THE RUSSIAN HACK

As I laid out last week, I provided information to the FBI on issues related to the Mueller investigation, so I'm going to include disclosure statements on Mueller investigation posts from here on out. I will include the disclosure whether or not the stuff I shared with the FBI pertains to the subject of the post.

Mueller's team just announced (and announced the transfer, as I predicted) of the Russian hack indictment, naming 12 GRU officers for the hack of the Hillary campaign, the DNC, and the DCCC. This will be a working thread.

Rod Rosenstein, as he did with the Internet Research Agency, made clear there are no Americans named in this indictment (and that those who interacted with Guccifer 2.0 and DC Leaks did not know they were interacting with Russians). That said, here are some of the interesting nods in it.

Other known conspirators

The indictment names 12 officers — and (as conspiracy cases often do) — persons known and unknown to the Grand Jury.

Hillary's campaign targeted more aggressively than previously reported

This is a detail I've known for quite some time: Hillary's campaign actually faced far more persistent hacking threats than previously known. Of absolutely critical importance, the indictment makes it clear that GRU hackers spear-phished Hillary's personal office on July

27, after Donald Trump asked Russia to find her emails.

> For example, on or about July 27, 2016, the Conspirators attempted after hours to spearphish for the first time email accounts at a domain hosted by a third-party provider and used by Clinton's personal office. At or around the same time, they also targeted seventy-six email addresses at the domain for the Clinton Campaign.

I know a key witness in that part of the hack has been waiting to share his story (he's quite happy this is finally out), so expect far more details on the targeting of the Hillary campaign itself, rather than just the DNC and DCCC, in coming days.

Wikileaks

The indictment doesn't name Wikileaks, but alleges that Guccifer 2.0 released additional stolen documents through a website maintained by "Organization 1." There's an entire section on communications between Guccifer 2.0 and Wikileaks (starting on page 17). Among other things it quotes Wikileaks as saying on July 6,

> if you have anything hillary related we want it in the next tweo [sic] days prefabl [sic] because the DNC [Democratic National Convention] is approaching and she will solidify bernie supporters behind her after.

This makes it clear that WikiLeaks was not only working directly with Guccifer 2.0, but doing so in ways that would antagonize Bernie-supporting progressives.

Cryptocurrency

The computer infrastructure (including computers

in the US) here was paid for by cryptocurrency, not via payments laundered through the embassy (one of several claims about funding made in the Steele dossier).

May through June 2016

The indictment names Ivan Sergeyovich Yermakov as the person who hacked into the DNC email server and stole the emails released via WikiLeaks. This hack date is critical to the timing of the narrative. The emails exfiltrated and provided to Wikileaks were stolen from May 25 through June 1.

Note, too, the indictment says hackers remained in the DNC computers through June.

Servers

The hackers used a server in AZ but then ran that through a server "overseas." The hackers leased a DCCC computer in Illinois. The use of infrastructure within the US suggests much of the hot air around transfer times — one of the key attempts to debunk the hack — is just that, hot air.

Targeted information

The indictment gives the search terms for some of the targeted information. For example, on April 15, 2016, the conspirators searched for Hillary, Cruz, and Trump, as well as "Benghazi investigations."

It describes a search on a server in Moscow for some of the terms used in the original Guccifer 2.0 post, including "some hundred sheets," "illuminati," "think twice about" "company's competence" (referring to CrowdStrike).

Crowdstrike

The indictment describes Crowdstrike's efforts to oust the hackers, but notes that a Linux

based version of X-Agent remained on DNC's network until October 2016.

Analytics

I have been saying forever that the easiest way to steal the election would be to steal Hillary's analytics. The indictment revals that,

> In or around September 2016, the Conspirators also successfully gained access to DNC computers hosted on a third-party cloud-computing service. These computers contained test applications related to the DNC's analytics. After conducting reconnaissance, the Conspirators gathered data by creating backups, or "snapshots," of the DNC's cloud-based systems using the cloud provider's own technology.

