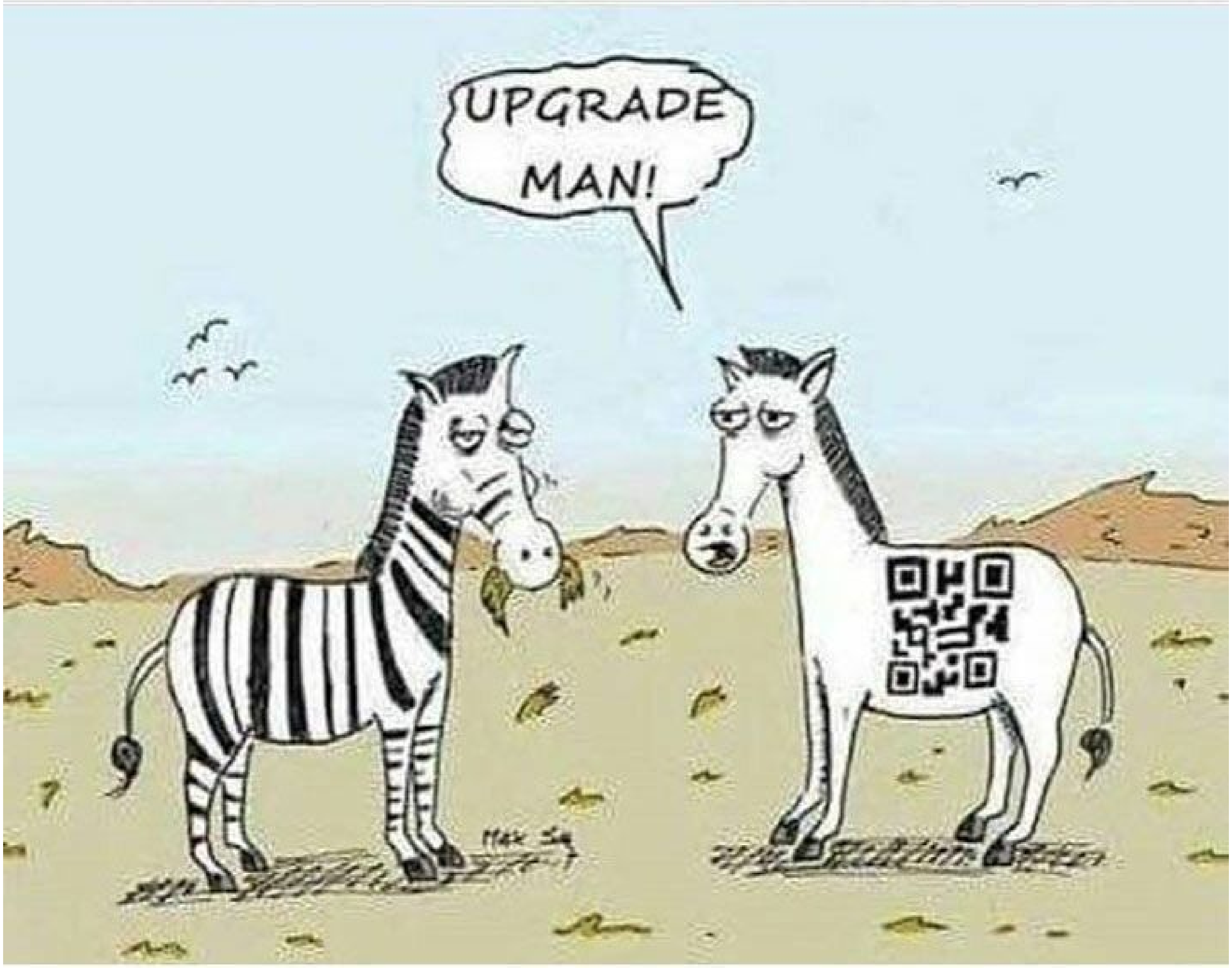
Security Now! #640 - 12-05-17

More News & Feedback

This week on Security Now!

