emptywheel

THE COMPARTMENTS IN WAPO'S RUSSIAN HACK MAGNUM OPUS

THE COMPARTMENTS IN WAPO'S RUSSIAN HACK MAGNUM OPUS

June 23, 2017 / 26 Comments / in 2016 Presidential Election, Russian hacks / by emptywheel

The WaPo has an 8300 word opus [https://www.washingtonpost.com/graphics/2017/world/nat security/obama-putin-election-hacking/?utm_term=.5b736c21cb91] on the Obama Administration's response to Russian tampering in the election. The article definitely covers new ground on the Obama effort to respond while avoiding making things worse, particularly with regards to imposing sanctions in December. It also largely lays out much of the coverage the three bylined journalists (Greg Miller, Ellen Nakashima, and Adam

Entous) have broken before, with new details. The overall message of the article, which has a number of particular viewpoints and silences, is this: Moscow is getting away with their attack.

"[B]ecause of the divergent ways Obama and Trump have handled the matter, Moscow appears unlikely to face proportionate consequences."

THE IMMACULATE INTERCEPTION: CIA'S SCOOP

WaPo starts its story about how Russia got away with its election op with an exchange designed to make the non-response to the attack seem all the more senseless. It provides a dramatic description of a detail these very same reporters broke on December 9 [https://www.emptywheel.net/2016/12/09/unpacking-new-cia-leak-dont-ignore-aluminum-tube-footnote/] : Putin, who was personally directing this effort, was trying to elect Trump.

> Early last August, an envelope with extraordinary handling restrictions arrived at the White House. Sent by courier from the CIA, it carried "eyes only" instructions that its contents be shown to just four people: President Barack Obama and three senior aides.
>
> Inside was an intelligence bombshell, a report drawn from sourcing deep inside the Russian government that detailed Russian President Vladimir Putin's direct involvement in a cyber

> campaign to disrupt and discredit the U.S. presidential race.
>
> [snip]
>
> The material was so sensitive that CIA Director John Brennan kept it out of the President's Daily Brief, concerned that even that restricted report's distribution was too broad. The CIA package came with instructions that it be returned immediately after it was read.
>
> [snip]
>
> In early August, Brennan alerted senior White House officials to the Putin intelligence, making a call to deputy national security adviser Avril Haines and pulling national security adviser Susan Rice side after a meeting before briefing Obama along with Rice, Haines and McDonough in the Oval Office.

While the sharing of this information with just three aides adds to the drama, WaPo doesn't consider something else about it. The inclusion of Rice and McDonough totally makes sense. But by including Avril Haines, Brennan was basically including his former Deputy Director who had moved onto the DNSA position, effectively putting two CIA people in a room with two White House people and the President. Significantly, Lisa Monaco — who had Brennan's old job as White House Homeland Security Czar and who came from DOJ and FBI before that — was reportedly excluded from this initial briefing.

There are a number of other interesting details about all this. First, for thousands of wordspace, the WaPo presents this intelligence as irreproachable, even while providing this unconvincing explanation of why, if it is so secret and solid, the CIA was willing to let WaPo put it on its front page.

> For spy agencies, gaining insights into the intentions of foreign leaders is among the highest priorities. But Putin is a remarkably elusive target. A former KGB officer, he takes extreme precautions to guard against surveillance, rarely communicating by phone or computer, always running sensitive state business from deep within the confines of the Kremlin.
>
> The Washington Post is withholding some details of the intelligence at the request of the U.S. government.

If this intelligence is so sensitive, why is even the timing of its collection being revealed here, much less its access to Putin?

That seemingly contradictory action is all the more curious given that not all agencies were as impressed with this intelligence as CIA was. It's not until much, much later in its report until WaPo explains what *remains true* as recently as Admiral Rogers' latest Congressional testimony: the NSA wasn't and isn't as convinced by CIA's super secret intelligence as CIA was.

> Despite the intelligence the CIA had produced, other agencies were slower to endorse a conclusion that Putin was personally directing the operation and wanted to help Trump. "It was definitely compelling, but it was not definitive," said one senior administration official. "We needed more."
>
> Some of the most critical technical intelligence on Russia came from another country, officials said. Because of the source of the material, the NSA was reluctant to view it with high confidence.

By the time this detail is presented, the narrative is in place: Obama failed to respond adequately to the attack that CIA warned about back in August.

The depiction of this top-level compartment of just Brennan, Rice, McDonough, and Haines is interesting background, as well, for the depiction of the way McDonough undermined a State Department plan to institute a Special Commission before Donald Trump got started.

