MUELLER'S LATEST INDICTMENT PROVES THAT EVERY ELECTRONIC DEVICE AND PC YOU TOUCH IS ALREADY SPIED ON IN HUNDREDS OF WAYS

Micah Lee

Illustration: Oivind Hovland/Getty Images

ON FRIDAY, Special Counsel Robert Mueller, as part of his investigation into interference with the 2016 presidential election, charged 12 Russian military intelligence officers with conducting "large-scale cyber operations to interfere with the 2016 U.S. presidential election." The indictment contains a surprising amount of technical information about alleged Russian cyberattacks against a range of U.S. political targets, including the Democratic Congressional Campaign Committee, the Democratic National Committee, members of Hillary Clinton's presidential campaign, the Illinois (probably) State Board of Elections, and an American election vendor, apparently VR Systems, and its government customers.

While the indictment only describes the U.S. government's charges in this case, the specific technical evidence presented is compelling and paints by far the most detailed and plausible picture yet of what exactly occurred in 2016.

It also sheds light on what the U.S. government is capable of doing when it investigates cyberattacks, as well as how Russia's Main Intelligence Directorate of the General Staff, or GRU, allegedly conducted the attacks — which it denies — and what operational security mistakes they made. Here are what I find to be the most compelling takeaways from the indictment.

A man walks past the building of the Russian military intelligence service in Moscow, Russia, Saturday, July 14, 2018. Twelve Russian military intelligence officers hacked into the Clinton presidential campaign and Democratic Party and released tens of thousands of private communications in a sweeping conspiracy by the Kremlin to meddle in the 2016 U.S. election, according to an indictment announced days before President Donald Trump's summit with Russian President Vladimir Putin. (AP Photo/Pavel Golovkin)Russia

A man walks past the building of the Russian military intelligence service in Moscow, Russia, on July 14, 2018.
Photo: Pavel Golovkin/AP

The Russians Got Caught Because They Didn't Compartmentalize Enough

The indictment says that the organization DCLeaks, which claimed that it was started by a group of "American hacktivists," and the persona Guccifer 2.0, who claimed to be a Romanian "lone hacker," are both controlled by the named Russian intelligence officers. DCLeaks operated the website dcleaks.com and the Twitter account @dcleaks_, and Guccifer 2.0 operated the website guccifer2.wordpress.com and the Twitter account @Guccifer_2.

Russian officers took steps to anonymize their hacking and infrastructure, according to the indictment, trying to leave no trace of their identity as they rented servers, registered internet domain names, and set up accounts for email, Twitter, and other uses. But they didn't do the best job compartmentalizing this infrastructure. This allowed Mueller's team to confirm that the same people were behind a number of ostensibly distinct operations: DCLeaks, Guccifer 2.0, the spear-phishing campaign, and the hacks of the DCCC and DNC networks.

For example, the spear-phishing emails that John Podesta, Clinton's campaign chair, and others received included links to the URL shortening service Bitly. The Bitly account that created these links was registered using the email address "dirbinsaabol@mail.com." The attackers used that same email address to create an account on a provider where they leased a server, which they paid for using an "online cryptocurrency service" (based on the wording of some instructions quoted in the indictment, I think the service in question may be BitPay). This same cryptocurrency account was used to pay for registering the domain name dcleaks.com. This means that whoever was behind the spear-phishing campaign (and thus the DCCC and DNC hacks) also bought the domain name dcleaks.com, and also leased this server.

Before I bring up another example, here's a quick note about how virtual private networks, or VPNs, work. VPNs can be used to conceal your internet protocol, or IP, address. When you connect to a website, for example twitter.com, while connected to a VPN, that website learns your VPN's internet address and not your real internet address.

Someone used "the same pool of bitcoin funds" to pay for a Malaysian VPN service, as well as a Malaysian server to host the dcleaks.com website, the indictment states. Months later, someone logged into the @Guccifer_2 Twitter account from that same Malaysian VPN account. This confirms that the same people who are behind dcleaks.com also have access to the @Guccifer_2 Twitter account.

What isn't mentioned in the indictment is that, on one occasion, someone reportedly logged into the @Guccifer_2 Twitter account without connecting to a VPN service first, revealing their real IP address. "Working off the IP address," the Daily Beast stated in March, "U.S. investigators identified Guccifer 2.0 as a particular GRU officer working out of the agency's headquarters on Grizodubovoy Street in Moscow."

