A TALE OF TWO GRU INDICTMENTS

Yesterday, DOJ indicted a bunch of GRU hackers again, in part for hacks in retaliation for anti-doping associations' reports finding a state-run Russian effort to help its athletes cheat (though also including hacks of Westinghouse and the Organization for the Prohibition of Chemical Weapons (OPCW)).

As the DNC GRU indictment did, this indictment provides a snapshot of the division of labor in GRU, made easier by the capture of four of these guys, with all their hacking toys in the trunk of their rented car, in the Netherlands. I find a comparison of the two indictments — of some of the same people for similar activity spanning the same period of time — instructive for a number of reasons.

The team

Consider the team.

There are Aleksei Morenets and Evgenii Serebriakov, whom the indictment calls "on-site GRU hackers who traveled to foreign countries with other conspirators, in some instances using Russian government issued diplomatic passports to conduct on-site operations." Serebriakov even has a title, "Deputy Head of Directorate," which sounds like a pretty senior person to travel around sniffing WiFi networks.

There are the three men we met in the DNC indictment, Ivan Yermakov, Artem Malyshev, and Dmitriy Badin, all of whom work out of Moscow running hacks. Yermakov and Malyshev were closely involved in both hacks in 2016 (as demonstrated by the timeline below).

Finally, there are Oleg Sotnikov and Alexey Minin, who joined Morenets and Serebriakov as they tried to hack the Organization for the Prohibition of Chemical Weapons (OPCW) and tried to hack the Spiez Chemical laboratory that was analyzing the Novichok used to poison Sergei Skripal.

There are slightly different tactics than in the DNC hack. For example, GRU used a bunch of bit.ly links in this operation (though some of those are an earlier campaign against Westinghouse). And they sent out hackers to tap into targets' WiFi networks directly, whereas none of the DNC hackers are alleged to have left Russia.

But there's a ton of common activity, notably the spearphishing of targeted individuals and the use of their X-Agent hacking tool to exploit targeted machines.

Overlapping hack schedule

I'm also interested in the way the WADA hack, in particular, overlaps with the DNC one. I've got a timeline, below, of the two indictments look like (I've excluded both the Westinghouse and OPCW hacks from this timeline to focus on the overlapping 2016 operations).

Yermakov and Malyshev are described by name doing specific tasks in the DNC hack though May 2016. By August, they have turned to hacking anti-doping targets. Yermakov, in particular, seems to play the same research role in both hacks.

Given the impact of these operations, it's fairly remarkable that such a small team conducted both.

Common bitcoin habits and possibly even infrastructure

There are also paragraphs in the WADA indictment, particularly those pertaining to the use of bitcoin to fund the operation used to substantiate the money laundering charge, that appear to be lifted in their entirety from the DNC one (or perhaps both come from DOJ or Western PA US Attorney boilerplate — remember that the DNC hack was originally investigated in Western PA, so this language likely originates there).

These include:

- 58/106: Describing how conspirators primarily used bitcoin to pay for infrastructure
- 59/107: Describing how bitcoin works, with examples specific to each operation provided
- 60/108: Describing how conspirators used dedicated email accounts to track bitcoin transactions
- 61/109: Describing how conspirators used the same computers to conduct hacking operations and facilitate bitcoin payments
- 62/110: Describing how conspirators also mined bitcoin and then used it to pay for servers, with examples specific to each operation
- 64/111: Describing how conspirators used the same funding structure and sometimes the same pool of funds to pay for hacking

> infrastructure, with examples specific to each operation provided

The similarity of these two passages suggests two things. First, it suggests that the August 8, 2016 transaction in the WADA indictment may have been orchestrated from the gfade147 email noted in the DNC indictment. With both, the indictment notes that “One of these dedicated accounts … received hundreds of bitcoin payment requests from approximately 100 different email accounts,” with the DNC indictment including the gfade147 address. (Compare paragraphs 60 in the DNC indictment with 108 in the WADA one.) That would suggest these two operations overlap even more than suspect.

That said, there’s one paragraph in the DNC indictment that doesn’t have an analogue in the WADA one, 63. It describes conspirators,

> purchasing bitcoin through peer-to-peer exchanges, moving funds through other digital currencies, and using pre-paid cards. They also enlisted the assistance of one or more third-party exchangers who facilitated layered transactions through digital currency exchange platforms providing heightened anonymity.

Given how loud much of these operations were, it raises questions about why some of the DNC hack (but not, at least by description) the WADA one would require “heightened anonymity.”

