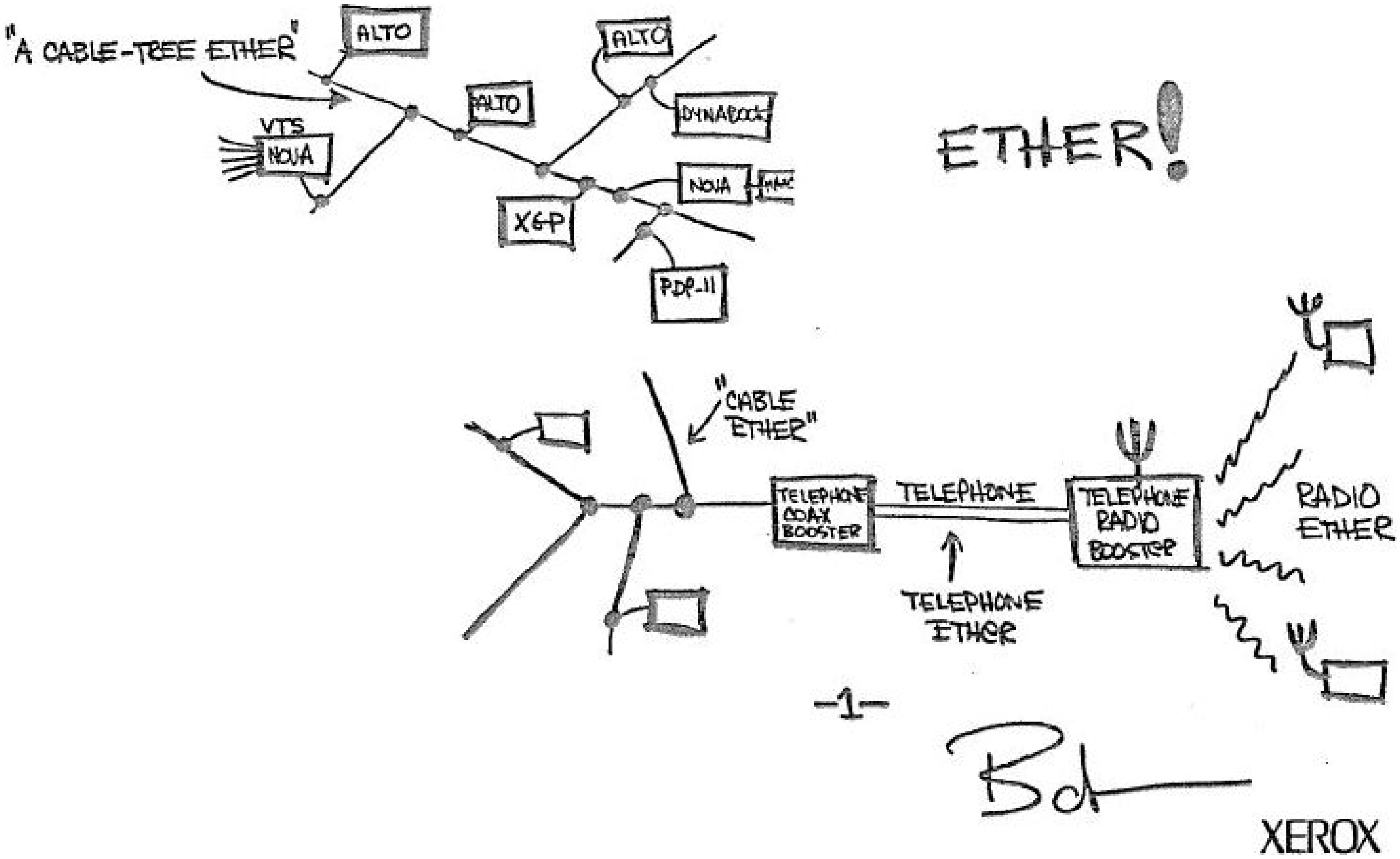
Security Now! #613 - 05-23-17

WannaCry Aftermath

This week on Security Now!

This week we examine a bunch of WannaCry follow-ups, including some new background, reports of abilities to decrypt drives, attacks on the Killswitch, and more. We also look at what the large StackOverflow site had to do to do HTTPS, the WiFi security of various properties owned by the US president, more worrisome news coming from the UK's Teresa May, the still sorry state of certificate revocation, are SSDs also subject to RowHammer-like attacks?, some miscellany, and closing the loop with our listeners.

Our Picture of the Week



Bob Metcalfe’s Ethernet turned 44 years old yesterday

WannaCry Followups

NSA officials worried about the day its potent hacking tool would get loose. Then it did.
https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html

The Washington Post:

When the National Security Agency began using a new hacking tool called EternalBlue, those entrusted with deploying it marveled at both its uncommon power and the widespread havoc it could wreak if it ever got loose.

Some officials even discussed whether the flaw was so dangerous they should reveal it to Microsoft, the company whose software the government was exploiting, according to former NSA employees who spoke on the condition of anonymity given the sensitivity of the issue.

But for more than five years, the NSA kept using it — through a time period that has seen several serious security breaches — and now the officials' worst fears have been realized. The malicious code at the heart of the WannaCry virus that hit computer systems globally late last week was apparently stolen from the NSA, repackaged by cybercriminals and unleashed on the world for a cyberattack that now ranks as among the most disruptive in history.

The failure to keep EternalBlue out of the hands of criminals and other adversaries casts the NSA's decisions in a harsh new light, prompting critics to question anew whether the agency can be trusted to develop and protect such potent hacking tools.

Current and former officials defended the agency's handling of EternalBlue, saying that the NSA must use such volatile tools to fulfill its mission of gathering foreign intelligence. In the case of EternalBlue, the intelligence haul was "unreal," said one former employee.

"It was like fishing with dynamite," said a second.

The NSA did not respond to several requests for comment for this article.

<< the story then goes on to reiterate background we've already discussed >>

As I said last week, I understand that this is an extremely tough call.

It's easy for those on the sidelines to jump up and down and say that the NSA should not secretly develop and then keep secret such powerful vulnerabilities. But I think it is very important to note that what is unfortunately missing from all of the reporting of this story, are ANY details of what use this long standing SMB vulnerability may have been to US national security during the time that it was both available for the NSA's use and secret. We don't know how useful it was. We don't know what valuable intelligence it may have uniquely allowed to be gathered.

So... horrific as its escape doubtless was, maybe, if we actually knew how our intelligence services had been able to use its unique powers during the time of its availability... we might feel differently. But we are unlikely to ever know one way or the other. My only point here is to observe that we do not have the benefit of the full story. We don't know that it might change our judgement, but without knowing, it has no opportunity to.