Russian Hackers May Have Leased Infrastructure From U.S. Providers Who Talked to Investigators

To take over first the DCCC network and then the DNC network, GRU hackers, according to the indictment, used a spear-phishing email, which tricked the recipient into entering their password on a malicious site. They then used the victim's credentials to access DCCC's internal network and installed custom malware called X-Agent on "at least ten DCCC computers," according to the indictment. Soon thereafter, the indictment states, the hackers pivoted to DNC's network. From one of the DCCC computers, the Russian hackers allegedly

"activated X-Agent's keylog and screenshot functions to steal credentials of a DCCC employee who was authorized to access the DNC network." Armed with DNC login credentials, they were able to access "approximately thirty-three DNC computers." Once on the DNC network, they compromised DNC's Microsoft Exchange Server, gaining access to thousands of emails.

After someone hacks a computer and installs spyware, the attacker then sends commands to the spyware to send data back to them. This is typically done by connecting to a computer known as a command and control, or C2, server.

According to the indictment, the computer that the Russians leased to act as X-Agent's C2 server was located in Arizona. After they had allegedly infected computers in the DCCC network with X-Agent, they logged into this C2 server in order to issue commands to specific hacked computers to log keystrokes and take screenshots.

The indictment goes so far as to specify exactly what data was collected on this C2 server, and at what times. For example, it says that on April 14, the Russians surveilled a DCCC employee's computer for eight hours, during which time they captured "communications with co-workers and the passwords she entered while working on fundraising and voter outreach projects."

In the midst of the hack, the DNC discovered what was going on and hired security firm CrowdStrike to investigate it for them. On June 15, CrowdStrike published a blog post, scarce on details, announcing the compromise of the DNC network and attributing the hack to Cozy Bear and Fancy Bear, code names for the GRU hacking units.

Five days after CrowdStrike's blog post, according to the indictment, the Russians allegedly deleted all of the logs from their C2 server that "documented their activities," including their login history.

The fact that the U.S. government had access to the keystrokes and screenshots collected by the C2 server, and even knew at what point in time the GRU agents deleted the activity logs and login history from the server, leads me to believe that the hosting provider likely started to cooperate with the investigation, including possibly sharing snapshots of the hard drive connected to the C2 server. This would allow the investigators to have access to this information.

It also appears that the hackers were unaware that the DNC was on to them until after CrowdStrike published their findings. They appeared to have deleted logs from their C2 server *after* U.S. investigators already had access to it.

In addition to leasing a server in Arizona, the Russians also allegedly leased a separate server in Illinois that they used for a separate piece of malware called X-

Tunnel, which was responsible for compressing and then uploading gigabytes of stolen documents from the DCCC and DNC networks to the server in Illinois "through encrypted channels." It is possible that government investigators obtained information from the hosting provider they leased this server from, as well.

Several Other Companies Must Also Have Talked to Investigators

The quantity of technical details related to GRU's 2016 cyberattacks show that the U.S. government has some impressive capabilities. But the primary capability they appear to have used wasn't technical, it was legal: the subpoena. The U.S. government can compel companies to hand over data.

Based on reading the indictment, I think that the U.S. government almost certainly received data from Bitly, Twitter, Facebook, Google, WordPress, and probably from several other companies, including BitPay or other cryptocurrency payment processors, VPN providers, VPS hosting providers, and domain name registrars, among others. (Twitter and WordPress declined to comment. BitPay said, "BitPay has received subpoenas from U.S. government agencies but how the information is to be used or why it is requested is not shared with us." Facebook and Google did not respond to a request for comment.)

With access to all of the information that companies have related to specific accounts, like IP addresses the attackers used to login to services from, time stamps of when they were active, copies of emails and direct messages sent, and potentially images of the hard drives attached to servers used in the attack, it's possible to paint a *very* detailed picture.

The U.S. (or a Partner) Likely Compromised At Least Two GRU Officers' Computers

One thing that stood out while reading the indictment is how many times the document mentioned exactly what one of the defendants, GRU cyber operations officer Ivan Yermakov, was researching on the internet, and when:

- "On or about March 28, 2016, YERMAKOV researched the names of Victims 1 and 2 and their association with Clinton on various social media sites."
- "For example, beginning on or about March 15, 2016, YERMAKOV ran a technical query for the DNC's internet protocol configurations to identify connected devices.", "On or about the same day, YERMAKOV searched for open-

source information about the DNC network, the Democratic Party, and Hillary Clinton.", "On or about April 7, 2016, YERMAKOV ran a technical query for the DCCC's internet protocol configurations to identify connected devices."

