Thread by @Cynacin: "1/ I have conducted extensive research on the media reports, forensic evidence, statements and indictments of the 12 Russians alleged to hav [...]"

58 tweets a day ago

Lycaon
@Cynacin

1/ I have conducted extensive research on the media reports, forensic evidence, statements and indictments of the 12 Russians alleged to have hacked Podesta, the DNC, and the DCCCC.

The information is frequently contradictory, self-refuting, and suspicious.

2/ In April 2016, Obama, the DNC and the Clinton campaign paid Perkins Coie nearly a million dollars who then paid Fusion GPS to research "Links between Trump and Russia".

thefederalist.com/2017/10/29/oba...

Obama's Campaign Paid $972,000 To Law Firm That Secretly Paid Fusion GPS In 2016

Since April of 2016, Obama's campaign organization has paid nearly a million dollars to the law firm that funneled money to Fusion GPS to compile a dossier of unverified allegations against Donald Trump.

OCTOBER 29, 2017 By Sean Davis

Former president Barack Obama's official campaign organization has directed nearly a million dollars to the same law firm that funneled money to Fusion GPS, the firm behind the infamous Steele dossier. Since April of 2016, Obama For America (OFA) has paid over $972,000 to Perkins Coie, records filed with the Federal Election Commission (FEC) show.

The Washington Post reported last week that Perkins Coie, an international law firm, was directed by both the Democratic National Committee (DNC) and Hillary Clinton's campaign to retain Fusion GPS in April of 2016 to dig up dirt on then-candidate Donald Trump. Fusion GPS then hired Christopher Steele, a former British spy, to compile a dossier of allegations that Trump and his campaign actively colluded with the Russian government during the 2016 election. Though many of the claims in the

3/ That same month:

- Perkins Coie also contacted Crowstrike to investigate a suspected DNC network intrusion.

- The website DCLeaks.com was registered.

By **CHRIS STOKEL-WALKER**

Sunday 5 March 2017

Dmitri Alperovitch says there are two types of organisations: "Those that know they've been hacked, and those that don't know right now, but have been hacked anyway." For the first few months of 2016, the Democratic National Committee (DNC), fell firmly into the second category. Working flat out to make Hillary Clinton the next president of the United States, its staff ignored warnings that they'd been hacked. But, by April 2016, they acknowledged something was wrong. That was when the DNC called Alperovitch and CrowdStrike, his Washington DC-based cybersecurity company.

CrowdStrike was born out of a frustration with the traditional way of dealing with hacks: occasionally updated anti-virus programmes looking for malicious software sent by bedroom hackers. Alperovitch, 36, (pictured) who was born in Moscow and moved to the US in his teens, and his co-founder George Kurtz, 46, knew this system well - they worked on it at security giant McAfee. "The threat landscape was changing dramatically," Alperovitch says. "It was very hard at McAfee to do anything about it. So George and I got together and said there's a better way."

35. More than a month before the release of any documents, the Conspirators constructed the online persona DCLeaks to release and publicize stolen election-related documents. On or about April 19, 2016, after attempting to register the domain electionleaks.com, the Conspirators registered the domain dcleaks.com through a service that anonymized the registrant. The funds used to pay for the dcleaks.com domain originated from an account at an online cryptocurrency service that the Conspirators also used to fund the lease of a virtual private server registered with the operational email account dirbinsaabol@mail.com. The dirbinsaabol email account was also used to register the john356gh URL-shortening account used by LUKASHEV to spearphish the Clinton Campaign chairman and other campaign-related individuals.

4/ Crowdstrike immediately installed a software application called FALCON onto the DNC's computers.

Similar to the anti-virus program Kaspersky, FALCON uploads monitoring information, suspicious files and system data to the cloud.

> Almost immediately, Falcon started lighting up with a number of indications of breaches of the DNC network"
>
> Dmitri Alperovitch, founder of Crowdstrike

5/ Crowdstrike did NOT follow multiple required procedures for computer forensics and evidence collection.

In doing so, Crowdstrike contaminated any evidence that may have been on those computer systems, making it inadmissible in court.

faqs.org/rfcs/rfc3227.h...

> George and I got together and said there's a better way."
>
> Up to 60 per cent of the hacks we read about don't use malware, Kurtz says. "They use credentials. They're social engineering." They're also carried out by state-sponsored groups specifically set up to engage in cyberwarfare with other countries. This new type of attack - bigger, bolder, but more secretive - goes undetected, often for hundreds of days, just as it did for the DNC.
>
> When CrowdStrike came to the DNC, it moved quickly. Using a system called Falcon, a two-megabyte agent installed on systems without the need for a reboot, it profiled every action that occurred at a programme level on the hundreds of machines owned by the DNC. One clue might be a programme behaving abnormally; it might be the unusual transfer of millions of documents. "We're not looking at any personal data, any documents or emails," explains Alperovitch. "We're just looking at what is being executed."

> 2.1 Order of Volatility
>
> When collecting evidence you should proceed from the volatile to the less volatile. Here is an example order of volatility for a typical system.
>
> - registers, cache
> - routing table, arp cache, process table, kernel statistics, memory
> - temporary file systems
> - disk
> - remote logging and monitoring data that is relevant to the system in question
> - physical configuration, network topology
> - archival media

> 2 Guiding Principles during Evidence Collection
>
> - Adhere to your site's Security Policy and engage the appropriate Incident Handling and Law Enforcement personnel.
> - Capture as accurate a picture of the system as possible.
> - Keep detailed notes. These should include dates and times. If possible generate an automatic transcript. (e.g., On Unix systems the 'script' program can be used, however the output file it generates should not be to media that is part of the evidence). Notes and print-outs should be signed and dated.
> - Note the difference between the system clock and UTC. For each timestamp provided, indicate whether UTC or local time is used.
> - Be prepared to testify (perhaps years later) outlining all actions you took and at what times. Detailed notes will be vital.
> - Minimise changes to the data as you are collecting it. This is not limited to content changes; you should avoid updating file or directory access times.
> - Remove external avenues for change.

> 2 Guiding Principles during Evidence Collection
>
> - Adhere to your site's Security Policy and engage the appropriate Incident Handling and Law Enforcement personnel.
> - Capture as accurate a picture of the system as possible.
> - Keep detailed notes. These should include dates and times. If possible generate an automatic transcript. (e.g., On Unix systems the 'script' program can be used, however the output file it generates should not be to media that is part of the evidence). Notes and print-outs should be signed and dated.
> - Note the difference between the system clock and UTC. For each timestamp provided, indicate whether UTC or local time is used.
> - Be prepared to testify (perhaps years later) outlining all actions you took and at what times. Detailed notes will be vital.
> - Minimise changes to the data as you are collecting it. This is not limited to content changes; you should avoid updating file or directory access times.
> - Remove external avenues for change.

6/ FALCON is an endpoint protection / anti-virus program, NOT a Digital Forensics and Evidence Collection program.

Such a program, if used after compromise, needs to be executed from external media. According to their statements, this did not occur.

7/ Crowdstrike has since claimed that they provided the FBI with exact system images however, the response timetable and their statements about installing FALCON contradict that claim.

Imaging and collecting evidence the proper way would have taken significantly more time.

> CrowdStrike was born out of a frustration with the traditional way of dealing with hacks: occasionally updated anti-virus programmes looking for malicious software sent by bedroom hackers. Alperovitch, 36, (pictured) who was born in Moscow and moved to the US in his teens, and his co-founder George Kurtz, 46, knew this system well - they worked on it at security giant McAfee. "The threat landscape was changing dramatically," Alperovitch says. "It was very hard at McAfee to do anything about it. So George and I got together and said there's a better way."

> The long answer is that there is no "server"—there are many different servers and pieces of internet infrastructure in question, and the United States intelligence community and independent security researchers have examined much of it and have all reached the same conclusion: Russia hacked the DNC.
>
> It is widely believed that CrowdStrike, a cybersecurity firm hired by the DNC to respond to the hack, gave an identical image of some of the servers to the FBI, which experts I've spoken to say would be more useful than giving the FBI a physical server itself. I say "widely believed," because we don't know exactly what CrowdStrike gave to the FBI. However, in March 2017, former FBI Director James Comey told Congress that the FBI got an "appropriate substitute" from CrowdStrike, and Mueller's indictment makes clear that the FBI has lots of information about the hack from both within the DNC and from other sources. CrowdStrike declined a request for comment from Motherboard.

8/ Any evidence collected after installing FALCON would have been tainted and inadmissible.

This likely explains the DNC's refusal to provide the FBI with physical access to their

motherboard.vice.com/en_us/article/...

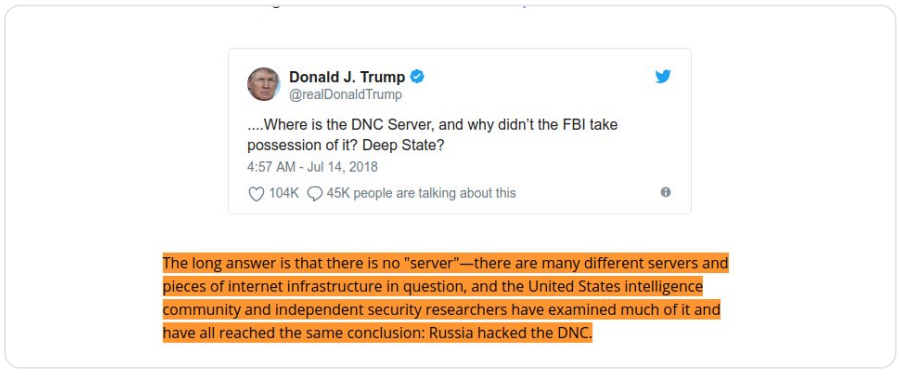

MOTHERBOARD

how digital fo

TRUMP | By Jason Koebler | Jul 16 2018, 4:23pm

Trump's Stupid 'Where Is the DNC Server?' Conspiracy Theory, Explained

Trump refuses to believe all the evidence that Russia hacked the DNC, because he understands nothing about how digital forensics works.


Donald J. Trump
@realDonaldTrump

....Where is the DNC Server, and why didn't the FBI take possession of it? Deep State?

4:57 AM - Jul 14, 2018

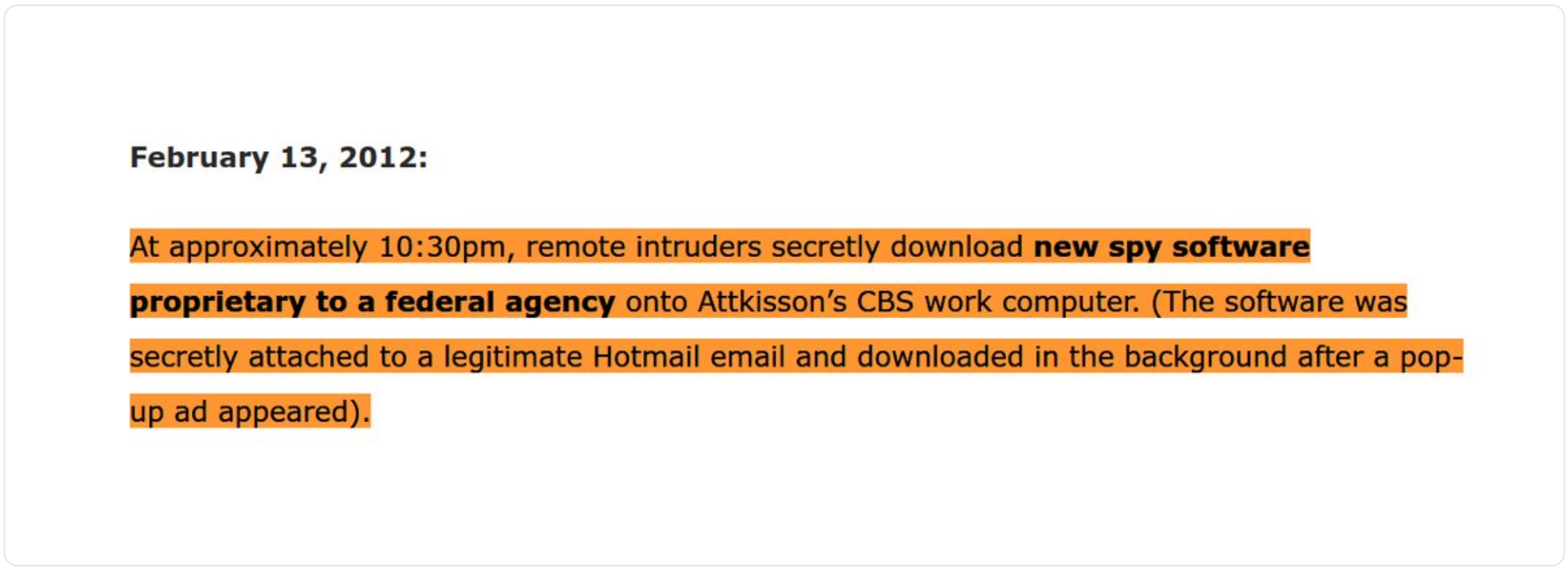
104K 45K people are talking about this

The long answer is that there is no "server"—there are many different servers and pieces of internet infrastructure in question, and the United States intelligence community and independent security researchers have examined much of it and have all reached the same conclusion: Russia hacked the DNC.

9/ On June 12, 2016 @JulianAssange publicly announced upcoming leaks concerning Hillary Clinton.

The Obama administration had been spying on journalists with malware installed on their computers, so it's likely they knew about the leaks beforehand.