PATCH Act: A New Bill Designed to Prevent Occurrences Like WannaCrypt
http://www.securityweek.com/patch-act-new-bill-designed-prevent-occurrences-wannacrypt

Following the worldwide WannaCrypt ransomware attack that leveraged the EternalBlue exploit developed by and stolen from the NSA, Microsoft's chief legal officer called for governments to stop stockpiling 0-day exploits. His arguments are morally appealing but politically difficult.

Now, however, he has partial support from a bi-partisan group of lawmakers: Senators Brian Schatz (D-Hawaii), Ron Johnson (R-Wis.), and Cory Gardner (R-Colo.) and U.S. Representatives Ted Lieu (D-Calif.) and Blake Farenthold (R-Texas). Schatz announced yesterday that they had introduced the 'Protecting Our Ability to Counter Hacking Act of 2017' -- the PATCH Act.

Its purpose is to establish a Vulnerability Equities Review Board with permanent members including the Secretary of Homeland Security, the Director of the FBI, the Director of National Intelligence, the Director of the CIA, the Director of the NSA, and the Secretary of Commerce -- or in each case the designee thereof.

Its effect, however, will be to seek a compromise between the moral requirement for the government to disclose vulnerabilities (Microsoft's Digital Geneva Convention), and the government's political expediency in stockpiling vulnerabilities for national security and deterrence purposes.

In a statement issued yesterday, Schatz wrote, "Striking the balance between U.S. national security and general cybersecurity is critical, but it's not easy. This bill strikes that balance. Codifying a framework for the relevant agencies to review and disclose vulnerabilities will improve cybersecurity and transparency to the benefit of the public while also ensuring that the federal government has the tools it needs to protect national security."

The bill does not go so far as to mandate the disclosure of all government 0-day exploits to relevant vendors for patching, but instead requires the Vulnerability Equities Review Board to develop a consistent and transparent process for decision-making. It will create new oversight mechanisms to improve transparency and accountability, while enhancing public trust in the process.

It further requires that "The head of each Federal agency shall, upon obtaining information about a vulnerability that is not publicly known, subject such information to the process established."

In this way, the Vulnerability Equities Review Board not only has oversight of all 0-day vulnerabilities held by the government agencies, it also maintains the controls "relating to whether, when, how, to whom, and to what degree information about a vulnerability that is not publicly known should be shared or released by the Federal Government to a non-Federal entity." That is, whether the public interest requires the vendor be able to patch the vulnerability.

The proposal is already receiving wide approval. Frederick Humphries, Microsoft's VP of US government affairs, tweeted, "We agree with the goals of the PATCH Act and look forward to working w-Sens @RonJohnsonWI @SenCoryGardner @brianschatz, Reps @farenthold @tedlieu to help prevent cyberattacks."

Thomas Gann, chief public policy officer at McAfee, commented: "All governments have to balance national security interests with economic interests. In some cases, governments have an interest in using certain vulnerabilities for intelligence gathering purposes to protect their national interests in ways that make it impossible to disclose. That said, we support the effort by Senators Schatz and Johnson to establish an equitable vulnerabilities review process. This will help facilitate the disclosure of previously unknown vulnerabilities. An improved process will help balance security and economic interests while also enhancing trust and transparency."

Megan Stifel, cybersecurity policy director at Public Knowledge, said, "We thank these legislators for leading this effort to foster greater transparency and accountability on the cybersecurity policy challenge of software and hardware vulnerabilities. We welcome this bill and similar efforts to enhance trust in the internet and internet-enabled devices."

-- My take: This is total nonsense --

A bunch of politicians who want to appear to be “responding” by creating more government bureaucracy... which is exactly what our present administration was elected to reduce.

This will simply add regulation without effect. The CIA and NSA will loudly -- and probably honestly -- assert their need for thes for national security. They will downplay the downside and explain how we're already losing the cyber war, and how forcing voluntary disarmament would be unilaterally laying down our arms and capitulating in the cyberwar.

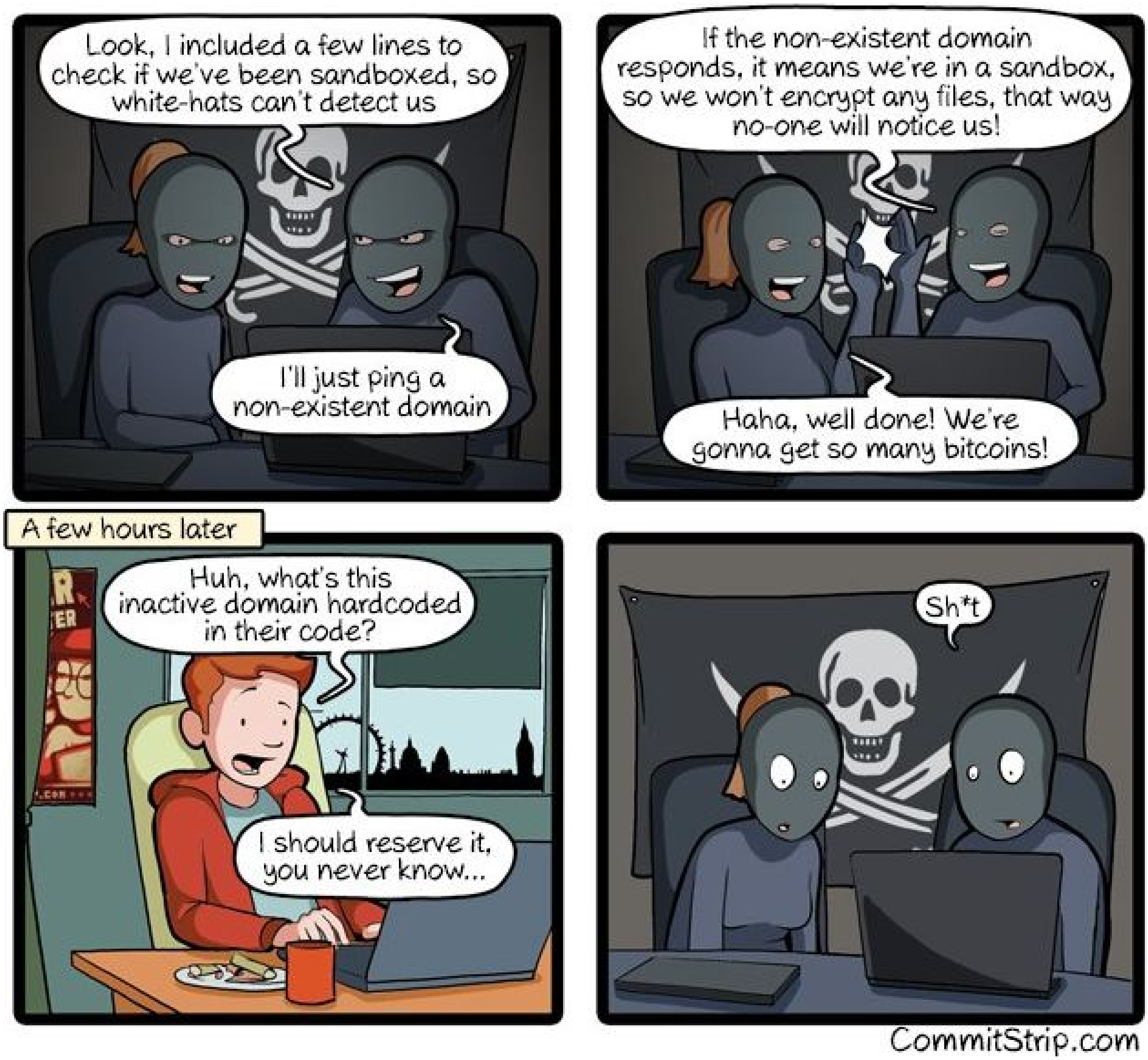
They'll argue that foreign governments, who lack the PATCH act's attempted oversight controls will STILL be free to discover and use the very same software flaws AGAINST us and that, as we have seen, even when patches were already made available, machines were STILL victimized. And they'll also note, correctly, that Microsoft ONLY back-patched XP and Vista *because* of the proven severity of the problem. If the SMB flaw had been quietly disclosed it would ONLY have been patched in maintained operating systems.