This week we discuss the long-awaited end of StartCom & StartSSL, inside last week's macOS passwordless root account access and problems with Apple's patches, the question of Apple allowing 3D facial data access to apps, Facebook's new and controversial use of camera images, in-the-wild exploitation of one of last month's patched Windows vulnerabilities, an annoying evolution in browser-based cryptocurrency mining, exploitation of Unicode in eMail headers, Google's advancing protection for Android users, a terrific list of authentication dongle-supporting sites and services, Mirai finds another 100,000 exposed ZyXEL routers, Google moves to reduce system crashes, a bit of miscellany including another security-related Humble Bundle offering and some closing the loop feedback from our terrific listeners.



Security News

StartCom says goodbye

A brief reminder of the troubled history of StartCom:

StartCom is a certificate authority based in Beijing, China which was primarily known for its StartSSL (certificate authority).
StartCom was operating branch offices in China, Hong Kong, the UK & Spain.

Then, due to multiple failures on the company's end, all Startcom certificates were removed from Mozilla Firefox in October 2016, from Google's Chrome in March 2017.

It was then discovered, due to some website shenanigans, that StartCom had been secretly acquired by WoSign Limited in Shenzen, Guangdong, China, through multiple companies, which also came to light during Mozilla's investigation related to the root certificate removal of WoSign and StartCom in 2016. Due to the sanctions of both Mozilla and Apple, the company announced it would be restructured during 2016 by WoSign parent Qihoo 360 Group, detaching StartCom from the beleaguered WoSign and making it a subsidiary of Qihoo.

At one point we noted here that StartCom's website was making some quite questionable and worrisome "fire sale" style offers:

- UNLIMITED number of 2-year Extended Validation SSL Certificates for FREE - up to 99 domains
- UNLIMITED number of 2-year Organization Validation SSL Certificates for FREE – multi-domain and wildcard
- UNLIMITED number of 3-year Organization Client Certificates for FREE
- ONE 3-year Code Signing Certificate - including kernel signing

A few week ago, on November 16th, 2017 StartCom announced termination of business.

Termination of StartCom business / 16th Nov. 2017

StartCom has played a critical role as a Certification Authority in data security and electronic commerce by providing an independent "trusted third party" guarantee all these years.

Around a year ago the majority of the browser makers decided to distrust StartCom, remove the StartCom root certificates from their root stores and not accept newly end entity certificates issued by StartCom.
Despite the efforts made during this time by StartCom, up to now, there has not been any clear indication from the browsers that StartCom would be able to regain the trust. Therefore, the owners of StartCom have decided to terminate StartCom as a Certification Authority (CA).

From January 1st, 2018, StartCom will not issue any new end entity certificate and will only provide validation services through its OCSP and CRL services for two years from January 1st, 2018. Starting 2020, all remaining valid certificates will be revoked.

StartCom wants to thank all of our customers and partners during these years for their support.

Why <blank> Gets You Root
... Tracking down the cause of a serious authentication flaw
https://objective-see.com/blog/blog_0x24.html

Patrick Wardle is the Chief Security Researcher of R&D at Synack. Objective-See ('S' 'E' 'E') is his site where he states:

"As Macs become more prevalent, so does macOS malware. Unfortunately, current Mac security and anti-virus software is fairly trivial to generically bypass. Objective-See was created to provide simple, yet effective OS X security tools. Always free of charge - no strings attached! I created Objective-See to publish the personal tools that I've created to secure my Mac computer.

Remember how a user needed to attempt to login as ROOT several times? It didn't work the first time? It turns out that what THAT was about was... As things stood last week, when a user (or an attacker) attempts to log into an account that is not currently enabled (i.e. root), for some unknown reason, the system will naively create that account with whatever password the user specifies...even if that password is blank. Then the user (or attacker) can readily log into that account.

So the first attempt enables the account and accepts whatever password -- even blank. And the SECOND attempt logs the user into the now-enabled account with that same (blank) password. Whoops!

... and, yes, it does also work remotely.

Function "od_verify_crypt_password" returns apparent success when it should not. The system assumes this means that the user-supplied password was correct, and so it is accepted. It turned out, though, that the non-zero return value from the function meant that the comparison process itself succeeded... NOT THAT THE password hashes matched! The password match information was returned in a different register... and was being ignored!

Apple Responds:

Shortly after posting this blog, Apple released a patch for both macOS 10.13 and 10.13.1.

The bug was assigned CVE-2017-13872, and Apple states in the security release notes that "a logic error existed in the validation of credentials." Their patch, they note, "improved credential validation."

