Security Now! #594 - 01-10-17
A look into PHP malware

This week on Security Now!

The US Federal Trade Commission steps into the IoT and home networking malpractice world, a radio station learns a lesson in what words NOT to repeat, Google plans to even eliminate the checkbox, a crucial caveat to the "passwords are long enough" argument, more cause to be wary of third-party software downloads, a few follow-ups to last week's topics, a bit of miscellany and a close look at a well-known piece of PHP malware.

From the "This Never Gets Old" department … another instance of Windows:

"I just wanted some water!"

Security News

FTC sues D-Link
Last Thursday, Jan 5th, 2016, the US Federal Trade Commission filed a lawsuit naming Taiwan-based D-Link Corporation and its US subsidiary, D-Link Systems, Inc., for its failure to take steps to secure their devices, thus leaving them vulnerable to hackers.

<quote> Plaintiff, the Federal Trade Commission ("FTC"), for its Complaint, brings this action under Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), to obtain permanent injunctive relief and other equitable relief against Defendants for engaging in unfair or deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), in connection with Defendants' failure to take reasonable steps to secure the routers and Internet-protocol cameras they designed for, marketed, and sold to United States consumers.

<<< a bunch of definitions and who's who... >>>

Under: Defendant's Security Failures
Defendants have failed to take reasonable steps to protect their routers and IP cameras from widely known and reasonably foreseeable risks of unauthorized access, including by failing to protect against flaws which the Open Web Application Security Project has ranked among the most critical and widespread web application vulnerabilities since at least 2007.

Among other things:
Defendants repeatedly have failed to take reasonable software testing and remediation measures to protect their routers and IP cameras against well known and easily preventable software security flaws, such as "hard-coded" user credentials and other backdoors, and command injection flaws, which would allow remote attackers to gain control of consumers' devices;

Defendant D-Link has failed to take reasonable steps to maintain the confidentiality of the private key that Defendant D-Link used to sign Defendants' software, including by failing to adequately restrict, monitor, and oversee handling of the key, resulting in the exposure of the private key on a public website for approximately six months; and

Defendants have failed to use free software, available since at least 2008, to secure users' mobile app login credentials, and instead have stored those credentials in clear, readable text on a user's mobile device.

THOUSANDS OF CONSUMERS AT RISK
16. As a result of Defendants' failures, thousands of Defendants' routers and cameras have been vulnerable to attacks that subject consumers' sensitive personal information and local networks to a significant risk of unauthorized access. In fact, the press has reported that Defendants' routers and cameras have been vulnerable to a range of such attacks and have been compromised by attackers, including by being made part of large scale networks of computers infected by malicious software, known as "botnets."

17. The risk that attackers would exploit these vulnerabilities to harm consumers was significant. In many instances, remote attackers could take simple steps, using widely available tools, to locate and exploit Defendants’ devices, which were widely known to be vulnerable. For example, remote attackers could search for vulnerable devices over the Internet and obtain their IP addresses using readily available tools, such as a popular search engine that can locate devices running particular software versions or operating in particular locations. Alternatively, attackers could use readily accessible scanning tools to identify vulnerable devices operating in particular areas or on particular networks. In many instances, an attacker could then take simple steps to exploit vulnerabilities in Defendants’ routers and IP cameras, impacting not only consumers who purchased these devices, but also other consumers, who access the Internet in public or private locations served by the routers or who visit locations under the IP cameras’ surveillance.

18. By creating these vulnerabilities, Defendants put consumers at significant risk of harm in a variety of ways. An attacker could compromise a consumer’s router, thereby obtaining unauthorized access to consumers’ sensitive personal information. For example, using a compromised router, an attacker could re-direct consumers seeking a legitimate financial site to a spoofed website, where they would unwittingly provide the attacker with sensitive financial account information. Alternatively, using a compromised router, an attacker could obtain consumers’ tax returns or other files stored on the router’s attached storage device or could use the router to attack other devices on the local network, such as computers, smartphones, IP cameras, or connected appliances. Similarly, by exploiting the vulnerabilities described in Paragraph 15, an attacker could compromise a consumer’s IP camera, thereby monitoring consumers’ whereabouts to target them for theft or other criminal activity or to observe and record over the Internet their personal activities and conversations or those of their young children. In many instances, attackers could carry out such exploits covertly, such that consumers would have no reason to know that an attack was ongoing. Finally, during the time Defendant D-Link’s private key was available on a public website, consumers seeking to download legitimate software from Defendants were at significant risk of downloading malware, signed by malicious actors using D-Link’s private key.