Different treatment of InfoOps

I’m perhaps most interested in the different treatment of the InfoOps side of the operation. As I noted here, in general there seems to be a division of labor at GRU between the actual hackers, in Unit 26165, which is located at 20

Komsomolskiy Prospekt, and the information operations officers, in Unit 74455, which is located in the "Tower" at 22 Kirova Street, Khimki. Both units were involved in both operations.

Yet the WADA indictment does not name or charge any Unit 74455 officers, in spite of describing (in paragraphs 1 and 11) how the unit acquired and maintained online social media accounts and associated infrastructure (paragraph 76 describes that infrastructure to be "procured and managed, at least in part, by conspirators in GRU Unit 74455"). Five of the seven named defendants in the WADA indictment are in Unit 26165, with Oleg Sotnikov and Alexey Minin not identified by unit.

By comparison, three of the 11 officers charged in the DNC indictment belong to Unit 744555.

And the WADA campaign *did* have a significant media component, as explained in paragraphs 76-87. The indictment even complains (as did DOJ officials as the press conference announcing this indictment) about,

> reporters press[ing] for and receiv[ing] promises of exclusivity in such reporting, with one such reporter attempting to make arrangements for a right of first refusal for articles on all future leaks and actively suggesting methods with whicch the conspiracy could search the stolen materials for documents of interest to that reporter (e.g., keywords of interest).

That said, the language in much of this discussion (see paragraphs 77 through 81) uses the passive voice — "were registered," "were named," "was posted," "were released," "were released," "were released," "were released" — showing less certainty about who was running that infrastructure.

That's particularly interesting given that the government clearly had emails between the Fancy

Bear personas and journalists.

One difference may be, in part, that in the DNC indictment, there are specific hacking (not InfoOps) actions attributed to two of the Unit 74455 officers: Aleksandr Osadchuk and Anatoliy Kovalev. Indeed, Kovalev seems to have been added on just for that charge, as he doesn't appear in the introduction section at the beginning of the indictment.

Whereas Unit 74455's role in the WADA indictment seems to be limited to running the InfoOps infrastructure.

Importance of WikiLeaks and sharing with Republicans

It's not clear how much we can conclude form all that. But the different structure in the DNC indictment does allow it to foreground the role of a number of others, such as WikiLeaks and Roger Stone and — as I suggested drop in some or all of those others in a future conspiracy indictment — that were a key part of the election operation.

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 and 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 10-19: Morenets travels to Rio de Janeiro

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 2-9, 2016: Conspirators use multiple IP addresses to connect to or scan WADA’s network

August 2-4, 2016: Yermakov researches WADA and its ADAM database (which includes the drug test results of the world’s athletes) and USADA

August 3, 2016: Conspirators register wada.awa.org

August 5, 9, 2016: Yermakov researches Cisco firewalls, he and Malyshev send specific WADA employees spearfish

August 8, 2016: Conspirators register wada-arna.org and tas-cass.org

August 8, 2016: .012684 bitcoin transaction directed by dedicated email account

August 13-19, 2016: Morenets and Serebriakov travel to Rio, while Yermakov supports with research in Moscow

August 14-18, 2016: SQL attacks against USADA

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 19, 2016: Serebriakov compromises a specific anti-doping official and obtains credentials to access ADAM database

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 1, 2016: Domains fancybear.org and fancybear.net registered

September 6, 2016: Conspirators compromise credentials of USADA Board member while in Rio

September 7-14, 2016: Conspirators try, but fail, to use credentials stolen from USADA board member to access USADA systems

September 12, 2016: Data stolen from WADA and ADAMS first posted, initially focusing on US athletes

September 12, 2016 to January 17, 2018: Conspirators attempt to draw media attention to leaks via social media

September 18, 2016: Morenets and Serebriakov travel to Lausanne, staying in anti-doping hotels, to compromise hotel WiFi

September 19, 2016 to July 20, 2018: Conspirators attempt to draw media attention to leaks via email

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 6, 2016: Emails stolen from USADA first released

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

December 6, 2016 – January 2, 2017: Using IP frequently used by Malyshev, conspirators compromise FIFA's anti-doping files

December 13, 2016: Data stolen from CCES released

January 19-24, 2017: Conspirators compromise computers of four IAAF officials

June 22, 2017: Data stolen from IAAF's network released

July 5, 2017: Data stolen from IAAF's network released

August 28, 2017: Data stolen from FIFA released

As I said in July, 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.*