Yeah... ya think???

What did the identical patches do? As expected, they now check the result of the 'match' variable after the call to od_verify_crypt_password, not just the success of the request to compare.

However, as we'll see... that was NOT the end of the story...

MacOS Update Accidentally Undoes Apple's "Root" Bug Patch
First: The application of the patch for High Sierra 10.13.1 broke file sharing for some users.
https://support.apple.com/en-us/HT208317
Not difficult to fix. User can use Terminal commands to get things working again. But that will eventually be needing yet another patch patch to fix that correctly.

But a bit more concerning is that if a user HAD patched their v10.13 macOS then upgraded to 10.13.1, THAT upgrade reintroduced the root login bug which was also originally present in v10.13.1. So, somehow, Apple failed to incorporate the fix into the latest OS release.

And... if the user of the now re-buggy v10.13.1 re-patched, the patch would not actually take effect until after a system reboot, though there was no indication that this was the case.

Apple's iPhone X realtime facial mapping data is available to apps.
The Washington Post: Apple is sharing your face with apps. That's a new privacy worry.
https://www.washingtonpost.com/news/the-switch/wp/2017/11/30/apple-is-sharing-your-face-with-apps-thats-a-new-privacy-worry/
https://measurekit.com/

"This app wants to access your camera."

Facebook Tests New CAPTCHA Tool That Asks Users to Upload a Photo of Their Face
https://www.bleepingcomputer.com/news/technology/facebook-tests-new-captcha-tool-that-asks-users-to-upload-a-photo-of-their-face/

Facebook is reportedly testing a new CAPTCHA system that requires users to upload a clear photo of their face to prove the account is not fake and belongs to a new person.

So, in other words, at various points in Facebook's authentication flow, Facebook may require its users to aim their smartphone's camera at their face to provide a unique and never-before-seen image of the user.

The new tests were first spotted last week by a US user and were reported by our friends at Bleeping Computer. The user wrote:

"Facebook is now locking users out of account features, then requiring that those users "verify" their account to get back in by scanning an image of their face."

The text for this new CAPTCHA test reads: "Please upload a photo of yourself that clearly shows your face. We'll check it and then permanently delete it from our servers."

This new system is designed to catch and block the creation of fraudulent and automated accounts.

Facebook confirmed the new CAPTCHA system and said its role is to "catch suspicious activity at various points of interaction on the site."

The new CAPTCHA system is automated, uses facial recognition, and requires the use of unique photos to prevent bots from taking existing photos of random people off the Internet or from other Facebook accounts to authenticate.

Facebook stated that the new CAPTCHA system is likely to pop up when users register new accounts, send friend requests, or set up or edit Facebook ads. At the moment, the new system is still under testing and they will not share details now or later to prevent manipulation.

And, as was reported elsewhere on the TWiT network recently, Facebook has been asking potential victims of revenge porn to upload nude photos of themselves in advance... so that those images can then be proactively blocked. The company said it would create a hash of the nude photo and using this hash, would ban other persons from uploading a copy of the image. While Facebook initially said that the system was fully automatic, the company later admitted that a Facebook employee would be manually reviewing all nude photo uploads.

Hackers Exploit Recently Disclosed Microsoft Office Bug to Backdoor PCs
Last month's Microsoft Patch Tuesday saw 53 vulnerabilities patched... and among them was a 17-year-old flaw in Microsoft Office which allows miscreants to install malware without any user interaction.

All versions of Microsoft Office released in the past 17 years were vulnerable to remote code execution flaw (CVE-2017-11882) that works against all versions of Windows operating system through and including the latest Microsoft Windows 10 Creators Update.

The ancient flaw exists in the longstanding DDE (Dynamic Data Exchange) subsystem which, due to improper memory operations, fails to properly handle objects in the memory, corrupting it in such a way that attackers can execute malicious code in the context of the logged-in user.

Exploitation of this vulnerability requires opening a specially crafted malicious file with an affected version of Microsoft Office or Microsoft WordPad software, which could allow attackers to remotely install malware on targeted computers.

And... it's happening now in the wild: A malicious RTF document with a .DOC extension leverage DDE to launch a PowerShell script which, in turn, runs a component of the "Cobalt Strike" pentesting library (https://www.cobaltstrike.com/) to then install malware into a user's machine after they open the malicious document. So it's not wormable -- SOME user interaction is required -- but merely opening and observing a document attachment.

