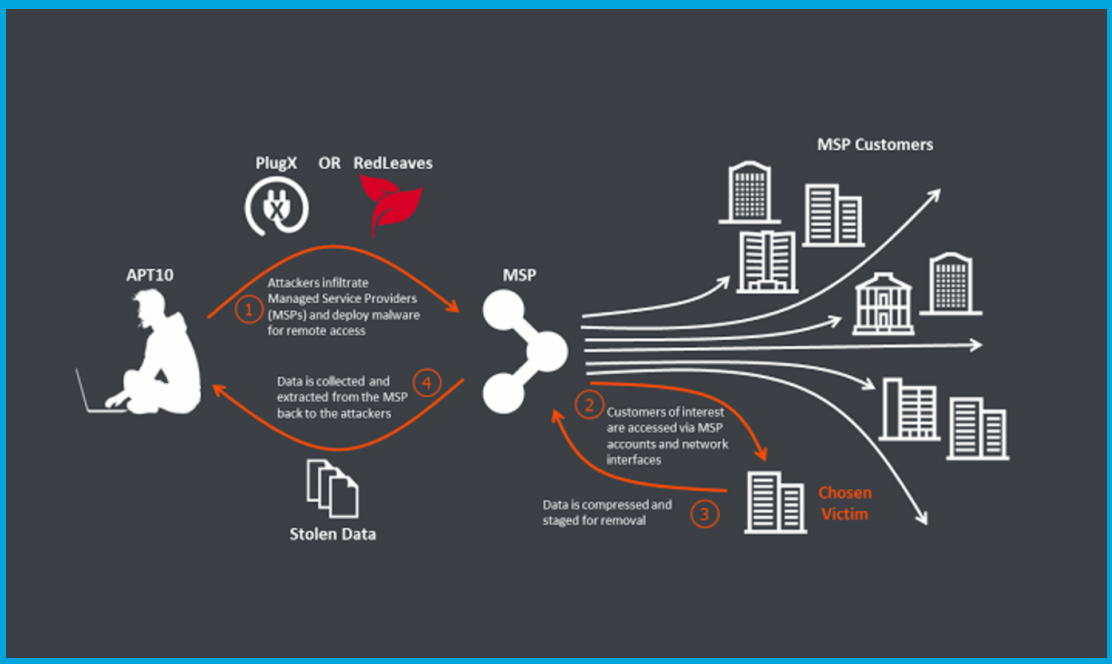
Security Newsletter

7 April 2017

Chinese Group Hacking Cloud Providers to Reach Into Secure Enterprise Networks



A cyber-espionage group that first surfaced in 2009 is using a novel tactic into hacking its targets by first breaching one of its cloud service providers, and then reaching inside the company's secure business network via the cloud service's approved communications channels.

This group's decision to hack the cloud service providers comes as these services are becoming more ubiquitous in enterprise networks, and almost all companies use one or more cloud services to handle some type of activity, may it be human resource management, inventory activities, email, or file sharing and hosting.

BAE and PwC didn't reveal a list of hacked cloud service providers, but the report also includes Indicators of Compromise (IoC), if sysadmins need to update their firewalls and security platforms.

Assessing the security of third parties before contracting with them is essential, but not sufficient. The industry will need to improve active monitoring of business dependancies if we want to efficiently prevent attacks in the future.

Read More

How To Secure Your Web App With HTTP Headers

In 2016, approximately 40% of data breaches originated from attacks on web apps. These days, understanding cyber-security is not a luxury but rather a necessity for web developers, especially for developers who build consumer-facing applications.

HTTP response headers can be leveraged to tighten up the security of web apps, typically just by adding a few lines of code. In this article, the author shows how web developers can use HTTP headers to build secure apps. While the code examples are for Node.js, setting HTTP response headers is supported across all major server-side-rendering platforms and is typically simple to set up.

This article covers disabling caching of confidential information, enforcing HTTPS, enhancing protection against XSS attacks, blocking click-jacking techniques, and more. **Remember that for the web to be truly awesome and engaging, it has to be secure.**

Read More

Check your site

No More Ransom — 15 New Ransomware Decryption Tools Available for Free

Started as a joint initiative by Europol, the Dutch National Police, Intel Security and Kaspersky Lab, No More Ransom is an anti-ransomware cross-industry initiative to help ransomware victims recover their data without having to pay ransom to cyber criminals. The online website not just educates computer users to protect themselves from ransomware, but also provides a collection of free decryption tools.

Keep in mind ransomware is not a end-user only issue. Crooks are more and more startingto leverage well-spread vulnerabilities to penetrate production servers and ask for ransom. This happened recently with the Apache Struts vulnerability we discussed in the newsletter on March 10.

