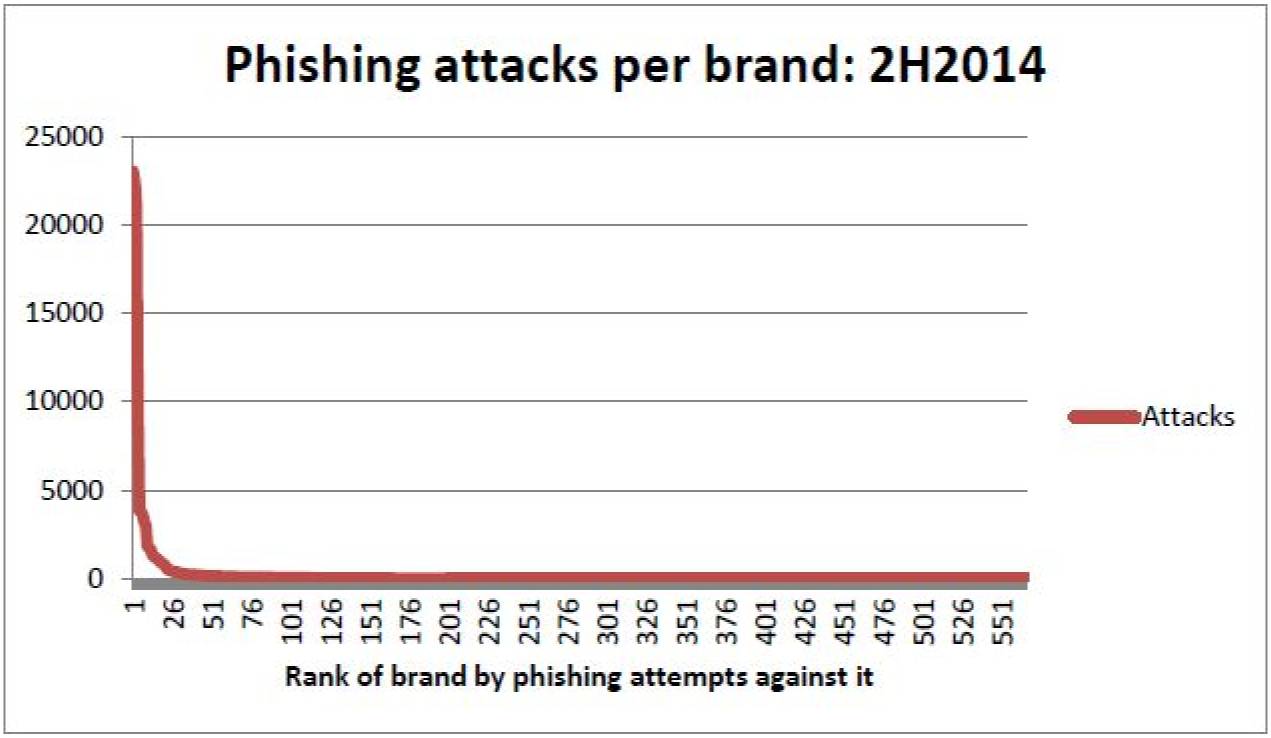
Security Now! #518 - 07-28-15

HORNET: A fix for TOR?

This week on Security Now!

- Fiat/Chrysler hacking follow-up.
- "StageFright" is right!
- The security practices of experts vs non-experts
- Major DMCA news
- The Anti-Phishing Working Group's Global Phishing Survey
- A terrific security webpage discovery.
- The right way to silence the Windows 10 upgrade pesterings.
- What is HORNET? Is it a fix for TOR?



Security News

Fiat Chrysler Recalls nearly 1.5 million Cars After Software Bug is Revealed.