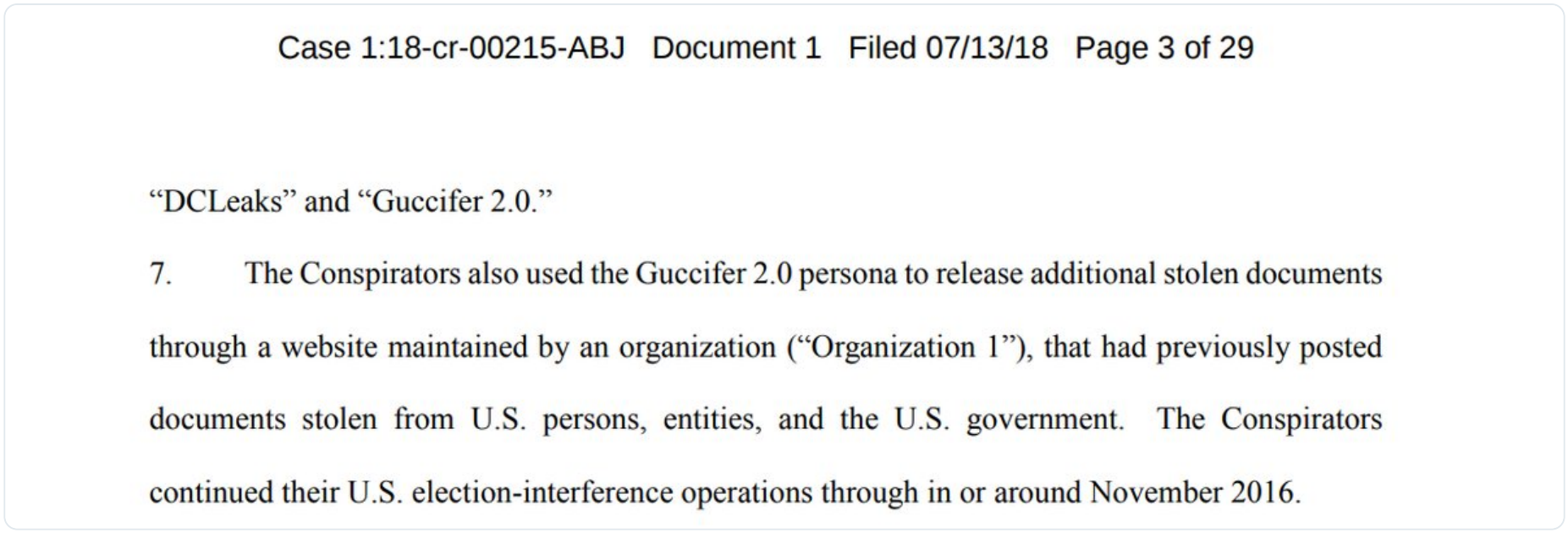
sharylattkisson.com/2017/12/05/oba...


February 13, 2012:

At approximately 10:30pm, remote intruders secretly download **new spy software proprietary to a federal agency** onto Attkisson's CBS work computer. (The software was secretly attached to a legitimate Hotmail email and downloaded in the background after a pop-up ad appeared).

10/ Mueller's case rests upon connecting the Guccifer 2.0 persona to alleged attacks and data disclosures. This is also highly suspicious.

justice.gov/file/1080281/d...


Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 3 of 29

"DCLeaks" and "Guccifer 2.0."

7. The Conspirators also used the Guccifer 2.0 persona to release additional stolen documents through a website maintained by an organization ("Organization 1"), that had previously posted documents stolen from U.S. persons, entities, and the U.S. government. The Conspirators continued their U.S. election-interference operations through in or around November 2016.

computerweekly.com/news/252445769...

The Guccifer deception

The GRU's hackers were caught red-handed in June 2016, when the *Washington Post* exposed evidence of their role. Within 24 hours, after the Post had asked Russia for comment, the hackers fabricated evidence and planted a false trail that the hacking was the work of an imaginary, lone Romanian called Guccifer 2.0. While this happened, GRU officers were spotted doing online searches to check English phrases while penning the first blog post for their Romanian fake, according to the DoJ indictment.

Guccifer 2.0's role was "falsely to undermine the allegations of Russian responsibility for the intrusion", according to the indictment. US and European intelligence agencies identified "Guccifer 2.0" as a Russian deception operation before Americans went to vote. Detailed evidence had not been publicly available until the publication of the indictment.

12/ That claim is dubious. APT28 & APT29 had been operating since at least 2007, had attacked governments and corps in Eastern Europe and had been attributed to Russia with "Moderate Confidence".

A WaPo article would not have scared them.

secureworks.com/research/threa...

Threat Group-4127 Targets Hillary Clinton Presidential Campaign

THURSDAY, JUNE 16, 2016
BY: SECUREWORKS COUNTER THREAT UNIT THREAT INTELLIGENCE

- **Author:** SecureWorks Counter Threat Unit™ Threat Intelligence
- **Date:** 16 June 2016

Summary

The Hillary Clinton email leak was the center of the latest scandal in the news caused by Threat Group-4127[1] (TG-4127). SecureWorks® Counter Threat Unit™ (CTU) researchers track the activities of Threat Group-4127, which targets governments, military, and international non-governmental organizations (NGOs). Components of TG-4127 operations have been reported under the names APT28, Sofacy, Sednit, and Pawn Storm. CTU™ researchers assess with moderate confidence that the group is operating from the Russian Federation and is gathering intelligence on behalf of the Russian government.

research on Trump.

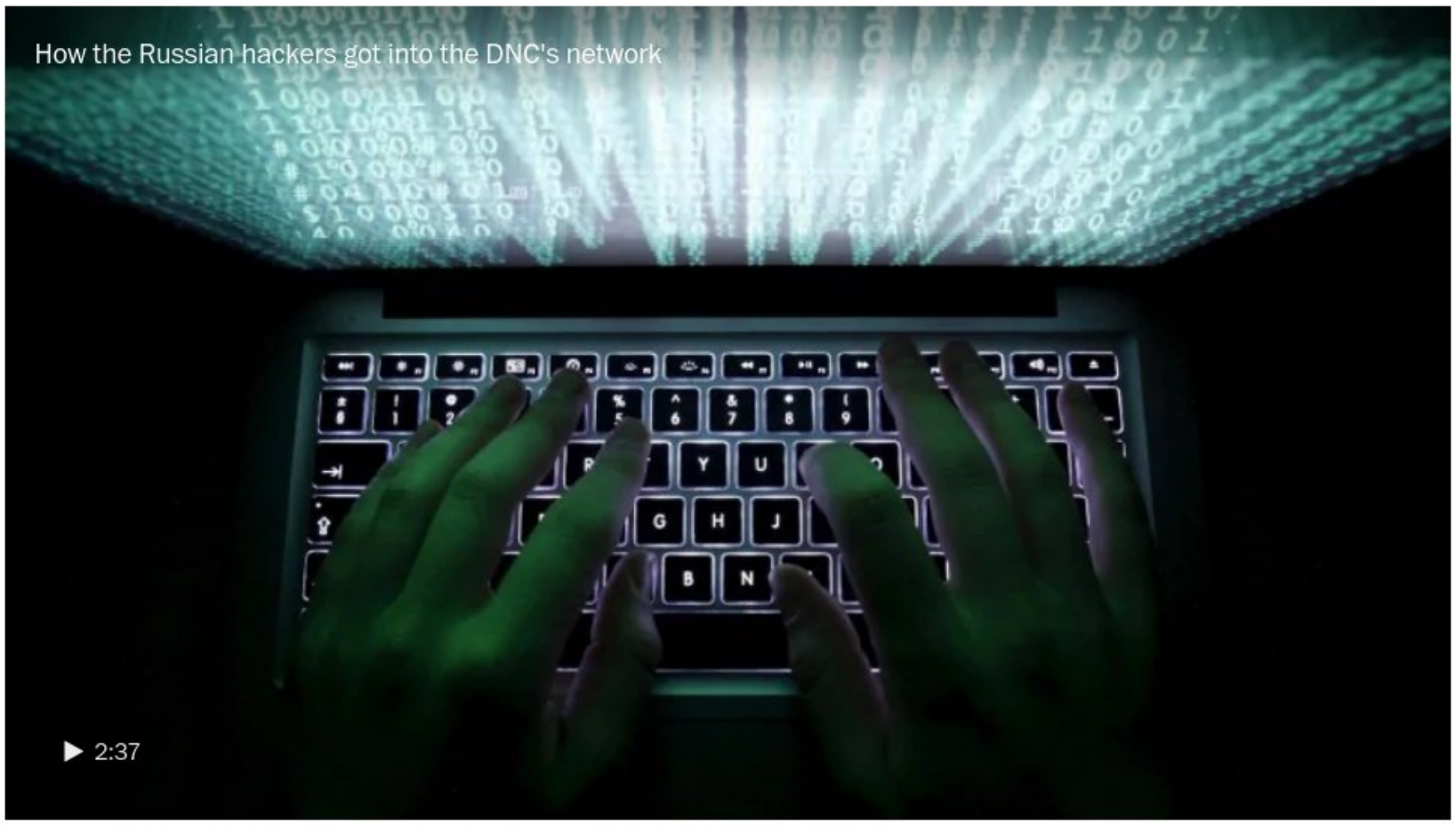
This was one of the first documents released by G2.

Clinton claimed the release was "damaging" to her campaign.

washingtonpost.com/world/national...

National Security

Russian government hackers penetrated DNC, stole opposition research on Trump



The Post's Ellen Nakashima goes over the events, and discusses the two hacker groups responsible. (Jhaan Elker/The Washington Post)

By Ellen Nakashima June 14, 2016 Email the author

14/ Everying in the Donald Trump Opposition research released by Guccifer 2 had already been publicly alleged EXCEPT accusations about Trump having corrupt ties to Russia.

guccifer2.wordpress.com/2016/06/15/dnc/

15/ WaPo claims that Cozy Bear (APT29) did not access financial or personal information, focusing on certain documents, and was "traditional espionage".

This characterization is in not representative of nation-state sponsored "traditional" espionage.

> Some of the hackers had access to the DNC network for about a year, but all were expelled over the past weekend in a major computer cleanup campaign, the committee officials and experts said.
>
> The DNC said that no financial, donor or personal information appears to have been accessed or taken, suggesting that the breach was traditional espionage, not the work of criminal hackers.
>
> The intrusions are an example of Russia's interest in the U.S. political system and its desire to understand the policies, strengths and weaknesses of a potential future president — much as American spies gather similar information on foreign candidates and leaders.

16/ This claim also contradicts existing research into APT29.

"These campaigns utilize a smash-and-grab approach involving a fast but noisy breakin followed by the rapid collection and exfiltration of AS MUCH DATA AS POSSIBLE".

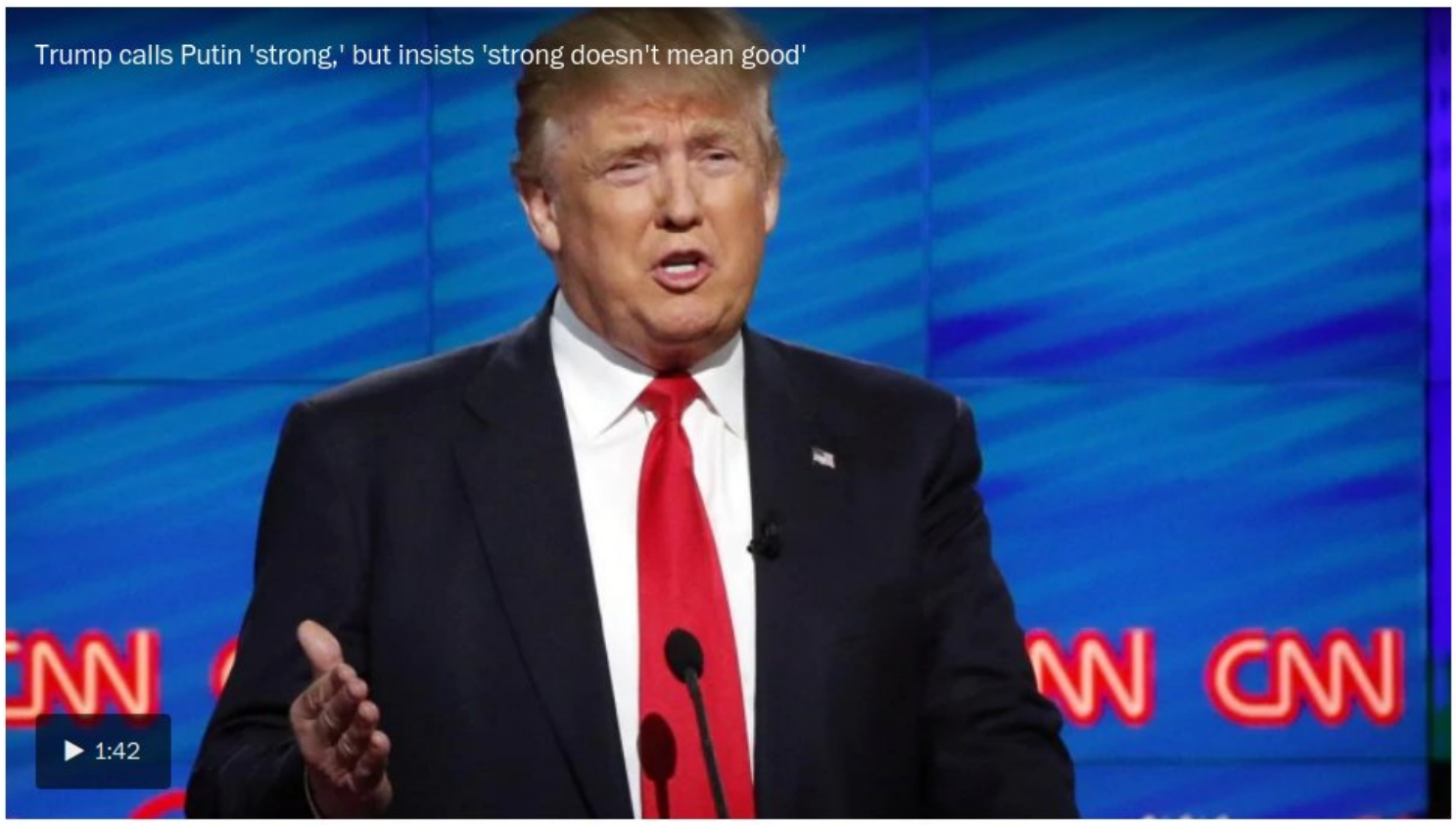
f-secure.com/documents/9965...

identify as MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke, and GeminiDuke. In recent years, the Dukes have engaged in apparently biannual large-scale spear-phishing campaigns against hundreds or even thousands of recipients associated with governmental institutions and affiliated organizations.