Preventing your system from being encrypted by ransomware with adequate security awareness, vulnerability patching and proper antivirus protection, as having backups in case you fail, will always be the best strategy. However, sometimes nothing goes to plan. As a last resort, don't forget to check on NoMoreRansom if a decryption tool is freely available.

Read More

Critical Xen hypervisor flaw endangers virtualized environments

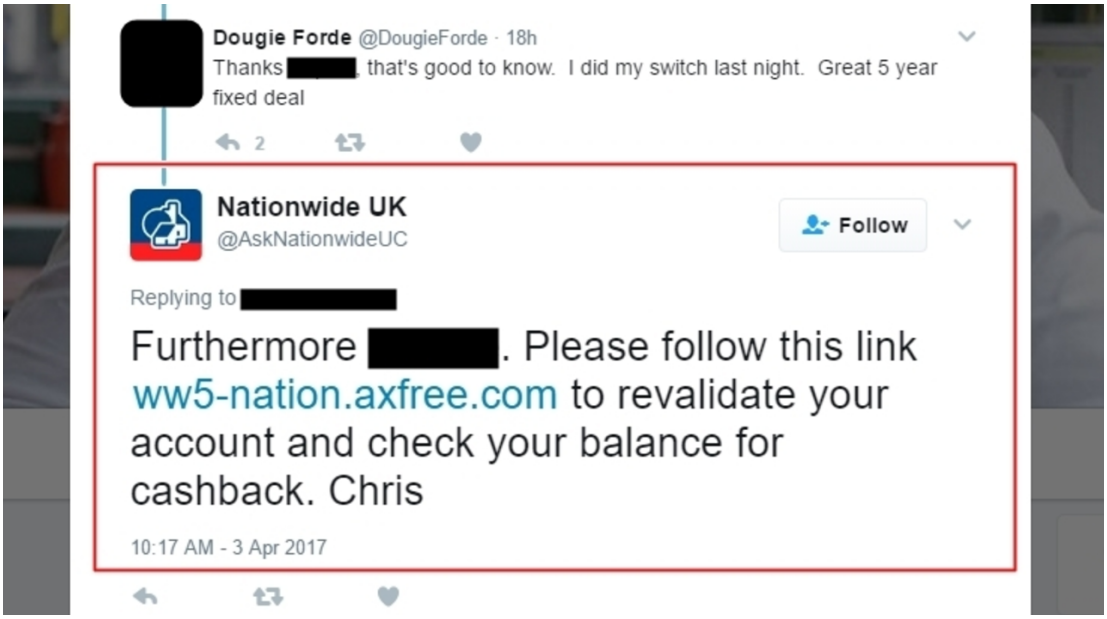
A critical vulnerability in the widely used Xen hypervisor allows attackers to break out of a guest operating system running inside a virtual machine and access the host system's entire memory.

This is a serious violation of the security barrier enforced by the hypervisor and poses a particular threat to multi-tenant data centers where the customers' virtualized servers share the same underlying hardware. The open-source Xen hypervisor is used by cloud computing providers and virtual private server hosting companies, as well as by security-oriented operating systems like Qubes OS.

The Xen project released a patch Tuesday that can be applied manually to vulnerable deployments. The good news is that the vulnerability can only be exploited from 64-bit paravirtualized guest operating systems. **Amazon Web Services said in an advisory that its customers' data and instances were not affected by this vulnerability and no customer action is required.**

Read More

Scammers Phishing for financial credentials on Twitter



Scammers are using Twitter as a vehicle to target people looking for customer support or asking general questions. They interject themselves into legitimate discussions, offering friendly chatter and a link that directs the target to a Phishing page designed to harvest credentials.

The scammers sign their messages with names, mimicking the real support accounts and adding an additional layer of legitimacy. In a flood of conversations on Twitter they might appear to be the real thing at a glance, and the target is already expecting a response.

The biggest red flag is the use of obvious unaffiliated domains on free hosting services like 16mb.com and axfree.com. However, at times the author has observed these Phishing accounts using the ow.ly URL shortening service as a mask. **Anyone asking for sensitive information via public channels (even verified accounts) should be treated as suspect.** If the matter is urgent or involves sensitive details, it's best to keep it off social media entirely and contact the bank via phone, or go to a local branch.