So, our takeaway here is: Be very sure that you have applied last month's patches across all systems, and even when THIS problem is fixed, use this as yet another example of why everyone should always be cautious and suspicious when opening documents sent via eMail.

Chrome browser based cryptocurrency mining runs after Chrome is closed.
https://thehackernews.com/2017/11/cryptocurrency-mining-javascript.html

The recent rise in Bitcoin price has created increased pressure to steal mining cycles from website visitors.

As we've previously reported, most of this mining appears to be injected by third parties, but that may also change as Bitcoins become increasingly valuable. And mining pools allow incremental value to be extracted for all work done.

So, now, we've seen some evolution in hacker cleverness. The Chrome browser uses a process-per-tab or window model, and the guys at MalewareBytes have found websites spawning a tiny and unseen "pop-under" window which can hide mining code... and which will, since it's in a separate window from Chrome and running in its own Windows process, continue running even after Chrome has been closed. Their blog posting last Wednesday was titled: "Persistent drive-by cryptomining coming to a browser near you."

MalwareBytes: "Since our last blog on drive-by cryptomining, we are witnessing more and more cases of abuse involving the infamous Coinhive service that allows websites to use their visitors to mine the Monero cryptocurrency. Servers continue to get hacked with mining code, and plugins get hijacked and affect hundreds or even thousands of sites at once.

One of the major drawbacks of web-based cryptomining we mentioned in our paper was its ephemeral nature compared to persistent malware that can run a miner for as long as the computer remains infected. Indeed, when users close their browser, the cryptomining activity will also stop, thereby cutting out the perpetrators' profit.

However, we have come across a technique that allows dubious website owners or attackers that have compromised sites to keep mining for Monero even after the browser window is closed. Our tests were conducted using the latest version of the Google Chrome browser. Results may vary with other browsers. What we observed was the following:

- A user visits a website, which silently loads cryptomining code.
- CPU activity rises but is not maxed out.
- The user leaves the site and closes the Chrome window.
- CPU activity remains higher than normal as cryptomining continues.

Okay... So the pop-under mining window will still have a visible presence on the toolbar, but many users may miss that. And any power user examining running tasks will see not only a persistent Chrome.exe process... but also that it is using up approximately 50% of the system's CPU resource. The hidden miners avoid being too greedy with sucking up CPU since they wish to remain hidden as long as possible.

What a world!... let's step back for a second and think about this:

MailSploit — Email Spoofing Flaw Affects Over 30 Popular Email Clients
https://www.mailsploit.com/index
Researcher Sabri Haddouche is a developer, pentester (penetration tester), bug hunter & privacy advocate. His day job is as part of the security team at Wire... and in his free time he dabbles with his own security project such as this one:

RFC1342 dating from 1992: "Representation of Non-ASCII Text in Internet Message Headers"
In other words, how to allow UNICODE characters in eMail To, From, and other headers.
(What could POSSIBLY go wrong?)

We're wrapping our eMail in anti-spoofing DMARC / DKIM / SPF signatures to prevent header spoofing. But the abuse of specially crafted UNICODE eMail headers allows the fraudulent sender to send an authentic fraudulent eMail which is valid from the spoofer... which all intermediate MTAs will check and happily forward... but which the user's eMail client will DISPLAY as being from another sender.

The spoofing bug was found and confirmed in 33 different products.

All vendors were contacted at least 3 months prior to the publication (which was today), some of them 4 or 5 months before the publication. As of Dec 5th 2017:

- It was fixed in 8 products (~ 24%)
- Triaged for 12 additional products (~ 36%)
- Two vendors (Mozilla and Opera) said they won’t fix the bug (they consider it to be a server-side problem) and another one (Mailbird) closed the ticket without responding.

As for the remaining 12 products (~ 36%), the vendors have received the bug report but have not commented on whether they will address it.