- "During that time, YERMAKOV researched PowerShell commands related to accessing and managing the Microsoft Exchange Server."
- "On or about May 31, 2016, YERMAKOV searched for open-source information about Company 1 [CrowdStrike] and its reporting on X-Agent and X-Tunnel."

How could the U.S. investigators have access to this information? Two explanations come to mind. The most likely is that the National Security Agency — or a foreign partner, like the Dutch intelligence service AIVD, reported to have provided information on the 2016 election-related hacks to U.S. authorities — compromised Yermakov's computer and regularly logged his keystrokes or accessed his browser history. Another explanation would be that Yermakov used Google while logged into an account to do these searches, and the investigators learned his search history from Google. I find the latter to be less convincing because the search engine Yandex is much more popular in Russia, and are GRU officers really stupid enough to use California-based Google?

Another defendant, Anatoly Kovalev, an officer assigned to a different GRU cyber unit, was mentioned only in connection to attacks on the U.S. election infrastructure, not on the Democrats specifically. But one mention stood out:

- "In or around August 2016, the Federal Bureau of Investigation issued an alert about the hacking of SBOE 1 [State Board of Election 1, probably the state of Illinois] and identified some of the infrastructure that was used to conduct the hacking. In response, KOVALEV deleted his search history. KOVALEV and his co-conspirators also deleted records from accounts used in their operations targeting state boards of elections and similar election-related entities."

How could U.S. investigators know that Kovalev deleted his search history, as well as records belonging to multiple online accounts? Again, I believe the most likely scenario is that the NSA compromised his computer, accessed his browser history, and perhaps logged his keystrokes and took screenshots from his computer using a C2 server of their own.

My guess is that after GRU's fatal mistake, logging into the @Guccifer_2 Twitter account from their Moscow-based IP address, U.S. investigators learned who worked in that office, what their roles were in the hack, and ultimately, infected some of their workstations with malware to gather further evidence.

3283618 01/30/2018 Metal shelves for crypto-currency mining. Eugene Odinokov/Sputnik via AP

Metal shelves for crypto-currency mining. Photo: Eugene Odinokov/Sputnik via AP

The U.S. Government Is Very Good at Tracking Bitcoin

The indictment accuses the Russians of conspiring to "launder the equivalent of more than $95,000 through a web of transactions structured to capitalize on the perceived anonymity of cryptocurrencies such as bitcoin."

Far from being anonymous, bitcoin transactions are stored forever in a public ledger known as the blockchain that's open for anyone on the internet to inspect. An account that holds bitcoin is called a "wallet," but unlike traditional bank accounts, bitcoin wallets are just a number — they don't include the identity or name of the owner. Because of this, if you're able to acquire bitcoin anonymously, as the Russian defendants allegedly tried to do, you can spend it on anything without the transactions being linked to you.

But it turns out, this is much harder than it seems.

One method to gain access to bitcoin anonymously is to "mine" it, which involves devoting large amounts of computer power toward solving math problems on random numbers over and over again until you're lucky enough to get a correct answer, in which case, a lot of money is added to your bitcoin wallet. According to the indictment, the Russians allegedly mined their own block of bitcoin. The indictment also alleges that the Russians used other methods to obtain bitcoin anonymously, including "purchasing bitcoin through peer-to-peer exchanges, moving funds through other digital currencies, and using pre-paid cards." The latter method refers to buying prepaid gift cards, debit cards, or other similar cards from physical retail stores using cash, and then anonymously reselling them on the internet in exchange for bitcoin.

One complication to using bitcoin anonymously is payment processors. While it's not necessary for bitcoin transactions, many websites that accept bitcoin as a type of payment use companies such as BitPay or Coinbase to help them process it. These payment processors often attach the buyer's email address and IP address to transactions.

The use of these payment processors, along with reusing the same email address for different transactions, helped the U.S. investigators follow the money. They were likely also helped by looking at what was purchased in bitcoin transactions.

For example, the indictment states the hackers used their freshly mined bitcoin to purchase dcleaks.com from a Romanian domain name registrar, and that a U.S.-based payment processing company was involved in the transaction. Because the block of bitcoin was used to purchase dcleaks.com, that block must be controlled by

GRU officers, and any other transactions from that same block also must have also originated from the GRU.