- Car owners can download and install themselves.
- FCA is sending out USB drives to owners of all affected vehicles.
- Owners can take their auto in for service.
- Sprint quickly moved to close off the communications side of the attack.
- Chris Valasek tweeted, Friday: “Looks like I can’t get to [Charlie’s] Jeep from my house via my phone. Good job FCA/Sprint!”
- FCA US LLC Chronology / Select 2013-2015 Vehicles / RA3/4 Improved Vehicle Security Protection
  - http://www-odi.nhtsa.dot.gov/acms/cs/jaxrs/download/doc/UCM483034/RMISC-15V461-1264.pdf
  - <quote> A communications port was unintentionally left in an open condition allowing it to listen to and accept commands from unauthenticated sources. Additionally, the radio firewall rules were widely open by default which allowed external devices to communicate with the radio. To date, no instances related to this vulnerability have been reported or observed, except in a research setting.

Significant Android problem found in ubiquitious "StageFright" module.

- DefCon / BlackHat.
- Just short of a billion Android devices (95%) are at risk.
- <quote> Gaining remote code execution privileges merely by having access to the mobile number? Enter Stagefright.
- Zimperium Mobile Security
  - http://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/
- https://threatpost.com/android-stagefright-flaws-put-950-million-devices-at-risk/113960
- http://www.darkreading.com/vulnerabilities---threats/stagefright-android-bug-heartbleed-for-mobile-but-harder-to-patch/d/d-id/1321477
- No user interaction required -- just send the phone an MMS message.
- For maximum performance, "Stagefright" is pure C++, thus, unlike with Java in a JVM, with full access to the system and full responsibility placed on the programmer.
- Android and derivative devices after and including version 2.2 are vulnerable.
- Devices running Android versions prior to Jelly Bean (roughly 11% of devices) are at the worst risk due to inadequate exploit mitigations.
- About a dozen problems were identified, about half allow for remote code execution.
- Seven CVE's have been assigned/reserved:
  - CVE-2015-1538, 1539, 3824, 3826, 3827, 3828, 3829
- Fixes for these issues require an OTA firmware update for all affected devices.
- Updates for Android devices have traditionally taken a long time to reach users.
- Devices older than 18 months are unlikely to receive an update at all.
- The Android ecosystem needs to recognize the severity and take immediate action.
- The Android ecosystem also needs to reconsider the business processes that prevent or slow the uptake of such fixes.
- SilentCircle's Blackphone and Mozilla Firefox since v38 are patched.
- POC will be released after the August conferences.

New research: Comparing how security experts and non-experts stay safe online

- USENIX Symposium on Usable Privacy and Security, July 22–24, 2015, Ottawa, Canada.
- http://googleonlinesecurity.blogspot.com/2015/07/new-research-comparing-how-security.html
- https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf
- 231 security experts who have at least five self-reported years in security.
- 294 regular non-expert computer users.

DMCA News:

- Court Backs Dismissal of Digital Copyright Claim
- Judge Emilio Garza, New Orleans 5th Circuit Court of Appeals:
  - "Merely bypassing a technological protection that restricts a user from viewing or using a work is insufficient to trigger the Digital Millennium Copyright Act's anti-circumvention provision."
  - http://www.courthousenews.com/2010/07/23/29099.htm
- General Electric did not infringe on a power supplier's digital copyrights when it used protected software unlocked through a hacked security key, the 5th Circuit ruled.
- "The DMCA prohibits only forms of access that would violate or impinge on the protections that the Copyright Act otherwise affords copyright owners."
- The ruling stems from a lawsuit filed by MGE UPS Systems, a manufacturer of uninterruptible power supply machines used by companies like Power Maintenance International (PMI), which was bought by GE in 2001. To fix the machines, technicians have to use MGE's copyrighted software programs. The software can be unlocked with an external hardware security key, called a "dongle." Dongles have expiration dates, passwords and a maximum number of uses. Years after MGE introduced this technology, hackers posted information online on how to bypass the hardware key. Once a key is cracked, the software can be freely used and copied.

