Security Newsletter

03 May 2021

Subscribe to this newsletter

Hackers Used ‘Mind-Blowing’ Bug to Sneak Past macOS Safeguards

With macOS malware on the rise, Apple has been busy in recent years adding layers of protections that make it a lot more difficult for malicious software to run on Macs.

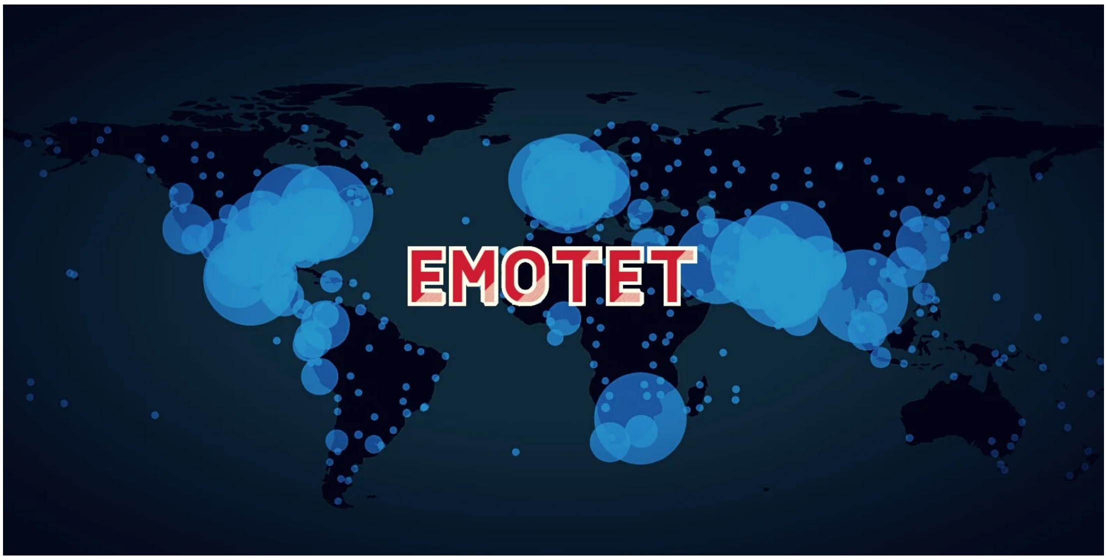
But a vulnerability in the operating system, publicly disclosed and patched on April 26, was exploited to bypass all of them.

Attackers could craft their malware strategically to trick the operating system into letting it run even if it failed key safety checks along the way.

Read More on Wired

Technical details on Objective-see

FBI shares 4 million email addresses used by Emotet with Have I Been Pwned



Millions of email addresses collected by Emotet botnet for malware distribution campaigns have been shared by the Federal Bureau of Investigation (FBI) as part of the agency's effort to clean infected computers.

Individuals and domain owners can now learn if Emotet impacted their accounts by searching the database with email addresses stolen by the malware.

Read More on Bleeping Computer

Even More on Troy Hunt's blog

More #News

- Task force proposes framework for combatting ransomware
- Previously undocumented backdoor targets Microsoft's Equation Editor
- Adobe releases open source 'one-stop shop' for security threat, data anomaly detection
- University of Minnesota responds to Linux security patch requests
- Office 365 security baseline adds macro signing, JScript protection
- Babuk quits ransomware encryption, focuses on data-theft extortion
- Microsoft finds critical code execution bugs in IoT, OT devices

#Breach Log

- FluBot Android Banking Malware Spreads Quickly Across Europe
- First Horizon bank online accounts hacked to steal customers' funds
- Hotbit cryptocurrency exchange down after hackers targeted wallets
- Your stolen ParkMobile data is now free for wannabe scammers
- Codecov starts notifying customers affected by supply-chain attack
- Brazil's Rio Grande do Sul court system hit by REvil ransomware
- DigitalOcean data breach exposes customer billing information
- Fourth time's a charm - OGUsers hacking forum hacked again
- Passwordstate hackers phish for more victims with updated malware
- UK rail network Merseyrail likely hit by Lockbit ransomware
- Experian API Exposed Credit Scores of Most Americans

#Patch Time!

- Apple Patches Zero-Day MacOS Bug That Can Bypass Anti-Malware Defenses
- ISC urges updates of DNS servers to wipe out new BIND vulnerabilities
- F5 BIG-IP Found Vulnerable to Kerberos KDC Spoofing Vulnerability
- Hackers Used to Be Humans. Soon, AIs Will Hack Humanity
- QNAP warns of AgeLocker ransomware attacks on NAS devices

#Tech and #Tools

- RotaJakiro: A long live secret backdoor with 0 VT detection
- The False Oracle — Azure Functions Padding Oracle Issue
- Added Security Measures and Changes in TLS 1.3

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 a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 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 is an innovation driven company that builds on trust.

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