III. RUSSIAN HACKING AND DUMPING OPERATIONS

Beginning in March 2016, units of the Russian Federation’s Main Intelligence Directorate of the General Staff (GRU) hacked the computers and email accounts of organizations, employees, and volunteers supporting the Clinton Campaign, including the email account of campaign chairman John Podesta. Starting in April 2016, the GRU hacked into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC). The GRU targeted hundreds of email accounts used by Clinton Campaign employees, advisors, and volunteers. In total, the GRU stole hundreds of thousands of documents from the compromised email accounts and networks. The GRU later released stolen Clinton Campaign and DNC documents through online personas, “DCLeaks” and “Guccifer 2.0,” and later through the organization WikiLeaks. The release of the documents was designed and timed to interfere with the 2016 U.S. presidential election and undermine the Clinton Campaign.

The Trump Campaign showed interest in the WikiLeaks releases and, in the summer and fall of 2016, the Trump Campaign stayed in contact about WikiLeaks’s activities. The investigation was unable to resolve WikiLeaks’s release of the stolen Podesta emails on October 7, 2016, the same day a video from years earlier was published of Trump using graphic language about women.

A. GRU Hacking Directed at the Clinton Campaign

1. GRU Units Target the Clinton Campaign

Two military units of the GRU carried out the computer intrusions into the Clinton Campaign, DNC, and DCCC: Military Units 26165 and 74455. Military Unit 26165 is a GRU cyber unit dedicated to targeting military, political, governmental, and non-governmental organizations outside of Russia, including in the United States. The unit was sub-divided into departments with different specialties. One department, for example, developed specialized malicious software (“malware”), while another department conducted large-scale spear phishing campaigns.

---


110 Netyksho Indictment ¶ 1.

111 Separate from this Office’s indictment of GRU officers, in October 2018 a grand jury sitting in the Western District of Pennsylvania returned an indictment charging certain members of Unit 26165 with hacking the U.S. Anti-Doping Agency, the World Anti-Doping Agency, and other international sport associations. United States v. Aleksei Sergeyevich Morenets, No. 18-263 (W.D. Pa.).

112 A spear phishing email is designed to appear as though it originates from a trusted source, and solicits information to enable the sender to gain access to an account or network, or causes the recipient to
secure bitcoins used to purchase computer infrastructure used in hacking operations.\textsuperscript{113}

Military Unit 74455 is a related GRU unit with multiple departments that engaged in cyber operations. Unit 74455 assisted in the release of documents stolen by Unit 26165, the promotion of those releases, and the publication of anti-Clinton content on social media accounts operated by the GRU. Officers from Unit 74455 separately hacked computers belonging to state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections.\textsuperscript{114}

Beginning in mid-March 2016, Unit 26165 had primary responsibility for hacking the DCCC and DNC, as well as email accounts of individuals affiliated with the Clinton Campaign:\textsuperscript{115}

- Unit 26165 used IT to learn about different Democratic websites, including democrats.org, hillaryclinton.com, dnc.org, and dccc.org.

began before the GRU had obtained any credentials or gained access to these networks, indicating that the later DCCC and DNC intrusions were not crimes of opportunity but rather the result of targeting.\textsuperscript{116}

- GRU officers also sent hundreds of spearphishing emails to the work and personal email accounts of Clinton Campaign employees and volunteers. Between March 10, 2016 and March 15, 2016, Unit 26165 appears to have sent approximately 90 spearphishing emails to email accounts at hillaryclinton.com. Starting on March 15, 2016, the GRU began targeting Google email accounts used by Clinton Campaign employees, along with a smaller number of dnc.org email accounts.\textsuperscript{117}

The GRU spearphishing operation enabled it to gain access to numerous email accounts of Clinton Campaign employees and volunteers, including campaign chairman John Podesta, junior volunteers assigned to the Clinton Campaign’s advance team, informal Clinton Campaign advisors, and a DNC employee.\textsuperscript{118} GRU officers stole tens of thousands of emails from spearphishing victims, including various Clinton Campaign-related communications.

download malware that enables the sender to gain access to an account or network. \textit{Netyksho} Indictment ¶ 10.

