Security Now! #566 - 06-28-16

Q&A #236

This week on Security Now!

- One Windows update was expensive for Microsoft
- A troubling court ruling about FBI hacking
- Hope for slow Windows 7 updates
- Comodo dips to a new low level of slimy behavior
- Malware moves to pure JavaScript
- Yet another way to exfiltrate data from an air-gapped computer
- A worrisome flaw found in most NetGear routers
- The COOLEST and truly brilliant idea of the year
- A bunch of quick miscellany
- And ten questions and comments from our terrific listeners!

Security News

(This week's TOP Tweet:)
Unwanted Windows 10 upgrade costs Microsoft $10,000
http://www.seattletimes.com/business/microsoft/microsoft-draws-flak-for-pushing-windows-10-on-pc-users/

- Matt Day / Seattle Times: (quotes MaryJo and Paul, too.)
  A few days after Microsoft released Windows 10 to the public last year, Teri Goldstein's computer started trying to download and install the new operating system.

  The update, which she says she didn't authorize, failed. Instead, the computer she uses to run her Sausalito, Calif., travel-agency business slowed to a crawl. It would crash, she says, and be unusable for days at a time.

  "I had never heard of Windows 10," Goldstein said. "Nobody ever asked me if I wanted to update."

  When outreach to Microsoft's customer support didn't fix the issue, Goldstein took the software giant to court, seeking compensation for lost wages and the cost of a new computer.

She won. Last month, Microsoft dropped an appeal and Goldstein collected a $10,000 judgment from the company.

<Then, further down...>

Mary Jo Foley, a journalist who has closely followed Microsoft for decades, wrote recently that the company has made saying no to Windows 10, particularly for nontech-savvy people, "nearly impossible to implement."

Paul Thurrott, another longtime Microsoft follower, criticized a recent pop-up asking users if they were ready to get Windows 10. In the prompt, the X in the upper-right corner — long known to Windows users as a way to exit a software program or abort a process — is interpreted by the update tool as an agreement to go ahead with Windows 10.

"The violation of trust here is almost indescribable," Thurrott wrote.

- Interview with San Jose Mercury News last week.
- Interview with Consumer Reports tomorrow.
- Never10 slowing down to <15k/day. Total GRC downloads: ~1,365,000
- For more, ComputerWorld's Gregg Keizer does a great job of chronicling her multi-month effort to work with Microsoft:
  http://www.computerworld.com/article/3089071/microsoft-windows/customer-wins-10k-judgement-from-microsoft-over-unauthorized-windows-10-upgrade.html
  (She spent days on the phone with Windows tech support, went to a local Microsoft store, and much more.)

Court Rules the FBI Does Not Need a Warrant to Hack a Computer
http://motherboard.vice.com/read/court-rules-the-fbi-does-not-need-a-warrant-to-hack-a-computer
Timeline:

- FBI takes over a child pornography site "Playpen" which is hidden behind TOR hidden services.
- Visiting creeps use TOR to hide their own IP address.
- FBI uses "NIT" - Network Investigative Technology - to plant code into subsequent visitors' computers.
- The FBI's NITware phones back to the FBI thus unmasking the visitor's true IP.

Some of the opinion hinges around IP addresses, and whether they are private and subject to the Fourth Amendment, or already public.:

- Henry Coke Morgan, Jr., a senior United States District Judge, wrote: "Generally, one has no reasonable expectation of privacy in an IP address when using the internet." This, he posits, is because we all voluntarily give up our IP addresses to third parties everyday, such as to our ISPs and any websites we visit. And when it comes to Tor, users have to connect to and disclose their IP address to an initial node of the network.

- This is being called similar to the "broken blinds" test which allows passing law

enforcement officers to legally peer into someone's home if their blinds are closed... but broken and allowing some visibility into the home.

- But... The FBI's investigative software grabbed more than just suspects' IP addresses. It also beamed their username and some other system information to the FBI; information that is undoubtedly within a user's computer.

- But this doesn't phase the judge Morgan either, who writes that the defendant "has no reasonable expectation of privacy in his computer."

- He writes: "The NIT only obtained identifying information; it did not cross the line between collecting addressing information and gathering the contents of any suspect's computer."

- And, most horrifyingly, he adds: "It seems unreasonable to think that a computer connected to the Web is immune from invasion. Indeed, the opposite holds true: in today's digital world, it appears to be a virtual certainty that computers accessing the Internet can—and eventually will—be hacked." He then references a series of media reports on high profile hacks. He posits that users of Tor cannot expect to be safe from hackers.
- The EFF is understandably apoplectic
    - https://www.eff.org/deeplinks/2016/06/federal-court-fourth-amendment-does-not-protect-your-home-computer
    - In a dangerously flawed decision unsealed today, a federal district court in Virginia ruled that a criminal defendant has no "reasonable expectation of privacy" in his personal computer, located inside his home. According to the court, the federal government does not need a warrant to hack into an individual's computer.

      The implications for the decision, if upheld, are staggering: law enforcement would be free to remotely search and seize information from your computer, without a warrant, without probable cause, or without any suspicion at all. To say the least, the decision is bad news for privacy. But it's also incorrect as a matter of law, and we expect there is little chance it would hold up on appeal.