The indictment is silent about what happened to this stolen analytics data.

Republicans

The indictment notes that DCLeaks also released emails of Republicans that were hacked in 2015 (though I think it actually included some that were more recent than that).

Alice Donovan

Alice Donovan pitched news articles to various outlets. It was also the name used for DC Leaks' Facebook account. This name (and a few others in the indictment) connects the hack and leak with the wider disinformation campaign.

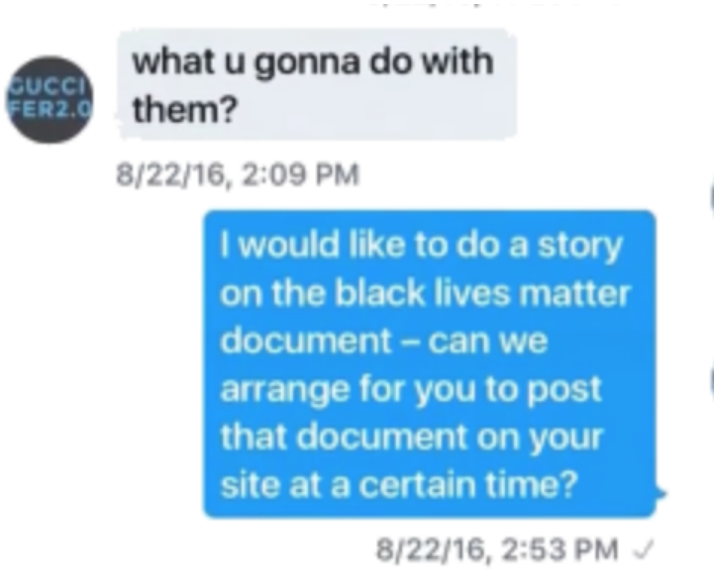
Requested Stolen

Information

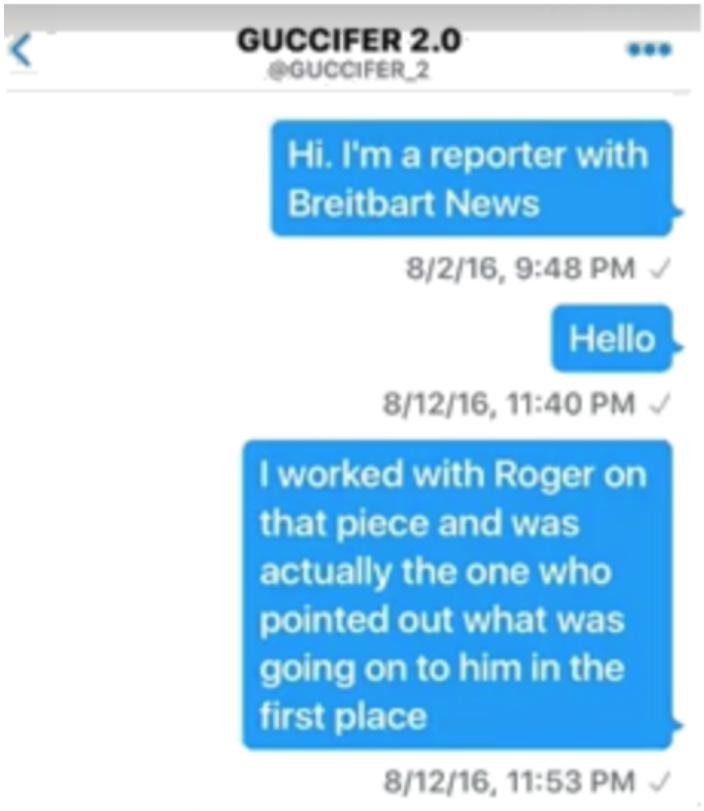
The indictment describes how a candidate for Congress asked for information. I think I know who this is, but need to check.

