How they did it (and will likely try again): GRU hackers vs. US elections

By Sean Gallagher

Published: 2018-07-27 · Archived: 2026-04-05 17:08:32 UTC

Skip to content

Latest Mueller indictment offers excruciating details to confirm known election pwnage.

#Cyberz. Credit: Aurich Lawson / Getty

#Cyberz. Credit: Aurich Lawson / Getty

In a press briefing just two weeks ago, Deputy Attorney General Rod Rosenstein announced that the grand jury assembled by Special Counsel Robert Mueller had returned an indictment against 12 officers of Russia's Main Intelligence Directorate of the Russian General Staff (better known as Glavnoye razvedyvatel'noye upravleniye, or GRU). The indictment was for conducting "active cyber operations with the intent of interfering in the 2016 presidential election."

The filing [PDF] spells out the Justice Department's first official, public accounting of the most high-profile information operations against the US presidential election to date. It provides details down to the names of those alleged to be behind the intrusions into the networks of the Democratic National Committee and the Democratic Congressional Campaign Committee, the theft of emails of members of former Secretary of State Hillary

Clinton's presidential campaign team, and various efforts to steal voter data and undermine faith in voting systems across multiple states in the run-up to the 2016 election.

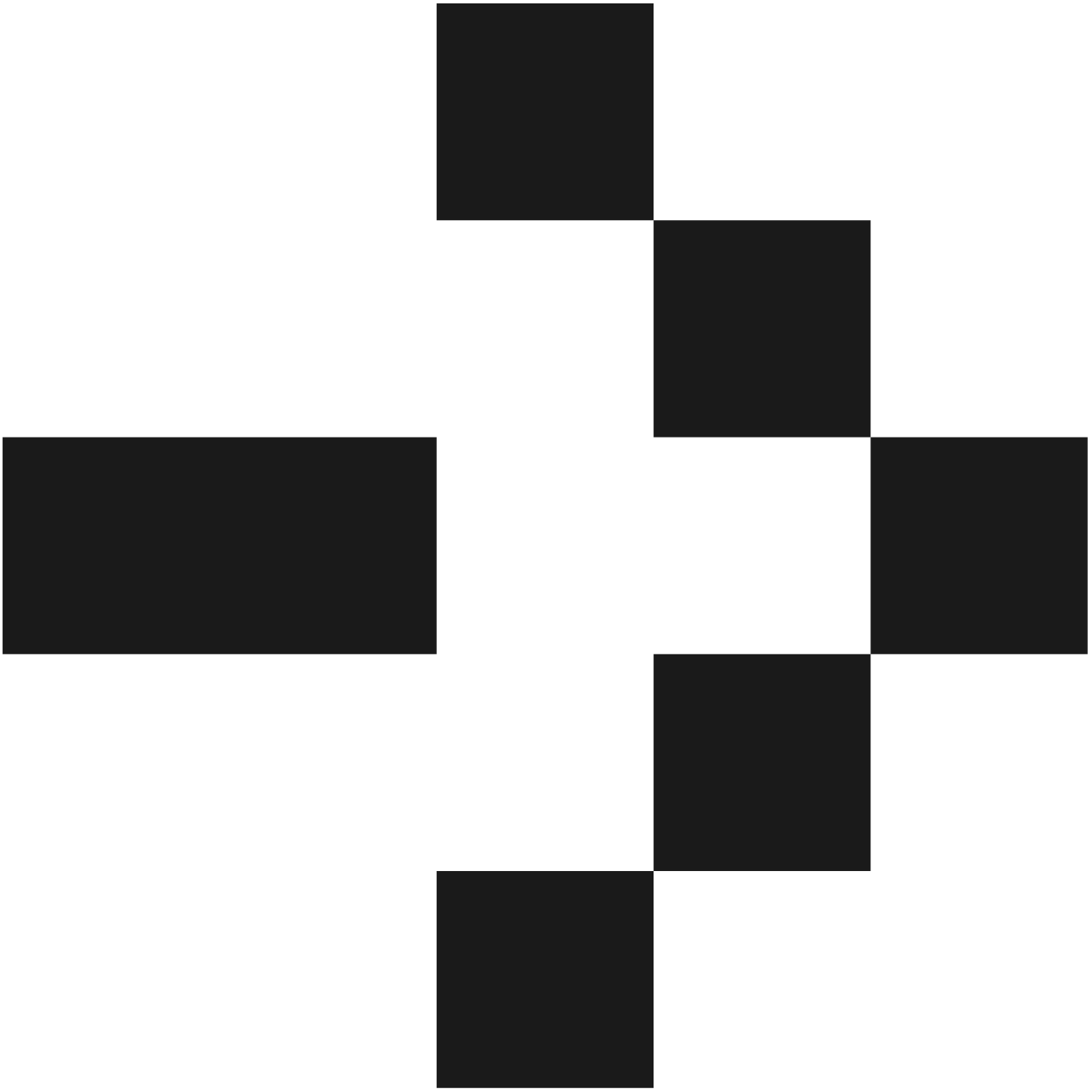
The allegations are backed up by data collected from service provider logs, Bitcoin transaction tracing, and additional forensics. The DOJ also relied on information collected by US (and likely foreign) intelligence and law enforcement agencies. Reading between the lines, the indictment reveals that the Mueller team and other US investigators likely gained access to things like Twitter direct messages and hosting company business records and logs, and they obtained or directly monitored email messages associated with the GRU (and possibly WikiLeaks). It also appears that the investigation ultimately had some level of access to internal activities of two GRU offices.