DEFENDANTS’ SECURITY STATEMENTS

19. Defendants have disseminated or caused to be disseminated to consumers statements regarding the security of their products, including their routers and IP cameras.

SECURITY EVENT RESPONSE POLICY

PROMOTIONAL CLAIMS

Easy to secure

Advanced Network Security

Under a heading “128-bit Security Encryption,” that the router: protects your network with 128-bit AES data security encryption – the same technology used in E-commerce or online banking.

VIOLATIONS OF THE FTC ACT

Unfairness

28. In numerous instances, Defendants have failed to take reasonable steps to secure the software for their routers and IP cameras, which Defendants offered to consumers, respectively, for the purpose of protecting their local networks and accessing sensitive personal information.

29. Defendants' practices caused, or are likely to cause, substantial injury to consumers in the United States that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

Security Event Response Policy Misrepresentation
31. Through the means described in Paragraph 20, Defendant DLS has represented, directly or indirectly, expressly or by implication, that Defendants took reasonable steps to secure their products from unauthorized access.

32. In truth and in fact, as described in Paragraphs 15-18, Defendants did not take reasonable steps to secure their products from unauthorized access.

Router Promotional Misrepresentations
34. Through the means described in Paragraph 21, Defendants have represented, directly or indirectly, expressly or by implication, that the routers described by these claims were secure from unauthorized access.

35. In truth and in fact, as described in Paragraphs 15-18, Defendants' routers were not secure from unauthorized access and control.

IP Camera Promotional Misrepresentations
37. Through the means described in Paragraph 22, Defendants have represented, directly or indirectly, expressly or by implication, that the IP cameras described by these claims were secure from unauthorized access and control.

38. In truth and in fact, as described in Paragraphs 15-18, Defendants' IP cameras were not secure from unauthorized access and control.

Router GUI Misrepresentations
40. Through the means described in Paragraph 23, Defendants have represented, directly or indirectly, expressly or by implication, that the routers described by these claims were secure from unauthorized access.

41. In truth and in fact, as described in Paragraphs 15-18, Defendants' routers were not secure from unauthorized access and control.

IP Camera GUI Misrepresentations
43. Through the means described in Paragraph 24, Defendants have represented, directly or indirectly, expressly or by implication, that the IP cameras described by these claims were secure from unauthorized access and control.

44. In truth and in fact, as described in Paragraphs 15-18, Defendants' IP cameras were not secure from unauthorized access and control.

Then a whole bunch of exhibit attachments.

https://arstechnica.com/wp-content/uploads/2017/01/ftcdlinkcomplaint.pdf

A radio station learns to be careful when saying the "A" "L" "E" "X" "A" word.

- The perils of automated purchasing is nothing new, especially for Amazon who has "Dash" buttons.

- One such instance occurred in Dallas, Texas last early last week, when a six-year-old asked her family's new Amazon Echo "can you play dollhouse with me and get me a dollhouse?" The device readily complied, ordering a KidKraft Sparkle mansion dollhouse, in addition to "four pounds of sugar cookies." The parents quickly realized what had happened and have since added a code for purchases. They have also donated the dollhouse a local children's hospital.

- So.. case closed, right?