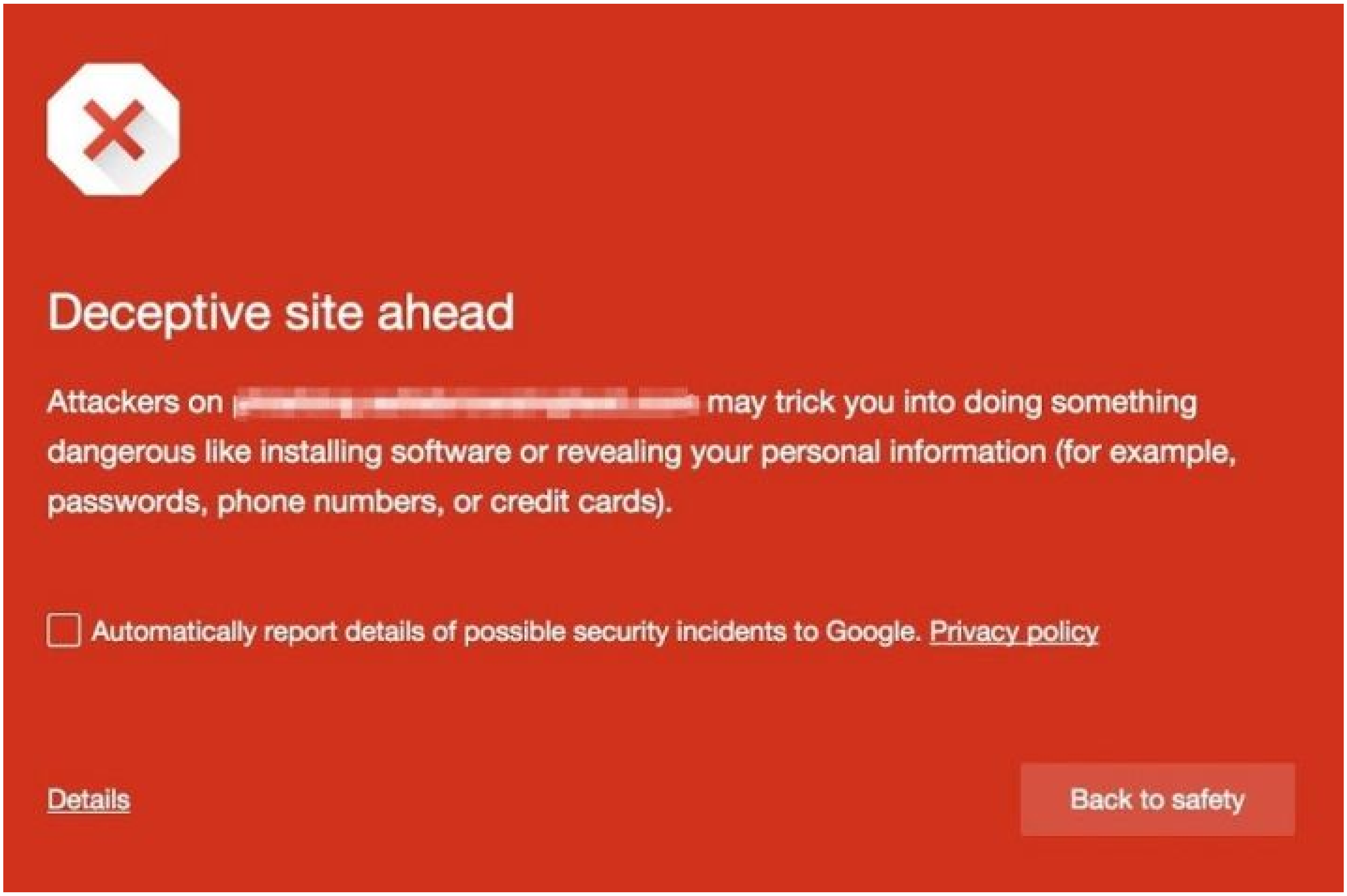
https://docs.google.com/spreadsheets/d/1jkb_ZybbAoUA43K902lL-sB7c1HMQ78-fhQ8nowJCQk/edit#gid=0

Note that in some instances this also creates a significant XSS (Cross-Site Scripting) vulnerability which a number of clients could fall victim to, and which some have addressed.

The response to this is been somewhat disappointing... so one wonders whether we're going to be seeing this technique employed and deployed by future spoofers.