Read More

Samsung's Android Replacement, Tizen, Is a Hacker's Dream

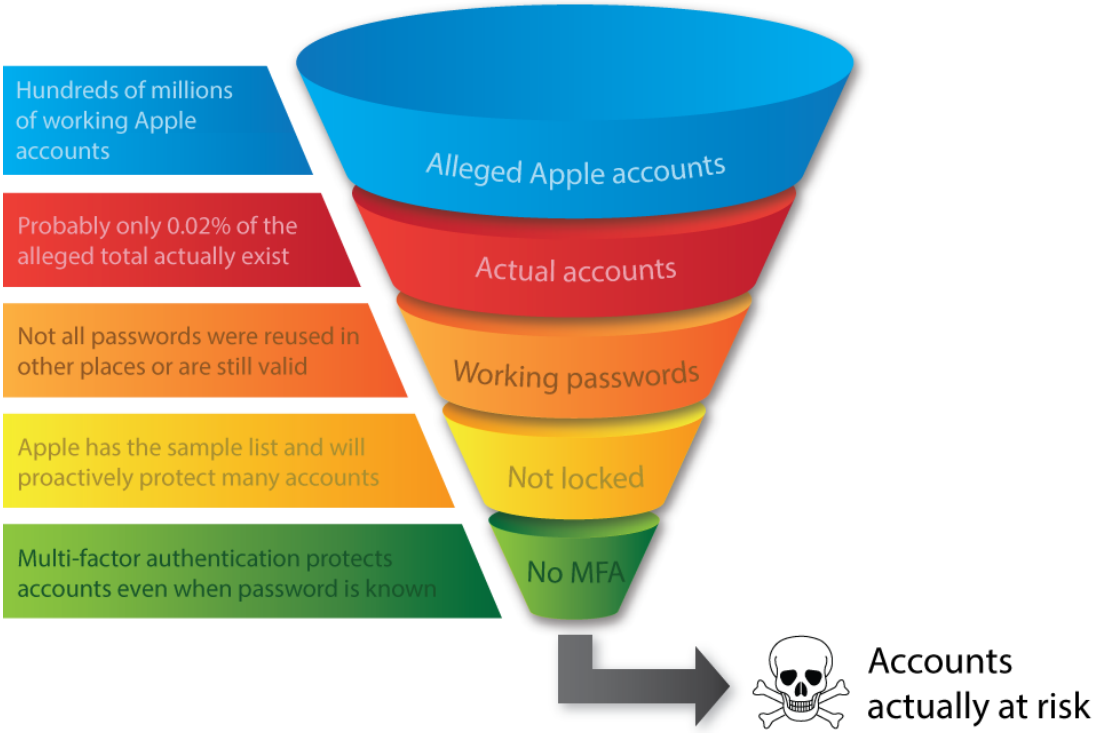
A researcher in Israel has uncovered 40 unknown vulnerabilities, or zero-days, that would allow someone to remotely hack millions of newer Samsung smart TVs, smart watches, and mobile phones already on the market, as well as ones slated for future release, without needing physical access to them. The security holes are in an open-source operating system called Tizen that Samsung has been rolling out in its devices over the last few years.

One security hole Neiderman uncovered was particularly critical. It involves Samsung's TizenStore app—Samsung's version of Google Play Store—which delivers apps and software updates to Tizen devices. Neiderman says a flaw in its design allowed him to hijack the software to deliver malicious code to his Samsung TV. Although TizenStore does use authentication to make sure only authorized Samsung software gets installed on a device, Neiderman found a heap-overflow vulnerability that gave him control before that authentication function kicked in.

Neiderman contacted Samsung months ago to report the problems he found but got only an automated email in response. When the journalist contacted the Korean company, a Samsung spokesperson sent a boilerplate response via email: *"Samsung Electronics takes security and privacy very seriously."*

Read More

Here's where the Apple accounts hackers are threatening to wipe came from



The tech news recently has seen quite a lot of chatter about an alleged haul of Apple credentials, apparently about 250 million of them in all, made by a group called the Turkish Crime Family (TCF). TCF tried to extort Apple as they threaten to delete account contents and remote-wipe Apple devices if payment isn't forthcoming by... today. The 7th of April. What data do they actually have?

By running Have I been pwned (HIBP) and having 2.6 billion accounts from various data breaches to refer to, Troy Hunt has got a great data set with which to reference incidents like this. In this article he describes what he has found and ultimately how he has identified where the vast majority of accounts have come from.

In a nutshell, **the list of Apple accounts is not hundreds of millions, it is instead less than 53k and it's compromised predominantly of accounts from the Evony data breach and a small handful of others.** The risk is no different to the one we're faced after every data breach: a bunch of people have reused their passwords and they're now going to have other accounts pwned as a result. That's a very different story to "hundreds of millions of Apple accounts will be reset and iPhones wiped".

I'll use this news as an opportunity to remind you that Troy Hunt's free service, Have I Been Pwned, allows you to find all email addresses on a particular domain you own that have been caught up in any of the data breaches currently in the system, in addition to notify you any future breaches of accounts on this domain. This is a great tool to warn your employees about possible password reuse attacks!

Read More

Have I Been Pwned?

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.