> Supporters' confidence was buoyed when McDonough signaled that he planned to "tabledrop" the proposal at the next NSC meeting, one that would be chaired by Obama. Kerry was overseas and participated by videoconference.

> To some, the "tabledrop" term has a tactical connotation beyond the obvious. It is sometimes used as a means of securing approval of an idea by introducing it before opponents have a chance to form counterarguments.
>
> "We thought this was a good sign," a former State Department official said.
>
> But as soon as McDonough introduced the proposal for a commission, he began criticizing it, arguing that it would be perceived as partisan and almost certainly blocked by Congress.
>
> Obama then echoed McDonough's critique, effectively killing any chance that a Russia commission would be formed.

Effectively, McDonough upended the table on those (which presumably includes the CIA) who wanted to preempt regular process.

Finally, even after these three WaPo journalists foreground their entire narrative with CIA's super duper scoop (that NSA is still not 100% convinced is one), they don't describe their own role in changing the tenor of the response on December 9 by reporting the first iteration of this story [https://www.emptywheel.net/2016/12/09/unpacking-new-cia-leak-dont-ignore-aluminum-tube-footnote/]

.

> "By December, those of us working on this for a long time were demoralized,"

> said an administration official involved in the developing punitive options.
>
> Then the tenor began to shift.
>
> On Dec. 9, Obama ordered a comprehensive review by U.S. intelligence agencies of Russian interference in U.S. elections going back to 2008, with a plan to make some of the findings public.

The WaPo's report of the CIA's intelligence changed the tenor back in December, and this story about the absence of a response might change the tenor here.

PRESENTING THE POLITICS AHEAD OF THE INTELLIGENCE

The WaPo's foregrounding of Brennan's August scoop is also important for the way they portray the parallel streams of the intelligence and political response. It portrays the Democrats' political complaints about Republicans in this story, most notably the suggestion that Mitch McConnell refused to back a more public statement about the Russian operation when Democrats were pushing for one in September. That story, in part because of McConnell's silence, has become accepted as true.

Except the WaPo's own story provides ample evidence that the Democrats were trying to get ahead of the formal intelligence community with respect to attribution, both in the summer, when Clapper only alluded to Russian involvement.

> Even after the late-July WikiLeaks dump, which came on the eve of the Democratic convention and led to the resignation of Rep. Debbie Wasserman Schultz (D-Fla.) as the DNC's chairwoman, U.S. intelligence officials continued to express uncertainty about who was behind the hacks or why they were carried out.
>
> At a public security conference in Aspen, Colo., in late July, Director of National Intelligence James R. Clapper Jr. noted that Russia had a long history of meddling in American elections but that U.S. spy agencies were not ready to "make the call on attribution" for what was happening in 2016.

And, more importantly, in the fall, when the public IC attribution came only *after* McConnell refused to join a more aggressive statement because the intelligence did not yet support it (WaPo makes no mention of it, but DHS's public reporting from late September [https://publicintelligence.net/dhs-election-cyber-threats/] still attributed the the threat to election infrastructure to "cybercriminals and criminal hackers").

> Senate Majority Leader Mitch McConnell (R-Ky.) went further, officials said, voicing skepticism that the underlying intelligence truly supported the White House's claims. Through a spokeswoman, McConnell

> declined to comment, citing the secrecy of that meeting.
>
> Key Democrats were stunned by the GOP response and exasperated that the White House seemed willing to let Republican opposition block any pre-election move.
>
> On Sept. 22, two California Democrats — Sen. Dianne Feinstein and Rep. Adam B. Schiff — did what they couldn't get the White House to do. They issued a statement making clear that they had learned from intelligence briefings that Russia was directing a campaign to undermine the election, but they stopped short of saying to what end.
>
> A week later, McConnell and other congressional leaders issued a cautious statement that encouraged state election officials to ensure their networks were "secure from attack." The release made no mention of Russia and emphasized that the lawmakers "would oppose any effort by the federal government" to encroach on the states' authorities.
>
> When U.S. spy agencies reached unanimous agreement in late September that the interference was a Russian operation directed by Putin, Obama directed spy chiefs to prepare a public statement summarizing the intelligence in broad strokes.

I'm all in favor of beating up McConnell, but there is no reason to demand members of Congress precede the IC with formal attribution for something like this. So until October 7, McConnell had cover (if not justification) for refusing to back a stronger statement.