\textsuperscript{113} Bitcoin mining consists of unlocking new bitcoins by solving computational problems. IT kept its newly mined coins in an account on the bitcoin exchange platform CEX.io. To make purchases, the GRU routed funds into other accounts through transactions designed to obscure the source of funds. \textit{Netyksho} Indictment ¶ 62.

\textsuperscript{114} \textit{Netyksho} Indictment ¶ 69.

\textsuperscript{115} \textit{Netyksho} Indictment ¶ 9.

\textsuperscript{116} See SM-2589105, serials 144 & 495.

\textsuperscript{117} Investigative Technique

\textsuperscript{118} Investigative Technique
2. Intrusions into the DCCC and DNC Networks

a. Initial Access

By no later than April 12, 2016, the GRU had gained access to the DCCC computer network using the credentials stolen from a DCCC employee who had been successfully spearphished the week before. Over the ensuing weeks, the GRU traversed the network, identifying different computers connected to the DCCC network. By stealing network access credentials along the way (including those of IT administrators with unrestricted access to the system), the GRU compromised approximately 29 different computers on the DCCC network.119

Approximately six days after first hacking into the DCCC network, on April 18, 2016, GRU officers gained access to the DNC network via a virtual private network (VPN) connection120 between the DCCC and DNC networks.121 Between April 18, 2016 and June 8, 2016, Unit 26165 compromised more than 30 computers on the DNC network, including the DNC mail server and shared file server.122

b. Implantation of Malware on DCCC and DNC Networks

Unit 26165 implanted on the DCCC and DNC networks two types of customized malware,123 known as "X-Agent" and "X-Tunnel"; Mimikatz, a credential-harvesting tool; and rar.exe, a tool used in these intrusions to compile and compress materials for exfiltration. X-Agent was a multi-function hacking tool that allowed Unit 26165 to log keystrokes, take screenshots, and gather other data about the infected computers (e.g., file directories, operating systems).124 X-Tunnel was a hacking tool that created an encrypted connection between the victim DCCC/DNC computers and GRU-controlled computers outside the DCCC and DNC networks that was capable of large-scale data transfers.125 GRU officers then used X-Tunnel to exfiltrate stolen data from the victim computers.

119 Investigative Technique
120 A VPN extends a private network, allowing users to send and receive data across public networks (such as the internet) as if the connecting computer was directly connected to the private network. The VPN in this case had been created to give a small number of DCCC employees access to certain databases housed on the DNC network. Therefore, while the DCCC employees were outside the DNC's private network, they could access parts of the DNC network from their DCCC computers.
121 Investigative Technique
122 Investigative Technique
123 "Malware" is short for malicious software, and here refers to software designed to allow a third party to infiltrate a computer without the consent or knowledge of the computer's user or operator.
124 Investigative Technique
125 Investigative Technique
To operate X-Agent and X-Tunnel on the DCCC and DNC networks, Unit 26165 officers set up a group of computers outside those networks to communicate with the implanted malware.\(^{126}\) The first set of GRU-controlled computers, known by the GRU as "middle servers," sent and received messages to and from malware on the DNC/DCCC networks. The middle servers, in turn, relayed messages to a second set of GRU-controlled computers, labeled internally by the GRU as an "AMS Panel." The AMS Panel served as a nerve center through which GRU officers monitored and directed the malware's operations on the DNC/DCCC networks.\(^{127}\)

The AMS Panel used to control X-Agent during the DCCC and DNC intrusions was housed on a leased computer located near T\(^{128}\) Arizona.\(^{128}\)

---

\(^{126}\) In connection with these intrusions, the GRU used computers (virtual private networks, dedicated servers operated by hosting companies, etc.) that it leased from third-party providers located all over the world. The investigation identified rental agreements and payments for computers located in, \textit{inter alia}, all of which were used in the operations targeting the U.S. election.

\(^{127}\) Netyksho Indictment ¶ 25.

\(^{128}\) Netyksho Indictment ¶ 24(c).

\(^{129}\) Netyksho Indictment ¶ 24(b).
The Arizona-based AMS Panel also stored thousands of files containing keylogging sessions captured through X-Agent. These sessions were captured as GRU officers monitored DCCC and DNC employees' work on infected computers regularly between April 2016 and June 2016. Data captured in these keylogging sessions included passwords, internal communications between employees, banking information, and sensitive personal information.

c. Theft of Documents from DNC and DCCC Networks

Officers from Unit 26165 stole thousands of documents from the DCCC and DNC networks, including significant amounts of data pertaining to the 2016 U.S. federal elections. Stolen documents included internal strategy documents, fundraising data, opposition research, and emails from the work inboxes of DNC employees.  