The WannaCry Killswitch:

We think we now understand the logic behind the seemingly braindead WannaCry Killswitch:

When malware is being forensically reverse-engineered its DNS queries are replied to with the IP of a local server and that server accepts connections from the malware in order to capture and understand the software's command and control system.

So the WannaCry authors added a "bogus server outreach" to a non-existent domain as a simple means of detecting when their software might be operating within a forensic "sandbox" for analysis.


Look, I included a few lines to check if we've been sandboxed, so white-hats can't detect us
I'll just ping a non-existent domain
If the non-existent domain responds, it means we're in a sandbox, so we won't encrypt any files, that way no-one will notice us!
Haha, well done! We're gonna get so many bitcoins!
A few hours later
Huh, what's this inactive domain hardcoded in their code?
I should reserve it, you never know...
Sh*t
CommitStrip.com

Meanwhile... Hackers Are Trying to Reignite WannaCry With Nonstop Botnet Attacks
https://www.wired.com/2017/05/wannacry-ransomware-ddos-attack/

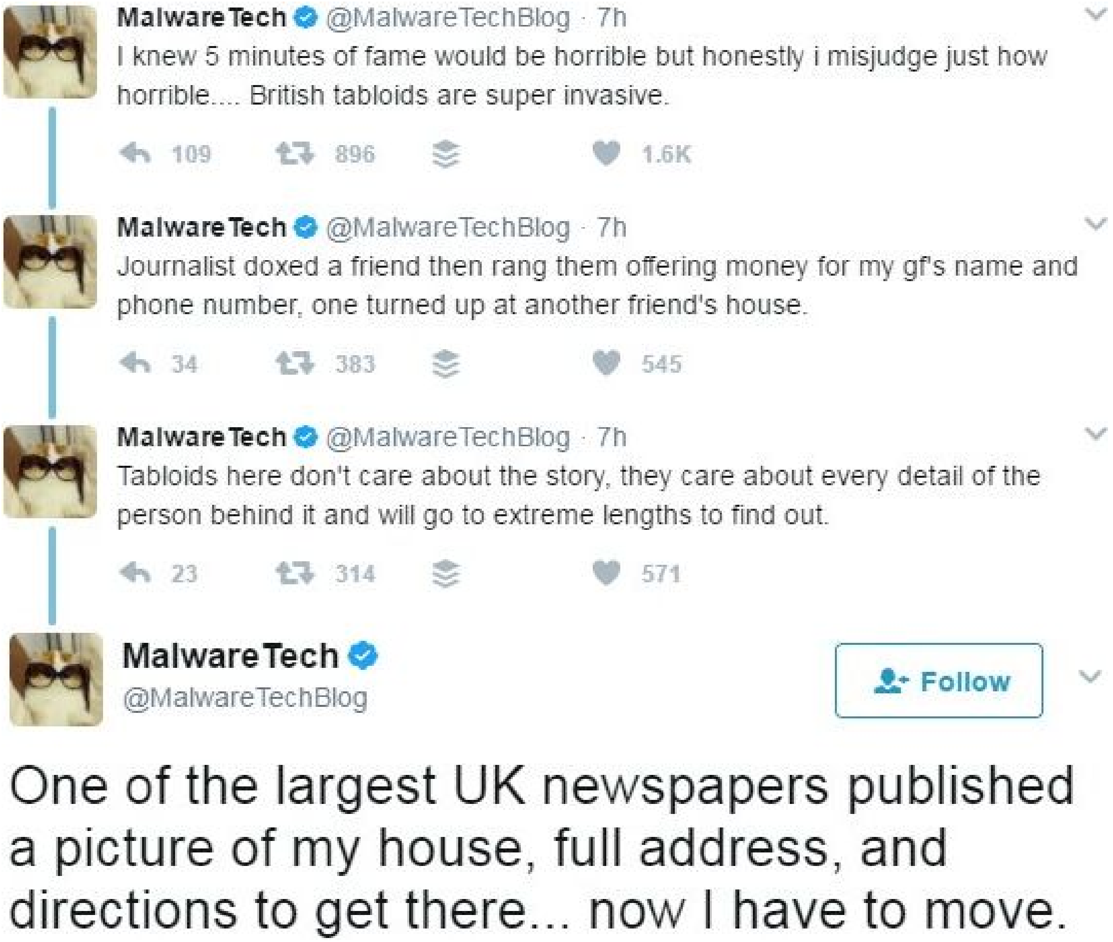
Various Mirai and Miria-derivative botnets are attacking the WannCry Killswitch server IP in an attempt to DDoS the server offline, thus reigniting the WannaCry infection.

But any newly infected or rebooted system only spends its first 24 hours scanning for other vulnerable machines. After that it shuts its scanners down to avoid obvious detection since IP spoofing cannot be used for TCP/4455 connections.