This is the first time that President Donald Trump's Justice Department has filed official charges against members of a Russian government agency for taking actions intended to influence the outcome of the 2016 presidential campaign—though Rosenstein was careful to assert that there was no allegation that votes were changed by this operation. The indictment details match up with much of what we've already learned about the information operations campaign run by the GRU. But the new findings went further, comfortably identifying each person behind the various elements of the campaign, from the first spear phish to the final data theft.

Yet, after a summit meeting with Russia's President Vladimir Putin just days following the indictment, Trump publicly expressed doubt that Russia was involved. The president has said that Putin strongly denied any interference in the election—even as the United States' own director of national Iintelligence, Dan Coats, reiterated the conclusion that Russia was responsible for the attacks. With such rhetoric, Trump has continued to send mixed messages about the findings of his own intelligence and law enforcement teams, while seeming to put more stock in Putin's insistence that the Russian government had nothing to do with any of this.

After digging into this latest indictment, the evidence suggests Trump may not have made a very good call on this matter. But his blaming of the victims of the attacks for failing to have good enough security, while misguided, does strike on a certain truth: the Clinton campaign, the DNC, and DCC were poorly prepared for this sort of attack, failed to learn lessons from history, and ignored advice from some very knowledgeable third parties they enlisted for help.

The GRU order of battle



An organizational chart of the two GRU units involved in the DNC, DCCC, Clinton campaign and state election organization hacks based on Special Counsel Robert Mueller's indictment.

The indictment includes a significant amount of detail about the organizational structure of the GRU units allegedly involved in the wide-ranging information operations during the US presidential election. The source of the attribution is not revealed in the indictment. However, the level of detail—including when certain individuals connected to remote applications—indicates that US intelligence and law enforcement officials were working with more than just the forensic data provided by CrowdStrike. Trump's "where's the server?" protests seem even less well grounded in reality than they did before.

The details in the newest indictment get down to the organizational division of labor at GRU. "There was one unit that engaged in active cyber operations by stealing information," said Rosenstein, "and a different unit that was responsible for disseminating the stolen information."

The espionage operation was run by Unit 26165, commanded by GRU Officer Viktor Borisovich Netykshko. Unit 26165 appears to be the organization behind at least part of the "threat group" of tools, techniques, and procedures known as "Fancy Bear," "Sofacy," "APT28," and "Sednit." Within the unit, two divisions were involved in the breaches: one specializing in operations and the second in development and maintenance of hacking tools and infrastructure.

The operations division, supervised by Major Boris Alekseyevich Antonov, specialized in targeting organizations of intelligence interest through spear-phishing campaigns and the exploitation of stolen credentials. Antonov's group included Ivan Sergeyevich Yermakov and Senior Lieutenant Aleksey Viktorovich Lukashev, according to the indictment, and they were responsible for targeting the email accounts that were exposed on the "DCLeaks" site prior to the election operations.

The second division, overseen by Lieutenant Colonel Sergey Aleksandrovich Morgachev, managed the development and maintenance of malware and hacking tools used by Unit 26165, including the X-Agent "implant." X-Agent is a signature tool of Fancy Bear operations—a cross-platform backdoor toolset with variants for Windows, MacOS, Android, and iOS. The Windows and MacOS versions of X-Agent are capable of recording keystrokes, taking screenshots, and exfiltrating files from infected systems back to a command and control server.

Lieutenant Captain Nikolay Kozacheck (who used the hacker monikers "kazak" and "blablabla1234465") was the primary developer and maintainer of X-Agent, according to the indictment, and he was assisted by another officer, Pavel Yershov, in preparing it for deployment. Once X-Agent was implanted on the DNC and DCCC networks, Second Lieutenant Artem Malyshev (AKA "djangomagicdev" and "realblatr") monitored the implants through the command and control network configured for the task.

The information operations unit, Unit 74455, was commanded by Colonel Aleksandr Vladimirovich Osadchuk. Unit 74455's members would be responsible for the distribution of some of the stolen data from the breaches through the "DCLeaks" and "Guccifer 2.0" websites. This group famously also reached out to WikiLeaks (referred to as "Organization 1" in the indictment) to amplify their information operation, and they promoted the leaks to journalists through GRU-controlled email and social media accounts.

Within Unit 74455, Officer Aleksy Potemkin—a department supervisor—oversaw information operations infrastructure. His group configured the DCLeaks and Guccifer 2.0 blogs and social media accounts that would later be used to spread data stolen from the DNC, DCCC, and Clinton campaigns. Osadchuk would also direct another information operation—assigning GRU Officer Anatoly Kovalev and others to conduct a campaign against state election boards and elections.

Reconnaissance

GRU officers scanned networks at the Democratic National Committee Headquarters in Washington, DC, shown here during a January 2017 protest, and gathered information on its systems and service providers.

GRU officers scanned networks at the Democratic National Committee Headquarters in Washington, DC, shown here during a January 2017 protest, and gathered information on its systems and service providers.

The GRU operation had conducted wide-ranging spear-phishing attacks against both Democrats and Republicans as far back as October 2015 with limited success. Members of John McCain's and Lindsey Graham's campaign staffs, as well as members of several other Republican congressional campaign staffs, had their emails stolen and later posted on the DCLeaks site. But as the presidential field narrowed, the GRU began to focus on the Democrats and Hillary Clinton's campaign.