Additional protections by Safe Browsing for Android users
Posted Friday by the Safe Browsing Team
https://security.googleblog.com/2017/12/additional-protections-by-safe-browsing.html

In our efforts to protect users and serve developers, the Google Safe Browsing team has expanded enforcement of Google's Unwanted Software Policy to further tamp down on unwanted and harmful mobile behaviors on Android. As part of this expanded enforcement, Google Safe Browsing will show warnings on apps and on websites leading to apps that collect a user’s personal data without their consent.



Deceptive site ahead

Attackers on [redacted] may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards).

□ Automatically report details of possible security incidents to Google. Privacy policy

Apps handling personal user data (such as user phone number or email), or device data will be required to prompt users and to provide their own privacy policy in the app. Additionally, if an app collects and transmits personal data unrelated to the functionality of the app then, prior to collection and transmission, the app must prominently highlight how the user data will be used and have the user provide affirmative consent for such use.

These data collection requirements apply to all functions of the app. For example, during analytics and crash reportings, the list of installed packages unrelated to the app may not be transmitted from the device without prominent disclosure and affirmative consent. These requirements apply to apps in Google Play and non-Play app markets. The Google Play team has also published guidelines for how Play apps should handle user data and provide disclosure.

Starting in 60 days, this expanded enforcement of Google's Unwanted Software Policy may result in warnings shown on user devices via Google Play Protect or on webpages that lead to these apps. Webmasters whose sites show warnings due to distribution of these apps should refer to the Search Console for guidance on remediation and resolution of the warnings. Developers whose apps show warnings should refer to guidance in the Unwanted Software Help Center. Developers can also request an app review using this article on App verification and appeals, which contains guidance applicable to apps in both Google Play and non-Play app stores. Apps published in Google Play have specific criteria to meet Google Play's enforcement of the Unwanted Software policy; these criteria are outlined in the Play August 2017 announcement.

First we had: Two Factor Auth (2FA) / List of websites and whether or not they support 2FA. https://twofactorauth.org/

Now we have "USB-Dongle Authentication" http://www.dongleauth.info/

List of websites and whether or not they support One Time Passwords (OTP) or Universal 2nd Factor (U2F). Also see the list of dongles and the protocol they support.

- Backup and Sync
- Cloud Computing
- Communication
- Cryptocurrencies
- Developer
- Domains
- Education
- Email
- Entertainment
- Finance
- Gaming
- Health
- Hosting/VPS
- Identity Management
- Investing
- Other
- Payments
- Remote Access
- Retail
- Security
- Social

The persistent danger presented by insecure internet-facing routers
Last week, researchers from China-based Netlab 360 spotted a new, publicly available Mirai variant.

The changes allowed the malware to spread to networking devices made by ZyXEL Communications that could be remotely accessed over telnet using default passwords. One of the exploits was published on October 31 -- but those routers were never updated.

Consequently, over a span of 60 hours starting on November 22, the newly enhanced stain of Mirai commandeered nearly 100,000 devices which almost without exception had IP addresses local to Argentina... suggesting that the outbreak was residing on the routers of customers of a regional ISP who was providing unsecured modems.

The governing CVE-2016-10401 vulnerability explains that affected ZyXEL devices all share the same fixed superuser password allowing remote attackers to obtain root access when a non-root account password is known. The exploit published on October 31 first logs in as a telnet user and then escalates privileges using the superuser password.

Fortunately, the two domains the attackers were using to control the newly infected devices were seized and quickly "sink-holed" which had the short-term effect of stopping the infection from spreading further and preventing the attackers from using the hijacked devices to cause Internet outages. But those 100,000 Internet-connected devices remain insecure, so they remain susceptible to takeover by any other Internet worms that might wish to take up residence.

Google to begin moving "code injectors" out of bounds.
Many Windows-resident external third-party applications such as accessibility or A/V software sink their hooks (literally) into web browsers through a proces known as code injection. This allows them to obtain the additional control they need to provide their required and additional features.

But... significant system instability occurs when this is done incorrectly. Google's telemetry has observed that over 15 percent of Chrome users running code-injecting third-party applications on their Windows machines experience crashes.

Consequently, in a Chromium Blog post last Thursday, Google announced its plan to roll-back and eventually block third-party software from injecting code into Chrome:

- April 2018 — With the release of Chrome 66, Google will begin informing users if code injection causes their browsers to crash, alerting them with the name of the responsible application and a guide to update or remove it.