The GRU began stealing DCCC data shortly after it gained access to the network. On April 14, 2016 (approximately three days after the initial intrusion) GRU officers downloaded rar.exe onto the DCCC’s document server. The following day, the GRU searched one compromised DCCC computer for files containing search terms that included “Hillary,” “DNC,” “Cruz,” and “Trump.” On April 25, 2016, the GRU collected and compressed PDF and Microsoft documents from folders on the DCCC’s shared file server that pertained to the 2016 election. The GRU appears to have compressed and exfiltrated over 70 gigabytes of data from this file server.

The GRU also stole documents from the DNC network shortly after gaining access. On April 22, 2016, the GRU copied files from the DNC network to GRU-controlled computers. Stolen documents included the DNC’s opposition research into candidate Trump. Between approximately May 25, 2016 and June 1, 2016, GRU officers accessed the DNC’s mail server from a GRU-controlled computer leased inside the United States. During these connections,

---

130 Netyksho Indictment ¶ 27-29; Investigative Technique
131 Investigative Technique
132 Investigative Technique
133 Investigative Technique
134 Investigative Technique
135 Investigative Technique

See SM-2589105-GJ, serial 649. As part of its investigation, the FBI later received images of DNC servers and copies of relevant traffic logs. Netyksho Indictment ¶ 28-29.
Unit 26165 officers appear to have stolen thousands of emails and attachments, which were later released by WikiLeaks in July 2016.\(^{136}\)

**B. Dissemination of the Hacked Materials**

The GRU’s operations extended beyond stealing materials, and included releasing documents stolen from the Clinton Campaign and its supporters. The GRU carried out the anonymous release through two fictitious online personas that it created—DCLeaks and Guccifer 2.0—and later through the organization WikiLeaks.

1. **DCLeaks**

The GRU began planning the releases at least as early as April 19, 2016, when Unit 26165 registered the domain dcleaks.com through a service that anonymized the registrant.\(^{137}\) Unit 26165 paid for the registration using a pool of bitcoin that it had mined.\(^{138}\) The dcleaks.com landing page pointed to different tranches of stolen documents, arranged by victim or subject matter. Other dcleaks.com pages contained indexes of the stolen emails that were being released (bearing the sender, recipient, and date of the email). To control access and the timing of releases, pages were sometimes password-protected for a period of time and later made unrestricted to the public.

Starting in June 2016, the GRU posted stolen documents onto the website dcleaks.com, including documents stolen from a number of individuals associated with the Clinton Campaign. These documents appeared to have originated from personal email accounts (in particular, Google and Microsoft accounts), rather than the DNC and DCCC computer networks. DCLeaks victims included an advisor to the Clinton Campaign, a former DNC employee and Clinton Campaign employee, and four other campaign volunteers.\(^{139}\) The GRU released through dcleaks.com thousands of documents, including personal identifying and financial information, internal correspondence related to the Clinton Campaign and prior political jobs, and fundraising files and information.\(^{140}\)

---

\(^{136}\) *Netyksho* Indictment ¶ 29. The last-in-time DNC email released by WikiLeaks was dated May 25, 2016, the same period of time during which the GRU gained access to the DNC’s email server. *Netyksho* Indictment ¶ 45.

\(^{137}\) *Netyksho* Indictment ¶ 35. Approximately a week before the registration of dcleaks.com, the same actors attempted to register the website electionleaks.com using the same domain registration service.

\(^{138}\) See SM-2589105, serial 181; *Netyksho* Indictment ¶ 21(a).

\(^{139}\) Investigative Technique

\(^{140}\) See, e.g., Internet Archive, “https://dcleaks.com/” (archive date Nov. 10, 2016). Additionally, DCLeaks released documents relating to Personal Privacy, emails belonging to U.S. House, and emails from 2015 relating to Republican Party employees (under the portfolio name “The United States Republican Party”). “The United States Republican Party” portfolio contained approximately 300 emails from a variety of GOP members, PACs, campaigns, state parties, and businesses dated between May and October 2015. According to open-source reporting, these victims shared the same