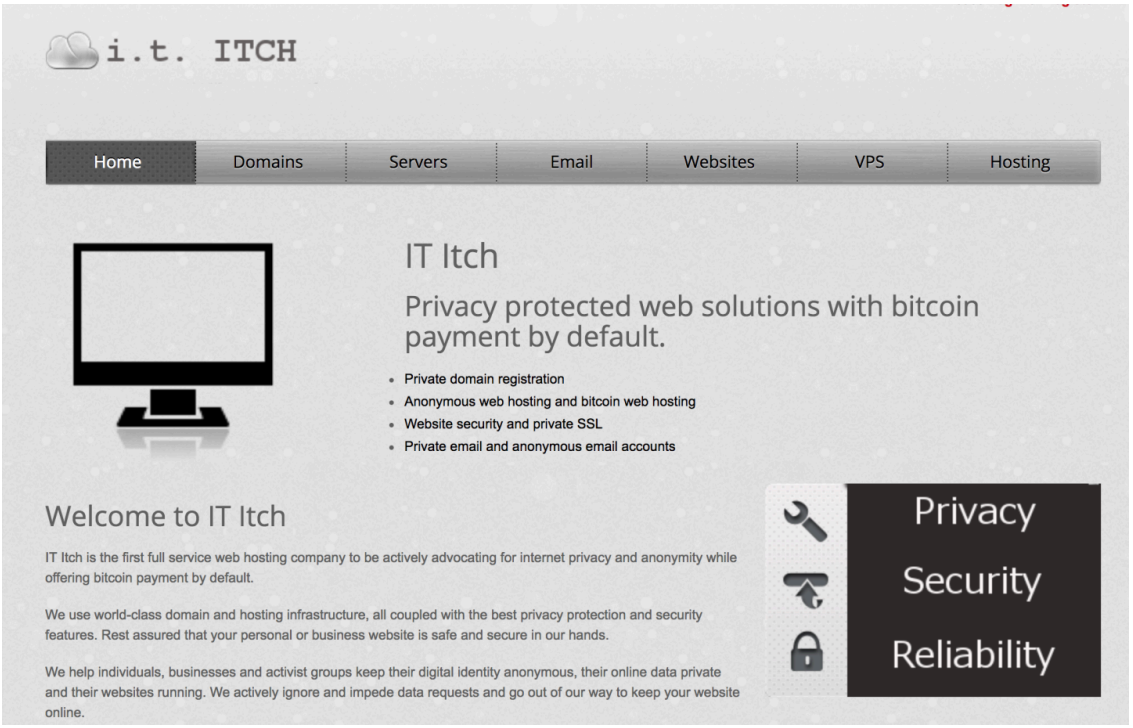
Starting some time during or before March 2016, Antonov's team began to conduct reconnaissance for attacks on organizations associated with the Democratic party. In mid-March, Yermakov performed some initial reconnaissance on the DNC and DCCC networks, scanning the DNC's and DCCC's Internet addresses to identify their infrastructure. He also performed some "open source" research on the organizations' infrastructure and service providers.

In the case of the Hillary For America campaign operation, according to the indictment, that infrastructure was largely based on Google's GSuite. However, many individuals still used personal Gmail accounts. Unfortunately, few if any members of the Clinton campaign staff, DNC, or DCCC used two-factor authentication—despite advice from outside advisors, including former DARPA cybersecurity program lead and longtime security researcher Peiter "Mudge" Zatko. As Zatko recently recounted in a Twitter thread:

> The most effort was expended on trying to get them (and any political candidacy that would listen to me) to implement rudimentary OPSEC protocols. [The] biggest pushback, from people now touting themselves as candidates for security advisors to new politicos, was surprising: They refused to require 2fa: it would be annoying. They pushed back on GSuite to enable document control/access/auditing: another email is too much. The bare minimum defense, which GOOG has made pretty easy to achieve (they were already using GOOG), which disproportionately raises adversary costs, was too much to ask. I offered to deploy 2fa, hardened computers, and configure the communal (cloud) work systems to protect their information. No cost. It was turned down. But I tried.

The lack of two-factor authentication left the Clinton campaign and other Democratic party officials particularly vulnerable to spear-phishing attacks… as the GRU would quickly demonstrate.

Infrastructure, bought with Bitcoin



I.T. Itch, a “bulletproof” domain registrar that was favored by the GRU and used to register at least one spoofed domain for the DCCC hack with a Bitcoin transaction.

I.T. Itch, a “bulletproof” domain registrar that was favored by the GRU and used to register at least one spoofed domain for the DCCC hack with a Bitcoin transaction.

The GRU units used cryptocurrency to procure virtual private network services, domain names, and leased servers—spending about $90,000 worth of Bitcoin to finance election hacking operations, according to the DOJ.

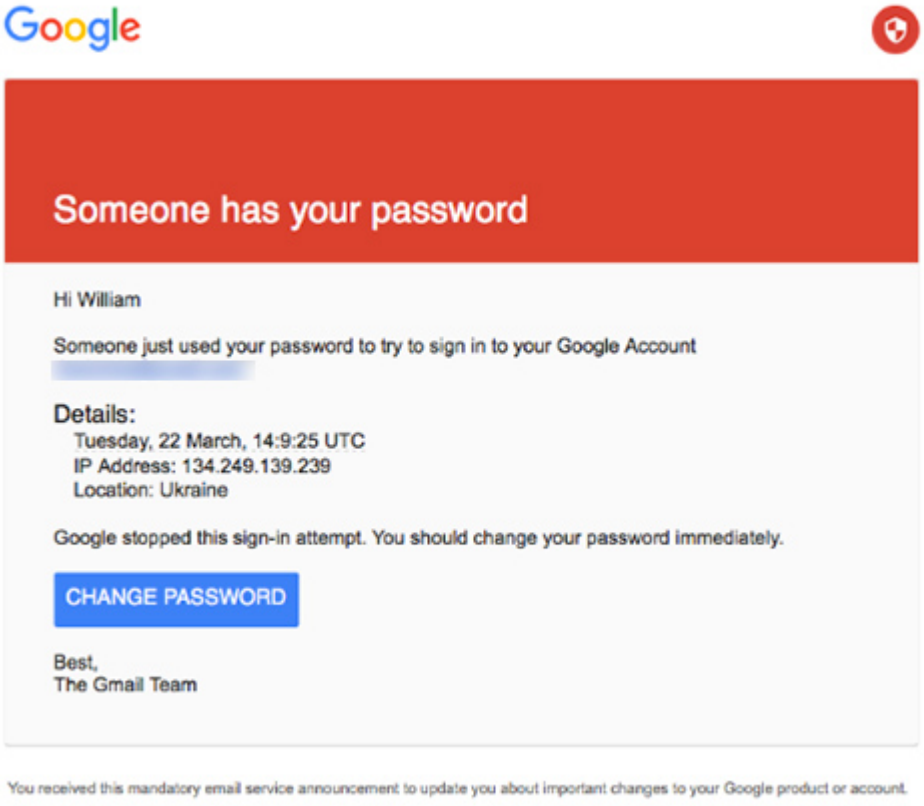
While they used hundreds of throwaway email addresses to obtain these services, a much smaller number of dedicated accounts associated with Bitcoin wallets were used as a sort of central GRU bank to make payments for those services. By analyzing the blockchain of the cryptocurrency used, they were able to link specific purchases to emails requesting payments sent to these accounts.