However, whenever any infected machine is rebooted it will check the Killswitch server then, if it does not receive a response, it will spend the next 24 hours scanning for other vulnerable machines.

Who is "MalwareTech" ??
He tried in vain to remain "cyber" and not identified in the physical world. Nowhere on either his Twitter page nor his blog there are any names, details, or head shots... which should be a clear indication that he wished to remain anonymous. But dogged British tabloid reporters dug deep into "MalwareTech's" online past and finally outed -- or doxxed -- him as being a 22-year old British security researcher named Marcus Hutchins.

However, thanks to being known, the ethical hacker group "HackerOne" have awarded Marcus $10,000 for his efforts which Marcus stated he intends to split between charity and educational resources for students who cannot afford them.



MalwareTech @MalwareTechBlog · 7h
I knew 5 minutes of fame would be horrible but honestly i misjudge just how horrible.... British tabloids are super invasive.

MalwareTech @MalwareTechBlog · 7h
Journalist doxed a friend then rang them offering money for my gf's name and phone number, one turned up at another friend's house.

MalwareTech @MalwareTechBlog · 7h
Tabloids here don't care about the story, they care about every detail of the person behind it and will go to extreme lengths to find out.

MalwareTech
@MalwareTechBlog

One of the largest UK newspapers published a picture of my house, full address, and directions to get there... now I have to move.

Decrypting WannaCry
Wannacry in-memory key recovery

The "CryptReleaseContext" function proactively wipes/zeroes memory under Windows 10, but NOT under XP and apparently also NOT under Win7, before the sensitive memory is released back to the operating system. So *IF* that temporary memory allocation has not been used and thus overwritten, and *IF* an infected and encrypted XP or Win7 machine has not been powered down... the key MIGHT be recoverable from the machine's RAM.

In tests on XP, the in-RAM key recovery was successful every time.

However... researchers have confirmed that the worm portion of WannaCry DOES NOT successfully infect XP or Windows Server 2003. The CryptoMalware *does* run on XP.

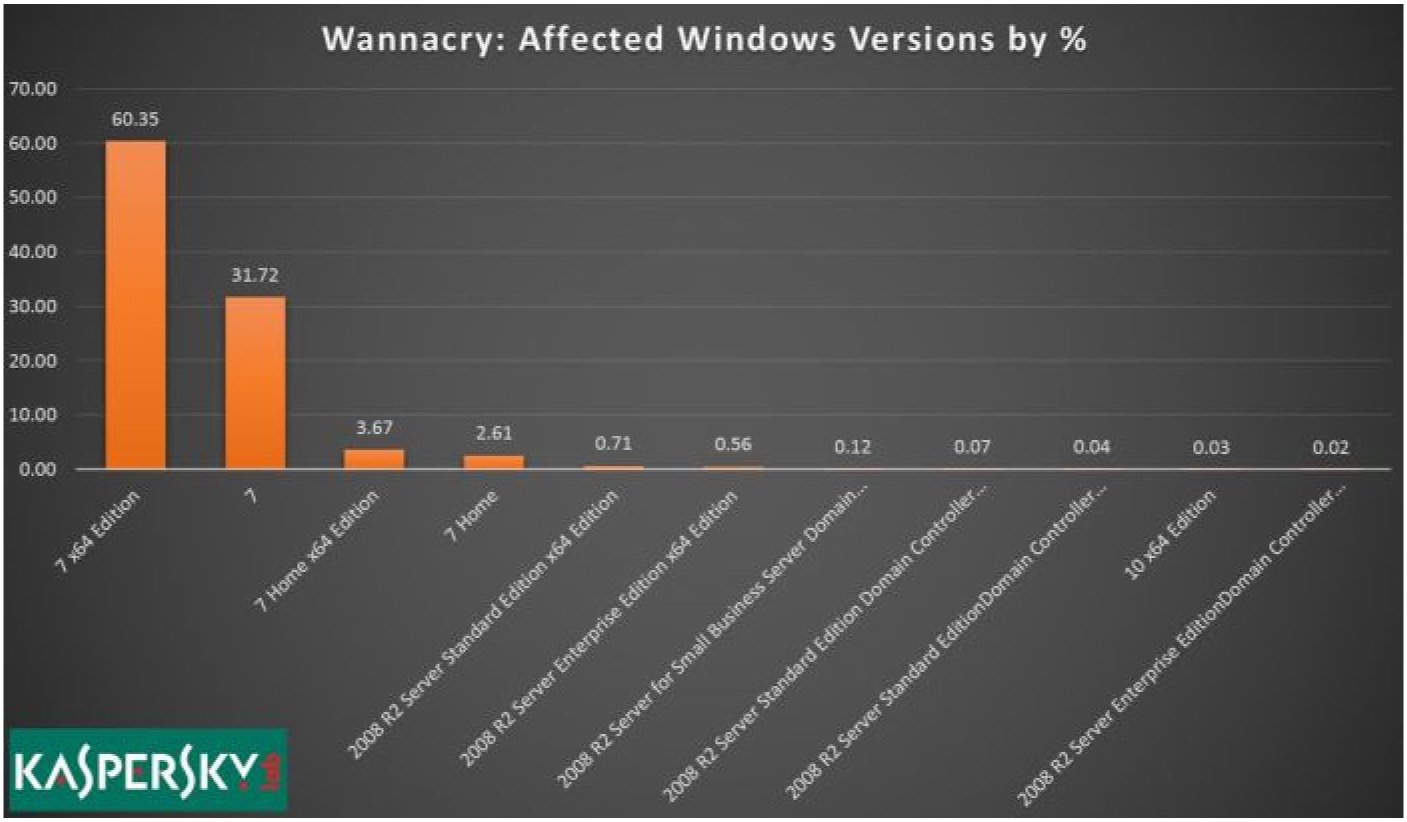
What's being found in RAM are the original two secret prime numbers used to form the RSA private key. If they can be recovered from RAM the machine's files can be decrypted.

- This appears to be the best one: https://github.com/gentilkiwi/wanakiwi/releases
- Earlier version needs private key: https://github.com/gentilkiwi/wanadecrypt
- Also... https://github.com/aguinet/wannakey

https://blog.comae.io/wannacry-decrypting-files-with-wanakiwi-demo-86bafb81112d

Simon Zerafa (@SimonZerafa) -- 5/20/17, 1:18 AM

- @SGgrc 98% of WannaCry victims running Windows 7.
- Can we finally nail the lid shut on the XP myth?
- https://www.bleepingcomputer.com/news/security/over-98-percent-of-all-wannacry-victims-were-using-windows-7/



How many infections?