U.S. investigators could have linked the pool of bitcoin that the Russians mined to DCLeaks via information from the domain registrar, the cryptocurrency payment processor, or even just from the email account that would have received notifications and receipts from these two companies.

The Government Captured DMs and Emails Between WikiLeaks and Guccifer 2.0; WikiLeaks Encouraged Misinformation About Source

According to the indictment, on June 22, WikiLeaks sent a message to Guccifer 2.0 (the indictment doesn't specify on which platform) asking that they "[s]end any new material [stolen from the DNC] here for us to review and it will have a much higher impact than what you are doing."

On July 6, WikiLeaks asked again: "if you have anything hillary related we want it in the next tweo [sic] days prefable [sic] because the DNC [Democratic National Convention] is approaching and she will solidify bernie supporters behind her after," adding that "we think trump has only a 25% chance of winning against hillary … so conflict between bernie and hillary is interesting."

On July 14, Guccifer 2.0 sent an email to WikiLeaks that included an encrypted attachment named "wk dnc link1.txt.gpg." But the body of the email was plaintext — unencrypted and vulnerable to interception by third parties. The indictment says that the unencrypted body explained that "the encrypted file contained instructions on how to access an online archive of stolen DNC documents." Four days later, WikiLeaks responded to this email in another plaintext email, saying that it had received "the 1Gb or so archive" and would release the documents that week.

On July 22, WikiLeaks published a database containing the hacked DNC emails.

The indictment doesn't publish the full text of this exchange of private messages and emails, although it seems clear from quotations in the indictment that Mueller's team possesses them. They are consistent, in both content and typo-ridden style, with previous leaked Twitter direct messages between WikiLeaks and its closest supporters. Surely WikiLeaks understood that its Twitter DMs and plaintext emails with its source, Guccifer 2.0, would eventually come to light.

Two and a half weeks after publishing the DNC emails, while being interviewed on a Dutch television show, WikiLeaks editor Julian Assange encouraged a conspiracy

theory that DNC staffer Seth Rich, who had just recently been killed in what the D.C. police say was a botched robbery, was his source for the DNC emails. After stating WikiLeaks sources face danger, Assange alluded to Rich's shooting, and again alluded to the risks faced by WikiLeaks sources, before stating "we don't comment on who our sources are."
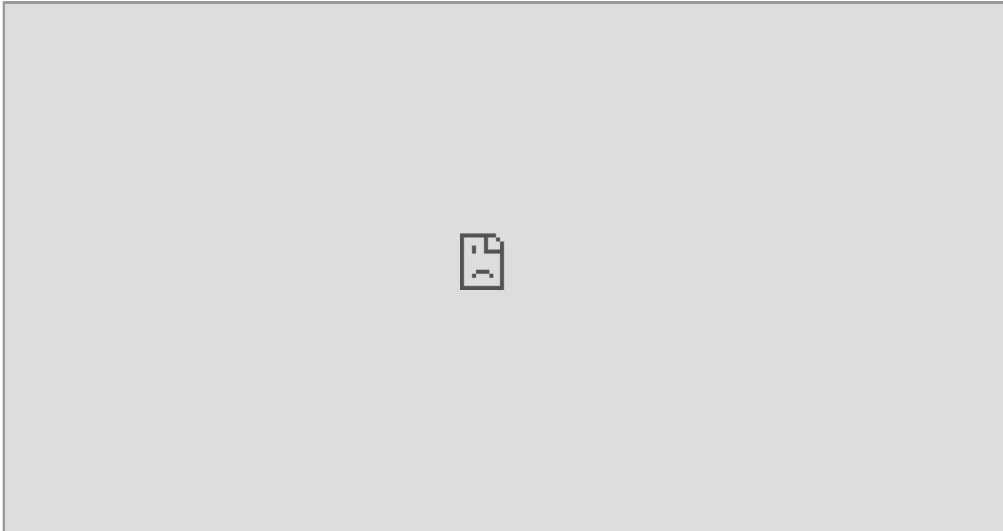
"Whistleblowers go to significant efforts to get us material, and often very significant risks," Assange said. "There's a 27-year-old, works for the DNC, who was shot in the back, murdered, just a few weeks ago, for unknown reasons as he was walking down the street in Washington."

