UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00208

UEFI BOOTKIT MALWARE KNOWN AS ESPECTER

DATE ISSUED: 11th October 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

By modifying the Windows Boot Manager, this rare Unified Extensible Firmware Interface (UEFI) bootkit gains persistence and drops a fully featured backdoor on the infected computer.

BREAKDOWN

The aim of the malware is to create a backdoor for attacker access with automated data exfiltration capabilities supporting a rich set of commands. This allows the attacker to steal documents, keylog records and enables them to monitor their victims screen and take screenshots. Because the purpose of the UEFI is to secure the computer components on startup at a firmware level, this is an ideal place to plant malware and makes it particularly difficult to detect or remove. ESET have dubbed the malware ESPecter as it takes hold of the EFI System Partition (ESP) which stores to kernel images used to boot the computers Operating System (OS) at device startup. By starting at such a low level, the malware is able to bypass the Windows Drive Signature Enforcement (DSE) security protections and run its own drivers. From here it can infiltrate other system processes to connect with the Command and Control (C2) server allowing the attacker to complete the machione takeover. This new variant is an evolution of the 2012 malware that use Master Boot Record (MBR) modification to gain persistence.

REMEDIATION STEPS

- It is currently unknown how the malware is being spread. Possibilities may include vulnerability exploitation or direct installation by a user with access to a device, secure boot is disabled or the operating system does not support secure boot.
- It is extremely difficult to remove a bootkit and is not guaranteed that reimaging the machine will work. Completely deleting the OS and performing bare metal re-installation is recommended, however not easily done.

REFERENCES & RESOURCES

ThreatPost https://threatpost.com/especter-bootkit-malware-espionage/175366/
ZDNet` https://www.zdnet.com/article/meet-especter-a-new-uefi-bootkit-for-cyber-spying/
We Live Security https://www.welivesecurity.com/2021/10/05/uefi-threats-moving-esp-introducing-especter-bootkit/