These campaigns utilize a smash-and-grab approach involving a fast but noisy break-in followed by the rapid collection and exfiltration of as much data as possible. If the compromised target is discovered to be of value, the Dukes will quickly switch the toolset used and move to using stealthier tactics focused on persistent compromise and long-term intelligence gathering.

17/ There was no intelligence assessment and the attribution of APT28 and APT29 to Russia was only with "moderate confidence" at the time.

Despite this, the WaPo article claimed it was Russia with 100% confidence and began framing the narrative that Trump was involved.



Donald Trump has repeatedly called Vladimir Putin a "strong" leader, but toes a fine line on praising the Russian president. (Peter Stevenson/The Washington Post)

"We're perceived as an adversary of Russia," he said. "Their job when they wake up every day is to gather intelligence against the policies, practices and strategies of the U.S. government. There are a variety of ways. [Hacking] is one of the more valuable because it gives you a treasure trove of information."

Russian President Vladimir Putin has spoken favorably about Trump, who has called for better relations with Russia and expressed skepticism about NATO. But unlike Clinton, whom the Russians probably have long had in their spy sights, Trump has not been a politician for very long, so foreign agencies are playing catch-up, analysts say.

18/ In the week leading up to the WaPo article, Fusion GPS made payments to journalists. While the specific entities are redacted on the unsealed court records, "The Washington Post" fits the size of the redaction and has been named by House and Senate investigators.

Fusion's specialty is seeding its opposition research into news stories, a modus operandi highlighted by a 2011 interview with co-founder Peter Fritsch.

http://www.mondaq.com/x/144198/Antigua+A+New+Spotlight

[redacted]

The Committee therefore seeks records related to Fusion's work on behalf of media companies, including to determine whether such companies were the beneficiary of dossier or other Russia-related information. [redacted]

19/ Fusion is best known for "seeding" their opposition research to the media.

The dossier alleges that Trump had corrupt ties to Russians, including the owners of Alfa Bank, who were hacking the DNC to influence the 2016 election.

Page 11/35

RUSSIA-US PRESIDENTIAL ELECTION: KREMLIN CONCERN THAT POLITICAL FALLOUT FROM DNC E-MAIL HACKING AFFAIR SPIRALLING OUT OF CONTROL

Summary

— Kremlin concerned that political fallout from DNC e-mail hacking operation is spiraling out of control. Extreme nervousness among associates as result of negative media attention/accusations

— Russians meanwhile keen to cool situation and maintain 'plausible deniability' of existing /ongoing and operations. Therefore unlikely to be any ratcheting up offensive plays in immediate future

— Source close to TRUMP campaign however confirms regular exchange with Kremlin has existed for at least 8 years, including intelligence fed back to Russia on oligarchs' activities in US

— Russians apparently have promised not to use 'kompromat' they hold on TRUMP as leverage, given high levels of voluntary co-operation forthcoming from his team

Detail

1. Speaking in confidence to a trusted associate in late July 2016, a Russian emigre' figure close to the Republican US presidential candidate Donald TRUMP's campaign team commented on the fallout from publicity surrounding the Democratic National Committee (DNC) e-mail hacking scandal. The emigre' said there was a high level of anxiety within the TRUMP team as a result of various accusations levelled against them and indications from the Kremlin that President PUTIN and others in the leadership thought things had gone too far now and risked spiralling out of control.

2. Continuing on this theme, the emigre' associate of TRUMP opined that the Kremlin wanted the situation to calm but for 'plausible deniability' to be maintained concerning its (extensive) pro-TRUMP and anti-CLINTON operations. S/he therefore judged that it was unlikely these would be ratcheted up, at least for the time being.

3. However, in terms of established operational liaison between the TRUMP team and the Kremlin, the emigre' confirmed that an intelligence exchange had been running between them for at least 8 years. Within this context PUTIN's priority requirement had been for intelligence on the activities, business and otherwise, in the US of leading Russian oligarchs and their families. TRUMP and his associates duly had obtained and supplied the Kremlin with this information.

20/ On October 31st, about a week before the November election, SLATE published an article alleging that a Trump server was communicating secretly with Alfa Bank.

slate.com/articles/news_...

Was a Trump Server Communicating With Russia?

This spring, a group of computer scientists set out to determine whether hackers were interfering with the Trump campaign. They found something they weren't expecting.

By Franklin Foer

Donald Trump gives a fist-pump to the ground crew as he arrives on his plane in St. Augustine, Florida, on Oct. 24.

Jonathan Ernst/Reuters

21/ The article claimed that DNS logs which were "impossible to fake" indicated the communication.

This statement is completely false.
DNS logs are simple text files and easy to fake.

DNS requests which use connection-less UDP, are also trivial to spoof.

Weaver's statement raises another uncertainty: *Are* the logs authentic? Computer scientists are careful about vouching for evidence that emerges from unknown sources—especially since the logs were pasted in a text file, where they could conceivably have been edited. I asked nine computer scientists—some who agreed to speak on the record, some who asked for anonymity—**if the DNS logs that Tea Leaves and his collaborators discovered could be forged or manipulated. They considered it nearly impossible. It would be easy enough to fake one or maybe even a dozen records of DNS lookups.** But in the aggregate, the logs contained thousands of records, with nuances and patterns that not even the most skilled programmers would be able to recreate on this scale. "The data has got the right kind of fuzz growing on it," Vixie told me. "It's the interpacket gap, the spacing between the conversations, the total volume. If you look at those time stamps, they are not simulated. This bears every indication that it was collected from a live link." I asked him if there was a chance that he was wrong about their authenticity. "This passes the reasonable person test," he told me. "No reasonable person would come to the conclusion other than the one I've come to." Others were equally emphatic. "It would be really, really hard to fake these," Davis said. According to Camp, "When the technical community examined the data, the conclusion was pretty obvious."

gave interviews perpetuating the completely false claim of "impossible to fake" DNS records.

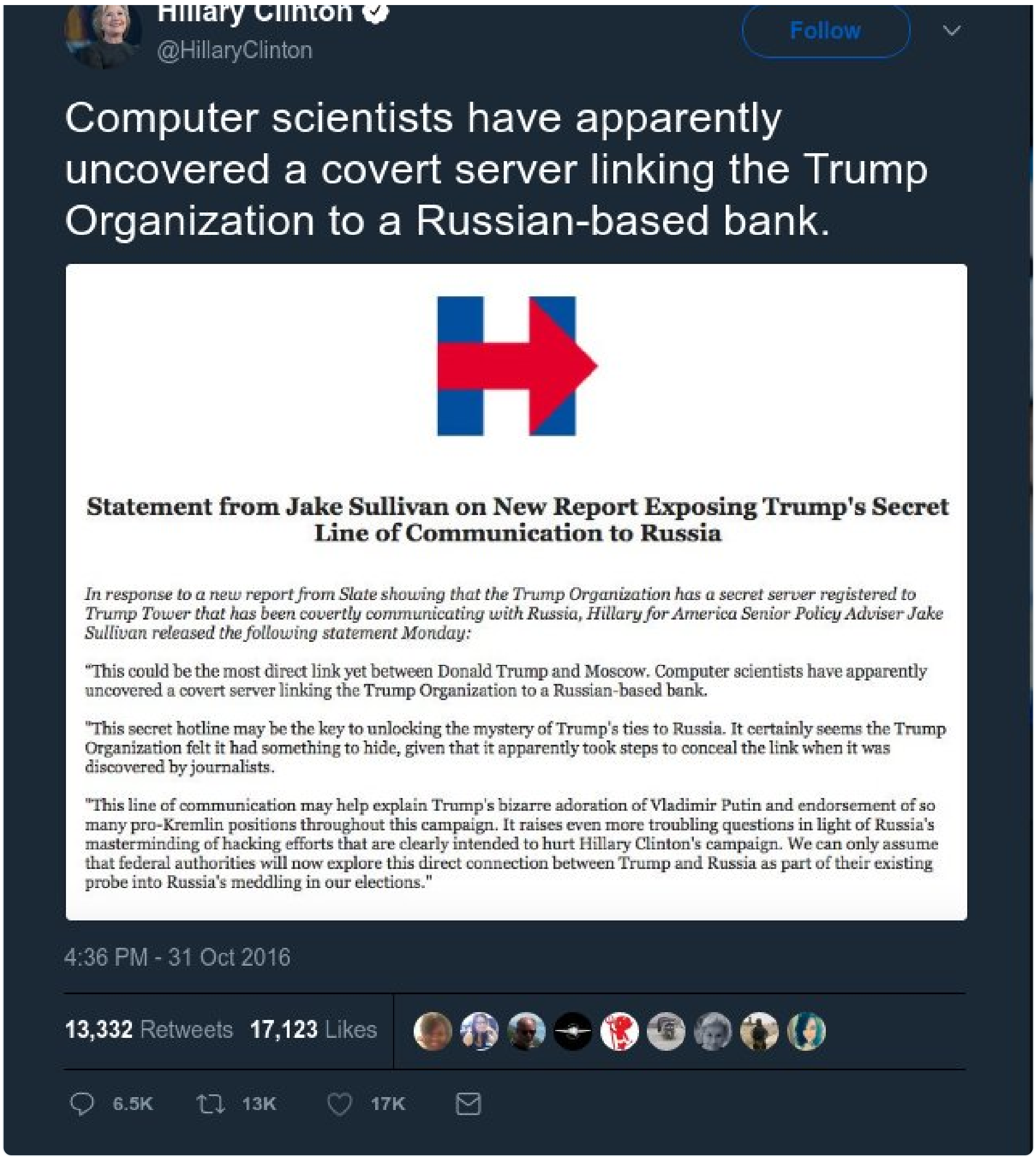
I called him out on Twitter, and he admitted it was untrue.

External Tweet loading...
If nothing shows, it may have been deleted
https://twitter.com/paulvixie/status/793855788053782528

23/ Hillary Clinton also made the claim.

Alfa Bank was listed on the FISA application.

External Tweet loading...
If nothing shows, it may have been deleted
https://twitter.com/HillaryClinton/status/793250312119263233



24/ Unsurprisingly, this claim was investigated and proven false.

Mueller's recent indictment of 12 Russians has nothing to do with Alfa Bank.

The owners of Alfa Bank, including German Khan, are now suing Christopher Steele for defamation.

IN THE SUPERIOR COURT OF THE DISTRICT OF COLUMBIA

CIVIL DIVISION

MIKHAIL FRIDMAN, PETR AVEN, AND GERMAN KHAN, Plaintiffs, -v- ORBIS BUSINESS INTELLIGENCE LIMITED AND CHRISTOPHER STEELE, Defendants.	2018 CA002667 B Judge Anthony C. Epstein

25/ At face value, this part of the indictment describes operational security measures commonly used by threat actors.

> 8. To hide their connections to Russia and the Russian government, the Conspirators used false identities and made false statements about their identities. To further avoid detection, the Conspirators used a network of computers located across the world, including in the United States, and paid for this infrastructure using cryptocurrency.

26/ Actions alleged in the indictment however, are opposite these operational security measures. Specifically, Guccifer 2 and the "mistakes" that provided "conclusive" attribution to Russia upon which the entirety of Mueller's case depends.

> Stolen Documents Released through Guccifer 2.0
>
> 40. On or about June 14, 2016, the DNC—through Company 1—publicly announced that it had been hacked by Russian government actors. In response, the Conspirators created the online persona Guccifer 2.0 and falsely claimed to be a lone Romanian hacker to undermine the allegations of Russian responsibility for the intrusion.
>
> 41. On or about June 15, 2016, the Conspirators logged into a Moscow-based server used and managed by Unit 74455 and, between 4:19 PM and 4:56 PM Moscow Standard Time, searched for certain words and phrases, including:

27/ When WaPo published the article (#13) on 06/14/16 (2 days after Assange announced the leaks) there was NO intelligence report and security pros had only MODERATE confidence that these actors were Russian.

So how could the DNC and WaPo report it with 100% confidence? 🧐

40. On or about June 14, 2016, the DNC—through Company 1—publicly announced that it had been hacked by Russian government actors. In response, the Conspirators created the online persona Guccifer 2.0 and falsely claimed to be a lone Romanian hacker to undermine the allegations of Russian responsibility for the intrusion.

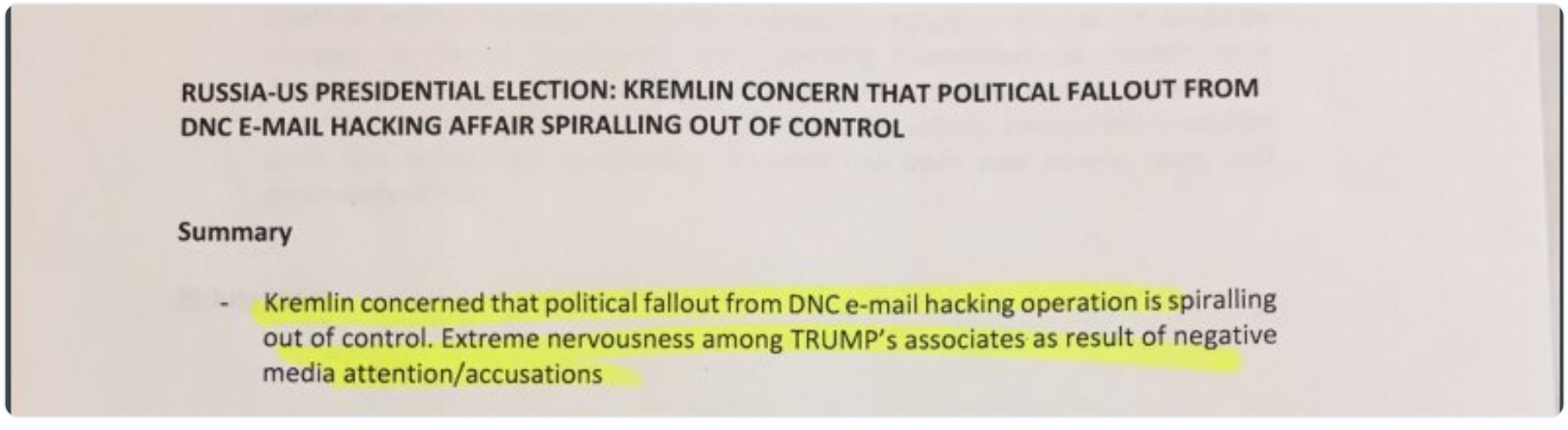
41. On or about June 15, 2016, the Conspirators logged into a Moscow-based server used and managed by Unit 74455 and, between 4:19 PM and 4:56 PM Moscow Standard Time, searched for certain words and phrases, including:

28/ Christopher Steele and his anonymous "sources" wrote the story.