It describes Guccifer 2.0 providing documents to Aaron Nevins, which I have covered repeatedly.

And it describes a journalist who obtained Black Lives Matters documents. As his DMs make clear, this was then Breitbart and current Sputnik journalist Lee Stranahan.



Stranahan is the journalist who helped Roger Stone write the column claiming that Guccifer 2.0 was an American.



It describes Guccifer 2.0's interactions with Roger Stone (see paragraph 44).

State and vendor servers

The language describing the efforts to hack state sites, starting on page 25, is very specific, down to the named GRU officer. It describes Kovalev stealing the information of 500,000 voters (this is probably from Illinois).

Note, the indictment describes Kovalev deleting information in response to an FBI alert on the hacks of the state server. It doesn't say whether he did so in response to public reporting on it.

Timeline

February 1, 2016: gfade147 0.026043 bitcoin transaction

March 2016: Conspirators hack email accounts of volunteers and employees of Hillary campaign, including John Podesta

March 2016: Yermakov spearphishes two accounts that would be leaked to DC Leaks

March 14, 2016 through April 28, 2016: Conspirators use same pool of bitcoin to purchase VPN and lease server in Malaysia

March 15, 2016: Yermakov runs technical query for DNC IP configurations and searches for open source info on DNC network, Dem Party, and Hillary

March 19, 2016: Lukashev spearphish Podesta personal email using john356gh

March 21, 2016: Lukashev steals contents of Podesta's email account, over 50,000 emails (he is named Victim 3 later in indictment)

March 25, 2016: Lukashev spearphishes Victims 1 (personal email) and 2 using john356gh; their emails later released on DCLeaks

March 28, 2016: Yermakov researched Victims 1 and 2 on social media

April 2016: Kozachek customizes X-Agent

April 2016: Conspirators hack into DCCC and DNC networks, plant X-Agent malware

April 2016: Conspirators plan release of materials stolen from Clinton Campaign, DCCC, and DNC

April 6, 2016: Conspirators create email for fake Clinton Campaign team member to spearphish Clinton campaign; DCCC Employee 1 clicks spearphish link

April 7, 2016: Yermakov runs technical query for DCCC's internet protocol configurations

April 12, 2016: Conspirators use stolen credentials of DCCC employee to access network; Victim 4 DCCC email victimized

April 14, 2016: Conspirators use X-Agent keylog and screenshot functions to surveil DCCC Employee 1

April 15, 2016: Conspirators search hacked DCCC

computer for “hillary,” “cruz,” “trump” and copied “Benghazi investigations” folder

April 15, 2016: Victim 5 DCCC email victimized

April 18, 2016: Conspirators hack into DNC through DCCC using credentials of DCCC employee with access to DNC server; Victim 6 DCCC email victimized

April 19, 2016: Kozachek, Yershov, and co-conspirators remotely configure middle server

April 19, 2016: Conspirators register dcleaks using operational email dirbinsaabol@mail.com

April 20, 2016: Conspirators direct X-Agent malware on DCCC computers to connect to middle server

April 22, 2016: Conspirators use X-Agent keylog and screenshot function to surveil DCCC Employee 2

April 22, 2016: Conspirators compress oppo research for exfil to server in Illinois

April 26, 2016: George Papadopolous learns Russians are offering election assistance in the form of leaked emails

April 28, 2016: Conspirators use bitcoin associated with Guccifer 2.0 VPN to lease Malaysian server hosting dcleaks.com

April 28, 2016: Conspirators test IL server

May 2016: Yermakov hacks DNC server

May 10, 2016: Victim 7 DNC email victimized

May 13, 2016: Conspirators delete logs from DNC computer

May 25 through June 1, 2016: Conspirators hack DNC Microsoft Exchange Server; Yermakov researches PowerShell commands related to accessing it

May 30, 2016: Malyshev upgrades the AMS (AZ) server, which receives updates from 13 DCCC and DNC computers

