently, security researchers have been analyzing and publishing details about "Iranukit" and "Bootkitty," malware that targets Linux systems with bootkits.

Also in #linux, Gridinsoft Blog, +197 feeds

Bootkitty: Analyzing the first UEFI bootkit for Linux

BlackCat • 86 WeLiveSecurity / 10d • BlackCat Threat Intelligence Reports • IoC > 9 hashes • 17 TTPs

We explain how the bootkit gets to the actual kernel patching later in the Linux kernel image decompression hook section; for now, just note that due to the lack of kernel-version checks in the function shown in Figure 4, Bootkitty can get to t…

Also in #linux, Gridinsoft Blog, +197 feeds

News

Bootkitty and Linux Bootkits: We've Got You Covered

12 TTPs • Eclypsium | Supply Chain Security for th... by Chris Garland / 4d • Bootkitty first UEFI bootkit for Linux

The Threat of Linux Bootkits Recently, security researchers have been analyzing and publishing details about "Iranukit" and "Bootkitty," malware that targets Linux systems with bootkits.

Also in #linux, Gridinsoft Blog, +197 feeds

Short Takes – 12-3-24

Chemical Facility Security News by PJCoyle / 5d

Code found online exploits LogoFAIL to install Bootkitty Linux backdoor .

First-ever Linux UEFI bootkit turns out to be student project

7 TTPs • First-ever Linux UEFI bootkit turns out ... / 6d • Original source: WeLiveSecurity / 11d • Bootkitty first UEFI bootkit for Linux

Bootkitty, a recently discovered boot-level UEFI rootkit for Linux, was evidently created by students participating in a cybersecurity training program at the South Korean Information Technology Research Institute (KITRI).

Also in #linux, Gridinsoft Blog, +197 feeds

Bootkitty UEFI bootkit origins, integrated exploit uncovered

CVE-2023-40238 (CVSS 5.5 ex) • SCM feed for Latest by SC Staff / 6d • 2 TTPs

Bootkitty has been integrated with a manipulated BMP file exploiting LogoFAIL-related vulnerability, tracked as CVE-2023-40238, to circumvent defenses provided by Secure Boot, compromise UEFI image parsing routines, and execu…

Also in The Information Tech..., Google Alert, +22 feeds

Bootkitty: The Game-Changing Malware Targeting Linux Systems

2 TTPs • CySecurity News - Latest Information Sec... by Shivani Tiwari / 6d

• Bootkitty first UEFI bootkit for Linux

This malware, named Bootkitty, introduces a new method of attacking Linux, which has traditionally been considered safer from such stealthy threats compared to Windows.

Also in #linux, Gridinsoft Blog, +197 feeds

Cybersecurity News: Hydra Market leader sentenced, Pegasus spyware arrest, SpyLoan malware targets millions

2 CVEs • CISO Series by Lauren Verno / 6d •

Poland arrests former spy chief

Bootkitty bootkit exploits LogoFAIL flaw Researchers have uncovered a Linux UEFI bootkit called 'Bootkitty' that exploits the LogoFAIL vulnerability (CVE-2023-40238), allowing attackers to bypass Secure Boot protections.

Also in #cybersecurity, Cyber Security Headl..., +85 feeds

See 26 more articles and social media posts