Fusion GPS disseminated the information to the media.

The MSM was not doing journalism.

They were helping the DNC and Fusion GPS construct a narrative.



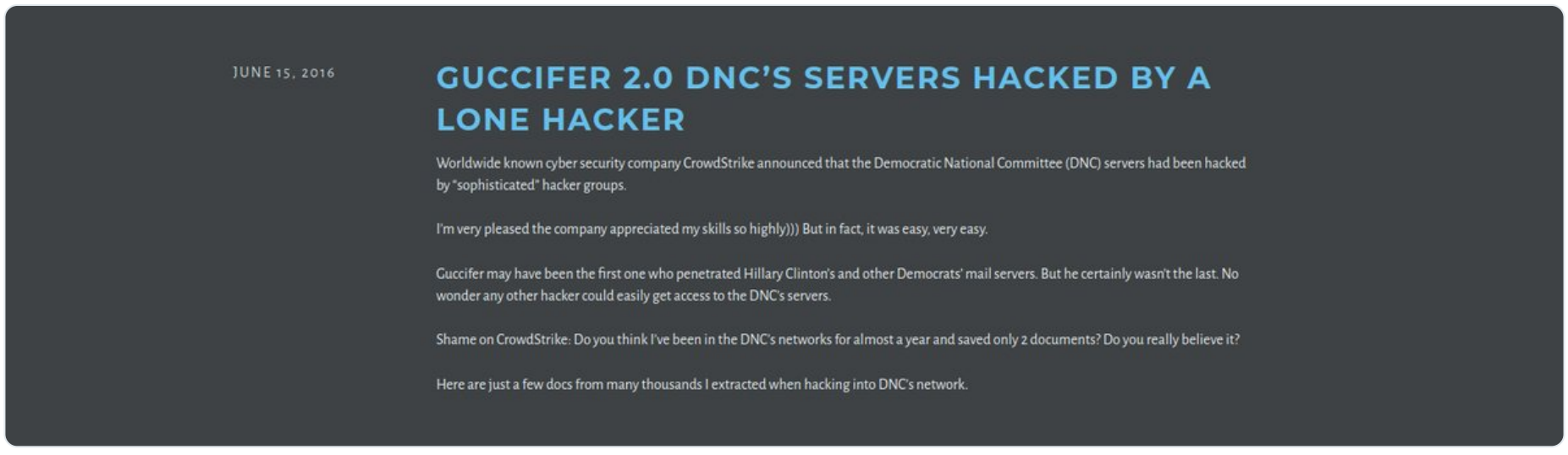
RUSSIA-US PRESIDENTIAL ELECTION: KREMLIN CONCERN THAT POLITICAL FALLOUT FROM DNC E-MAIL HACKING AFFAIR SPIRALLING OUT OF CONTROL

Summary

- Kremlin concerned that political fallout from DNC e-mail hacking operation is spiralling out of control. Extreme nervousness among TRUMP's associates as result of negative media attention/accusations

29/ Fusion & Clinton knew that a fake dossier and fake news would convince some of the public, but that it would not be convincing enough to connect Trump to the alleged crime, nor would it be enough to prosecute.

They needed something else...



JUNE 15, 2016

GUCCIFER 2.0 DNC'S SERVERS HACKED BY A LONE HACKER

Worldwide known cyber security company CrowdStrike announced that the Democratic National Committee (DNC) servers had been hacked by "sophisticated" hacker groups.

I'm very pleased the company appreciated my skills so highly))) But in fact, it was easy, very easy.

Guccifer may have been the first one who penetrated Hillary Clinton's and other Democrats' mail servers. But he certainly wasn't the last. No wonder any other hacker could easily get access to the DNC's servers.

Shame on CrowdStrike: Do you think I've been in the DNC's networks for almost a year and saved only 2 documents? Do you really believe it?

Here are just a few docs from many thousands I extracted when hacking into DNC's network.

30/ According to the indictment, the "Russians" allegedly had a network of servers located all over the world and spent over $90,0000 USD on additional infrastructure.

threatconnect.com/blog/guccifer-...

> In our initial Guccifer 2.0 analysis, ThreatConnect highlighted technical and non-technical inconsistencies in the purported DNC hacker's story as well as a curious theme of French "connections" surrounding various Guccifer 2.0 interactions with the media. We called out these connections as they overlapped, albeit minimally, with FANCY BEAR infrastructure identified in CrowdStrike's DNC report.
>
> Now, after further investigation, we can confirm that Guccifer 2.0 is using the Russia-based Elite VPN service to communicate and leak documents directly with the media. We reached this conclusion by analyzing the infrastructure associated with an email exchange with Guccifer 2.0 shared with ThreatConnect by Vocativ's Senior Privacy and Security reporter Kevin Collier. This discovery strengthens our ongoing assessment that Guccifer 2.0 is a Russian propaganda effort and not an independent actor.

31/ Claiming experienced, highly skilled hackers with Russian intel were so startled by a WaPo article that they decided to buy a Russian VPN service, create a fake persona, then forget to the connect to the VPN is utterly and completely ridiculous.

motherboard.vice.com/en_us/article/...

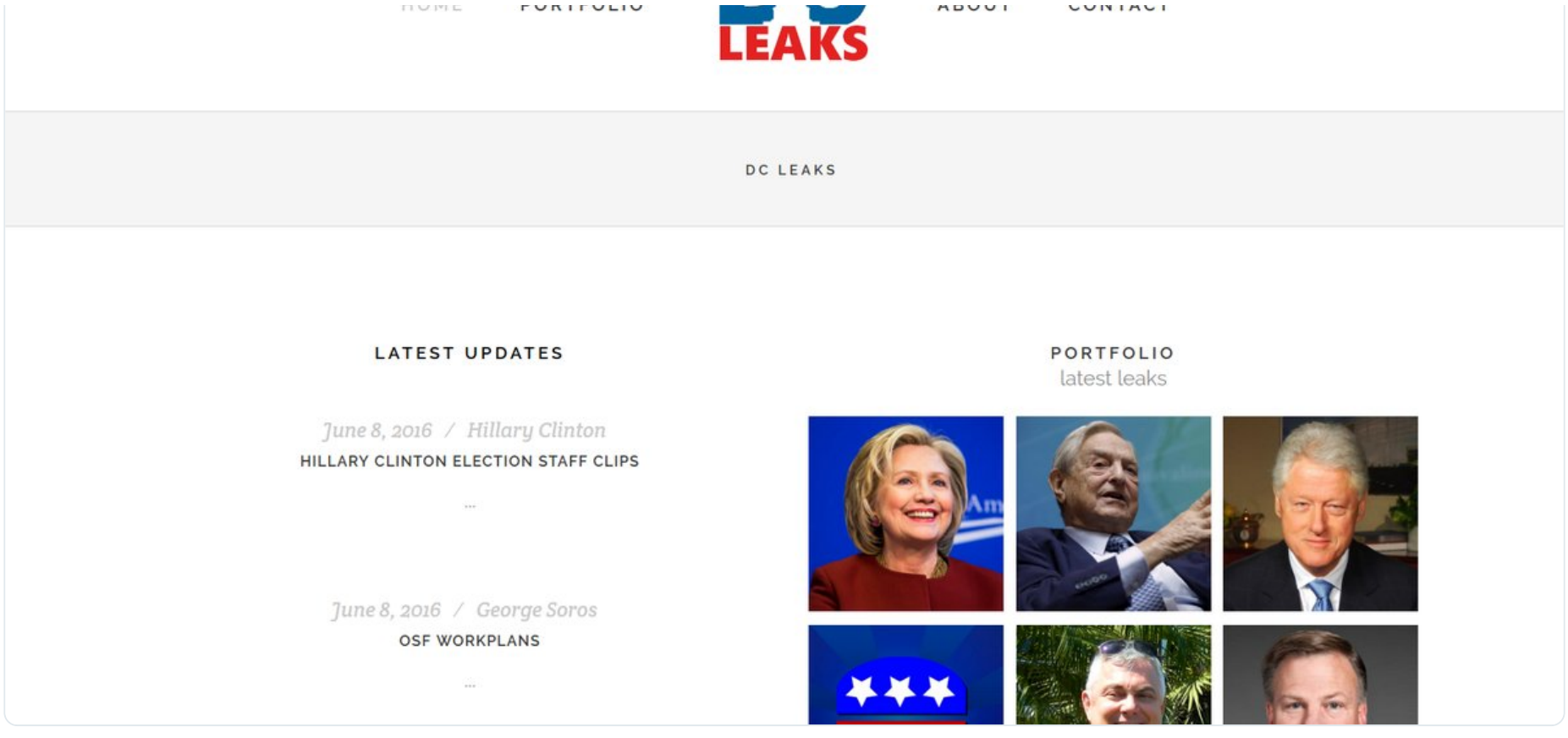
A screenshot of the beginning of my conversation with Guccifer 2.0.

> That's according to an anonymous source close to the US government investigation, run by special counsel Robert Mueller, who told The Daily Beast that American investigators have identified two people behind the Guccifer 2.0 persona, both officers of the GRU. The investigators were apparently able to unmask the hacker thanks to one crucial mistake: the hacker forgot to turn on his VPN once, revealing his real IP address, presumably when he used either WordPress or Twitter.

32/ The indictment alleges that DCleaks was created by the conspirators.

But DCLeaks contained nothing directly linking it to Russia.

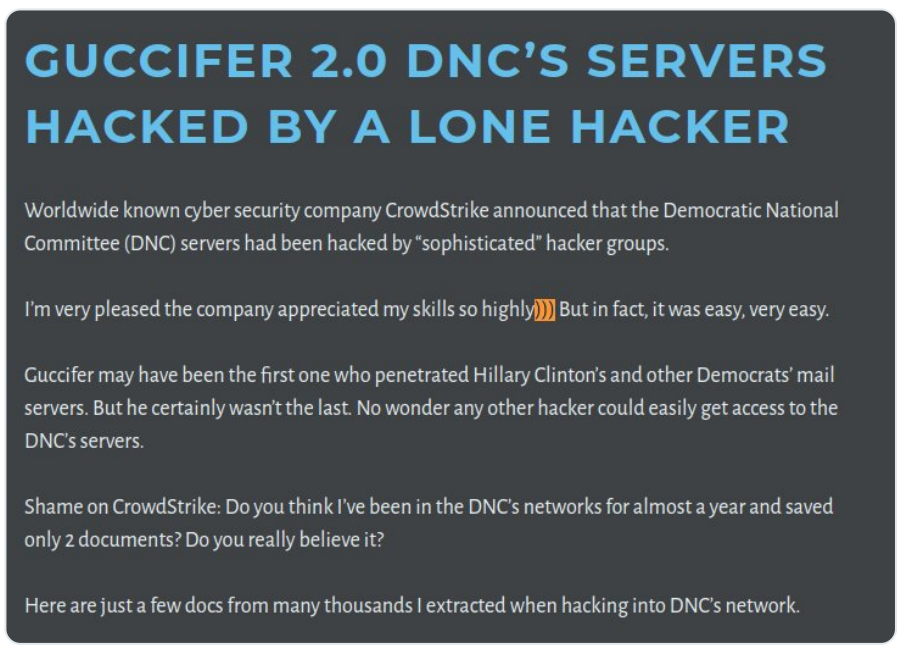
web.archive.org/web/2016061314...



33/ G2's blog was written in broken English.

G2's blog used Russian-language specific punctuation such as triple-parenthesis ")))", the Russian-language equivalent of a smiley face (Сма́йлик).

DCLeaks was in fluent English and used NO Russian-specific punctuation.


GUCCIFER 2.0 DNC'S SERVERS HACKED BY A LONE HACKER

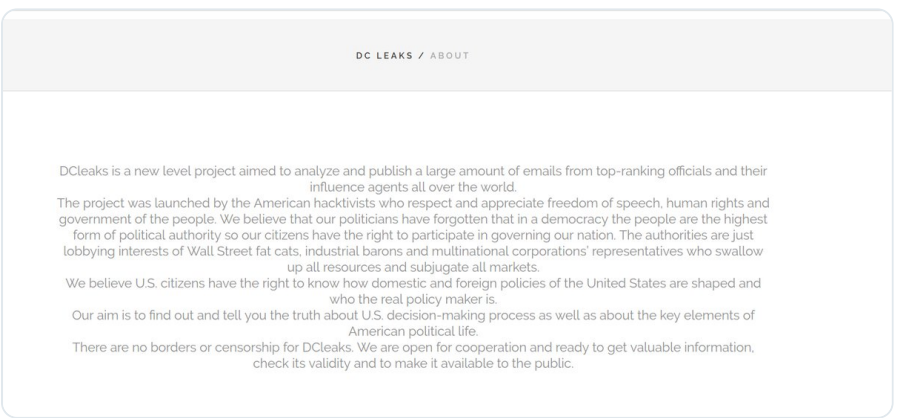
Worldwide known cyber security company CrowdStrike announced that the Democratic National Committee (DNC) servers had been hacked by "sophisticated" hacker groups.

I'm very pleased the company appreciated my skills so highly))) But in fact, it was easy, very easy.