May 31, 2016: Yermakov researches Crowdstrike and X-Agent and X-Tunnel malware

June 2016: Conspirators staged and released tens of thousands of stolen emails and documents

June 1, 2016: Conspirators attempt to delete presence on DCCC using CCleaner

June 2, 2016: Victim 2 personal victimized

June 8, 2016: Conspirators launch dcleaks.com, dcleaks Facebook account using Alive Donovan, Jason Scott, and Richard Gingrey IDs, and @dcleaks_ Twitter account, using same computer used for other

June 9, 2016: Don Jr, Paul Manafort, Jared Kushner have meeting expecting dirt from Russians, including Aras Agalarov employee Ike Kaveladze

June 10, 2016: Ike Kaveladze has calls with Russia and NY while still in NYC

June 14, 2016: Conspirators register actblues and redirect DCCC website to actblues

June 14, 2016: WaPo (before noon ET) and Crowdstrike announces DNC hack

June 15, 2016, between 4:19PM and 4:56 PM Moscow Standard Time (9:19 and 9:56 AM ET): Conspirators log into Moscow-based sever and search for words that would end up in first Guccifer 2.0 post, including “some hundred sheets,” “illuminati,” “think twice about company’s competence,” “worldwide known”

June 15, 2016, 7:02PM MST (12:02PM ET): Guccifer 2.0 posts first post

June 15 adn 16, 2016: Ike Kaveladze places roaming calls from Russia, the only ones he places during the extended trip

June 20, 2016: Conspirators delete logs from AMS panel, including login history, attempt to reaccess DCCC using stolen credentials

June 22, 2016: Wikileaks sends a private message

to Guccifer 2.0 to “send any new material here for us to review and it will have a much higher impact than what you are doing.”

June 27, 2016: Conspirators contact US reporter, send report password to access nonpublic portion of dcleaks

Late June, 2016: Failed attempts to transfer data to Wikileaks

July, 2016: Kovalev hacks into IL State Board of Elections and steals information on 500,000 voters

July 6, 2016: Conspirators use VPN to log into Guccifer 2.0 account

July 6, 2016: Wikileaks writes Guccifer 2.0 adding, “if you have anything hillary related we want it in the next tweo [sic] days prefabl [sic] because the DNC [Democratic National Convention] is approaching and she will solidify bernie supporters behind her after”

July 6, 2016: Victim 8 personal email victimized

July 14, 2016: Conspirators send WikiLeaks an email with attachment titled wk dnc link1.txt.gpg providing instructions on how to access online archive of stolen DNC documents

July 18, 2016: WikiLeaks confirms it has “the 1Gb or so archive” and would make a release of stolen documents “this week”

July 22, 2016: WikiLeaks releases first dump of 20,000 emails

July 27, 2016: Trump asks Russia for Hillary emails

July 27, 2016: After hours, conspirators attempt to spearphish email accounts at a domain hosted by third party provider and used by Hillary’s personal office, as well as 76 email addresses at Clinton Campaign

August 2016: Kovalev hacks into VR systems

August 15, 2016: Conspirators receive request

for stolen documents from candidate for US congress

August 15, 2016: First Guccifer 2.0 exchange with Roger Stone noted

August 22, 2016: Conspirators transfer 2.5 GB of stolen DCCC data to registered FL state lobbyist Aaron Nevins

August 22, 2016: Conspirators send Lee Stranahan Black Lives Matter document

September 2016: Conspirators access DNC computers hosted on cloud service, creating backups of analytics applications

October 2016: Linux version of X-Agent remains on DNC network

October 7, 2016: WikiLeaks releases first set of Podesta emails

October 28, 2016: Kovalev visits counties in GA, IA, and FL to identify vulnerabilities

November 2016: Kovalev uses VR Systems email address to phish FL officials

January 12, 2017: Conspirators falsely claim the intrusions and release of stolen documents have “totally no relation to the Russian government”