Many of the transactions from these accounts were initiated from computers used in the DNC/DCCC hacking campaign. Some of the evidence of this activity likely comes from US-based payment processors, including a hosting provider that the GRU officers leased servers from. With those GRU servers, one was in an Illinois data center and acted as the relay for data exfiltration from the DNC and DCCC networks; two more were used later to attack the DNC's cloud services. Another GRU account was used to lease a server in Arizona that acted as the primary command and control server for the DNC and DCCC operations.

Yet another account tracked by investigators was connected to multiple infrastructure purchases. In 2015, it was used to pay for a renewal of "linuxkrnl.net"—a domain used as part of the infrastructure for a Linux version of the X-Agent implant that would eventually be discovered at the DNC. The same account was also used to finance the registration of the "DCLeaks.com" domain through a Romanian registrar to help with spear-phishing domains such as accounts-qooqle.com and account-gooogle.com, and to lease a virtual private server. The email account tied to that server, dirbinsaabol@mail.com, was used to register a Bitly URL shortener account ("john356gh") used for GRU spear-phishing operations.

On March 14, 2016, another of the Bitcoin accounts traced to the GRU was used to pay for a VPN service, according to the indictment. That service would be used later to register the Guccifer 2.0 Twitter account. "The remaining funds from that bitcoin address were then used on or about April 28, 2016, to lease a Malaysian server that hosted the dcleaks.com website," the indictment stated.

Spear phishing



The spear-phishing message sent to Clinton campaign volunteer William Rinehart. Similar emails were sent to Clinton Campaign Chairman John Podesta and others working for Clinton.

According to the indictment, on March 19, 2016, Lukashev worked with others on his team to craft spear-phishing emails, using a Bitly URL-shortening account registered under the user name "john356gh" to create malicious links back to a spoofed Google sign-in page. The Bitly account, as Ars reported in December of 2016, was heavily used by the GRU unit in a months-long string of spear-phishing attacks to steal email credentials.

The links, embedded in messages that spoofed a Google security warning, were sent to a number of Clinton campaign senior staffers, including Clinton Campaign Chairman John Podesta, Campaign Manager Robby Mook, and Senior Foreign Policy Advisor Jake Sullivan. Podesta clicked on the link, thus giving up his Google account credentials.

Another set of spear-phishing links was created on March 25 and used to target even more people associated with the Clinton campaign. Two, referred to as "Victim 1" and "Victim 2" in the indictment, succumbed to spear-phishing messages sent three days later, after Lukashev and his team researched their connection to the campaign through social media. These would appear to be William Rinehart (a Clinton volunteer in Hawaii) and Sarah Hamilton (a campaign PR consultant in Chicago)—both of whom had emails up until March 28 stolen (and later posted to DCLeaks). Both were using their personal Gmail accounts. Others targeted would include former Secretary of State Colin Powell and employees of the DNC and DCCC.

On April 6, according to the indictment, Lukashev and his team constructed a new spear-phishing attack using a malicious link disguised as a spreadsheet named "hillary-clinton-favorable-rating.xlsx." That document link, emailed from an address spoofing the account of a "known member of the Clinton campaign," connected back to a GRU-controlled Web server and prompted targets for network login credentials. The email was sent to the accounts of more than 30 Clinton campaign workers. Another similar phishing email was sent to at least one employee of the DCCC, who clicked the link and gave up her DCCC network credentials.

The pillaging commences

With the DCCC login credentials in hand, Lukashev and his team were able to remotely connect to the DCCC network and begin to move laterally, installing X-Agent on at least 10 computers, according to the indictment. Using the Arizona server as a relay point, they began to collect keystroke capture data and screenshots. They also remotely installed a file compression tool to make archives of files.

Kozachek's X-Agent support team began monitoring the malware implants deployed by Lukashev's group. On April 19, Kozachek and Yershov configured a "middle" server on an overseas host to act as a relay between the X-Agent implants and the top-level command and control server to further obscure the data trail as they began to steal files and other data.

That extra layer was deployed a day after a major score—X-Agent had recorded the credentials of a DCCC staffer who had access to the DNC's network, giving Unit 26165 a way to move laterally onto the DNC's servers. Using X-Agent's search function, the hacking team began to gather up documents from the DNC and DCCC servers, using search terms that included "Hillary," "Cruz," and "Trump."

On April 22, the GRU team began compressing the data into archive files for exfiltration. They then deployed X-Tunnel, another tool from the Fancy Bear kit, to provide an encrypted tunnel to move stolen files over to another server GRU leased in Illinois, starting on April 28. To conceal the tunnel from prying eyes, they used the domain

misdepatrment.com—a misspelling of the domain of the DNC's IT service provider MIS Department. The GRU had registered this in March during the reconnaissance phase of the hack.

