kindred

Security Newsletter

1 October 2018

Subscribe to this newsletter

New UEFI LoJax Malware Can Survive After OS Re-installation and Hard Disk Replacement

Security researchers from ESET found first ever APT28 group used UEFI rootkit in wild. The UEFI rootkits are hard to detect and extremely dangerous, they persist even after operating system reinstallation and even a hard disk replacement. The Unified Extensible Firmware Interface(UEFI) is a replacement for BIOS that connects computer's firmware to its operating system.

To reach the UEFI/BIOS settings, all tools use the kernel driver of the RWEverything tool that allows modification of the settings in the firmware of almost any hardware. The driver is signed with a valid certificate. If write operations are denied, the malicious tool exploits a four-year-old race condition vulnerability in UEFI (CVE-2014-8273) to bypass the defenses. The purpose of the rootkit is just to drop malware into the Windows operating system and make sure that it executes at startup.

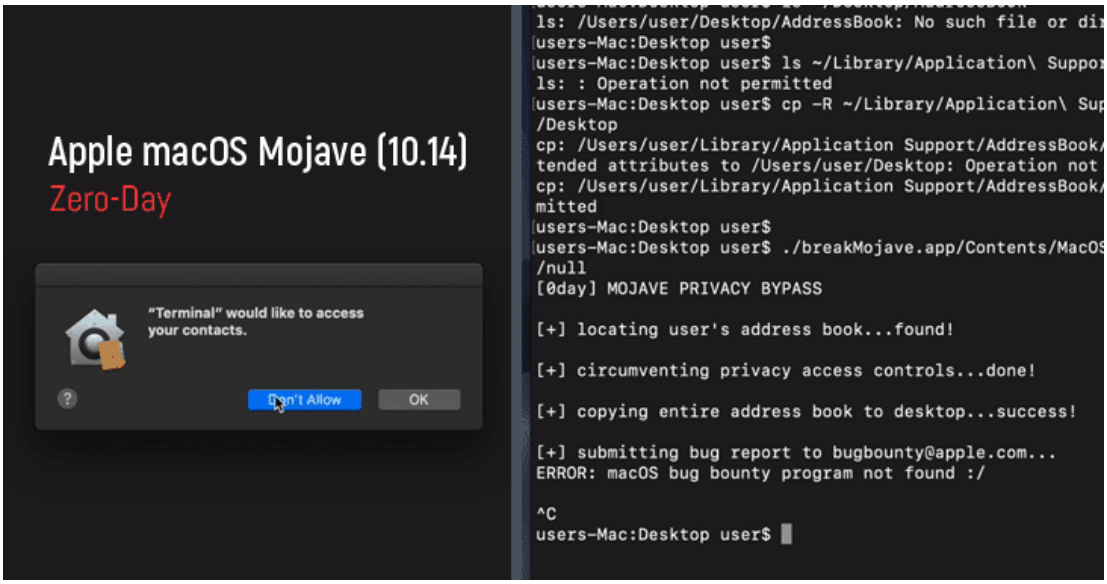
By enabling Secure Boot you can avoid such infection. Make sure that you are using the latest available UEFI/BIOS available for your motherboard. If your system infected Flashing UEFI/BIOS or replacing the motherboard is the only solution.

Read More on GBHacker

Even More on BleepingComputer

Research Whitepaper from ESET

MacOS Mojave 10.14 Zero-Day Vulnerability - bypasses new Privacy feature



The same day Apple released its latest macOS Mojave operating system, a security researcher demonstrated a potential way to bypass new privacy implementations in macOS using just a few lines of code and access sensitive user data.

On Monday, Apple started rolling out its new macOS Mojave 10.14 operating system update to its users, which includes a number of new privacy and security controls, including authorization prompts. Wardle tweeted a video Monday showing how he was able to bypass the permission requirements on a dark-themed Mojave system by running just a few lines of code simulating a malicious app called "breakMojave," which allowed him to access to the address book and copy it to the macOS desktop.

It should be noted that the flaw does not work with all of the new privacy protection features implemented by Apple in macOS Mojave, and hardware-based components, like the webcam and microphone, are not affected. Wardle has not released details beyond just the proof-of-concept video until the company patches the issue in order to prevent abuse. Until then, Mojave users are recommended to be cautious about what apps they run.

Read More on The Hacker News

Original Announcement

Cutting room floor

- Looking after the corporate Apple mobile fleet? Beware: MDM onboarding is 'insecure'
- New VirusTotal Enterprise Offers Private Graphs, Faster Searches
- New Linux Kernel Bug Affects Red Hat, CentOS, and Debian Distributions
- Wendy's faces lawsuit for unlawfully collecting employee fingerprints
- Cisco Releases Alerts for 14 High Severity Bugs
- Feature, Bug or Just a Huge Security Risk? Skype for Business, Examined
- Gone in 15 Minutes: Australia's Phone Number Theft Problem
- Hey Facebook: Quit discouraging people from using 2FA
- Password managers can be tricked into believing that malicious Android apps are legitimate
- Almost Every Major Free VPN Service is a Glorified Data Farm
- Open-source software supply chain vulns have doubled in 12 months
- Microsoft: Here's why we're declaring end of password era
- How to measure risk with a better OKR.

#Tech and #Tools

- Encrypting SNI: Fixing One of the Core Internet Bugs
- From Kekeo to Rubeus
- Juicy Potato (abusing the golden privileges)
- Browser Reaper - Warning - Will crash your Browser (and maybe the OS)
- CSParse: A tool to evaluate Content Security Policies.
- Use YubiKey security key to sign into AWS Management Console
- New Mimikatz version to bypass Windows 10 Credential Guard
- Authentication bypass vulnerability in Western Digital My Cloud allows escalation to admin privileges
- VirtualBox VRDP Guest-to-Host Escape
- WinSecCheck: Detect security features in Windows binaries.
- Bypassing Duo Two-Factor Authentication (Fail Open)
- SQLi Without Quotes
- Using “magic” DNS-resolutions to track suspicious domains
- Unlock a Mustang GT - HackRF/Universal Hacker Radio
- sri-check: A Burp Suite extension for identifying missing Subresource Integrity attributes.

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us