Malware Tech: The latest unique IPs count from the WannaCry sinkhole is 416,989 (not including the 604,102 unique IPs from manual visits to the domain).

Security News

All IT Jobs Are Cybersecurity Jobs Now / WSJ Behind paywall
The rise of cyberthreats means that the people once assigned to setting up computers and email servers must now treat security as top priority.

HTTPS comes to Stack Overflow: The End of a Long Road
Yesterday, the well known, very popular and quite sprawling StackExchange family of developer-oriented websites completed their conversion to HTTPS.

Nick Craver is a Software Developer and Systems Administrator for Stack Exchange who spearheaded this work and yesterday detailed the journey in a blog post:
https://nickcraver.com/blog/2017/05/22/https-on-stack-overflow/

Nick is sick and tired of everyone saying "just use Let's Encrypt" as if that would simply solve every problem. Nick's detailed posting is linked above and will be of interest to anyone who wants to better understand why "just use Let's Encrypt" is not the answer.

To get some sense for the nature of the challenge, Nick notes that:

- We have hundreds of domains (many sites and other services)
- Many second-level domains (stackoverflow.com, stackexchange.com, askubuntu.com, etc.)
- Many 4th level domains (e.g. meta.gaming.stackexchange.com)
- We allow user submitted & embedded content (e.g. images and YouTube videos in posts)
- We serve from a single data center (latency to a single origin)
- We have ads (and ad networks)
- We use websockets, north of 500,000 active at any given (connection counts)
- We get DDoSed (proxy)
- We have many sites & apps communicating via HTTP APIs (proxy issues)
- We’re obsessed with performance (maybe a little too much)

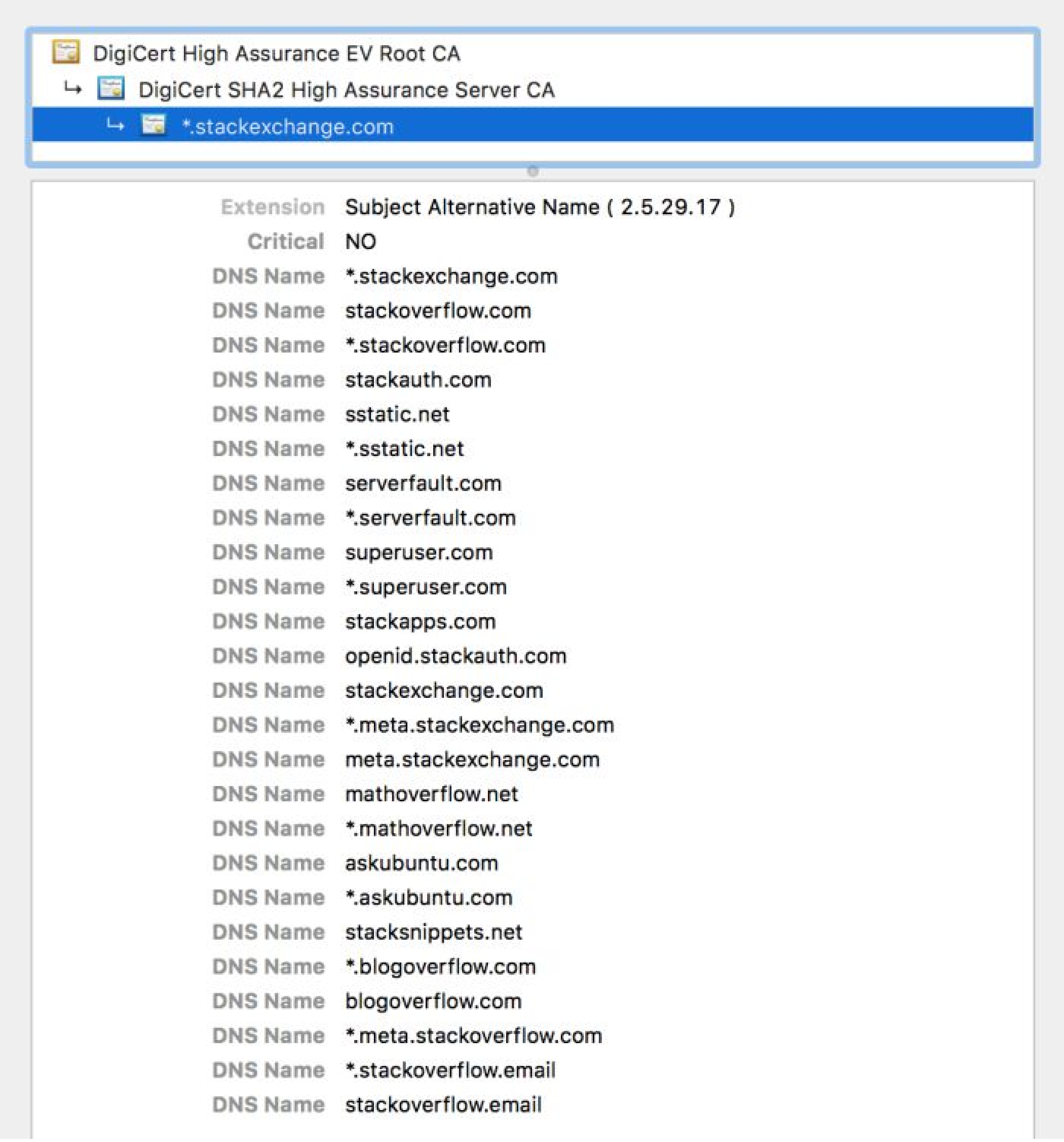
To summarize:

The most common question we get: “Why not use Let’s Encrypt?”

Answer: because they don’t work for us. Let’s Encrypt is doing a great thing. I hope they keep at it. If you’re on a single domain or only a few domains, they’re a pretty good option for a wide variety of scenarios. We are simply not in that position. Stack Exchange has hundreds of domains. Let’s Encrypt doesn’t offer wildcards. These two things are at odds with each other. We’d have to get a certificate (or two) every time we deployed a new Q&A site (or any other service). That greatly complicates deployment, and either a) drops non-SNI clients (around 2% of traffic these days) or b) requires far more IP space than we have.

Another reason we want to control the certificate is we need to install the exact same certificates on both our local load balancers and our CDN/proxy provider. Unless we can do that, we can’t failover (away from a proxy) cleanly in all cases. Anyone that has the certificate pinned via HPKP (HTTP Public Key Pinning) would fail validation. We’re evaluating whether we’ll deploy HPKP, but we’ve prepped as if we will later.

