H-ISAC
HEALTH - ISAC

THREAT BULLETINS

Eclypsium Researchers Release Technical Details on Malicious Bootkits

○○○ TLP:WHITE

Oct 22, 2021

In the past several weeks, two separate bootkits have been reported publicly, FinSpy and ESPecter. These malicious tools bypass operating system security capabilities by executing first and modifying the kernel as it loads in the boot process.

Eclypsium researchers have been tracking these bootloaders for an extended period of time, and new indicators of compromise (IOCs) have been released to specifically identify the types of attacks by these bootloaders.

The Health-ISAC Threat Operations Center is releasing these reports, which can be accessed here, for FinSpy, and here, for ESPecter, to improve the overall security and threat awareness of the Health-ISAC member community.

Sources

Eclypsium: Fighting Back Against Bootkits

Eclypsium: FinSpy UEFI and MBR BootKit

Alert ID 933c1857

View Alert

Tags ESPecter, Eclypsium, FinSpy Malware, bootkit payload, bootkit module, bootkits, bootkit, FinSpy

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.