Guccifer may have been the first one who penetrated Hillary Clinton's and other Democrats' mail servers. But he certainly wasn't the last. No wonder any other hacker could easily get access to the DNC's servers.

Shame on CrowdStrike: Do you think I've been in the DNC's networks for almost a year and saved only 2 documents? Do you really believe it?

Here are just a few docs from many thousands I extracted when hacking into DNC's network.


DC LEAKS / ABOUT

DCleaks is a new level project aimed to analyze and publish a large amount of emails from top-ranking officials and their influence agents all over the world.
The project was launched by the American hacktivists who respect and appreciate freedom of speech, human rights and government of the people. We believe that our politicians have forgotten that in a democracy the people are the highest form of political authority so our citizens have the right to participate in governing our nation. The authorities are just lobbying interests of Wall Street fat cats, industrial barons and multinational corporations' representatives who swallow up all resources and subjugate all markets.
We believe U.S. citizens have the right to know how domestic and foreign policies of the United States are shaped and who the real policy maker is.
Our aim is to find out and tell you the truth about U.S. decision-making process as well as about the key elements of American political life.
There are no borders or censorship for DCleaks. We are open for cooperation and ready to get valuable information, check its validity and to make it available to the public.

34/ The documents from G2 were opened on a RU-lang system and barely edited (such as by adding a space to a line), then saved.

This left Russian-language forensic artifacts on the files.

@with_integrity has covered this: g-2.space

(No, this has NOT been debunked)

There is a difference between independently verifiable evidence and the activity somebody claims to have engaged i
claims of hacking were independently verifiable and several were debunked by ThreatConnect. - There is nothing de

The "evidence" that he's Russian, should be understood in the following context:

- He CHOSE to name his computer account after the founder of the Soviet Secret Police.
- He CHOSE to create/open and then save documents so the Russian name was written to metadata.
- He CHOSE to use a Russian VPN service to cloak his IP address.
- He CHOSE to use public web-based email services that would forward his cloaked IP.
- He CHOSE to use the above to contact various media outlets on the same day.

35/ Guccifer 2

Who the media wants you to believe was a Russian smokescreen,

Proceeded to reach out to members of the Trump campaign, Republican candidates, and journalists.

If G2 was a Russian smokescreen...

Why would they use it to communicate with the Trump campaign?

CBS NEWS / *March 14, 2017, 6:58 PM*

Trump adviser Roger Stone admits contact with Guccifer 2.0 during campaign

Share / Tweet / Reddit / Flipboard / Email

WASHINGTON -- Trump campaign associates have denied coordinating with the Russians during the presidential election. But one of the president's close friends and advisers is now acknowledging some contact with a Twitter handle U.S. officials considered a front for Russian intelligence.

Roger Stone / CBS NEWS

"There's no collusion here," Roger Stone told CBS News correspondent Jeff Pegues, while he admitted to contact with Guccifer 2.0, the Twitter handle that released hacked election information believed stolen from Democratic Party servers.

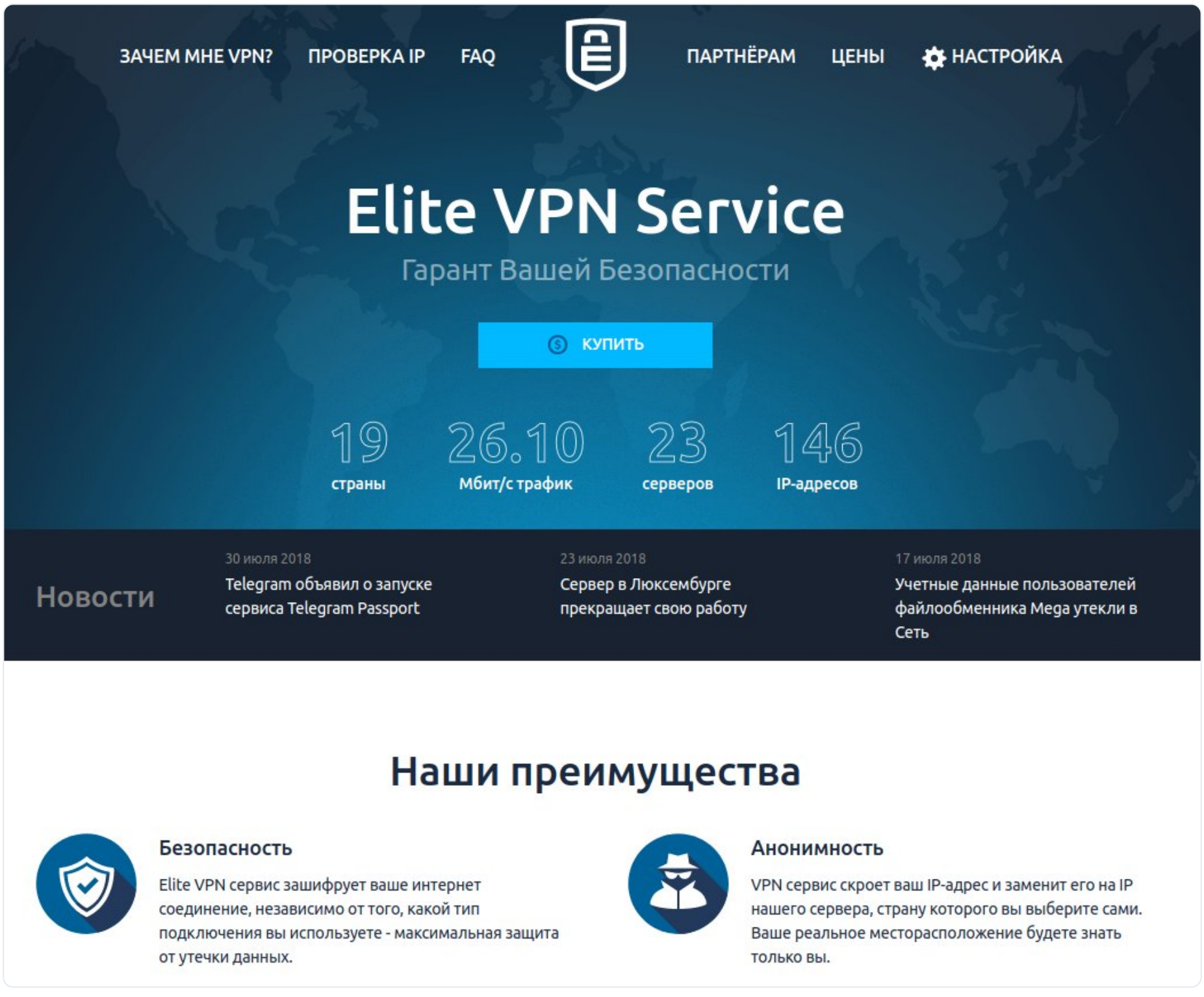
"At the time I had my one and only communications with it," Stone said.

"Well wait a second, you had more than just one contact with this person, you had one, two, at least three between August 12th and September 9th," Pegues said.

"Right, I would refer to it as an exchange," Stone replied.

That "exchange" appears to have started after Guccifer's first account was suspended and then re-activated in mid-August.

36/ The Official Narrative states that G2 was created by nervous GRU agents working with Trump to make investigators believe that the attack (if it even occurred) was perpetrated by an obscure Romanian hacker.



37/ According to Glenn Simpson's sworn testimony before the Permanent Select Committee on Intelligence, the Russian government retained Natalia Veselnitskaya and the law firm Baker Hostetler to fight the Magnitsky act and defend Prevezon Holdings, accused of money laundering.

Natalia Veselnitskaya or came to know her?

A Sure. I think this is largely included in the previous answer, but I was retained by Baker Hostetler, and didn't know of her existence until they told me there was a lawyer for the Prevezon company, a Russian lawyer. And eventually, they mentioned her a few times, and eventually they mentioned her name. And at some point, you know, they introduced me to her.

Q Do you recall when that was?

A I don't. I assume it was sometime in mid-2014.

Q And I assume that you have seen reporting, or otherwise know that she attended what has become known as the Trump Tower meeting on June 9, 2016?

A Yes.

38/ According to unsealed bank records obtained by the HPSCI, Baker Hostetler paid Fusion GPS hundreds of thousands of dollars in 2016 alone.

Over $265,000 was paid to Fusion in March, 2016.

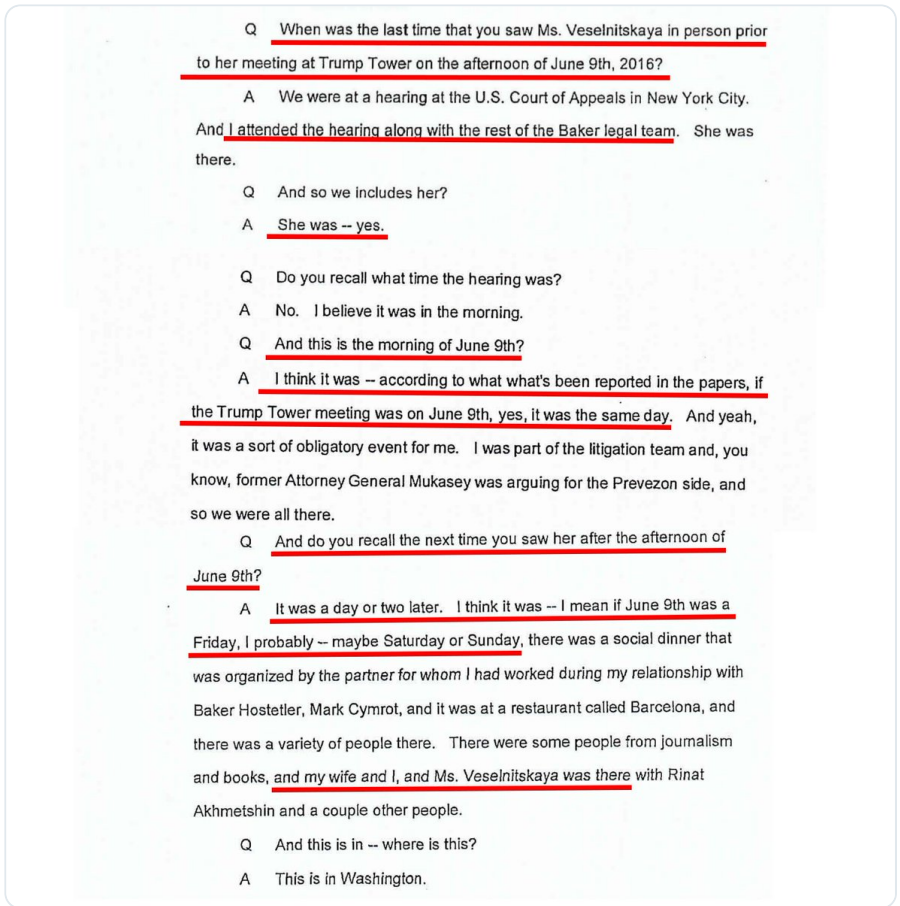
Baker Hostetler – Transaction Nos. 4-11

We seek re-production of records related to payments to Fusion from Baker Hostetler, and the production of one additional payment thereto.

4.	Debit	Baker Hostetler	12/13/16	$20,000	77
5.	**Credit**	**Baker Hostetler**	**3/7/16**	**$102,064.30**	**102**
6.	**Credit**	**Baker Hostetler**	**3/18/16**	**$165,859.15**	**103**
7.	**Credit**	**Baker Hostetler**	**8/18/16**	**$109,976.98**	**119**
8.	**Credit**	**Baker Hostetler**	**9/6/16**	**$8179.21**	**121**
9.	**Credit**	**Baker Hostetler**	**10/27/16**	**$59,425.37**	**129**
10.	**Credit**	**Baker Hostetler**	**10/31/16**	**$23,615.32**	**131**
11.	**Credit**	**Baker Hostetler**	**10/31/16**	**$54,530.29**	**132**
12.	Credit	[redacted]	8/16/16	[redacted]	120
13.	Credit	[redacted]	1/26/17	[redacted]	144
14.	Credit	[redacted]	6/9/16	[redacted]	175

39/ Simpson's testimony before the HSPCI and the Senate also revealed that not only did Fusion GPS have contact with Natalia Veselnitskaya...

He met with her the morning of the Don Jr. Trump Tower meeting and the day afterwards.



Q When was the last time that you saw Ms. Veselnitskaya in person prior to her meeting at Trump Tower on the afternoon of June 9th, 2016?

A We were at a hearing at the U.S. Court of Appeals in New York City. And I attended the hearing along with the rest of the Baker legal team. She was there.

Q And so we includes her?

A She was -- yes.

Q Do you recall what time the hearing was?

A No. I believe it was in the morning.

Q And this is the morning of June 9th?