- July 2018 — Chrome 68 will start blocking third-party software from injecting code into Chrome processes. But if this blocking prevents Chrome from starting, the browser will restart and allow the injection. But it will also display a warning for guiding users to remove that particular software.

- January 2019 — With no exception, starting with Chrome 72, Google will completely block code injection by any third-party software.

Google's timeline announcement notes that there are safe alternative means for achieving the same things -- using the Native Messaging API calls or create a Chrome extensions to add functionality to the web browser. According to Google, these methods can be used by developers to retain their app features without having to risk browser crashes.

SpinRite

Rana Omar
Location: Canberra, Australia
Subject: Spinrite yet again saves the day

Hi Steve,

Hope you and Leo are well. Big fan of the security now show. Love the work both of you do.

I thought I'd finally share my story on how spin rite saved my day (you would've probably had enough of these stories by now). After listening to you mentioning other spin rite users' feedback all these times, I thought I knew the ins and outs of the whole process but boy I was wrong.

I've had a single 3TB NAS drive which I had been using for years with all sorts of data on it. One day the drive suddenly died and I thought to myself that me being the spin rite expert (after listening to this pod cast), this will be walk in the park for me to restore.
In windows OS, the drive would show as MBR/RAW, and SpinRite wasn't completely happy with it either. I can't remember the exact message. I decided to pick up and scan the drive anyway. SpinRite encountered trouble that caused it to stop before it was completed. So I came to terms with the failure to complete the scan message and thought the drive is never going to be brought back. I let it go for few months and bought a new NAS with multiple drive bays.

I realised after a few weeks ago that you had mentioned a similar scenario, suddenly it dawned on me and I sprinted towards my PC to plug in the drive and to my surprise found out the drive started working and allowed me to backup almost all the data off it (there were few folders which I couldn't backup but they were not important anyway).

All this time, I didn't think to plug in the drive on my PC to check. I am so glad that I didn't throw the it away.

The lesson here is that if spin rite shows you that it had failed to complete the scan, in reality it has done enough "magic" to bring it back to life.

As always thank you very much for the awesome product, can't wait for the new version.
Keep up the good work.
Thank you.

Miscellany

Packet Clearing House - Points of Presence
https://www.pch.net/about/pops

Humble Bundle: Network & Security Certification (by Wiley)
https://www.humblebundle.com/books/network-security-certification-books

13 days.

$1:

- MCSA Windows Server 2012 R2 Installation and Configuration Study Guide: Exam 70-410
- MCSA Windows Server 2012 R2 Administration Study Guide: Exam 70-411
- MCSA Windows Server 2012 R2 Configuring Advanced Services Study Guide: Exam 70-412
- Mastering System Center 2012 R2 Configuration Manager
- Mastering Hyper-V 2012 R2 with System Center and Windows Azure

$8:

- CompTIA Network+ Study Guide Exam N10-006 Third Edition
- Cisco Networking Essentials / Second Edition
- Microsoft Windows Networking Essentials
- Data Storage Networking: Real World Skills for the CompTIA Storage+ Certification and Beyond

$15:

- CompTIA Security+ Study Guide: Exam SY0-401 / Sixth Edition
- Network Attacks and Exploitation: A Framework
- Network Security Bible / Second Edition
- Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails

Closing The Loop

nick / @theNickNiti
@SGgrc ios 11.2 is almost useable on my iphone 7.... looks like most “glitches” fixed, maybe apple actually qc’d this ver!

theblacktandog / @theblacktandog
@SGgrc Wow! Quad 9 and Firefox 57. ????

dan kutka @dkutka25
@SGgrc quad9 does have a secondary secure dns adress at 149.112.112.112 I do have some devices that require 2 unique dns address and this solves that issue

Tracy Lipp / @LA_in_Helsinki
@GibsonResearch I don’t think IOS is to blame with instability issues in your phone. I have the same phone. In Finland it works perfect. Just got to LA, am using T-Mobile & it’s terrible. Phone is occasionally unresponsive and unstable. It didn’t do this at all in Finland.

Yann Saint-Laurent @yannstlo
@SGgrc on the last episode of SN, you talk about an HP printer that the drive was encrypted, it gets swapped to a non encrypt-able then back to a FIPS Encrypted drive. If the drive is providing the encryption, how could it now be readable? Is the private key still in the printer?