And while the report describes Brennan's efforts to brief members of Congress (and the reported reluctance of Republicans to meet with him), it doesn't answer what remains a critical and open question: whether Brennan's briefing for Harry Reid was different [https://www.emptywheel.net/2017/05/24/john-brennan-denies-a-special-harry-reid-briefing/] — and more inflammatory — than his briefing for Republicans, and whether that was partly designed to get Reid to serve as a proxy attacker on Jim Comey and the FBI.

> Brennan moved swiftly to schedule private briefings with congressional leaders. But getting appointments with certain Republicans proved difficult, officials said, and it was not until after Labor Day that Brennan had reached all members of the "Gang of Eight" — the majority and minority leaders of both houses and the chairmen and ranking Democrats on the Senate and House intelligence committees.

Nor does this account explain another thing: why Brennan serially briefed the Gang of Eight, when past

experience is to brief them in groups, if not all together.

In short, while the WaPo provides new details on the parallel intelligence and political tracks, it reinforces its own narrative while remaining silent on some details that are critical to that narrative.

THE COMPARTMENTS

The foregrounding of CIA in all this also raises questions about a new and important detail about (what I assume to be the subsequently publicly revealed, though this is not made clear) Task Force investigating this operation: it lives at CIA, not FBI.

> Brennan convened a secret task force at CIA headquarters composed of several dozen analysts and officers from the CIA, the NSA and the FBI.
>
> The unit functioned as a sealed compartment, its work hidden from the rest of the intelligence community. Those brought in signed new non-disclosure agreements to be granted access to intelligence from all three participating agencies.
>
> They worked exclusively for two groups of "customers," officials said. The first was Obama and fewer than 14 senior officials in government. The second was a team of operations specialists at the CIA, NSA and FBI who took direction from the task force on where to aim their subsequent efforts to collect more intelligence on Russia.

Much later in the story, WaPo reveals how, in the wake of Obama calling for a report, analysts started looking back at their collected intelligence and learning new details.

> Obama's decision to order a comprehensive report on Moscow's interference from U.S. spy agencies had prompted analysts to go back through their agencies' files, scouring for previously overlooked clues.
>
> The effort led to a flurry of new, disturbing reports — many of them presented in the President's Daily Brief — about Russia's subversion of the 2016 race. The emerging picture enabled policymakers to begin seeing the Russian campaign in broader terms, as a comprehensive plot sweeping in its scope.

It's worth asking: did the close hold of the original Task Force, a hold that appears to have been set by Brennan, contribute to the belated discovery of these details revealing a broader campaign?

THE SURVEILLANCE DRIVEN SANCTIONS

I'm most interested in the description of how the Obama Admin chose whom to impose sanctions on, though it includes this bizarre claim.

> But the package of measures approved by Obama, and the process by which they were selected and

> implemented, were more complex than initially understood.
>
> The expulsions and compound seizures were originally devised as ways to retaliate against Moscow not for election interference but for an escalating campaign of harassment of American diplomats and intelligence operatives. U.S. officials often endured hostile treatment, but the episodes had become increasingly menacing and violent.

Several of the details WaPo presents as misunderstood (including that the sanctions were retaliation for treatment of diplomats) were either explicit in the sanction package or easily gleaned at the time [https://www.emptywheel.net/2017/01/01/a-deep-dive-on-the-obama-response-to-russian-dnc-hack-and-theft-and-harassment/] .

One of those easily gleaned details is that the sanctions on GRU and FSB were mostly symbolic. WaPo uses the symbolic nature of the attack on those who perpetrated the attack as a way to air complaints that these sanctions were not as onerous as those in response to Ukraine.

> "I don't think any of us thought of sanctions as being a primary way of expressing our disapproval" for the election interference, said a senior administration official involved in the decision. "Going after their

> intelligence services was not about economic impact. It was symbolic."
>
> More than any other measure, that decision has become a source of regret to senior administration officials directly involved in the Russia debate. The outcome has left the impression that Obama saw Russia's military meddling in Ukraine as more deserving of severe punishment than its subversion of a U.S. presidential race.
>
> "What is the greater threat to our system of government?" said a former high-ranking administration official, noting that Obama and his advisers knew from projections formulated by the Treasury Department that the impact of the election-related economic sanctions would be "minimal."