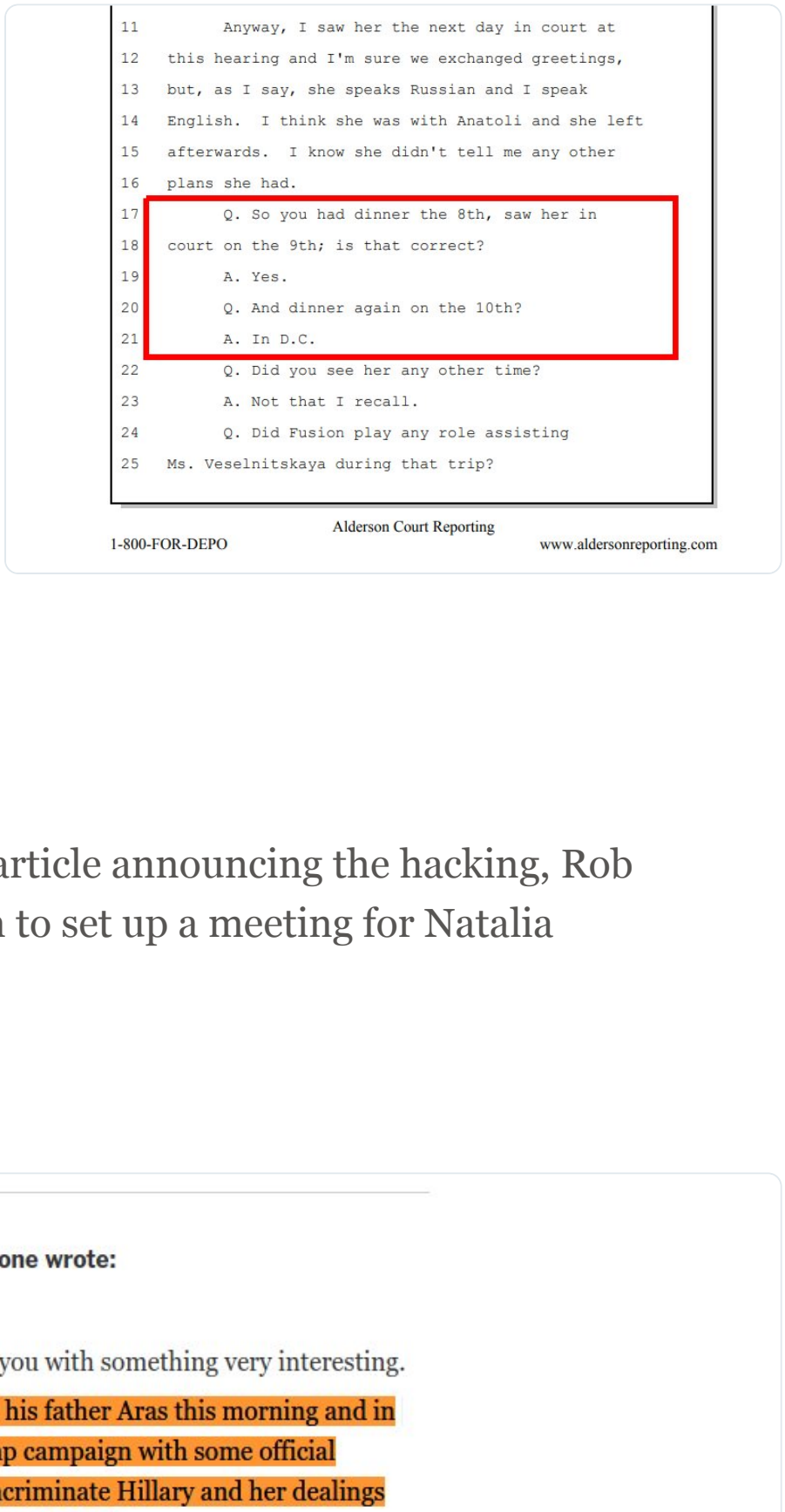
A I think it was -- according to what what's been reported in the papers, if the Trump Tower meeting was on June 9th, yes, it was the same day. And yeah, it was a sort of obligatory event for me. I was part of the litigation team and, you know, former Attorney General Mukasey was arguing for the Prevezon side, and so we were all there.

Q And do you recall the next time you saw her after the afternoon of June 9th?

A It was a day or two later. I think it was -- I mean if June 9th was a Friday, I probably -- maybe Saturday or Sunday, there was a social dinner that was organized by the partner for whom I had worked during my relationship with Baker Hostetler, Mark Cymrot, and it was at a restaurant called Barcelona, and there was a variety of people there. There were some people from journalism and books, and my wife and I, and Ms. Veselnitskaya was there with Rinat Akhmetshin and a couple other people.

Q And this is in -- where is this?

A This is in Washington.



Anyway, I saw her the next day in court at this hearing and I'm sure we exchanged greetings, but, as I say, she speaks Russian and I speak English. I think she was with Anatoli and she left afterwards. I know she didn't tell me any other plans she had.

Q. So you had dinner the 8th, saw her in court on the 9th; is that correct?

A. Yes.

Q. And dinner again on the 10th?

A. In D.C.

Q. Did you see her any other time?

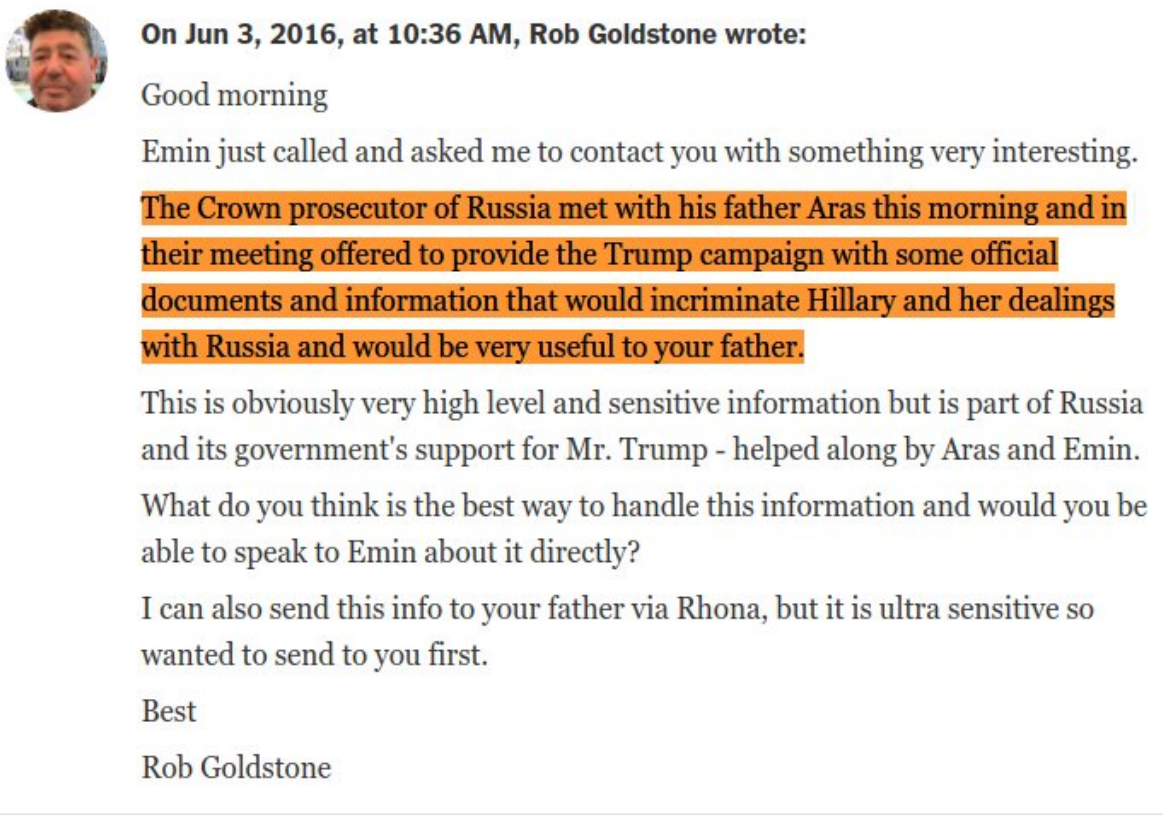
A. Not that I recall.

Q. Did Fusion play any role assisting Ms. Veselnitskaya during that trip?

Alderson Court Reporting
1-800-FOR-DEPO www.aldersonreporting.com

40/ One June 3rd, prior to the June 14 WaPo article announcing the hacking, Rob Goldstone reached out to the Trump campaign to set up a meeting for Natalia Veselnitskaya with @DonaldJTrumpJr.

nytimes.com/interactive/20...



On Jun 3, 2016, at 10:36 AM, Rob Goldstone wrote:

Good morning

Emin just called and asked me to contact you with something very interesting.

The Crown prosecutor of Russia met with his father Aras this morning and in their meeting offered to provide the Trump campaign with some official documents and information that would incriminate Hillary and her dealings with Russia and would be very useful to your father.

This is obviously very high level and sensitive information but is part of Russia and its government's support for Mr. Trump - helped along by Aras and Emin.

What do you think is the best way to handle this information and would you be able to speak to Emin about it directly?

I can also send this info to your father via Rhona, but it is ultra sensitive so wanted to send to you first.

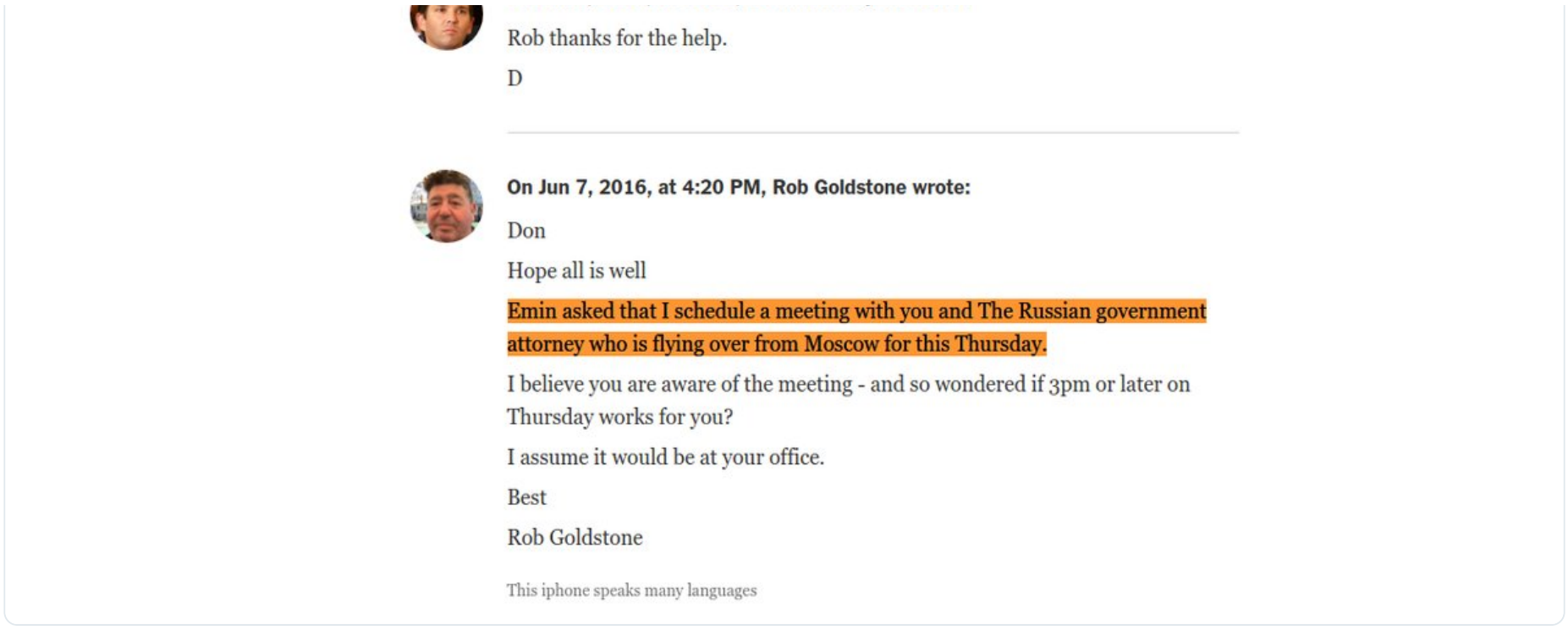
Best

Rob Goldstone

41/ Goldstone wrote Natalia had compromising info on Hillary Clinton.

Unbeknownst to Don Jr. and the Trump campaign, that information would be presumed to have been obtained during the alleged DNC data breach.

This was clearly a setup orchestrated by Fusion GPS.



42/ The pseudo-Romanian persona Guccifer 2 and the Russian attorney Natalia Veselnitskaya were not the only alleged Fusion GPS operatives secretly working to tie the hacking story to Trump and Russia.

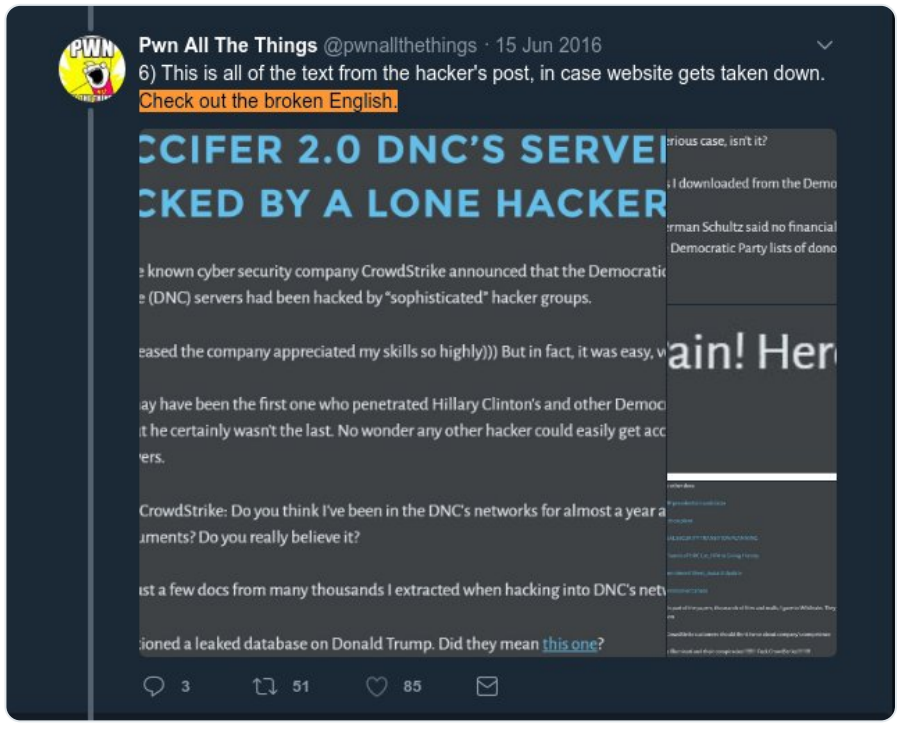
43/ A former British Intelligence (GCHQ) employee named Matt Tait is our next piece of the puzzle.

In order for Fusion's Russia hacking deception scheme to succeed, public opinion needed to be controlled both online and offline.

44/ On June 15th, using his Twitter account >> @pwnallthethings <<

Matt Tait tweeted a thread analyzing the Guccifer 2 site, highlighting out all of the various "Russian" indicators that were [deliberately planted] on the blog and posted documents.

