Threatwatch

Play store spyware

A new piece of Android malware, dubbed ANDROIDOS_MOBSTSPY by Trend Micro, affected more than 100,000 users in 196 countries before Google removed it from the Play store, the security firm said. And although it's no longer available for download, the spyware continues to steal personal information from infected devices. It was hidden within six apps, one of which – Flappy Birr Dog – remained in the store for over a year. There's more information here: http://bit.ly/2C8p8h4.

New side channel attacks

A new side-channel attack is capable of extracting sensitive information from Windows and Linux PCs by examining page caches, according to a team of five academics and security researchers. Attacks using these techniques could even be carried out remotely in some cases. And because the attack works at the operating system level and is wholly software based, it is hardware agnostic, meaning it doesn't matter what architecture the machine is running on. The exploit abuses the mincore system call for Linux and the QueryWorkingSetEx system call for Windows to force disk writes or loads during which an attacker can work out what kind of data was in the cache. There are full details in the paper at: https://arxiv.org/pdf/1901.01161.pdf.

Facial fail

The Consumers Association in the Netherlands has found that, of 110 smartphones using facial recognition for unlocking, 42 could be fooled using a photograph of the owner. They included devices from top brands such as Alcatel, Asus, Blackberry, Huawei, LG, Motorola, Nokia, Samsung, Sony and Xiaomi, although the nine Apple iPhone models tested all resisted this form of attack. Full details (in Dutch) are here: http://bit.ly/2CVBPxs.

Cisco privilege escalation

Tenable has uncovered a privilege escalation vulnerability in Cisco's Adaptive Security Appliance (ASAv). If certain configurations settings are set, ordinary users can run commands that normally requiring high-level privileges. Using only HTTP requests, a user could change or download the current configuration and even replace the firmware. ASAv is a virtual solution that provides similar capabilities to Cisco's physical devices, including firewall, intrusion prevention and VPN. The problem affects Adaptive Security Appliance 9.9.2 and Cisco has designated the vulnerability as CVE-2018-15465. There's more information here: http://bit.ly/2TBpuE5.

Tampermonkey blacklisted

A version of the Tampermonkey plugin is being blocked by the Opera browser because it is being abused by malware. Tampermonkey is used to run 'userscripts' that add functionality to websites, such as being able to download YouTube videos. However, version 4.7.54, which is available from the Chrome Web Store, was being installed by malware via Opera and Chrome's alternative distribution options. While the plugin is now being blocked by Opera, the firm has not made it clear exactly how it is being exploited: however, BleepingComputer found that at least one piece of ad injection malware was using the software. There's more here: http://bit.ly/2M1Z4ZO.

confident in their organisation's ability to recover their data in time to avoid business or customer disruption. More than half (56%) of organisations don't have a recovery plan in place and nearly 70% of executives believe that cyber attacks are a data security issue rather than a recovery one."

The report is available here: http://bit.ly/2SNIGOM.

Avast report highlights IoT vulnerabilities

The latest 'Threat Landscape Report' from Avast highlights the problem of vulnerable Internet of Things (IoT) devices which form a key element in an ever-growing attack surface.

Some form of Internet connection will soon become the norm for electronic devices, Avast claims, yet security continues to be an afterthought, if it's considered at all. This is greatly contributing to an attack surface that is growing faster than at any time in history.

"While the biggest brand names' smart devices often come with embedded security options, some producers skimp on security either to keep costs low for consumers or because they are not experts in security," says the report. "Considering a smart home is only as safe as its weakest link, this is a mistake. History tends to repeat itself and so we can expect to see IoT malware evolve, becoming more sophisticated and dangerous, similar to how PC and mobile malware evolved."

The report particularly cites the problem of insecure home routers. We've already seen instances of routers being infected to form botnets that were subsequently used to mount distributed denial of service (DDoS) attacks or perform crypto-mining. But Avast claims there is worse to come.

"In 2019, we expect to see hijacked routers used to steal banking credentials, for example, where an infected router injects a malicious HTML frame to specific web pages when displayed on mobile," it says. "This new element could ask mobile users to install a new banking app, for instance and the malicious app will then capture authentication messages. In 2018, we observed a content injection method with coinmining elements on Mikrotik routers and in 2019 we expect to see this both escalate in number and to diversify in how content injection capabilities are used."

The report is available here: http://bit.ly/2REihG6.

North Korean defectors targeted

Personal information concerning nearly 1,000 people who defected from North Korea has been hacked.

A phishing attack against one of the 25 'Hana' centres in South Korea, which provide support to defectors, succeeded in gaining access to at least one computer.

"Recognising a possibility of one personal computer at the Hana Centre in North Gyeongsang Province having been hacked, we carried out an onsite probe on December 19 in co-operation with the provincial government and the centre and confirmed the computer was infected with a malicious code," the Ministry of Unification said. "In that computer, there was a file containing personal information of North Korean defectors. The file was confirmed to have been leaked."

An internal email account was hijacked to make the phishing attack appear more credible. The data accessed included names, birth dates and current physical addresses.

The South Korean Government currently provides assistance, including jobs, medical and legal support, to around 32,000 defectors from the north.