In the midst of everything, the distribution team at Unit 74455 was preparing to enter the game. On April 19, someone using the same Mail.com email address used to set up the Bitly account attempted to register the domain electionleaks.com—and when that failed, this person pivoted to DCleaks.com. While the registration service provided anonymity, the payment for the domain was made in cryptocurrency from an online account previously linked to the email address by a payment for a virtual private server.

Next came the mail servers. Yermakov was observed researching PowerShell commands related to Microsoft Exchange Server between May 25 and June 1, and he managed to export thousands of emails from accounts on the server. During the same period, Malyshev was observed using the command and control server to ship upgrades and additional modules to the X-Agent implants on the DNC and DCCC networks. Meanwhile, the hacking team regularly deleted Windows log files to cover their tracks—including purging an event log on May 13.

Burned and burning

The Guccifer 2.0 weblog on WordPress.com.

The Guccifer 2.0 weblog on WordPress.com.

By this time, the DNC's IT staff had determined something bad was going on. The DNC called in CrowdStrike to assist in late May. Starting in June, Crowdstrike began to take steps to block communications from the implants, but the Linux system infected with an X-Agent variant continued to be active until October 2016. The GRU hacking team wasn't giving up its foothold without a fight.

As it became clearer that their X-Agent installs had been burned, Yermakov was tracking reporting from Crowdstrike about X-Agent and X-Tunnel. On June 1, as Crowdstrike began to try to shut down the intrusion on the DNC network, the GRU hacking team tried to cover its tracks on the DCCC network—installing and running CCleaner to purge files.

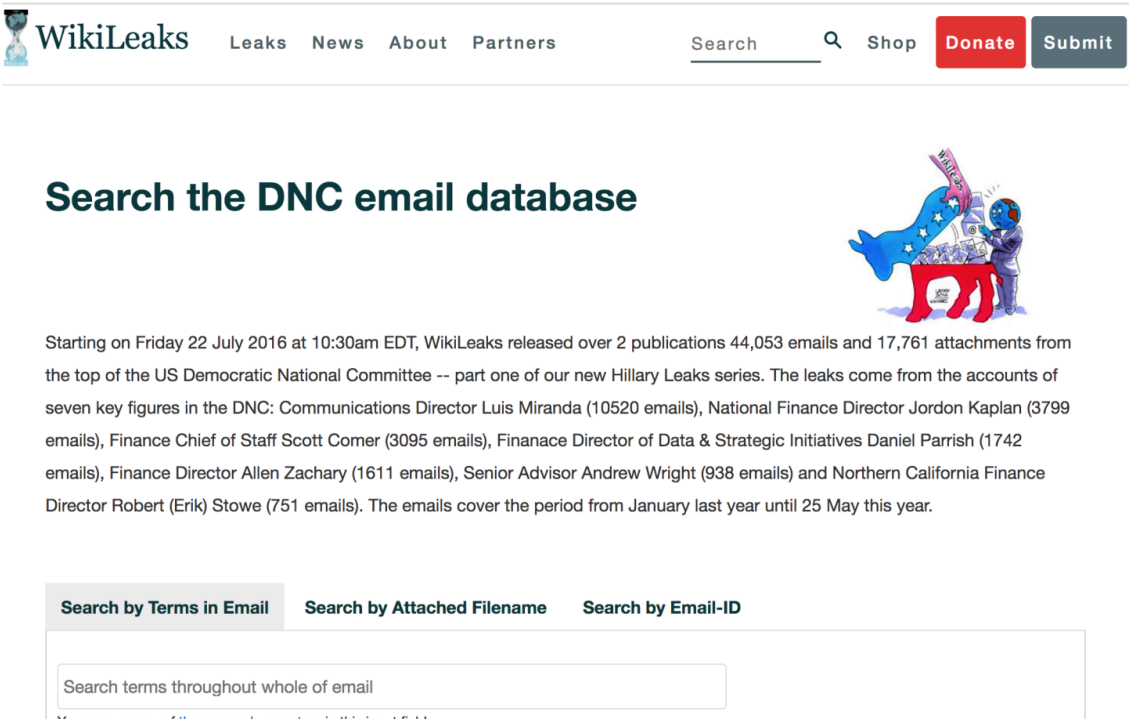
As the intelligence stream was lost, the information operations game began—particularly with the launch of DC Leaks' website, Facebook, and Twitter account on June 8. Logs from Twitter show that the @dcleaks_ account was registered from the same computer used to create @BaltimoreIsWhr—an account that attempted to create buzz around the hashtag #BlacksAgainstHillary through posts exhorting others to "join our flash mob."

There was little to gain traction with in the first DC Leaks postings—the emails on the site were scattershot leftovers from previous phishing efforts, including those stolen emails from Republican congressional campaigns and others targeting military officers and defense contractors. When it came to the Democrats, initially the DC Leaks site posted only a few campaign-related materials. Only later would stolen emails from Clinton campaign volunteers be added to the odd mix of documents eventually thrown up on the DC Leaks site.

In mid-June as Crowdstrike announced that the DNC had been hacked by what the company identified as Russian government actors, the GRU units prepared a nasty going away present for the DCCC. They registered actblues.com, a domain similar to that of the DCCC's fundraising contractor ActBlue. Using stolen DCCC credentials, they gained access to the DCCC Web server and changed the link for contributions to direct visitors to their fake domain. This may have been intended to provide cover for the operation, making it look like a financially motivated attack.