Three things that might play into the mostly symbolic targeting of FSB, especially, are not mentioned. First, WaPo makes no mention of the suspected intelligence sources who've been killed since the election, most credibly Oleg Erovinkin [https://cgrozev.wordpress.com/2017/01/14/tower-of-cards-part-1/] , as well as a slew of other suspect and less obviously connected deaths. It doesn't mention the four men Russia charged with treason [https://www.emptywheel.net/2017/02/26/reuters-confirms-krebs-supposition-on-russian-treason-charges/] in early December. And it doesn't mention DOJ's indictment of the Yahoo hackers

[https://www.emptywheel.net/2017/03/18/why-would-an-fsb-officer-use-a-yahoo-email-account-to-spy-for-russia/] , including one of the FSB officers, Dmitry Dokuchaev, that Russia charged with treason (not to mention the inclusion within the indictment of intercepts between FSB officers). There's a lot more spy vs. spy activity going on here that likely relates far more to retaliation or limits on US ability to retaliate, all of which may be more important in the medium term than financial sanctions.

Given the Yahoo and other indictments working through San Francisco (including that of Yevgeniey Nikulin [https://www.emptywheel.net/2017/06/02/putin-starts-talking-about-hackers-art-in-advance-of-yevgeniy-nikulin-extradition/] , who claims FBI offered him a plea deal involving admitting he hacked the DNC), I'm particularly interested in the shift in sanctions from NY to San Francisco, where Nikulin and Dokuchaev's victims are located.

> The FBI was also responsible for generating the list of Russian operatives working under diplomatic cover to expel, drawn from a roster the bureau maintains of suspected Russian intelligence agents in the United States.
>
> [snip]
>
> The roster of expelled spies included several operatives who were suspected of playing a role in Russia's election interference from within the

> United States, officials said. They declined to elaborate.
>
> More broadly, the list of 35 names focused heavily on Russians known to have technical skills. Their names and bios were laid out on a dossier delivered to senior White House officials and Cabinet secretaries, although the list was modified at the last minute to reduce the number of expulsions from Russia's U.N. mission in New York and add more names from its facilities in Washington and San Francisco.

And the WaPo's reports confirm what was also obvious: the two compounds got shut down (and were a priority) because of all the spying they were doing.

> The FBI had long lobbied to close two Russian compounds in the United States — one in Maryland and another in New York — on the grounds that both were used for espionage and placed an enormous surveillance burden on the bureau.
>
> [snip]
>
> Rice pointed to the FBI's McCabe and said: "You guys have been begging to do this for years. Now is your chance."
>
> The administration gave Russia 24 hours to evacuate the sites, and FBI agents watched as fleets of trucks

> loaded with cargo passed through the compounds' gates.

Finally, given Congress' bipartisan fearmongering about Kaspersky Lab, I'm most interested that at one point Treasury wanted to include them in sanctions.

> Treasury Department officials devised plans that would hit entire sectors of Russia's economy. One preliminary suggestion called for targeting technology companies including Kaspersky Lab, the Moscow-based cybersecurity firm. But skeptics worried that the harm could spill into Europe and pointed out that U.S. companies used Kaspersky systems and software.

In spite of all the fearmongering, no one has presented proof that Kaspersky is working for Russia (there are even things, which I won't go in to for the moment, that suggest the opposite). But we're moving close to de facto sanctions against Kaspersky anyway, even in spite of the fact (or perhaps because) they're providing better intelligence [https://www.emptywheel.net/2017/06/19/the-outdated-xp-testimony-to-congress/] on WannaCry than half the witnesses called as witnesses to Congress. But discrediting Kaspersky undercuts one of the only security firms in the world who, in addition to commenting on Russian hacking, will unpack America's own hacking. You sanction Kaspersky, and you expand the asymmetry with

which security firms selectively scrutinize just Russian hacking, rather than all nation-state hacking.

THE LOOMING CYBERATTACK AND THE SILENCE ABOUT SHADOW BROKERS

Which brings me to the last section of the article, where, over 8000 words in, the WaPo issues a threat against Russia in the form of a looming cyberattack Obama approved before he left.

WaPo's early description of this suggests the attack was and is still in planning stages and relies on Donald Trump to execute.

> Obama also approved a previously undisclosed covert measure that authorized planting cyber weapons in Russia's infrastructure, the digital equivalent of bombs that could be detonated if the United States found itself in an escalating exchange with Moscow. The project, which Obama approved in a covert-action finding, was still in its planning stages when Obama left office. It would be up to President Trump to decide whether to use the capability.

But if readers make it all the way through the very long article, they'll learn that's not the case. The finding has already been signed, the implants are already being placed (implants which would most likely be discovered by Kaspersky), and for Trump to stop it, he would have to countermand Obama's finding.