I’ve gotten a lot of raised eyebrows at our main certificate having all of our primary domains + wildcards. Here’s what that looks like:



DigiCert High Assurance EV Root CA
↳ DigiCert SHA2 High Assurance Server CA
↳ *.stackexchange.com

Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	*.stackexchange.com
DNS Name	stackoverflow.com
DNS Name	*.stackoverflow.com
DNS Name	stackauth.com
DNS Name	sstatic.net
DNS Name	*.sstatic.net
DNS Name	serverfault.com
DNS Name	*.serverfault.com
DNS Name	superuser.com
DNS Name	*.superuser.com
DNS Name	stackapps.com
DNS Name	openid.stackauth.com
DNS Name	stackexchange.com
DNS Name	*.meta.stackexchange.com
DNS Name	meta.stackexchange.com
DNS Name	mathoverflow.net
DNS Name	*.mathoverflow.net
DNS Name	askubuntu.com
DNS Name	*.askubuntu.com
DNS Name	stacksnippets.net
DNS Name	*.blogoverflow.com
DNS Name	blogoverflow.com
DNS Name	*.meta.stackoverflow.com
DNS Name	*.stackoverflow.email
DNS Name	stackoverflow.email

And guess who StackExchange chose??

In Nick's Q&A is the "Q"

Q: Where do you get certificates?
A: We use DigiCert, they’ve been awesome.

They got DigiCert to make them a very special Extended Validation certificate with a massive SAN (Subject Alternative Name) record to enumerate all of their various domains. Issuing that would have taken a great deal of careful work, since they would need to verify and prove ownership of every root second level domain.

Hacking Mar-a-Lago
ProPublica and Gizmodo co-published their report.
https://www.propublica.org/article/any-half-decent-hacker-could-break-into-mar-a-lago
http://gizmodo.com/any-half-decent-hacker-could-break-into-mar-a-lago-we-1795276155

Two weeks ago, on a sparkling spring morning, we went trawling along Florida’s coastal waterway. But not for fish.

We parked a 17-foot motor boat in a lagoon about 800 feet from the back lawn of The Mar-a-Lago Club in Palm Beach and pointed a 2-foot wireless antenna that resembled a potato gun toward the club. Within a minute, we spotted three weakly encrypted Wi-Fi networks. We could have hacked them in less than five minutes, but we refrained.

A few days later, we drove through the grounds of the Trump National Golf Club in Bedminster, New Jersey, with the same antenna and aimed it at the clubhouse. We identified two open Wi-Fi networks that anyone could join without a password. We resisted the temptation.

We have also visited two of President Donald Trump’s other family-run retreats, the Trump International Hotel in Washington, D.C., and a golf club in Sterling, Virginia. Our inspections found weak and open Wi-Fi networks, wireless printers without passwords, servers with outdated and vulnerable software, and unencrypted login pages to back-end databases containing sensitive information.

The risks posed by the lax security, experts say, go well beyond simple digital snooping. Sophisticated attackers could take advantage of vulnerabilities in the Wi-Fi networks to take over devices like computers or smart phones and use them to record conversations involving anyone on the premises.

“Those networks all have to be crawling with foreign intruders, not just ProPublica,” said Dave Aitel, chief executive officer of Immunity, Inc., a digital security company, when we told him what we found.

Security lapses are not uncommon in the hospitality industry, which — like most industries and government agencies — is under increasing attack from hackers. But they are more worrisome in places where the president of the United States, heads of state and public officials regularly visit.

U.S. leaders can ill afford such vulnerabilities. As both the U.S. and French presidential campaigns showed, hackers increasingly exploit weaknesses in internet security systems in an effort to influence elections and policy. Since the election, Trump has hosted Chinese President Xi Jinping, Japanese Prime Minister Shinzo Abe and British politician Nigel Farage at his properties. The cybersecurity issues we discovered could have allowed those diplomatic discussions — and other sensitive conversations at the properties — to be monitored by hackers.

Theresa May to create new internet to be controlled and regulated by government
http://www.independent.co.uk/life-style/gadgets-and-tech/news/theresa-may-internet-conservatives-government-a7744176.html

Theresa May is planning to introduce huge regulations on the way the internet works, allowing the government to decide what is said online.

The plans will allow Britain to become "the global leader in the regulation of the use of personal data and the internet", the manifesto claims.

The manifesto suggests that the government might stop search engines like Google from directing people to pornographic websites. "We will put a responsibility on industry not to direct users – even unintentionally – to hate speech, pornography, or other sources of harm," the Conservatives write.

Particular focus has been drawn to the end of the manifesto, which makes clear that the Tories want to introduce huge changes to the way the internet works.

"Some people say that it is not for government to regulate when it comes to technology and the internet," it states. "We disagree."

"In harnessing the digital revolution, we must take steps to protect the vulnerable and give people confidence to use the internet without fear of abuse, criminality or exposure to horrific content", the manifesto claims in a section called 'the safest place to be online'.

"Our starting point is that online rules should reflect those that govern our lives offline," the Conservatives' manifesto says, explaining this justification for a new level of regulation.

"It should be as unacceptable to bully online as it is in the playground, as difficult to groom a young child on the internet as it is in a community, as hard for children to access violent and degrading pornography online as it is in the high street, and as difficult to commit a crime digitally as it is physically."

The manifesto also proposes that internet companies will have to pay a levy, like the one currently paid by gambling firms. Just like with gambling, that money will be used to pay for advertising schemes to tell people about the dangers of the internet, in particular being used to "support awareness and preventative activity to counter internet harms", according to the manifesto.

The Conservatives will also seek to regulate the kind of news that is posted online and how companies are paid for it. If elected, Theresa May will "take steps to protect the reliability and objectivity of information that is essential to our democracy" – and crack down on Facebook and Google to ensure that news companies get enough advertising money.

If internet companies refuse to comply with the rulings – a suggestion that some have already made about the powers in the Investigatory Powers Act – then there will be a strict and strong set of ways to punish them.

"We will introduce a sanctions regime to ensure compliance, giving regulators the ability to fine or prosecute those companies that fail in their legal duties, and to order the removal of content where it clearly breaches UK law," the manifesto reads.

In laying out its plan for increased regulation, the Tories anticipate and reject potential criticism that such rules could put people at risk.

"While we cannot create this framework alone, it is for government, not private companies, to protect the security of people and ensure the fairness of the rules by which people and businesses abide," the document reads. "Nor do we agree that the risks of such an approach outweigh the potential benefits."