At the same time, Unit 74455 launched the Guccifer 2.0 persona on WordPress. On June 15, as the unit prepared Guccifer's first post, they logged in to a server in Moscow to search for translations of Russian phrases that were then included in the first post—an attempt to convince the world that a single lone hacker had been responsible for the whole DNC and DCCC hack.

A little help from a friend



The WikiLeaks DNC email database. GRU transferred gigabytes of DNC, DCC, and Clinton campaign data to WiklLeaks at the organization's urging.

The WikiLeaks DNC email database. GRU transferred gigabytes of DNC, DCC, and Clinton campaign data to WiklLeaks at the organization's urging.

In the summer of 2016, the hacking team was cleaning house—wiping logs from the Arizona server on June 20 to cover their tracks, for instance. Simultaneously, these hackers were still trying to re-establish a foothold on the DNC and DCCC networks with previously stolen credentials.

Ultimately, the information ops team got rolling with a little help from the outside world. On June 22, someone from WikiLeaks sent a private message to Guccifer 2.0 on Twitter: "Send any new material here for us to review and it will have a much higher impact than what you are doing." The GRU team attempted to send files multiple times, unsuccessfully.

Meanwhile, the Unit 74455 team was busy reaching out to reporters, including The Smoking Gun. Via the Guccifer 2.0 persona, the hackers offered to give "private access" to files via the DC Leaks server on June 27. They gave The Smoking Gun editor William Bastone access to the emails of Sarah Hamilton. (Bastone was the first to tie Guccifer 2.0 to DC Leaks).

On July 6, WikiLeaks messaged the Guccifer 2.0 Twitter account again, trying to close the deal: "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."

The Unit 74455 team responded: "ok … I see."

Whoever was using the WikiLeaks Twitter account soon expanded on the urgency of the request. "We think trump has only a 25% chance of winning against Hillary … so conflict between Bernie and Hillary is interesting."

On July 14, 2016, the GRU team finally sent an email to WikiLeaks with the attachment "wk dnc link1.txt.gpg"—a PGP-encrypted file with instructions on how to get to archives of the stolen DNC documents. "The Conspirators explained to [WikiLeaks] that the encrypted file contained instructions on how to access an online archive of stolen DNC documents," the indictment states. A day later, someone from WikiLeaks replied that they had downloaded "the 1Gb or so archive" and would push out a release of the documents within the week.

WikiLeaks released the DNC emails and files on July 22, just three days before the Democratic National Convention. They declined to say where the cache came from. Then, in the month before the election, WikiLeaks released the stolen emails of John Podesta. "Between on or about October 7, 2016 and November 7, 2016, Organization 1 released approximately thirty-three tranches of documents that had been stolen from the chairman of the Clinton Campaign," Mueller said in the indictment. "In total, over 50,000 stolen documents were released."

Retargeting

> The NSA analyst report that contractor Reality Winner leaked, revealing GRU attacks on county voting agencies in Florida. Credit: Ars Technica

On the Russian side, efforts continued to re-establish a beachhead within the DNC and DCCC. In September, GRU hacking efforts were shifted away from the DNC's internal network and turned on systems hosted in the cloud—including a development and test server for an analytics platform being used by DNC. The GRU team was able to obtain "snapshots" of the virtual machines with DNC data sets and then move them to an account that they had set up with the same hosting service. The indictment does not name the service.

Other hacking attempts pivoted to new targets. On July 27, just after then-candidate Donald Trump "joked" about Russia finding Clinton's "missing emails" from her private mail server, Unit 26165 launched a renewed spear-phishing campaign against Clinton. An "after hours" wave of phishing messages directly targeted email accounts on the domain used by Clinton's personal office for the first time. In total, 76 accounts of Clinton campaign staffers were also targeted in this wave.

Also in July, Unit 74455 finally diversified—in addition to intel distribution, the unit threw its hat into the hacking ring. Kovalev and others had been performing reconnaissance on state boards of election and other state election-related systems since June, and they had performed searches for state political party email addresses, "including filtered queries for email addresses listed on state Republican Party websites," Mueller stated in the indictment.

In July, Kovalev and his team used that info to hack into the Illinois State Board of Elections' Paperless Online Voter Application system (identified in the indictment as "SBOE1"), stealing 500,000 voter registration records that included names, dates of birth, addresses, partial Social Security numbers, and full driver's license numbers. The attack forced Illinois to revert to paper voter registration only for more than a week while the system was hardened.

Kovalev and others on his team would continue to probe state and county systems for vulnerabilities—in October, they probed the websites of counties in Georgia, Iowa, and Florida in search of vulnerabilities, according to the indictment. And in the run-up to the election in November, Kovalev's team sent spear-phishing emails to election officials in some Florida county—spoofing an email account from the election systems vendor, VR Systems. "The

spear-phishing emails contained malware that the conspirators embedded into Word documents bearing [VR System's] logo," the indictment noted.

Some of the details of these network attacks were reported in an FBI "Flash" memo in August of 2016, while others emerged from an NSA analyst report leaked last June by former NSA contractor Reality Winner. But the intent of the attacks was fairly clear: these GRU units wanted to disrupt voter registration and raise doubts about the integrity of the election itself.