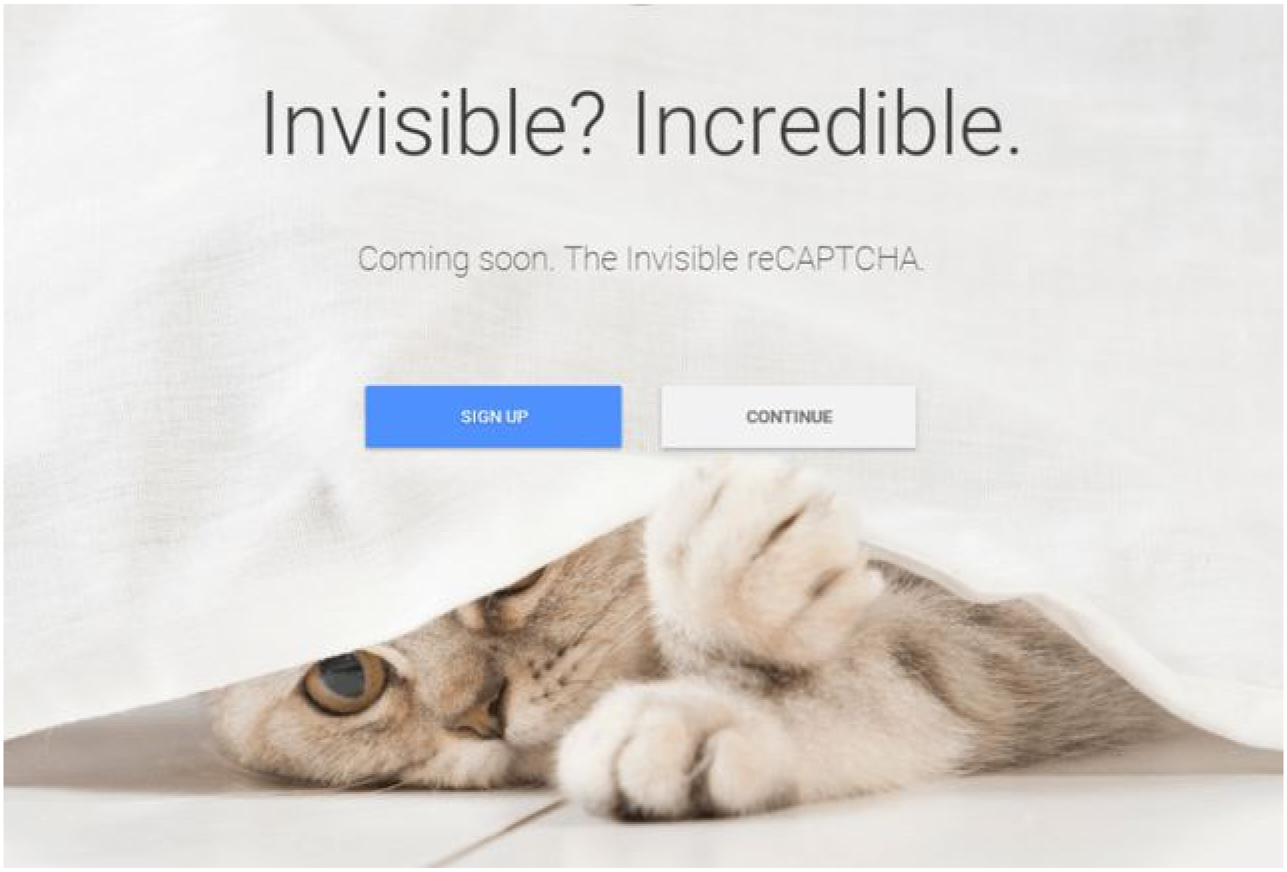
- The story was picked up and covered by San Diego, California's CW6 News. At the end of the story, Anchor Jim Patton remarked: "I love the little girl, saying '[A-Word] ordered me a dollhouse,'" According to CW6 News, Echo owners who were watching the broadcast found that the remark triggered orders on their own devices.

- Patton didn't think that any of the devices went through with their purchases, who told reporters that the station had received a handful of reports of viewer devices attempting to order a dollhouse after hearing his remarks.

- We note that the Echo's settings can be adjusted through the device's app, and users can either turn off voice ordering altogether, or add a passcode to prevent accidental purchases.

- Links:
  - http://gizmodo.com/tv-report-on-accidental-amazon-orders-triggers-attempte-1790958217
  - http://www.cw6sandiego.com/news-anchor-sets-off-alexa-devices-around-san-diego-ordering-unwanted-dollhouses/
  - http://www.theregister.co.uk/2017/01/07/tv_anchor_says_alexa_buy_me_a_dollhouse_and_she_does
  - http://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse

The next step in CAPTCHAS: Invisible CAPTCHAS



Invisible? Incredible.