External Tweet loading...
If nothing shows, it may have been deleted
https://twitter.com/pwnallthethings/status/744088859747717120



45/ Matt Tait claims that his "timely research" into Guccifer 2 lead him to being contacted on Twitter by a man identified as "Peter Smith", supposedly a well-connected Republican who needed assistance verifying stolen documents from Hillary Clinton.

lawfareblog.com/time-i-got-rec...

> A while later, on June 14, the *Washington Post* reported on a hack of the DNC ostensibly by Russian intelligence. When material from this hack began appearing online, courtesy of the "Guccifer 2" online persona, I turned my attention to looking at these stolen documents. This time, my purpose was to try and understand who broke into the DNC, and why.
>
> A few weeks later, right around the time the DNC emails were dumped by Wikileaks—and curiously, around the same time Trump called for the Russians to get Hillary Clinton's missing emails—I was contacted out the blue by a man named Peter Smith, who had seen my work going through these emails. Smith implied that he was a well-connected Republican political operative.

46/ Tait claims that Peter Smith provided a Republican document naming himself and various Trump campaign officials including Steve Bannon, Kellyanne Conway, Sam Clovis, and Lt. Gen. Mike Flynn @GenFlynn.

Someone was trying to connect the Trump campaign to the stolen data.

> Officials identified in the document include Steve Bannon, now chief strategist for President Donald Trump; Kellyanne Conway, former campaign manager and now White House counselor; Sam Clovis, a policy adviser to the Trump campaign and now a senior adviser at the Agriculture Department; and retired Lt. Gen. Mike Flynn, who was a campaign adviser and briefly was national security adviser in the Trump administration.

47/ Mr. Tait, a British citizen who is currently living and working in the US at @UTAustin, claims that his "discoveries" on Guccifer 2 and contacts with Peter Smith

His behavior proves otherwise.

48/ Mr. Tait's "recruitment" by the "Russians" - who claimed to be deeply connected to Trump's campaign and the Republican party - was of interest to the Special Counsel.

Tait would provide oral testimony to Robert Mueller.

businessinsider.com/mueller-trump-...

described being "recruited to collude with the Russians

Natasha Bertrand Oct. 17, 2017, 2:40 PM

A cybersecurity researcher who described being recruited to vet hacked Hillary Clinton emails last year by a GOP operative tied to President Donald Trump's campaign team has been interviewed by the FBI's special counsel, Robert Mueller, Business Insider has learned.

The former national security adviser Michael Flynn. Thomson Reuters

Mueller interviewed Matt Tait, a former information-security specialist at Britain's Government Communications Headquarters who tweets as @pwnallthethings , several weeks ago, said a source familiar with the matter.

The interview was part of a broader effort by Mueller to examine the relationship between the longtime GOP operative, Peter Smith, and the former national security adviser Michael Flynn and whether Flynn played any role in seeking out the stolen emails during the election. Smith killed himself in May after talking to The Wall Street Journal about his experience.

49/ Tait has made numerous suspicious or misleading statements defending Christopher Steele, claiming special knowledge about Steele's reputation and his "contacts in Moscow".

twitter.com/search?f=tweet...

50/ Tait even reviewed the FISA warrant app and attacked @DevinNunes,

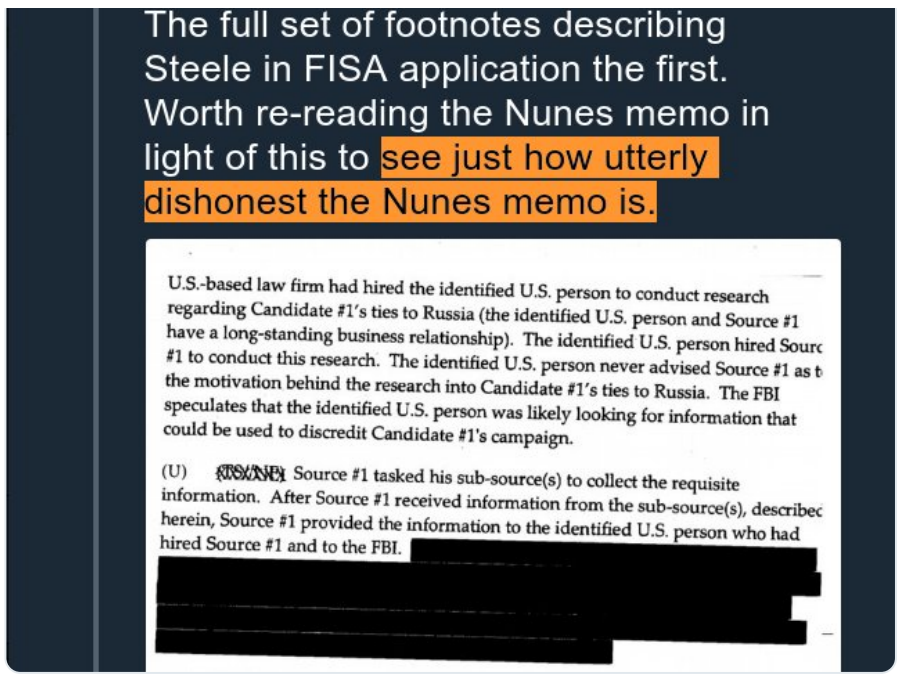
Claiming the Nunes memo was completely dishonest.

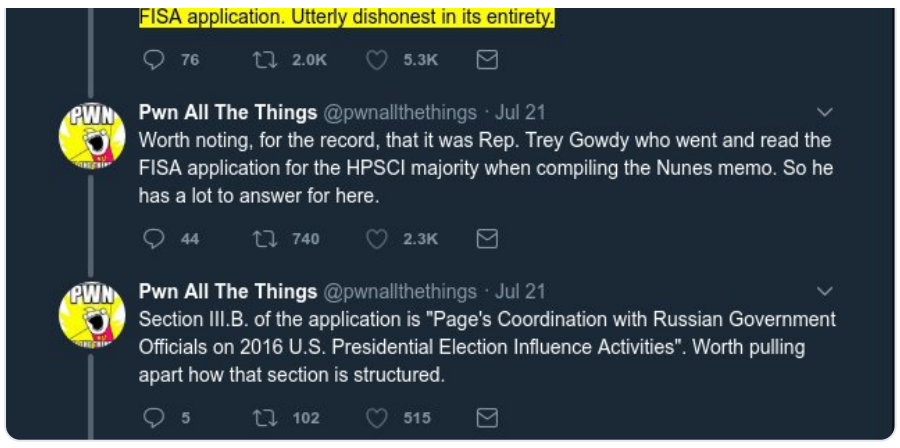
That is a FALSE statement.

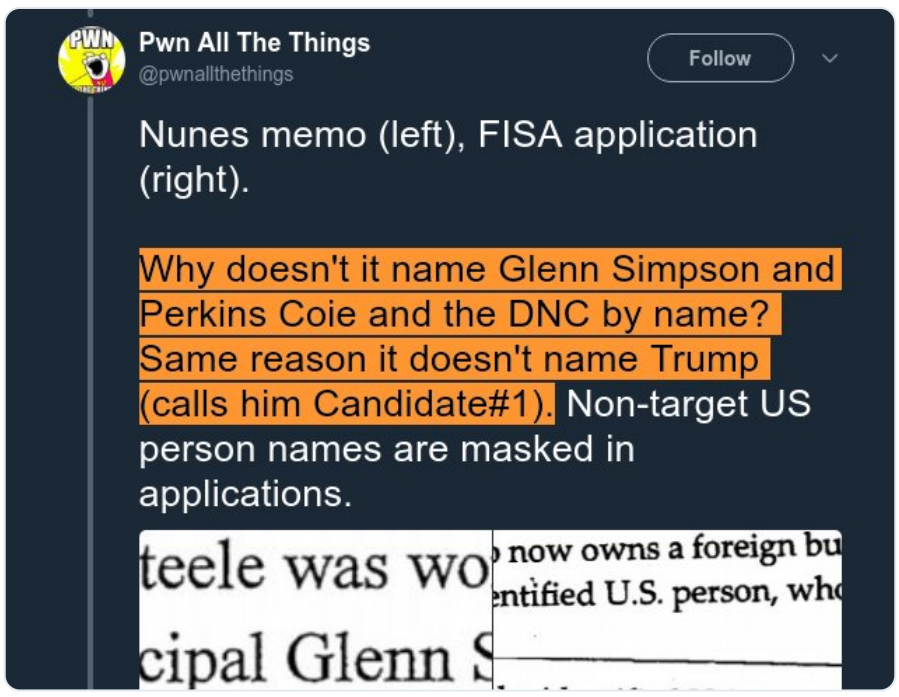
The application should have indicated funding by Campaign #2 (DNC/Clinton).

FBI completely avoided it.

External Tweet loading...
If nothing shows, it may have been deleted
https://twitter.com/pwnallthethings/status/1020847275017494528



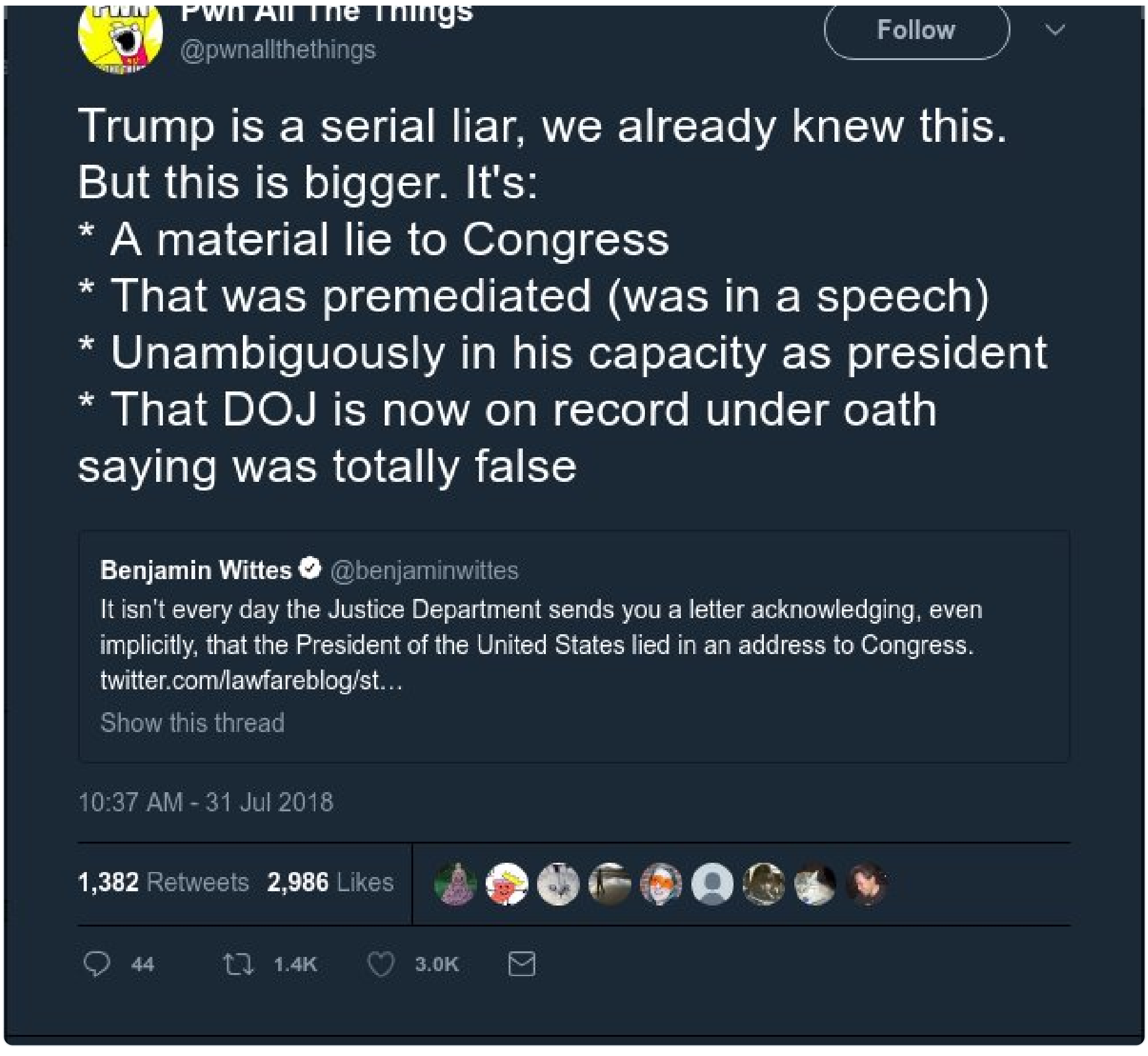




51/ For a Briton doing "innocent" research who has "no connection or interest" with Clinton, DNC, Fusion or Steele,

Making numerous slanderous, deceptive or special-knowledge statements and having contact with SC Robert Mueller is EXTREMELY SUSPICIOUS..