An update on the state of Certificate Revocation

CRL - Certificate Revocation Lists

- The original granddaddy solution.
- Each CA serves a growing list of administratively revoked certificates.
- Unfortunately, the lists are now massive and take time to download. And the concept is inherently inefficient since a browser only wants to find ONE possible certificate -- which almost certainly will NOT be present in the list -- but the whole point is that it needs to be sure.

CRLSets

- Google went their own way and created a wholly non-functional solution known as CRLSETs, which is small list containing known high-profile revoked certificates. When I realized this, I pointed it out by creating a deliberately revoked certificate. Google responded by adding that certificate to their CRLSET list. So I created another deliberately pre-revoked certificate... which Chome honors.

- Firefox shows "SEC_ERROR_REVOKED_CERTIFICATE"

OCSP - Online Certificate Status Protocol

- Real time certificate status verification.
- The server's certificate contains the URL for real time re-verification of any certificate's current validity status.
- But this additional per-cert query takes time.
- Firefox currently does this for all certificates, but as we'll see in a minute, that, too, is changing.
- The problem is... what happens with the OCSP server is down? This happened last week for the Let's Encrypt OCSP service and caused significant havoc.
- If no OCSP response is received does the client fail or allow?
- If client's allow without confirmed denial then bad guys can simply block the receipt of the denial.
- If clients fail without confirmation then major outages can occur.

OCSP Stapling - Have the server "staple" a freshly signed assertion from the certificate's CA.

- This eliminates the overhead of an additional OCSP lookup.
- However, the stapled OCSP cannot be part of the certificate since it's constantly changing. So it is ADDED to the TLS handshake by servers that know to do this.
- But that means that a stolen certificate that has been revoked can still be used by bad guys simply by not stapling an OCSP assertion.

So to this system we introduce "OCSP Must Staple".

- This binds a stapling REQUIREMENT into the original certificate so that a stapled OCSP *must* be provided for the client to accept the certificate as valid.

The problem is... neither of the two majority web servers on the Internet today, Apache with ~46% share and Nginx with ~20% both have badly broken OCSP.

- The way you would want OCSP to be handled is for the server to periodically reach out and refresh its certificates' OCSP stapling information well in advance of the staple's expiration. This would allow for time in the event of any trouble.

- But, if Apache tries to renew the OCSP response and gets an error from the OCSP server – e. g. because it’s currently offline, DDoSed, or whatever – it will discard the existing still valid OCSP response and replace it with the error. And will then send out stapled OCSP errors. This was reported in 2014 and still remains unfixed.

- NginX is similarly broken.

- https://blog.hboeck.de/archives/886-The-Problem-with-OCSP-Stapling-and-Must-Staple-and-why-Certificate-Revocation-is-still-broken.html

Meanwhile... Firefox is considering giving up on OCSP for DV certs
Bug 1366100 - Disable OCSP fetching for domain-validated certificates
https://bugzilla.mozilla.org/show_bug.cgi?id=1366100

<quote> Telemetry indicates that fetching OCSP results is an important cause of slowness in the first TLS handshake. Firefox is, today, the only major browser still fetching OCSP by default for DV certificates.

Earlier we tried reducing the OCSP timeout to 1 second (based on CERT_VALIDATION_HTTP_REQUEST_SUCCEEDED_TIME), but that seems to have caused only a 2% improvement in SSL_TIME_UNTIL_HANDSHAKE_FINISHED.

This bug is to disable OCSP fetching for DV certificates. OCSP fetching should remain enabled for EV certificates.

OCSP stapling will remain fully functional. We encourage everyone to use OCSP stapling.

SSD Drives Vulnerable to Attacks That Corrupt User Data
https://www.bleepingcomputer.com/news/hardware/ssd-drives-vulnerable-to-attacks-that-corrupt-user-data/

Researchers have discovered that the latest generation of MLC (multi-level cell) SSDs can be subject to physical adjacency disturbances similar to what we've seen with DRAM and the RowHammer attacks.

"Program Interference" occurs when data is deliberately written in specific ways and in MLC SSDs results in a 4.9 factor increase in the SSD's error rate. This can corrupt the SSD's stored data and shorten the device's lifetime.

"Read Disturb" occurs when a large number of specially patterned reads are performed within a short time. The researchers said these read disturb errors will "corrupt both pages already written to partially-programmed wordlines and pages that have yet to be written"... thus ruining the SSD's ability to store data in a reliable manner in the future.

https://people.inf.ethz.ch/omutlu/pub/flash-memory-programming-vulnerabilities_hpca17.pdf

Twitter and Do Not Track
https://support.twitter.com/articles/20169453#

<quote> Twitter has discontinued support of the Do Not Track browser preference. While we had hoped that our support for Do Not Track would spur industry adoption, an industry-standard approach to Do Not Track did not materialize. We now offer more granular privacy controls, and you can learn more about them outlined in the articles below.

So this means that Twitter is no longer respecting the user's browser sending of the DNT:1 query header. They have chosen to ignore it. It's difficult to see how, if they were truly concerned about respecting privacy, they would choose to disable a privacy-enhancing feature that they had already implemented.

So what must actually be happening is that they WANT to be able to track users whose browsers are sending out the Do Not Track beacon, and this statement is the way they are justifying that. They are essentially saying: "Other services are ignoring their visitors' explicit requests to not be tracked, so we're going to also."

LastPass Authenticator with Cloud Sync

- Robert (@Leonidas_I) -- 5/18/17, 2:27 PM
  @SGgrc @LastPass Authenticator can now back up your two-factor data online
  http://www.androidpolice.com/2017/05/18/lastpass-authenticator-can-now-back-two-factor-data-online/

- Samuel Movi (@samuelmovi) -- 5/19/17, 9:17 AM
  @SGgrc I guess you won't be using your QR print-outs much, in the future LastPass will store two-factor codes alongside your passwords
  https://www.engadget.com/2017/05/19/lastpass-two-factor-code-storage

- Sean Stephens (@DarkElfLX) -- 5/20/17, 5:30 AM
  @SGgrc someone @LastPass is listening to #SecurityNow LastPass authenticator now backs up to LastPass account for recovery and sync.

This is not a good thing. Multifactor security requires heterogenous deployment. The idea is that my password and my TOTP must BOTH be provided. But if the same service contains BOTH my password and my master set of TOTP keys, a single compromise of that service renders my entire use of a second factor meaningless.

Also, I don't WANT an authenticator that IS willing to export my TOTP keys. Anyone who gains control of a device's UI could export the key set. The OPTIMAL solution is what I am doing and what I have recommended: Choose an Authenticator App that deliberately DOES NOT allow for TOTP key export and take responsibility for managing your TOTP keys yourself. Yes, it's more work... but it's also the only way to actually obtain the security offered by a second factor.