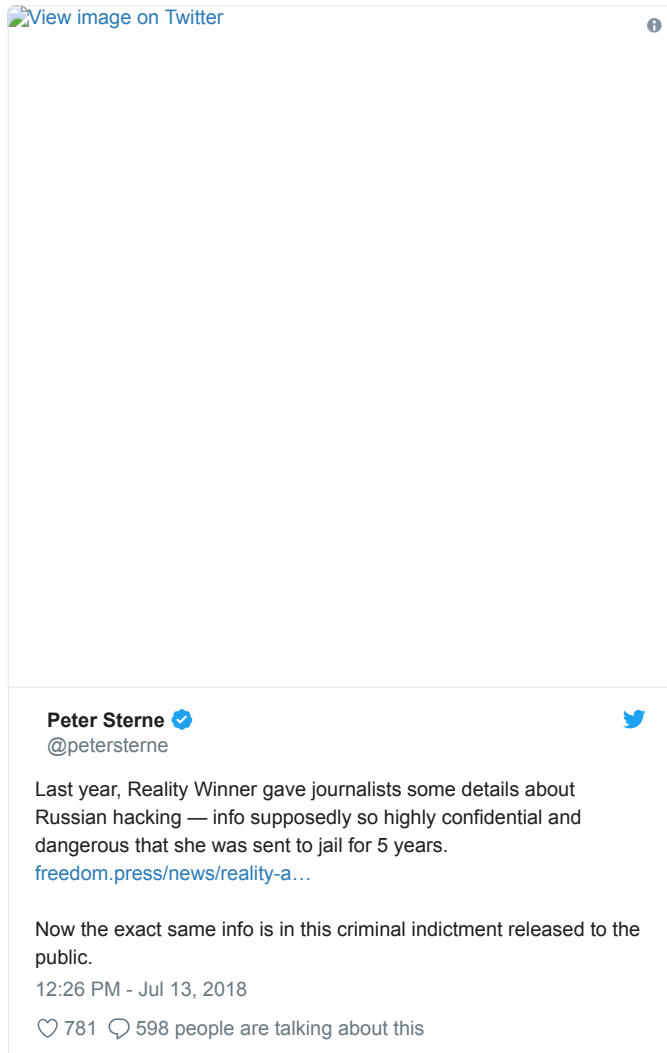WikiLeaks did not respond to a request for comment.

Whistleblower Reality Winner Is in Prison for Leaking Essentially the Same Information Now Being Used as Evidence Against Russian Officers

In the Trump administration's first leak prosecution, 26-year-old former NSA contractor Reality Winner was indicted under the Espionage Act for disclosing a classified document to a news organization. The news organization in question is widely reported to be The Intercept, which published a top-secret document describing in detail a GRU plot to hack American election vendor VR Systems, and then target its customers — local election officials in swing states — with a spear-phishing campaign.

At least some state election officials learned about GRU's spear-phishing attack from reading about it in the news, not from the federal government

— prompttingtwo of them, North Carolina and Virginia, both VR Systems customers, to begin searching their internal emails for evidence of being targeted by the spear-phishing campaign.

Two and a half weeks before Mueller's office issued the indictment against these 12 GRU officers, Winner entered into a plea deal with the Justice Department, pleading guilty to one count of violating Section 793 of the Espionage Act and agreeing to serve 63 months in prison and three years of supervised release.

View image on Twitter

Peter Sterne ✔
@petersterne

Last year, Reality Winner gave journalists some details about Russian hacking — info supposedly so highly confidential and dangerous that she was sent to jail for 5 years.
freedom.press/news/reality-a…

Now the exact same info is in this criminal indictment released to the public.

12:26 PM - Jul 13, 2018

♡ 781 ◯ 598 people are talking about this

The key information that Winner is said to have released to journalists — that NSA had evidence that Russia conducted cyberattacks against the the U.S. electoral system — is now being publicly used to indict the GRU agents who allegedly planned and executed that attack. (Other information from the document linked to Winner does not appear in the indictment.)

Winner is currently awaiting her sentencing hearing in county jail in Lincolnton, Georgia, where she's been since her arrest in June 2017. After she's sentenced, she'll

be transferred to federal prison, where, if she serves the full 63 months she agreed to in her plea deal, she'll be scheduled for release in 2022.

Update: July 19, 2018

The story was updated to note the possibility of a foreign partner helping U.S. intelligence obtain access to Russian targets.

Why should we trust US Intelligence now? (investmentwatchblog.com)
by alexmark to **politics** (**+35**|**-2**)

comments