"Could have been lots of people"

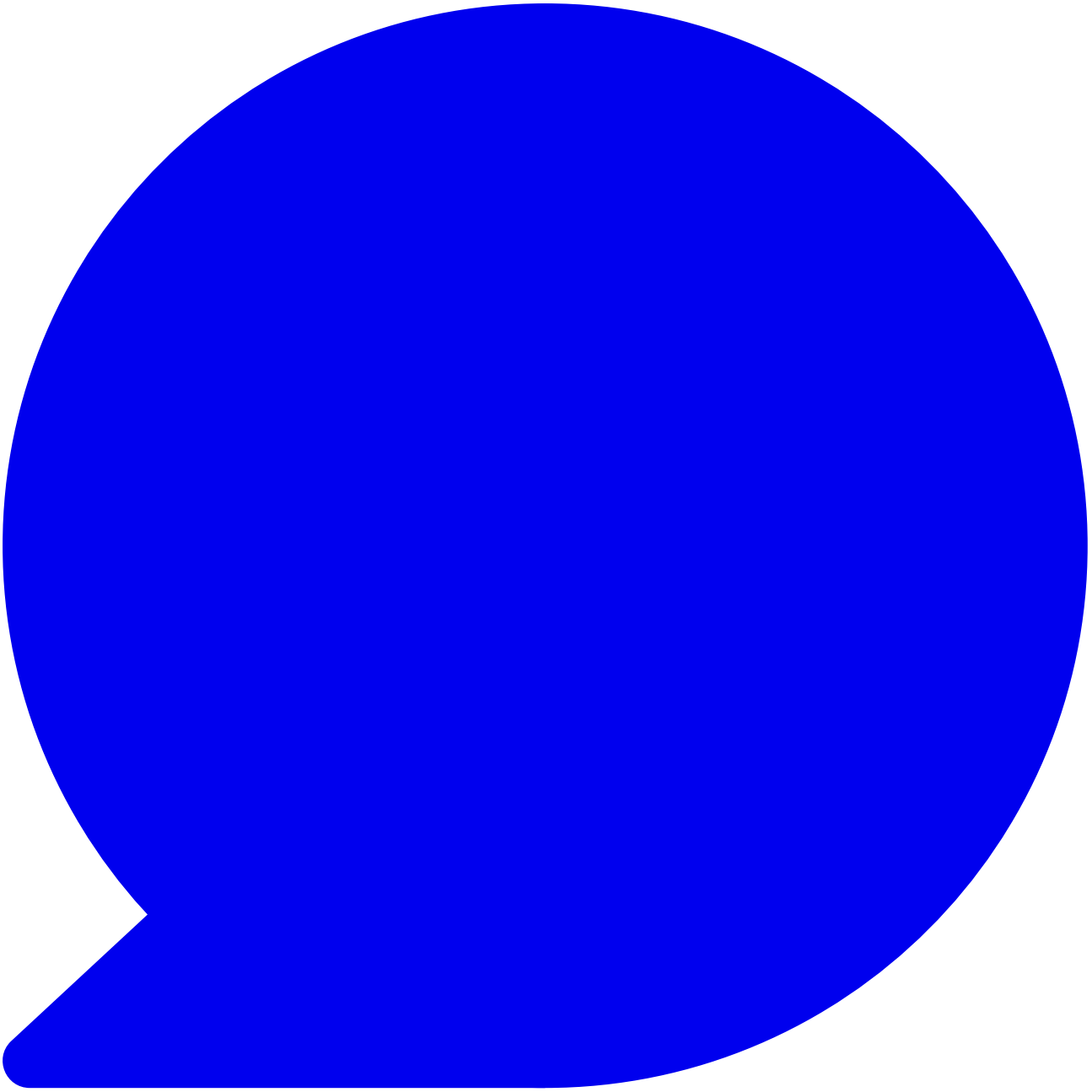
The allegations presented in Mueller's indictment, Rosenstein said in his public statement, were backed by significant evidence. Rosenstein said it was enough evidence that he believed the Justice Department could win a conviction in court. Of course, it's doubtful that any of the 12 indicted GRU officers will ever step into a US courtroom. And, based on the assessment of the US intelligence community, as expressed by Director of National Intelligence Dan Coats at the recent Aspen Security Forum, the GRU and other Russian intelligence agencies are targeting, and will continue to target, the upcoming US midterm elections.

After apparently initially dismissing the findings of the investigation and of the US intelligence community in Helsinki, President Trump's position on what to do has been fluid to say the least. First, in comments from the White House, Trump tried to say that he meant that he believed the intelligence community's findings that Russia had interfered in the 2016 election—but then added that it could have been others in an apparent detour from his script. Statements he has made in interviews since have also been contradictory.