Coming soon. The Invisible reCAPTCHA.

https://www.google.com/recaptcha/intro/comingsoon/invisible.html
https://developers.google.com/recaptcha/docs/invisible

Using the Invisible reCAPTCHA:

- To invoke the invisible reCAPTCHA, you can either:
  - Automatically bind the challenge to a button or
  - Programmatically bind the challenge to a button or
  - Programmatically invoke the challenge.

In other words... you can have your own button appearance, looking like whatever you wish, OR you can have client-side JavaScript automatically run upon page load and invoke Google's next-generation "Invisible CAPTCHA" to perform seamless and invisible on-the-fly bot detection.

"Cracking 12 Character & Above Passwords"

http://www.netmux.com/blog/cracking-12-character-above-passwords

Why are 12+ character passwords vulnerable?
Practically speaking, people who manually create passwords above 10 characters, for the most part, use common words or phrases. Why do they do this? Because remembering the password "horsebattery123" is way easier than "GFj27ef8%k$39". It's just simple human behavior exhibiting path of least resistance that will always exist and, until auto-generating password managers gain mass adoption, this vulnerability will always be around. I agree that XKCD's

password strength cartoon of four random words is sound but only for non-fast hashing algorithms like bcrypt.

In this article we will demonstrate Combo and Hybrid Attacks using Hashcat that will expand your cracking knowledge toolkit. These examples will show how an attacker can efficiently attack this larger keyspace, with modern hardware, and make these so called strong passwords succumb to his cracking methodology.

(And... server side PBKDF is crucial, too!)

XMPP gets e2e encrpypted group chats

- "eXtensible Messaging and Presence Protocol"
- As Wikipedia succinctly summarizes it:
  https://en.wikipedia.org/wiki/XMPP
  XMPP is a communications protocol for message-oriented middleware based on XML (Extensible Markup Language). It enables the near-real-time exchange of structured yet extensible data between any two or more network entities. Originally named Jabber, the protocol was developed by the Jabber open-source community in 1999 for near real-time instant messaging (IM), presence information, and contact list maintenance. Designed to be extensible, the protocol has been used also for publish-subscribe systems, signalling for VoIP, video, file transfer, gaming, the Internet of Things (IoT) applications such as the smart grid, and social networking services.

  Unlike most instant messaging protocols, XMPP is defined in an open standard and uses an open systems approach of development and application, by which anyone may implement an XMPP service and interoperate with other organizations' implementations. Because XMPP is an open protocol, implementations can be developed using any software license; although many server, client, and library implementations are distributed as free and open-source software, numerous freeware and commercial software implementations also exist.

  The Internet Engineering Task Force (IETF) formed an XMPP working group in 2002 to formalize the core protocols as an IETF instant messaging and presence technology. The XMPP Working group produced four specifications (RFC 3920, -21, -22, -23), [since then, various of them have been updated and superceded by newer specifications.] In addition to these core protocols standardized at the IETF, the XMPP Standards Foundation (formerly the Jabber Software Foundation) is active in developing open XMPP extensions.

  XMPP-based software is deployed widely across the Internet, and by 2003, was used by over ten million people worldwide, according to the XMPP Standards Foundation.

- OMEMO
  - Is a recent (2014) improvement over OTR which adds multi-user chat and multi-device support.
  - It is inspired and based on Open Whisper Systems' Axolotl protocol developed for Signal.
  - Not backwards-compatible with OTR, but is being standardized as the new

end-to-end encryption mechanism on XMPP: https://conversations.im/omemo/
    - Conversations.im/xeps/multi-end.html
    - No server-side support required but is enhanced by Message Carbons (XEP-0280) and Message Archive Management (XEP-0313) especially for multi-device support
    - Other secure chat protocols are in development, for example OTRv4 and n1sec.
    - The server does know who the participants are, but not what's being said.
    - For more, see: https://we.riseup.net/riseup/xmpp