> The implants were developed by the NSA and designed so that they could be triggered remotely as part of retaliatory cyber-strike in the face of Russian aggression, whether an attack on a power grid or interference in a future presidential race.
>
> Officials familiar with the measures said that there was concern among some in the administration that the damage caused by the implants could be difficult to contain.
>
> As a result, the administration requested a legal review, which concluded that the devices could be controlled well enough that their deployment would be considered "proportional" in varying scenarios of Russian provocation, a requirement under international law.
>
> The operation was described as long-term, taking months to position the implants and requiring maintenance thereafter. Under the rules of covert action, Obama's signature was all that was necessary to set the operation in motion.
>
> U.S. intelligence agencies do not need further approval from Trump, and officials said that he would have to issue a countermanding order to stop it. The officials said that they have seen no indication that Trump has done so.

Whatever else this article is designed to do, I think, it is designed to be a threat to Putin, from long gone Obama officials.

Given the discussion of a looming cyberattack on Russia, it's all the more remarkable WaPo breathed not one word about Shadow Brokers, which is most likely to be a drawn out cyberattack by Russian affiliates on NSA. Even ignoring the Shadow Brokers' derived global ransomware attack in WannaCry, Shadow Brokers has ratcheted up the severity of its releases, including doxing NSA's spies and hacks of the global finance system [https://www.emptywheel.net/2017/04/19/the-doxing-of-equation-group-hackers-raises-questions-about-the-legal-role-of-nation-state-hackers/] , It has very explicitly fostered tensions [https://www.emptywheel.net/2017/05/16/shadow-brokers-further-incites-war-between-scumbag-microsoft-lawyer-and-nsa/] between the NSA and private sector partners (as well as the reputational costs on those private sector partners). And it has threatened to leak still worse, including NSA exploits against current Microsoft products and details of NSA's spying on hostile nuclear programs [https://www.emptywheel.net/2017/05/17/shadow-brokers-all-your-bases-belong-to-us/] .

The WaPo is talking about a big cyberattack, but an entity that most likely has close ties to Russia has been conducting one, all in plain sight. I suggested back in December that Shadow Brokers was essentially holding NSA hostage [https://www.emptywheel.net/2016/12/21/a-nice-little-nsa-youve-got-here-itd-be-a-shame-if/] in part as a way to constrain US intelligence retaliation

against Russia. Given ensuing events, I'm more convinced that is, at least partly, true.

But in this grand narrative of CIA's early warning and Obama's inadequate response, details like that remain unsaid.

Tags: Adam Schiff, Avril Haines, Denis McDonough, Dianne Feinstein, Dmitry Dokuchaev, Harry Reid, Jim Comey, John Brennan, Kaspersky Lab, Lisa Monaco, Mitch McConnell, Oleg Erovinkin, Shadow Brokers, Susan Rice, Vladimir Putin, WannaCry, Yevgeniy Nikulin

Share this entry

26

REPLIES

RickR
June 23, 2017 at 1:50 pm

EW Tweet: Why not Lisa Monaco in 1st briefing?

Perhaps because she was to attend upcoming Bilderberg meeting (06/01/17)?
Seems a bit far out on the calendar to affect this but? Could not find out how far in advance invitations go out. Up to a year wouldn't surprise me.

Reply

SpaceLifeForm
June 23, 2017 at 7:16 pm

Year or two. Security planning.
All 'Super Duper Top Secret' of course until it becomes obvious or leaked.

Next one will not be at Trump Tower based on latest intel.

Reply

RickR
June 23, 2017 at 10:21 pm

Hard info or educated guess? I'd understand that far out for planning but seems invitees would be shorter notice. I expect it varies. If Monaco was an early invitee we might wonder if her presence in O's admin was more than meets the eye.

Attendees this year:
http://www.bilderbergmeetings

Note David Patraeus back from the dead.
Especially interesting Lindsey Graham & Tom Cotton. Seems a little early in the Cotton career. They're sizing up the rising star? Thought we might get some clues to what the MoU's are thinking from these two after Bilderberg. Cotton seems to be biz as usual kick-ass GOP. Graham, though, seems a bit

less vocal but more serious in demeanor than he was pre-Bilderberg.

Reply

SpaceLifeForm
June 24, 2017 at 1:56 pm

My ref to TT and the intel was snarky, I admit.
But almost certainly fact due to three reasons.

1. Last meeting three weeks ago was at the Westfields Marriott in Chantilly, Virginia, not far from White House.

2. President Trump was a heavy topic of discussion.

3. Almost certainly, next years meeting will be Europe.

I can not find a link to where I read about the one year ahead (at lesst). I probably read it twenty years ago, so the site may be gone.