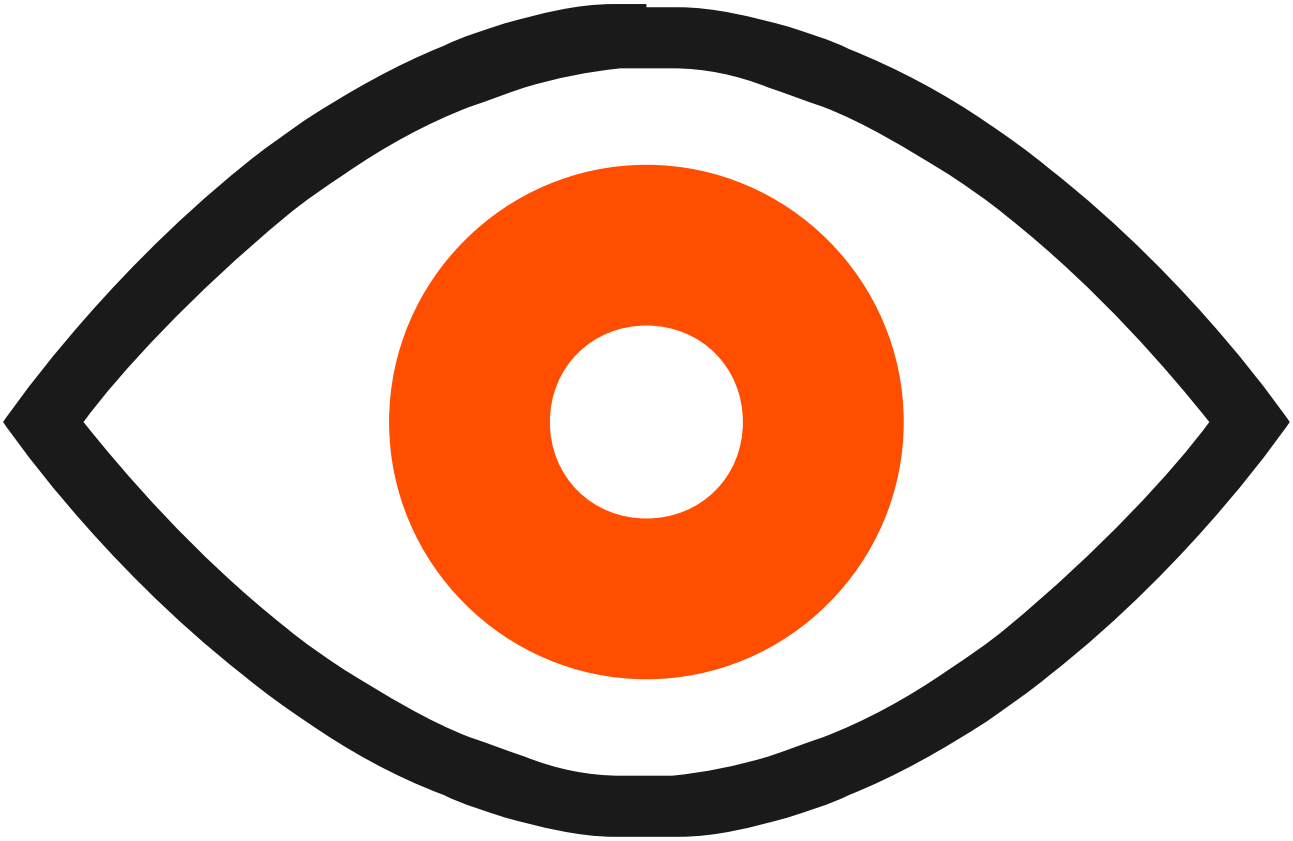
If anything, the indictment may provide the GRU with an important after-action report: it demonstrates where their own operational security failed, revealing their involvement. And while the DNC and DCCC may have improved their defenses, state and local officials and individual congressional campaigns remain as vulnerable as ever. In fact, the president plans on holding a National Security Council meeting today, July 27, to discuss election security ahead of the fall midterms. Right now, it seems likely the July 13 indictment won't be the last time we read about the kinds of attacks that got the GRU inside the DNC, DCCC, and Clinton campaign.

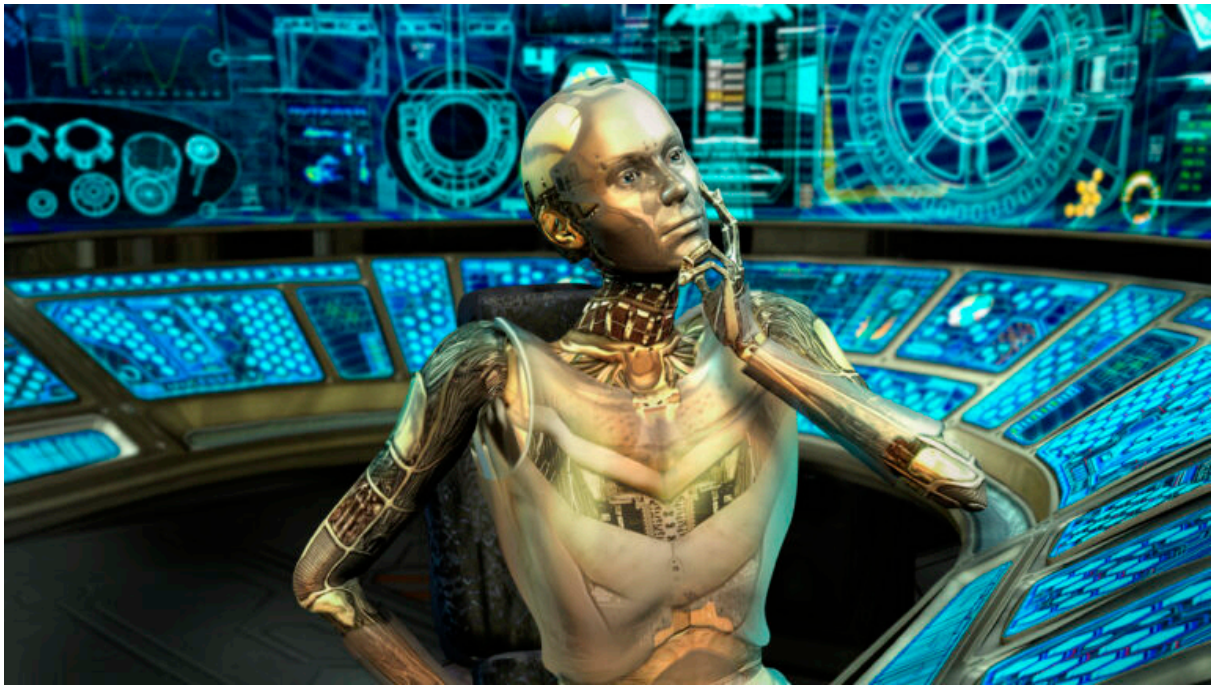
Listing image: Aurich Lawson / Getty

Sean was previously Ars Technica's IT and National Security Editor. After over 20 years in technology journalism, including over 9 at Ars, he pivoted to cybersecurity threat research, first at Sophos and now as a security research engineer at Cisco ‘s Talos Intelligence Group. A former Navy officer, he lives and works in Baltimore, Maryland.



654 Comments



1. 
2.
3.
4.
5.