  In its lawsuit against GE and PMI, MGE claimed a group of PMI employees had at least one copy of software obtained from a hacked machine. It said GE used the software 428 times between June 2000 and May 2002, even after a judge barred GE from using MGE's software and trade secrets.

  A jury awarded MGE more than $4.6 million in damages for copyright infringement and misappropriation of trade secrets, but the trial judge dismissed its Digital Millennium Copyright Act claim.

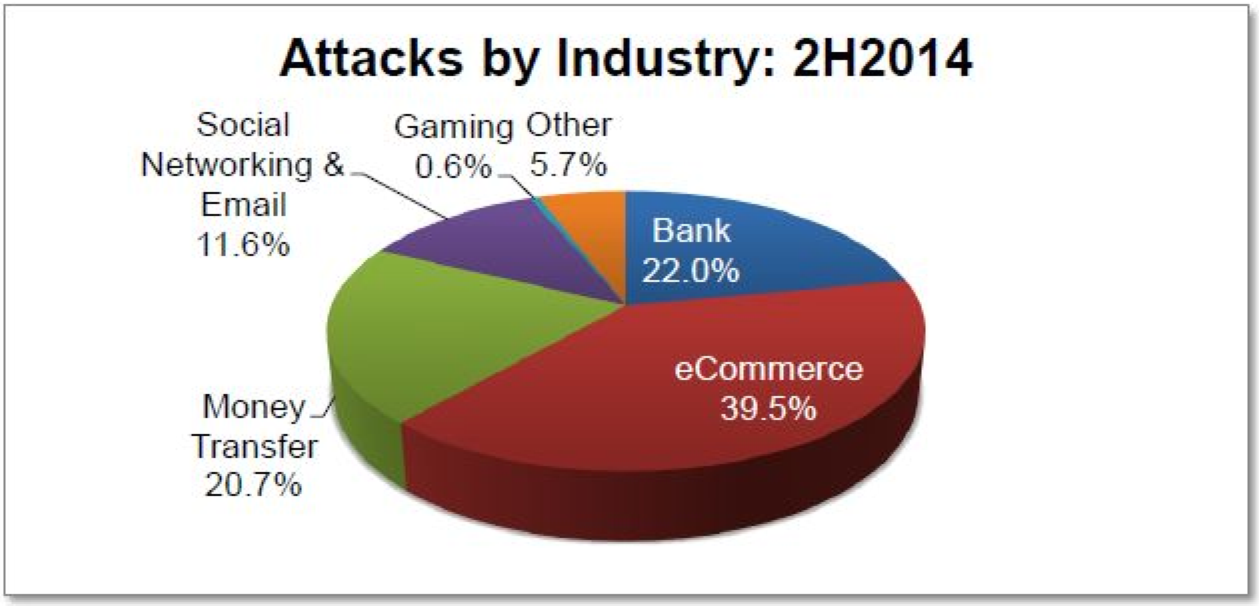
  MGE appealed, arguing that its dongles barred the kind of access to its software that the Act is meant to prevent.

  But the 5th Circuit said MGE "advances too broad a definition of 'access.'"

  "Without showing a link between 'access' and 'protection' of the copyrighted work, the DMCA's anti-circumvention provision does not apply. The owner's technological measure must protect the copyrighted material against an infringement of a right that the Copyright Act protects, not from mere use or viewing."
- http://www.ca5.uscourts.gov/opinions%5Cpub%5C08/08-10521-CV0.wpd.pdf

The Anti-Phishing Working Group (APWG) recently released their Global Phishing Survey