But this will tell you that the planning almost

certainly has to be a minimum of one year.

http://www.sourcewatch

Resorts and hotels where the meetings are held are cleared of residents and visitors and surrounded by soldiers, armed guards, Secret Service, state and local police. Conference areas are scanned for bugging devices prior to every meeting.

Reply

SpaceLifeForm
June 23, 2017 at 2:48 pm

Some group is definitely trying to sell a story.
I wonder if they are trying to corner the market on red herrings. Maybe by causing the flash crash on ether cryptocurrency this past week?
(Of course one should not trade on margin)

Brennan serial briefings. Two possible reasons: Sow disinformation/confusion and/or attempt to find leakers (secret intel verbal watermarking). Do not know his motive for this approach, but suspect most leaks are coming from within IC agencies, not Go8.

Brennan secret task force convened before or after Obama updated EO12333 for intel sharing?

No way Trump could countermand a looming cyberattack. Just can not see it happening.
Hell, he would have to be aware of it and then it would look horrible for him politically because the order to do so would certainly be leaked. Note Russia was hit hard by Wannacry. It was a warning.

I believe the implants most likely are already deployed. Even if Trump were to order cancel of op, it could still occur at a future point in time. It is just a matter of time before it is discovered, and then can be exploited anyway regardless of the view of any current or future U.S. president. SB possibly know how to do it at this point, There are so many hints out there that given enough time, money, and brainpower, sufficient effort will find it.

I can think of multiple ways of how it can be done, already buried in silicon.

Wannacry?

Reply

> **Bardi**
> June 23, 2017 at 8:29 pm
>
> Perhaps you should read this:
>
> https://www.nytimes.com/2017/06/22/
> attack-nsa-cyberweapons.html
>
> Reply
>
> > **SpaceLifeForm**
> > June 24, 2017 at 3:12 pm
> >
> > Thank you. Excellent report. I hope everyone here reads it

even if they do not completely understand the tech. It is damning enough that just by reading the article a non-techie should be able to appreciate the looming danger. Hopefully.

A couple of things. NSA had/gave bad info and FBI distracted. See my post(s) below on the MS source code dump.

The NSA person (CIA mole?) gave out bad info with regard to antivirus. You should only run one antivirus if any. A lot of times, they will conflict with each other. But, more importantly, it increases the attack surface because the antivirus code already has elevated privilege and it just makes it easier for an attacker.

Note: The attack vector for EternalBlue and DoublePulsar may have nothing to do with any antivirus attack surface. I really doubt it.
At this point in time, imho, running any antivirus software on a Windows computer is just security theatre. You may be better off *NOT* running any antivirus software at all and just

using common sense. Not opening anything recieved unless you were expecting it and it came from a trusted source. Even then, you can not trust.

—

Six years ago, Mr. Ben-Oni had a chance meeting with an N.S.A. employee at a conference and asked him how to defend against modern-day cyberthreats. The N.S.A. employee advised him to "run three of everything": three firewalls, three antivirus solutions, three intrusion detection systems. And so he did.

But in this case, modern-day detection systems created by Cylance, McAfee and Microsoft and patching systems by Tanium did not catch the attack on IDT. Nor did any of the 128 publicly available threat intelligence feeds that IDT subscribes to. Even the 10 threat intelligence feeds that his organization spends a half-million dollars on annually for urgent information failed to report it. He has since

threatened to return their products.

[Defense in depth – fail]

…

Last month, he personally briefed the F.B.I. analyst in charge of investigating the WannaCry attack. He was told that the agency had been specifically tasked with WannaCry, and that even though the attack on his company was more invasive and sophisticated, it was still technically something else, and therefore the F.B.I. could not take on his case.

[So, Wannacry is also a distraction and resource waster for FBI. Chasing ghosts]

Reply

John Casper

June 23, 2017 at 2:53 pm

Wow!

Riveting!

Reply

P J Evans

June 23, 2017 at 3:30 pm

Kaspersky has a lot of the PC security market outside of business. I wonder how – or if – that plays into this.

Reply

seedeevee

June 23, 2017 at 3:59 pm

"As a result, the administration requested a legal review"

Hahahahah! I'm sure Obama, Brennan and Rice made sure it was all on the up and up.

Reply

SpaceLifeForm

June 23, 2017 at 4:27 pm

Hmmmmmmm. Note those not mentioned.

