kindred

Security Newsletter

21 June 2017

More evidence Mac ransomware exists

We've been saying it for some time: Mac malware is rare compared to the stuff that targets Windows. But Apple computers are far from immune.

This year's SophosLabs malware forecast included Mac malware geared towards harvesting data, providing covert remote access to thieves and holding files for ransom.

Now comes word of a new piece of Mac ransomware, which SophosLabs has identified as OSX/Ransom-A. Widely reported as an example of ransomware-as-a-service (RaaS) for Macs, it has become popularly known as MacRansom.

Read More

Samsung Left Millions Vulnerable to Hackers Because It Forgot to Renew a Domain, Researchers Say

Samsung, the most popular smartphone maker in the world, left millions of customers vulnerable to hackers after it let expire a domain that was used to control a stock app installed on older devices, security researchers say.

If you own an older Samsung smartphone, chances are you have a stock app designed to recommend other popular apps named S Suggest installed on it. The company says it discontinued S Suggest in 2014, and it recently let one of the domains used to control the app —ssuggest.com—expire, according to a security researcher who took over the domain.

Read More

CIA Created Toolkit for Hacking Hundreds of Routers Models

After a two-week hiatus, WikiLeaks dumped new files as part of the Vault 7 series that supposedly contains CIA-made hacking tools the organization claims it received from hackers and agency insiders.

Today's dump includes the documentation for a CIA tool named CherryBlossom, a multi-purpose framework developed for hacking hundreds of home router models.

Read More

Adobe Patches Nine Security Flaws in Flash Player

Adobe released today four security bulletins announcing patches for products such as Flash Player, Shockwave Player, Captivate, and Digital Editions.

In total, these four security bulletins fix 20 security flaws, among which the most crucial are the ones in the Flash and Shockwave players, the products with the larger userbases.

Of the four security bulletins, the one for Flash Player comes with a priority of "1" — the highest — so make sure to install it as soon as possible.

Read More

Nearly One Million Systems Provide "Guest" SMB Access, Most Are Linux

There are 2,306,820 devices connected to the Internet at the moment that feature open ports for SMB services, the same protocol that was used to infect hundreds of thousands of computers with the WannaCry ransomworm a month ago.

Of these, 42%, or nearly 970,000, provide "guest" access, meaning anyone can access data shared via the SMB file-sharing protocol without needing to provide authentication.

The exploits used by WannaCry didn't necessarily need guest access, but only that the system be connected to the Internet. Providing guest access opens the machine to less complex exploits

Read More

Decrypted: Kaspersky Releases Decryptor for the Jaff Ransomware

We are happy to report that the Fedor Sinitsyn, a senior malware analyst at Kaspersky Labs, has discovered a weakness in the Jaff ransomware and was able to release a decryptor for all variants that have been released to date. For those who were infected with the Jaff Ransomware and had their files encrypted with the .jaff, .wlu, or .sVn extensions, this decryptor can recover your files for free.

Read More

Lessons from TV5Monde 2015 Hack

This week during the SSTIC2017 annual cyber security conference, a French conference running consecutively since 2004, the National Cybersecurity Agency of France (ANSSI) gave a presentation detailing their 2015 audit of their investigation and remediation of the intrusion which affected TV5Monde television network channel. This intrusion was allegedly conducted by the Fancy Bear/APT28 actor, and resulted into broadcasting and social media sabotage.

Read More

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.