External Tweet loading...
If nothing shows, it may have been deleted
https://twitter.com/pwnallthethings/status/1024363492483186693

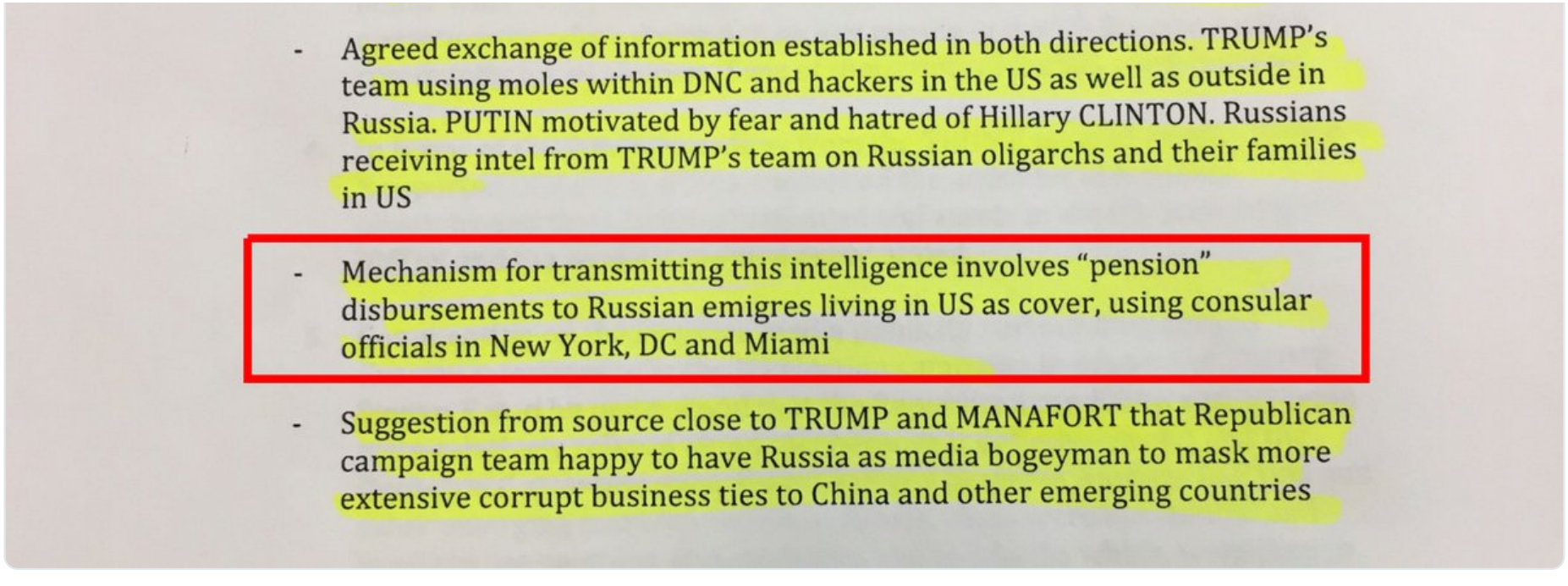


52/ All the known communication from the "Russian hackers" occurred on Twitter or by unencrypted email.

The "hackers" were not concerned about being secretive.

They wanted this communication to be exposed!!

Contradicting both the Mueller indictment and dossier allegations.



53/ The contradictory information and highly suspicious events which may constitute a conspiracy against the United States still leaves unanswered questions.

Such as: What really occurred at the DNC?

Let's explore that. 😎

54/ As I discussed in tweets Nos. 4-8, when Crowdstrike arrived at the DNC in April 2016, they did NOT conduct a Digital Forensics and Incident Response investigation.

They installed their endpoint security agent FALCON onto the DNC's hundreds of computer systems.

Henry, whom he has known for many years.

Within 24 hours, CrowdStrike had installed software on the DNC's computers so that it could analyze data that could indicate who had gained access, when and how.

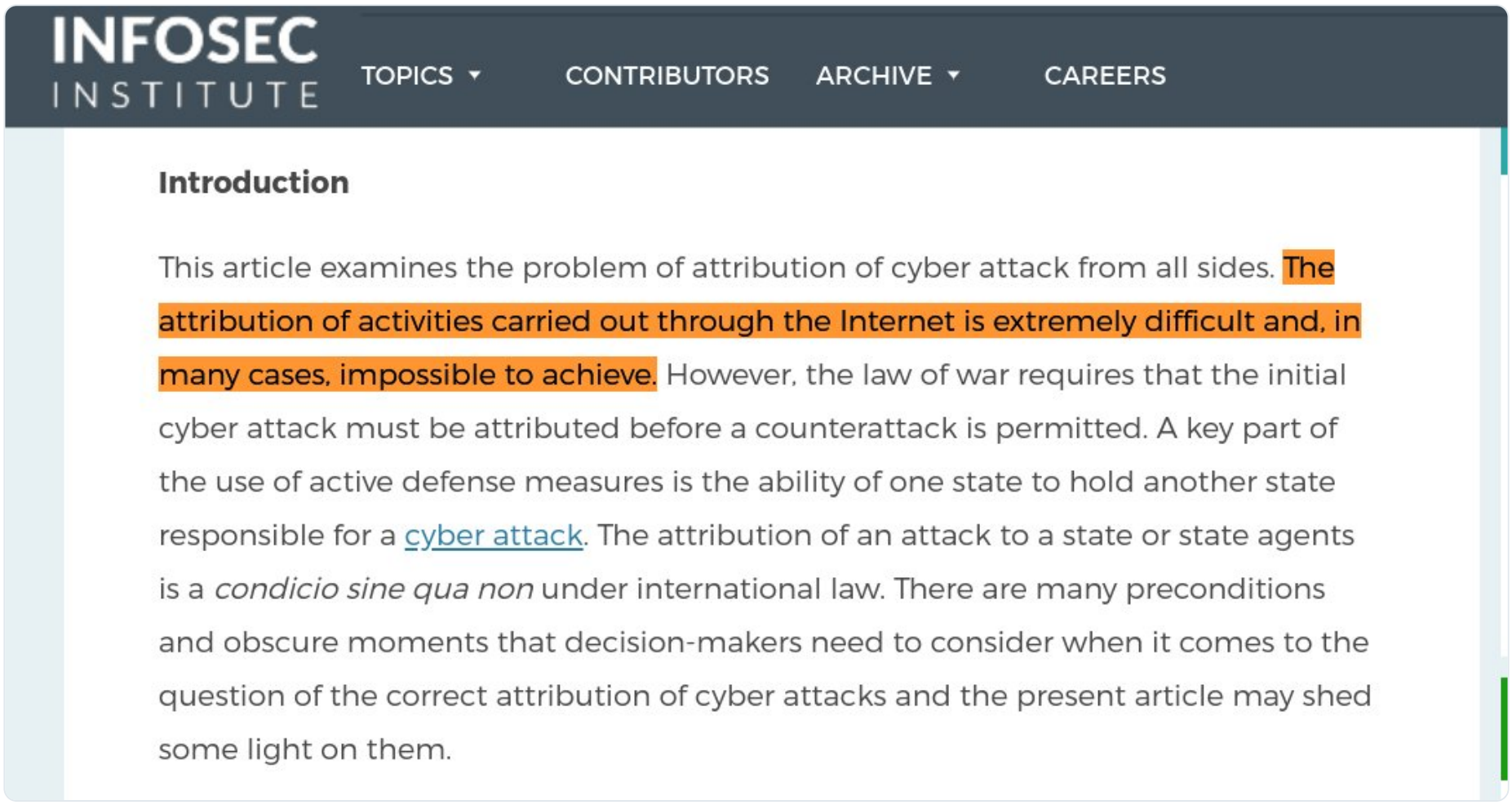
The firm identified two separate hacker groups, both working for the Russian government, that had infiltrated the network, said Dmitri Alperovitch, CrowdStrike co-founder and chief technology officer. The firm had analyzed other breaches by both groups over the past two years.

55/ Crowdstrike claims that their cloud-based software "instantly lit up" and they knew right away it was the Russian government.

Clearly a fictitious statement. 😂

Even with AI, cyber attack attribution is extremely difficult, sometimes impossible.

resources.infosecinstitute.com/attribution-pr...



56/ One of the features of Crowdstrike's endpoint security agent is Data Loss Prevention (DLP).

DLP detects potential data exfiltration from insider threats, such as an employee copying sensitive files to a portable USB drive.

crowdstrike.com/blog/the-secur...

Resources – "People Doing All the Things"

If you've successfully identified the tools you need to secure your environment, the underlying question you should be asking yourself is whether you actually have the staff to support those tools. Vendors always have a way of making their tools look effortless to run and maintain. Often, however, these functions require constant attention from dedicated resources.

Consider for a moment whether your security team is fully utilizing the tools you already have. Even the best-in-class technologies can be easily bypassed if they're not configured and maintained. Putting a firewall on your network is nothing more than a pass-through point unless the rule set and ACLs are defined. Similarly, IPS devices, DLP solutions, and any other tool in your repertoire require hand-holding. Beyond the initial setup, someone also needs to be looking at the resulting alerts and logs to determine where "badness" lives.

57/ Insider Threats account for nearly 75% of all Security Breach incidents.

securityintelligence.com/news/insider-t...

@threadreaderapp unroll

More from @Cynacin see all

Lycaon
@Cynacin

2 days ago

#FusionGPS is being sued for defamation. The foundation of their defense: [the dossier] "only contains loose, figurative or hyperbolic langue that cannot be reasonably interpreted as stating actual, provable facts." 🤦‍♂ What a bunch of clowns. 🤡 #Dossier is bullshit.

Not sure if the asshole clowns 🤡 working for #FusionGPS realize this or not but... When they "briefed" the media on their quasi-intelligence propaganda bullshit.... Many Americans thought the dossier DID contain actual, provable facts. They still do.

Even the @FBI thought the #dossier contained actual

Read 3 tweets

Lycaon
@Cynacin

3 days ago

Hello, #FusionGPS... You don't know me but... I know you. I want to play a game.

0:00 / 0:04

2/ Last year #FusionGPS, your bank records were subpoenaed by the HPSCI. You convinced the committee that

Read 11 tweets

Lycaon
@Cynacin

3 days ago

Hacking emails to influence the election doesn't sound like a real solid plan to me. Sounds like a really stupid plan, actually. Sounds invented.

have infected them with ransomware and extorted them for $100 million.

Work my shit all up in their intranets then one night BAM crypt their files. 2015 and 2016 were big years for ransomware. Remember the hospitals, government agencies, etc. that got infected? They were extorted for millions in bitcoin. healthcareitnews.com/news/hollywood...

Read 11 tweets

Related threads

Daniel Ruiz
@DRuizG80

5 days ago

Okay, what follows next are my opinions and and does not constitute investment advice. Before I get started, please be aware today's sales report is bad and the stock will likely trade down on the news.

I would give the stock a few days to digest the news before taking any action.

I'll start with fundamentals. Here's a look at wholesales vs sales. To be perfectly honest, I expected better than +11% y/y in July after the sharp drop in 2017.

Read 36 tweets

🇺🇸 Jayne Q. Patriot 🇬🇧 {☆}
@JayneQPatriot

a month ago

1/87-In 2016 @realDonaldTrump's speech on Globalism "woke" me to the massive corruption in our government: It's no longer Left vs Right, it's: WEALTHY CRIMINALS (#Globalists) VS WE THE PEOPLE (Patriots & @POTUS) #MAGA #QAnon #GreatAwakening #WalkAway

2/87-This is going to be a LONG thread, for those in a hurry... I recommend the "Agenda Explained" series by @RockingMrE: youtube.com/playlist?list=... Start w/the "Globalist Agenda" in under 11 minutes! 👌🤓 @POTUS #MAGA #KAG #QAnon #WalkAway #GreatAwakening #WWG1WGA

Read 88 tweets

lex
@lex6m

a month ago

Thread. Selected list of #indictments for week of June 30, 2018 👇

1. Luis Rodriguez has been charged with laundering hundreds of thousands in drug proceeds thru Las Vegas real estate and shell corporations to send the proceeds to drug traffickers & money launderers in Mexico. #drugtrafficking #moneylaundering #mexico justice.gov/usao-sdny/pr/l...

2. Liberian War Criminal Living in Delaware County Convicted of Immigration Fraud and Perjury #Woewiyu #NPFL #CharlesTaylor #samueldoegovernment #Liberia justice.gov/usao-edpa/pr/l...

Read 24 tweets

Trish Malone
@monkeycomics

2 months ago

I got to explain #GayPanic and #UselessLesbian to my pysch today 😂 These are terms I just learned (over the last few months myself) that described succinctly, what the heck is going on with my brain. To unpack these terms, I'm going to start you with Sappho. -

- “Sweet mother, I cannot weave – slender Aphrodite has overcome me with longing for a girl.” –Sappho To everyone, we've almost all been in this feeling. (i cannot speak for Ace) Someone we see or meet, and their presence just #dazzles us into #malfunction (however brief) -

- it's a pretty common #human #feeling. (again, cannot speak for Ace, and that's ok, y'all are lovely :)) now here's where #GayPanic sets in... we feel the feels, omg, wow, and our

Read 17 tweets

Litsa Dremousis

Lola

I watched the first ep of @RoseanneOnABC on Hulu b/c I want to be fair. 1) Roseanne Barr is still funny, Laurie Metcalf & John Goodman are among the best actors in the U.S., & Sarah Gilbert is nailing it. 2) That said, it reinforces SO many harmful tropes & creates new ones.

3) Why add a Black granddaughter, only to have her grandmother make a "take a knee" joke in front of her? That's not a loving grandma. And please recall ABC killed the @blackishabc ep @funnyblackdude Kenya Barris wrote about taking a knee *after the episode was filmed.*

4) Pretend the Connors were a family of color. Would Trumpists believe that economic hardships befell the family? Or would they be told, a la Paul Ryan & pretty much each

Read 10 tweets

#HappyNewYear2018 STILL waiting 4 #Mueller 2 investigate #DNC #Clinton COLLUSION😵 w/ Ukraine 2 interfere in election. They admit it. There's ACTUAL evidence. Who was Chalupa in contact w/ at DOJ spring 2016? @ChuckGrassley ???
➡grassley.senate.gov/news/news-rele...

🤰UN General Assembly meeting in NYC Sept 2016, HRC met w/ world leaders. SAME TIME, across town, Clinton Global Initiative held annual meeting. 3 heads of state attended. Did foreign dignitaries & biz partners give $ thinking she'd win😷? #PayToPlay ✕
clintonfoundation.org/clinton-global...

During campaign, Sept 2016, Clintons have foreign

Read 16 tweets

Trending hashtags

#Soros #wirefraud #SunyPolytechnic #Agenda2030 #mentalhealthmatters #Crowdstrike #Philippines #LaRaza #ExMuslims #Trump #drugsmuggling #Winning #poultry #drugtrafficking #CulturalMarxist #InternetCrimesAgainstChildren #arkansas #HB2 #MichaelRuffatto #AdamMiles #sheldonsilver #JohnPatriceHale #Sentenced #dossier #borderpatrol