- XMPP clients that support Omemo
    - Conversations (android) – integrated support, works nicely. support for muc, but only in specific situations.
    - gajim (gtk) – via plugin github.com/omemo/gajim-omemo
    - Cryptocat (ios, android, mac, linux, windows) – no muc, still requires cryptocat xmpp server, afaik
    - Chatsecure (ios, android) – in next release (will be first OMEMO compatable iOS app) github.com/ChatSecure/ChatSecure-iOS/is...
    - Monal (ios, mac) – in progress github.com/anurodhp/Monal/issues/9
    - Tor Messenger (linux, windows, mac) – in progress trac.torproject.org/projects/tor/ticket...
    - InstantBird (Tor Messenger upstream) – in progess bugzilla.mozilla.org/show_bug.cgi?id=12...
    - Jitsi (java) – in progress github.com/jitsi/jitsi/issues/199
    - Let’s Chat (web) – in progress github.com/sdelements/lets-chat/issues/...
    - Pidgin (windows, linux) – in progress developer.pidgin.im/ticket/16801

- Links:
    - https://account.conversations.im/
    - https://xmpp.org/
    - https://www.jabber.org/

Simon Zerafa shared a tweet with Paul Thurrott and me:

- https://twitter.com/GossiTheDog/status/817089856316784643
- Kevin Beaumont (@GossiTheDog) / Verified account
  Ahahaha, just found a Windows 10 install ISO on BitTorrent which includes a scheduled task to download and run a ransomware EXE after 90 days.

Web site password length limit follow-up...

- James P (@jpancoast) - 1/5/17, 10:31 AM
  @SGgrc When I see password length limits on websites it makes me wonder if they're not hashing the password on the backend.

Explaining more of the Apple ATS security troubles

- Aaron Bishop (@Aaron Bishop) - 1/4/17, 5:28 AM
  I'm an app developer who links to 3rd party web sites and have had issues with ATS on some sites because they don't allow any ECDHE cipher suites. ATS only allows for ECDHE,

and my guess is that the sites don't allow it either because they haven't updated and modified their suites OR they are afraid of lawsuit for usinc ECC. Just thought you might like to know since I haven't heard anything about ATS requiring ECDHE with regards to patent lawsuits. I don't know if ECDHE falls under that patent, but the key words are enough for a chilling effect.

- https://www.ssllabs.com/ssltest/viewClient.html?name=Apple%20ATS&version=9&platform=iOS%209

Miscellany

GRC's DNS Benchmark is triggering Cox's Zeus Trojan/bot detection system!

- (Via Twitter DM) Hi Steve: Just got an email from Cox (seems to be from them, based on the header):

- (As I write this, might be your DNS Benchmark that triggered this.) =========== Cox has identified that one or more of the computers behind your cable modem are likely infected with the Zeus Trojan/bot, also known as Zbot. =========

  My first question is: How can Cox see what's behind our modem? We're running NAT routers. Second, the only thing that changed over the past day is that I replaced our previous Routers with LinkSys running dd-wrt (a.k.a. Tomato.) Could DNSMasq be causing this false positive? Oh - I also ran your DNS Nameserver Benchmark the other night and rebuilt our list of name servers. Perhaps that unusual traffic was it? Third, when did Cox start caring if a key logger is installed on one of our computers? Again, how would Cox know? Is Cox seeing a bunch of data coming out of our router all of a sudden? (DNS Benchmark would do that.)

Norway to terminate FM Radio and switch to DAB

- (Digital Audio Broadcasting)
- Norway doesn't have any AM radio.
- Norway's terrain makes analog FM radio broadcasting especially challenging and expensive.
- The Norwegian government estimates that a total of $23.5 million annually will be saved for stations after the switchover is complete.
- Some FM stations will begin going silent this week as they switch over to DAB and the switchover will be complete by year's end.
- Two years ago half of the country had already switched because there were only 5 FM stations but 20 DAB stations.
- Today, 70% of the population have DAB at home, but about 2 million automobiles are lagging and would be without radio reception, which might pose a safety hazard.
- The phase over will be region by region.
- http://radio.no/

SpinRite

Glasair pilot (@Glasair pilot) - 1/2/17, 7:38 PM

Hey Steve: A SpinRite story for you. I built a RAID 10 recently using four identical brand new Western Digital Black Caviars. To my surprise, the RAID went critical twice in two weeks shortly after. (Interestingly, the drives didn't have a problem rebuilding. Therein lays a clue.)

Naturally, I was disappointed, since the drives were new. Since I thought I might have to fight WD over RMA's, I decided to run SR so I could document bad sectors or any other problems. I started out running Level 3, but SR reported that would take 3 days at that level. So I ran Level 2 instead to cut it down to a day.