Under pressure, Western tech firms bow to Russian demands to share cyber secrets

http://mobile.reuters.com/article/idUSKBN19E0XB

Western technology companies, including Cisco, IBM and SAP, are acceding to demands by Moscow for access to closely guarded product security secrets, at a time when Russia has been accused of a growing number of cyber attacks on the West, a Reuters investigation has found.

Reply

SpaceLifeForm
June 23, 2017 at 5:51 pm

Quickly, some angles may have been addressed.

https://threatpost.com/cisco-patches-xxe-dos-code-execution-vulnerabilities/126488/

Cisco patched three vulnerabilities in three products this week that if exploited, could have resulted in a denial of service, crash, and in some instances, arbitrary and remote code execution.

…

The vulnerabilities were three of 25 different security issues Cisco warned about on Wednesday.

Reply

SpaceLifeForm
June 23, 2017 at 4:50 pm

OT: Is Gannon the new Yoo?

http://www.npr.org/2017/06/21/533822177/democrat seek-records-on-jared-kushner-as-administration-tries-to-stifle-oversi

"It is unclear why Mr. Kushner continues to have access to classified information while these allegations are being investigated," says the letter,

which seeks similar records on former national security adviser Michael Flynn

….

The Trump administration has ignored hundreds of congressional letters of inquiry.

It is also brandishing a legal opinion, crafted by the Justice Department, holding that most of Congress lacks the constitutional power to conduct oversight of the executive branch.

[Most of Congress? I must disagree]

Reply

GKJames
June 23, 2017 at 5:52 pm

Is that a bit naive re: McConnell? It's a certainty that Mitch's response would have been different if the allegation — however thin — were that it was Clinton whom the Kremlin was aiming to get elected.

Reply

SpaceLifeForm
June 23, 2017 at 6:39 pm

Finally, some traction. Thank you Zack for covering.
Been saying this has been going on for years, nee decades. Since y2k.
(Hope you caught that an article your wrote about a hack dump included you in the dump. I wrote about it here)

This is about BGP hijacking and control of 'upstream' routers. And insecure DNS. Many or most 'upstream' routers and/or DNS servers under control or influence via IC-Spycorp partnerships. This is why FISC is useless, because via this 12333 route (no pun intended), FISC is just security theatre.

—

NSA's use of 'traffic shaping' allows unrestrained spying on Americans

By using a "traffic shaping" technique, the National Security Agency sidestepped legal restrictions imposed by lawmakers and the surveillance courts.

http://www.zdnet.com/google-amp/article/legal-loopholes-unrestrained-nsa-surveillance-on-americans/

A new analysis of documents leaked by whistleblower Edward Snowden details a highly classified technique that allows the National Security Agency to "deliberately divert" US internet traffic, normally safeguarded by constitutional protections, overseas in order to conduct unrestrained data collection on Americans.

According to the new analysis, the NSA has clandestine means of "diverting portions of the river of internet traffic that travels on global communications cables," which allows it to bypass protections put into place by Congress to prevent domestic surveillance on Americans.

[Note: FISC is totally powerless to stop this]

Reply

SpaceLifeForm

June 23, 2017 at 6:56 pm

Microsoft bravado on win10s to hacked – 3 hours.

http://www.zdnet.com/google-amp/article/microsoft-no-known-ransomware-windows-we-tried-to-hack-it/

Reply

lefty665

June 23, 2017 at 8:40 pm

Nice analysis Marcy. Looks like the Wash Post is up to its usual tricks. In all a lot more flash and smoke mixed with some inside the administration process that may compromise sources and methods, but very little more substance. All seems designed to fuel "The Russians did it, and Trump's people talked to (gasp) Russians" hysteria.

Although buried deep in the article, the NSA's lack of confidence in Brennan's CIA super secret Putin poop leapt off the page at me when I read it. Don't suppose the Israelis would use Brennan to further their own interests do you? Perish that thought, or that he might be working for them.

We can expect the GRU and FSB to be working in support of Russian interests just as the NSA and FBI do for the US. It is a long way from there to Trump collaborating with the Ruskies to overturn the election. Who knows? Da Shadow (Brokers) knows. Also nice to see that Kerry's neocon driven predilection for flying off the handle got squelched once again.

Reply

RickR

June 23, 2017 at 11:36 pm

Picking up on SpaceLifeForm's comment (06/23 @ 9:45PM – Thanks!) in the "Penetrated…" post:

8300 word WaPo opus and no mention of Mike Rogers at all? NSA was mentioned. He's been head of NSA and Cyber Command since 04/14. Still is. Was he firewalled? Wouldn't WaPo have asked that and commented on whatever answer they got?
Recall that WaPo (11/19/16) reported that Carter and Clapper had recommended that Rogers be terminated for poor performance in internal security and leadership style. Recall too that Rogers met with Trump shortly after the election without notifying his supervisors; odd for a military guy.

