Week
4
September
2019

Weekly
Newsletter on
Cyber Security
News That

PURPLE POST

Main Cyber Security News this week

Microsoft Nodersok!

Apple – IOS Again!

McAfee Publishes Cloud Security Report

Microsoft Releases fix for Internet Explorer Zero-day bug

Ransomware

- TFlowers
- REvil was GandCrab

Apple issues off band security Updates

What should keep you awake

Both Microsoft & Apple had a bad week last week.

Microsoft Nodersok Malware has the potential to affect millions of users. Your immediate approach to this attack would be to disallow HTA execution privilege for all and open it up as the case warrants. Nodersok can execute with admin privileges and currently, there is no defence other than what is outlined above.

In general Windows 10 seems to have a lot of security issues. Active and frequent patching of the OS seems to be the only way out, for now.

Apple has issued quite a few warnings & patches with varying degrees of success. After the infamous third-party keyboard vulnerability last week, Apple issued a slew of security updates.

Apple finished off the week with news of another unfixable vulnerability on almost all IOS devices, allowing these devices to be jailbroken.

In my opinion, this week's news exposes the increasing sophistication of attackers & attractiveness of the targets rather than any one platform being inherently buggy. It is technical karma, catching up, I think.

And, this week's problems are not specific to any one industry.

- Sridhar Parthasarathy

PURPLE TEAM

Cyber Security News in Detail.

(Click the snippet titles to read more)

McAfee Cloud Security Report

McAfee released Cloud-Native: The Infrastructure-as-a-Service Adoption and Risk Report, covering new research on Infrastructure-as-a-Service (IaaS) incidents in the cloud. The results of the survey demonstrate that 99 percent of IaaS misconfigurations go unnoticed—indicating awareness around the most common entry point to new "Cloud-Native Breaches" (CNB) is extremely low.

IE Zero Day bug & fix

The zero-day (CVE-2019-1367) was reported to Microsoft by Clément Lecigne of Google's Threat Analysis Group. It's a remote code execution (RCE) flaw in the browser's scripting engine that could allow an attacker to:

"… install programs; view, change, or delete data; or create new accounts with full user rights.

Tflower Ransomware

The Canadian Centre for Cyber Security (CCCS) has released an advisory on a new ransomware campaign. The malware, named TFlower, may infect users via exposed, unpatched Remote Desktop Protocol (RDP) services.

MS-ISAC Advisory on PHP Vulnerability

The Multi-State Information Sharing & Analysis Center (MS-ISAC) has released an advisory on a vulnerability in Hypertext Preprocessor (PHP). An attacker could exploit this vulnerability to take control of an affected system.

Apple security updates

Apple has released security updates to address vulnerabilities in multiple products. An attacker could exploit one of these vulnerabilities to obtain access to sensitive information.

Please follow the links for the following products and apply the necessary updates:

- macOS Mojave 10.14.6 Supplemental Update 2, Security Update 2019-005 High Sierra, and Security Update 2019-005 Sierra
- watches 5.3.2
- iOS 12.4.2

Microsoft Nodersok malware

Thousands of Windows computers across the world have been infected with a new strain of malware that downloads and installs a copy of the Node.js framework to convert infected systems into proxies and perform click-fraud. The malware, named Nodersok (in a Microsoft report) and Divergent (in a Cisco Talos report), was first spotted over the summer, distributed via malicious ads that forcibly downloaded HTA (HTML application) files on users' computers…

Apple Unfixable IOS vulnerability

Security researcher Axi0mX published the exploit, called "checkm8," Friday on GitHub. It affects every Apple device with an A5 through A11 chipset, meaning every iPhone model from 4S to X. Though it isn't an all-in-one jailbreak on its own, the exploit provides an extensive foundation for researchers to build off of in customizing jailbreaks for every vulnerable model of device that would allow them to totally take over the unit, run software far beyond what Apple normally allows, and program apps to interact and share data in ways that Apple's protections usually preclude.

In Other News ...

NIST ZTA (Zero Trust Architecture)

NIST has published the draft discussing the core logical components that make up a zero-trust architecture (ZTA) network strategy. Zero trust refers to an evolving set of network security paradigms that narrows defenses from wide network perimeters to individuals or small groups of resources.

FBI Podcast – Teens & Gaming

The FBI is seeing an increase in sextortion on online gaming platforms.
Sextortion is a federal crime that happens when an adult coerces a child into producing sexually explicit images of themselves and sending them over the Internet.
Assistant Section Chief Brian Herrick explains how offenders are enticing teenagers...
This is important if you have teenaged children

REvil Ransomware's Connection with GandCrab

The REvil (also known as Sodinokibi) ransomware was first spotted in the wild (ITW) on April 17, when threat actors leveraged an Oracle WebLogic exploit to deliver both REvil and GandCrab. The interesting thing is that on May 31, 2019, the developers of the highly profitable GandCrab 'ransomware-as-a-service' announced that they were retiring after earning over $2 billion USD since January 2018.
REvil is the new avatar of GandCrab, without doubt.

Apple actively prevents use of non-Apple spares

Apple's iPhone 11, iPhone 11 Pro, and iPhone 11 Pro Max will offer up a new warning if a repair technician ever uses a non-genuine Apple display when repairing a broken device.
Unable to verify this iPhone has a genuine Apple display" will show up in the General > About section of the Settings app if a repair shop uses an unverified display component.