Surprisingly, no bad sectors reported! And SMART data was good too. But more importantly, after running the drives through SpinRite at Level 2… no more Critical RAID errors!

I think what's happening is similar with what SSD guys are finding. If I have it right, a RAID Controller waits a certain amount of time for a drive to acknowledge a write is complete. If the drive takes too long, say, due to a sector relocation, then the Controller assumes the drive has failed and takes it off-line, and marks the RAID critical. (Ostensibly the WD Red NAS drives mitigate this in their firmware.) By running a drive through SpinRite at Level 2, any questionable sectors are exercised out. And viola! The RAID hasn't failed since!

☠️ A look into PHP Malware ☠️

The Daily Beast coverage:
"How the U.S. Hobbled Its Hacking Case Against Russia and Enabled Truthers"
http://www.thedailybeast.com/articles/2017/01/06/how-the-u-s-enabled-russian-hack-truthers.html

The department released 876 internet IP addresses it says is linked to Grizzly Steppe hacking, and urged network administrators everywhere to add the list to their networking monitoring. Lists of IP addresses used by hackers can be useful "indicators of compromise" in network security—admins can check the list against access logs, or program an intrusion detection system to sound the alarm when it sees traffic from a suspect address. But that assumes that the list is good: carefully culled, and surrounded with enough context that administrators know what to do when they get a hit.

The DHS list is none of these things, as Lee, founder of the cyber security firm Dragos, discovered when he ran the list against a stored cache of known clean traffic his company keeps around for testing. The results stunned him. "We had thousands of hits," he says. "We had an extraordinary high amount of false positives on this dataset… Six of them were Yahoo e-mail servers.”

It turns out that some, perhaps most, of the watchlisted addresses have a decidedly weak connection to the Kremlin, if any. In addition to the Yahoo servers, about 44 percent of the addresses are exit nodes in the Tor anonymity network,

We did learn a bit more about what triggered the Vermont’s Electric Utility’s concern last week:

The consequences of the over inclusive list became apparent last week, when a Vermont utility company, Burlington Electric Department, followed DHS’s advice and added the addresses to its network monitoring setup. It got an alert within a day. The utility called the feds, and *The Washington Post* soon broke the distressing news that “Russian hackers penetrated [the] U.S. electricity grid through a utility in Vermont.”

The story was wrong. Not only was the laptop in question isolated from the utility’s control systems, the IP address that triggered the alert wasn’t dangerous after all: It was one of the Yahoo servers on the DHS list, and the alert had been generated by a Burlington Electric employee checking email. The *Post* article was later corrected, but not before Vermont Senator Patrick Leahy issued a statement condemning the putative Russian attack.

The Daily Beast:

[...] But to analysts in the computer security industry, the hackers are old, familiar adversaries that they’ve been watching under a microscope for the better part of a decade.

The first group, called “Fancy Bear” or APT28 has been active since at least mid-2007. The group typically begins its attacks with targeted spearphishing emails crafted to trick the recipient into clicking on a link or downloading a malicious file. Then the group installs backdoors controlled through a cloud of command-and-control servers deployed around the world. Its targets have included NATO, several U.S. defense contractors, the German parliament and, after Russia’s doping scandal began, the World Anti-Doping Agency. One of the command-and-control servers used in the DNC hack was reportedly also used in the *Bundestagand* intrusion.

The other group, commonly called “the Dukes” or APT29, was first spotted operating in Chechnya in 2008. Stealthier and more cautious than Fancy Bear, the Dukes have nonetheless been detected infiltrating the White House, the State Department, and the Joint Chiefs of Staff. Known for innovation—one attack campaign used Twitter as a command-and-control channel—they have their own fleet of customizable malware, including a program called Seaduke that they only bring out for the really important targets, and which was found again on the DNC’s network.