      (It also was not the central component of the judge's decision, which also diminishes the likelihood that it will become reliable precedent.) But the decision underscores a broader trend in these cases: courts across the country, faced with unfamiliar technology and unsympathetic defendants, are issuing decisions that threaten everyone's rights.

Bizarre interminable Win7 Updating getting resolved

- InfoWorld's Woody Leonard "Woody on Windows":
- Microsoft releases KB 3161647, KB 3161608 to fix slow Windows 7 update scans
- http://www.infoworld.com/article/3086811/microsoft-windows/microsoft-releases-kb-3161647-kb-3161608-to-fix-slow-windows-7-update-scans.html
- <quote> "Early results look promising: the many-hours-long Win7 waits may be behind us"
- OPTIONAL!!! ---> KB3161608 <--- Just got it TODAY!

Comodo tries to usurp the Let's Encrypt trademark

- https://letsencrypt.org/2016/06/23/defending-our-brand.html
- <Let's Encrypt> Some months ago, it came to our attention that Comodo Group, Inc., is attempting to register at least three trademarks for the term "Let's Encrypt," for a variety of Certificate Authority-related services. These trademark applications were filed long after the Internet Security Research Group (ISRG) started using the name Let's Encrypt publicly in November of 2014, and despite the fact Comodo's "intent to use" trademark filings acknowledge that it has never used "Let's Encrypt" as a brand.

  We have forged relationships with millions of websites and users under the name Let's Encrypt, furthering our mission to make encryption free, easy, and accessible to everyone. We've also worked hard to build our unique identity within the community and to make that identity a reliable indicator of quality. We take it very seriously when we see the potential for our users to be confused, or worse, the potential for a third party to damage the trust our users have placed in us by intentionally creating such confusion. By attempting to register trademarks for our name, Comodo is actively attempting to do just that.

- Comodo CEO goes onto Comodo's forums claiming that Let's Encrypt stole their idea of 90-day short-life certificates. He ranted on and on, defensively.

- Comodo NO.
  - DigiCert for certs.
  - Hover for non-free but inexpensive and no B.S. domain names.

Malware moves to JavaScript (Sophos Naked Security Blog)

- https://nakedsecurity.sophos.com/2016/06/20/ransomware-thats-100-pure-javascript-no-download-required/
- In 2015, Word Macros were the #1 infection vector.
- Now: "Invoice.txt.js"
- Remember:
  - Windows doesn't show file extensions by default. So a file called Invoice.txt.js shows up as Invoice.txt.
  - Windows uses a weird yellow parchment scroll icon to denote .JS files... so it looks like a document.
- Typically, the malicious JavaScript connects to a download server, fetches the actual ransomware in the form of a Windows program (an .EXE file), and launches it to complete the infection.
- Now, however, there's a new approach:
  - 100% JS malware.
  - All the JS public key and symmetric key crypto has been developed publicly and is freely available.
- What to do:
  - Associate .JS files with Notepad.
    - "Open With..." and "[x] Always use this app to open .js files."

In the: Yet another way to exfiltrate data from air-gapped computer department:

- Researchers make malware that steals data by spinning your computer's fans:
- http://motherboard.vice.com/read/researchers-make-malware-that-steals-data-by-spinning-your-computers-fans
- This also takes the cake for the worst, most cringe-worthily named hack as far:
- "Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers"
- https://arxiv.org/ftp/arxiv/papers/1606/1606.05915.pdf
- Israeli security researchers
- Constraint is the time required for the fan to change speed between 4100 and 4500 PRM.
- 10 bits/minute or 600 bits/hour or 14.4kbits/day.

NetGear routers have a worrisome (though not showstopping) vulnerability

- Google: Web GUI Password Recovery and Exposure Security Vulnerability
- http://kb.netgear.com/app/answers/detail/a_id/30632
- http://bit.ly/sn-566 for long list of affected routers
- <quotes>
    - NETGEAR is aware of the security issue that can expose web GUI login passwords while the password recovery feature is disabled. This vulnerability occurs when an attacker can access the internal network or when remote management is enabled on the router.
    - NETGEAR is working on a firmware fix and will email the download information to all registered users when the firmware becomes available. To register your product, visit https://my.netgear.com/register/.
    - NETGEAR strongly recommends that you follow these two steps to remediate the vulnerability:
        - Manually enable the password recovery feature on your device.
        - Ensure that remote management is disabled. (Remote management is disabled by default.)

- Enabling "Password Recovery" reveals two sets of preset "favorite pet" security questions.
    - User fills-in the proper answers.

The COOLEST truly new and brilliant idea of the week:

- https://www.youtube.com/watch?v=TZEYQUngEug
- CES Interview with Innomdle Lab: Vibrating Body Tissue for private smart-watch calls.
- Place finger on ear means no speakers.

Miscellany

- (((Pending HSF breakthrough)))
- Leo: The last Terminator movie was a TON of fun!!
- "The Strain" on FX - 7.5/10 83% Rotten Tomatoes
    - Season #3 begins August 28th

SpinRite

Steve Reed in Rockville, Maryland:

Ended a much longer note with:
"Thanks for the time you put into the podcast & all the other great products you make. I have our company halfway to a site license and expect to get the other 2 very soon (every time SpinRite fixes a drive, we buy another license)."