Miscellany

Yesterday was the 44th Anniversary of the Invention of Ethernet

- Bob Metcalfe (Verified account) @BobMetcalfe
  Ethernet's 44th birthday is Monday. I sketched this to include in a typed memo on May 22, 1973 at the Xerox Palo Alto Research Center.

The Ethernet was a truly brilliant invention.

- At the time, solutions involved some sort of centralized controller to negotiate access.
- IBM came up with the Token Ring / lost token / token regeneration / etc.
- Ethernet: Peers who obey a common and simple set of rules.
  - <rules>
- The only problem is a fast collapse as traffic approaches the media's speed limit.

Esther Dyson's "PC Forum 1984" Flicker Photos
https://www.flickr.com/photos/pcforum/sets/72157626570344759

This week's "Groan Worthy" riddle:

- How did the WannaCry Hackers get away? …
  They RanSomWare.

SpinRite

Richard Romick (Richard Romick) -- 5/21/17, 9:26 AM
I have a quick SpinRite testimonial for you. Sorry if I make any twitter faux pas, as this is the first time I have sent a message.

It started when my WD My Book Live Duo NAS told me one of the drives were failing. While I don't have any reason to mistrust WD, I felt it was a conflict of interest when their device says I need to buy a new WD hard drive (the NAS requires a specific line of WD hard drives to operate normally). Therefore, I decided to SpinRite it.

I grabbed an old ASUS desktop computer out of the closet, and happy to see that the motherboard reported SMART statistics to SpinRite. I ran a level 2 SpinRite scan on it. The scan was all blue across the board, and the ECC statistics looked good (no red).

However, whenever I stuck the hard drive back in the NAS and ran a long test, everything was good to go again. I'm guessing SpinRite performed some refreshing of data it found hard to read, which the NAS had interpreted as the drive failing. Thanks for the great product, I am now running both drives on level 4 just to be even more sure.

Barry Coggins (@barry_coggins) -- 5/21/17, 9:28 AM
Laptop was running hot w/loud fan speed... ran SpinRite and all is well and quiet again. @SGgrc

Closing The Loop

mcepl (mcepl) - 5/22/17, 5:47 AM
Hi, Steve. Let me react in longer form on SN612 and your refection on "blaming the victim". I am afraid that the advice you gave was so simplistic as dangerous. Yes, I can imagine that some MRI machine (completely air gapped) really can run whatever archaeological system one chooses. I understand that you (with some level of understanding of computer security) can run Windows XP on your machine (although, IIRC, even you are now on supported Windows 7, aren’t you?). However, when we are talking about 90% of NHS computers, then I assume neither air-gapping nor sophisticated use of computer can be assumed there. However, my biggest problem with this whole affair that I have been shouting to anybody whom I could to talk to, that to use general purpose desktop-oriented operating system for everything including things are clearly inappropriate (like arrival/departures monitors; twitter.com/l0gg0l/status/?) is crazy and should be stopped. Yes, I work for RHT, buut I would never think that even RHEL would be good idea to be used there (and it is a way more modular, so it can be stripped down more). You don't need even hard drive for such monitors (or they should be read-only) ? jjust receive message via network and display it! Why do you need Internet Explorer, Notepad, and FreeCell for that?

Bob Beaudoin (Bob Beaudoin) - 5/22/17, 11:37 AM
Did you hang on to the minted bit coins. Sure worth something now.

If you bought $100 of Bitcoin 7 years ago, you'd be sitting on $72.9 million today.
If You Bought $100 of Bitcoin 7 Years Ago, You'd Be Sitting on $72.9 Million Now"></a><div class='story' style=' border: 0px solid green;'><h3><a href='/news/2017/05/22/if_you_bought_100_bitcoin_7_years_ago_youd_be_sitting_on_729_million_now/' target='_blank' title="If You Bought $100 of Bitcoin 7 Years Ago, You'd Be Sitting on $72.9 Million Now">If You Bought $100 of Bitcoin 7 Years Ago, You'd Be Sitting on $72.9 Million Now</a></h3><p>

Talk about a serious case of regret: assuming the math is actually correct, those who were smart enough to buy $100 of bitcoin at the 0.003 cent price on May 22, 2010 are now definitive millionaires. The price of bitcoin hit a fresh record high on Monday nearing $2,200. Seven years ago today, someone spent 10,000 bitcoin on two Papa John's pizzas: this was the first transaction using the cryptocurrency.

Yesterday marked the seven-year anniversary of Bitcoin Pizza Day -- when a programmer named Laszlo Hanyecz spent 10,000 bitcoin on two Papa John's pizzas.

More important than the episode being widely recognized as the first transaction using the cryptocurrency is what it tells us about the bitcoin rally that saw it break through the $2,100 mark on Monday. Bitcoin was trading as high as $2,185.89 in the early hours of Monday morning, hitting a fresh record high, after first powering through the $2,000 barrier over the weekend, according to CoinDesk data.

Kostas Kritsilas (Kostas Kritsilas) - 5/21/17, 8:38 PM
Steve: In show 612, you were talking about the Android "O" restructuring, and its similarity to Windows NT's HAL. You had some difficulty remembering the third architecture supported. I'm pretty sure it was DEC's Alpha. In addition, later on it supported Power PC and Itanium (the latter two in Windows 2000). Later than that was ARM

ETC Maryland (@etc_md) -- 5/18/17, 7:36 AM

- @SGgrc Windows ‘S’ is not better because it's closed..it is still windows and will not be secure.
- @SGgrc Just because an ecosystem is closed doesn't = secure.
- If that was the case then opensource means less secure, it doesn't.

Re: @SGgrc SN 609, How are all these people able to unlock others iOS devices when after a few incorrect attempts, iOS enforces the passcode?

A: The device must store a "fail count" somewhere in nonvolatile memory. So they take a pre-guesses snapshot, make the maximum number of failed guesses, then restore the snapshot to reset the failure count... and make another round of guesses, then repeat!

Sassy ManJohnson (@sassymanjohnson) -- 5/19/17, 12:35 PM
@SGgrc question from security now this week: how did folks get to the source code to wanacry?

A: IDA Disassembler:
https://www.hex-rays.com/products/ida/

jc (@brundle56uk) -- 5/22/17, 12:34 PM
@SGgrc I keep asking why NTP can't be hacked, no response, but we're at a level that in theory it could? If not, why not, podcast please