Now Trump says, "Well I just heard today for the first time that Obama knew about Russia a long time before the election, and he did nothing about it."

Really? Did Rogers just hear it today too? Do he and Trump speak?
I gotta think Trump's "…. just heard today for the first time…." ain't quite true.

Reply

trevanion

June 24, 2017 at 8:49 am

No doubt a suitably higher church explanation for all of this will soon be provided via some David Ignatius stenography.

Reply

lefty665
June 24, 2017 at 10:39 am

Who would anyone believe anything coming out of CIA? Their mission is propaganda, deception and manipulation. No matter the issue they are always grinding an axe. A reasonable expectation is that there is an inverse correlation between the drama a CIA presentation is wrapped in and truth.

Reply

SpaceLifeForm
June 24, 2017 at 12:25 pm

Opps. Microsoft source code dump. Enough at least for new exploits.

https://www.theregister.co.uk/2017/06/23/windows_

The leaked code is Microsoft's Shared Source Kit: according to people who have seen its contents, it includes the source to the base Windows 10 hardware drivers plus Redmond's PnP code, its USB and Wi-Fi stacks, its storage drivers, and ARM-specific OneCore kernel code.

Reply

> ### SpaceLifeForm
> June 24, 2017 at 3:30 pm

A strange game.

Thinking leaked on purpose.

I recommend that you have a working up-to-date Linux or MacOS computer on your LAN. Just in case. Even then, things could go sideways anyway.

If possible, try to have a Linux or BSD firewalll/router in place too.

Reply

SpaceLifeForm
June 24, 2017 at 4:27 pm

And this would to me explain why it was intentional.

Note that the hole that allows the exploit is likely so old (64 bit XP), that Vista and Win 7 would be targetable, besides 8 and 10.

Sounds like the vector for Wannacry I have been looking for. And, as noted above, how IDT was attacked and FBI is being distracted,
Wannacry was just a warning, and now everyone that was hit by Wannacry most certainly should assume at tbis point that their machine already has a persistent rootkit installed,

ready to participate in a massive DDoS.

Anyone hitt by Wannacry, even if only one machine on their LAN, should at this point assume their entire LAN had been compromised.

https://en.m.wikipedia.org/wiki

Kernel Patch Protection (KPP), informally known as PatchGuard, is a feature of 64-bit (x64) editions of Microsoft Windows that prevents patching the kernel. It was first introduced in 2005 with the x64 editions of Windows XP and Windows Server 2003 Service Pack 1.

https://www.theregister.co.uk/2

GhostHook is nonetheless dangerous because it runs under the radar at such a low level that it avoids detection by antivirus or personal firewall technologies. Attack scenarios would include using malware or a hacking tool to compromise a target system before deploying GhostHook to establish a permanent, stealthy presence on a compromised x64 Windows 10 computer.

Attackers might be able to use the method to plant a rootkit in the kernel – completely undetectable to third-party security products and invisible to Microsoft's PatchGuard itself.

Reply

> **SpaceLifeForm**
> June 24, 2017 at 6:29 pm
>
> Cisco says they can stop. Doubt it. Lke FBI, chasing ghosts.
>
> https://www.wsj.com/articles/cisco-bets-on-security-to-drive-switch-sales-1497981600
>
> Networking giant reveals security service it says can identify and stamp out malicious software cloaked by encryption
>
> Reply

SpaceLifeForm
June 24, 2017 at 6:11 pm

And make sure your non-Windows boxen on your LAN are up-to-date, as in real soon now.

Also tells you that ASLR on 64 bit machines is just more security theatre.

If you do not understand the tech, you probably will not want to read thIs.

But, you want your non-Windows machines to be up to date, because they may be your only working machines at some point.

https://threatpost.com/stack-clash-vulnerability-in-linux-bsd-systems-enables-root-access/126355/

Reply

SpaceLifeForm
June 24, 2017 at 5:50 pm

LOL Good to see someone elected not buying the BS someone is trying to sell these days.

Perhaps SB is dumping and attacking because no one has joined the wine-of-the-month club?

Or maybe they are trying to drive up pub sales?

From @HenrySmithUK

https://mobile.twitter.com/HenrySmithUK/status/878

Sorry no parliamentary email access today – we're under cyber attack from Kim Jong Un, Putin or a kid

in his mom's basement or something…

Reply