- https://blog.digicert.com/survey-finds-123972-unique-phishing-attacks-worldwide/
- http://internetidentity.com/wp-content/uploads/2015/05/APWG_Global_Phishing_Report_2H_2014.pdf
- There were at least 123,972 unique phishing attacks worldwide.
    - An attack is defined as a phishing site that targets a specific brand or entity.
- The attacks occurred on 95,321 unique domain names.
    - The most ever recorded in a half-year period.
- The number of domain names in the world grew from 279.5 million in April 2014 to 287.3 million in December 2014. (7.8 million in 9 months)
- 95,321 breakdown:
    - 27,253 malicious registrations for the purpose.
    - 68,303 were hacked or compromised web hosting.
- 75% of malicious registrations were in just 5 TLDs:
    - .COM, .TK, .PW, .CF, and .NET.
- 569 targeted institutions.
- Average attack uptime was ~30 hours.
- Median uptime was ~10 hours.
- So half of all phishing attacks are up for at least 10 hours.
- Attacks occurred in 272 TLDs, 56 of them new.
- Only ~2 percent of all phishing domain names contained a brand name or variation.
- Distribution is HEAVILY SKEWED:
- 3/4th of attacks were against the top 10 targets.
    - Top 3: Apple, PayPal, and Taobao.com
- Each suffered over 20,000 phishing attacks against their respective services and brands.
- These top three were the targets of nearly 54 percent of the world's phishing attacks.



Fabulous Security Information Aggregation Page: InfoSecIndustry

- http://www.infosecindustry.com/
- Similar to: https://www.privacytools.io/

How to permanently shutdown Windows 10 upgrade notification

- http://winsupersite.com/windows-10/disabling-windows-10-upgrade-notification
- "GWX" - Get Winows 10
- HKLM\SOFTWARE\Policies\Microsoft\Windows\GWX
  - DWORD value DisableGWX set to 1

Miscellany:

Over the weekend I read "The Martian"

- "Read"... as in raster-scanned printed pages of text.
- Only one huge mistake that stood out

Errata:

System Restore does NOT FIX user files... only the system's files.

- I knew better! :(

SpinRite:

Jason Robohm in Allen, Texas
Subject: Home Security DVR - HD Failure / Recovery
Date: Wed, 15 Jul 2015 13:38:45 -0000

Steve,

I wanted to pass along a testimonial on SpinRite. We have an alarm company (ADT Pulse) provided DVR for the cameras outside our home. Recently the DVR's alarm was periodically sounding (all hours of the night as one would expect - thank you Murphy) letting us know the HD was in an error state. Rebooting the DVR only seemed to make the HD error alarms more frequent. So we just unplugged it to get some sleep. After three failed ADT service appointments to replace the DVR unit, I figured it couldn't hurt to crack the DVR open and see what was inside - a simple 1TB WD Green SATA HD. Seeing that, I quickly grabbed my trusty copy of SpinRite, attached the DVR's HD to my PC's SATA cable, and booted up into SpinRite. 90min later - running on setting #2 - SpinRite declared it was done. Interestingly enough, SpinRite did not show any errors / corrected sectors?!? Having heard that this is common when SpinRite induces the drive to fix itself by showing it its own problems, I shrugged and placed the SpinRite'ed HD back into the DVR unit and powered it up. Guess what - NO HD Alarm and a fully functional DVD. All of the recorded video streams are still there as well!

Thank you Steve for such a great product and I know we all look forward to 6.1+ versions in the near future!

Sincerely,
Jason

HORNET: A new high-speed anonymity network

"HORNET" : High-Speed Onion Routing at the NETwork layer.

Five researchers from the UK, US, and Switzerland.

- http://www.dailydot.com/politics/hornet-tor-anonymity-network/
- http://arxiv.org/abs/1507.05724v1

Network Layers:

- HTTP (application layer)
- TLS - SSL (session layer) - Secure Sockets LAYER
- TCP / UDP (transport layer)
- IP (network layer)
- Ethernet / ATM / Frame Relay (data link layer)
- Physical

Bottom Line:

- A fix for TOR's performance problem (at HUGE COST)
- NOT a fix for TOR's broken anonymity guarantees.
    - But... =IF= it was ever Internet wide?? Hmmmm.