Security companies can tell you much more about these groups, their code, their infrastructures, and their methods. (The Finnish security firm F-Secure has an excellent 34-page write-up of the Dukes, and FireEye has a deep dive into Fancy Bear, among many other reports by different companies.) (PDF) From analysis of the dozens of malware packages used exclusively by these hackers, researchers can tell you that they’re usually compiled on machines with the language set to Russian. Both groups operate during working hours in Russia, and take Russian holidays off. Their targets are radically different from those of for-profit criminals hackers in Eastern

Europe or anywhere else—no banks, no retailers with credit card numbers to steal—always governments, companies, journalists, NGOs, and other targets that the Russian government would be interested in.

In other words, these hackers don't operate like 14-year-olds. They sometimes use off-the-shelf hacking tools, but more often they deploy industrial scale malware no teenagers have access to. They hit targets of interest to spies, not kids. And virtually all the public analysis of these two groups concluded—well before it became a political issue with the DNC hack—that they are likely controlled by the Russian government.

The evidence, then, that Russia interfered with the election is already solid, and is supported by years of work by the security industry. "If you've been following along, all the evidence that matters is already public," Lee notes. "This is one case out of hundreds that they've investigate involving the same hackers. It's all very, very consistent, it all makes sense, it's all very, very solid," he says. "It's just that the government is now confusing everyone."

<<sigh>>

How are we to understand what happened here? Perhaps the mixture of Internet-illiterate politicians coupled with the demands of bureaucratic management.

It MUST BE that we have -- probably deep within the NSA -- skilled professional hackers who know all this and who are no more happy with this than the industry's technical security experts. And this must have been like calling most companies and speaking to "technical support" -- you're not talking to an expert. You know.... you wind up talking to someone who thinks "IP" is something that happens when you wake up in the middle of the night.

"P.A.S. 3.1.0"

https://www.wordfence.com/blog/2016/12/russia-malware-ip-hack
https://www.wordfence.com/blog/2017/01/election-hack-faq/

What is PHP?

- Server-side native code (GRC style: ShieldsUP, eCommerce, Perfect Passwords, SSL Fingerprints, Cookie Forensics, DNS Spoofability, etc.)
- Client-side runs in browser: Off The Grid (local Latin square generation), Password Haystacks, etc.
- Server-side scripting interpretation: Perl, PHP, Ruby, Java, Python, JavaScript

- This is a powerful architecture... but with this comes a great deal of responsibility: Now, web page CONTENT is being scanned by the web server for "things to do" which it then does on the fly. This is exactly the same as with all the problems we've seen with SQL databases over the years, where web pages embed commands to retrieve and display data from a back-end SQL database. But if attackers are ever able to get their own submitted SQL commands to be displayed and interpreted by the web server, commands like "Drop Table" can inflict significant damage.

- And so it is with PHP. There's nothing inherently vulnerable about PHP. It's just crucial that the power of server-side time-of-delivery interpretation not be allowed to see attacker-supplied text as valid PHP code to be executed.

What is "P.A.S. v.3.1.0" ??

It's a PHP function containing an encrypted blob of text which is decrypted when the attacker supplies the decryption password. After the PHP is uploaded to a web server the attacker accesses the file through a web browser, enters the password (which is then stored in a cookie so it doesn't need to be reentered) and the blob is decrypted and executed ON THE WEB SERVER.

The result is a well-known and common attack toolkit known as a "Web Shell" containing the following features:

- File browser/explorer.
- File search function.
- A database client to download the contents of a hacked site database.
- Network tools including a port scanner and the ability to bind a service to a port.
- A tool to brute force attack passwords on FTP and POP3 services.
- A command line client to run arbitrary operating system commands.
- A utility to view server configuration info.

... and it's freely available (for free) on the Internet with an optional Bitcoin support donation.

How does such malware infect a WordPress or other PHP site?

That's unclear (because it shouldn’t happen and protections are in place to prevent it)... but some theories are:

- WordPress website owners have other malware installed on their workstations and that malware attempts to install PAS on their WordPress websites.
- A related CSRF (cross site request forgery) vulnerability is used to install the malware.
- Users are voluntarily installing this on their own websites after downloading it from a malicious website thinking it is safe.
- Attackers are compromising websites through some other means and then using the compromised credentials to manually sign in and install PAS with a standard browser. These sign-ins could be partially or fully automated.

The bottom line is... there is absolutely NOTHING particularly impressive or unique about this piece of malware provided by the DHS and FBI. It is freely downloadable by anyone on the Internet.

~30~