[redacted] DIRNSA

National Security Agency

# Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors, [redacted] Target U.S. Companies and Local U.S. Government Officials Using Voter Registration-Themed Emails, Spoof Election-Related Products and Services, Research Absentee Ballot Email Addresses; August to November 2016 (TS//SI//OC/REL TO USA, FVEY/FISA)

(U//FOUO) INTELLIGENCE PURPOSES ONLY: (U//FOUO) The information in this report is provided for intelligence purposes only but may be used to develop potential investigative leads. No information contained in this report, nor any information derived therefrom, may be used in any proceeding (whether criminal or civil), to include any trial, hearing, or other proceeding before any court, department, agency, regulatory body, or other authority of the United States without the advance approval of the Attorney General and/or the agency or department which originated the information contained in this report. These restrictions apply to any information extracted from this document and used in derivative publications or briefings.

(U//FOUO) CYBERSECURITY INFORMATION: (U//FOUO) The unclassified data in this report is protected from public disclosure by Federal Law. This report includes sensitive technical information related to computer network operations that could be used against U.S. Government information systems. Any scanning, probing, or electronic surveying of IP addresses, domains, email addresses, or user names identified in this report is strictly prohibited. Information identified as UNCLASSIFIED//FOR OFFICIAL USE ONLY may be shared for cybersecurity purposes at the UNCLASSIFIED level once it is disassociated from NSA/CSS. Consult the originator prior to release of this information to any foreign government outside of the original recipients.

## SUMMARY (U)

(TS//SI//OC/REL TO USA, FVEY/FISA) Russian General Staff Main Intelligence Directorate actors [redacted] executed cyber espionage operations against a named U.S. Company in August 2016, evidently to obtain information on elections-related software and hardware solutions, according to information that became available in April 2017. The actors likely used data obtained from that operation to create a new email account and launch a voter registration-themed spear-phishing campaign targeting U.S. local government organizations. The spear-phishing emails contained a Microsoft Word document trojanized with a Visual Basic script which, when opened, would spawn a PowerShell instance [redacted]

Declassify On: 20420505

[redacted]DIRNSA

and beacon out to malicious infrastructure. In October 2016, the actors also created a new email address that was potentially used to offer election-related products and services, presumably to U.S.-based targets. Lastly, the actors sent test emails to two non-existent accounts ostensibly associated with absentee balloting, presumably with the purpose of creating those accounts to mimic legitimate services.

**Campaign Against U.S. Company 1 and Voter Registration-Themed Phishing of U.S. Local Government Officials (S//SI//REL TO USA, FVEY/FISA)**

**Russian Cyber Threat Actors Target U.S. Company 1 (S//REL TO USA, FVEY/FISA)**

(TS//SI//OC/REL TO USA, FVEY/FISA) Cyber threat actors [redacted] executed a spear-phishing campaign from the email address noreplyautomaticservice@gmail.com on 24 August 2016 targeting victims that included employees of U.S. Company 1, according to information that became available in April 2017.[1] This campaign appeared to be designed to obtain the end users' email credentials by enticing the victims to click on an embedded link within a spoofed Google Alert email, which would redirect the user to the malicious domain [redacted].[2] The following potential victims were identified:

- U.S. email address 1 associated with U.S. Company 1,
- U.S. email address 2 associated with U.S. Company 1,
- U.S. email address 3 associated with U.S. Company 1,
- U.S. email address 4 associated with U.S. Company 1,
- U.S. email address 5 associated with U.S. Company 1,
- U.S. email address 6 associated with U.S. Company 1, and
- U.S. email address 7 associated with U.S. Company 1.

(TS//SI//OC/REL TO USA, FVEY/FISA) Three of the malicious emails were rejected by the email server with the response message that the victim addresses did not exist. The three rejected email addresses were U.S. email address 1 to 3 associated with U.S. Company 1.

---

1. (TS//SI//OC/REL TO USA, FVEY/FISA) *The GRU* [redacted] *is also rendered as military unit* [redacted]
2. (TS//SI//OC/REL TO USA, FVEY/FISA) *For additional information on* [redacted] *and its cyber espionage mandate, specifically directed at U.S. and foreign elections, see* [redacted]

[redacted] DIRNSA

(TS//SI//OC/REL TO USA, FVEY) COMMENT: The [redacted] actors were probably trying to obtain information associated with election-related hardware and software applications. It is unknown whether the aforementioned spear-phishing deployment successfully compromised all the intended victims, and what potential data from the victim could have been exfiltrated. However, based upon subsequent targeting, it was likely that at least one account was compromised.

**Cyber Threat Actors Create Spoofed Account and Voter Registration-Themed Targeting of Local Government Officials (TS//SI//OC/REL TO USA, FVEY/FISA)**

(TS//SI//OC/REL TO USA, FVEY/FISA) The [redacted] cyber threat actors created a new operational email account vr.elections@gmail.com with the username "U.S. Company 1" on 27 October 2016. (COMMENT: It is likely that the cyber threat actors created this email address to appear as if they were an employee of U.S. Company 1.) The cyber threat actors had in the email account two trojanized Microsoft Word documents with the titles "New_EViD_User_Guides.docm" and "NEW_Staging_Checklist_AIO_Style_EViD.docm". Both of these documents had identical content and hash values, and contained the same malicious Visual Basic script. The body of the trojanized documents contained detailed instructions on how to configure EViD software on Microsoft Windows machines. According to EViD's FAQ website (UNCLASSIFIED), EViD software allows poll workers to quickly check a voter's registration status, name and address. (END OF COLLATERAL)

(TS//SI//OC/REL TO USA, FVEY/FISA) Subsequently, the cyber threat actors used the vr.elections@gmail.com account to contact U.S. email addresses 1 to 122 associated with named local government organizations. (COMMENT: It possible that the targeted email addresses were obtained from the previously compromised account(s) of U.S. Company 1.) The "NEW_Staging_Checklist_AIO_Style_EViD" document was last modified on 31 October 2016 and the "New_EViD_User_Guides" document was last modified on 1 November 2016. (COMMENT: This likely indicates that the spear-phishing campaign occurred either on 31 October or 1 November , although th e exact date of the spear-phishing campaign was not confirmed.)

(TS//SI//REL TO USA, FVEY) COMMENT: Given the content of the malicious email it was likely that the threat actor was targeting officials involved in the management of voter registration systems. It is unknown whether the aforementioned spear-phishing deployment successfully compromised the intended victims, and what potential data could have been accessed by the cyber actor.

**Technical Analysis of the Trojanized Documents (U//FOUO)**

(TS//SI//OC/REL TO USA, FVEY/FISA) Both trojanized Microsoft Word documents contained a malicious Visual Basic script that spawns PowerShell and uses it to execute a series of commands to retrieve and then

run an unknown payload from malicious infrastructure located at a U.S. IP address on port 8080, probably running Microsoft-IIS/7.5 Server. (COMMENT: The unknown payload very likely installs a second payload which can then be used to establish persistent access or survey the victim for items of interest to the threat actors.) The request used a user-agent string of "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko". Lastly, the malicious Microsoft Word documents hashed to the following values:

- MD5 Hash:5617e7ffa923de3a3dc9822c3b01a1fd,
- SHA-1 Hash:602aa899a6fadeb6f461112f3c51439a36ccba40, and
- SHA-256 Hash:f48c9929f2de895425bdae2d5b232a726d66b9b2827d1a9ffc75d1ea37a7cf6c.

**Operational Accounts Spoofing Legitimate Elections-Related Services (S//REL TO USA, FVEY)**

**Spoofing Email Address Associated With U.S. Company 2 (U//FOUO)**

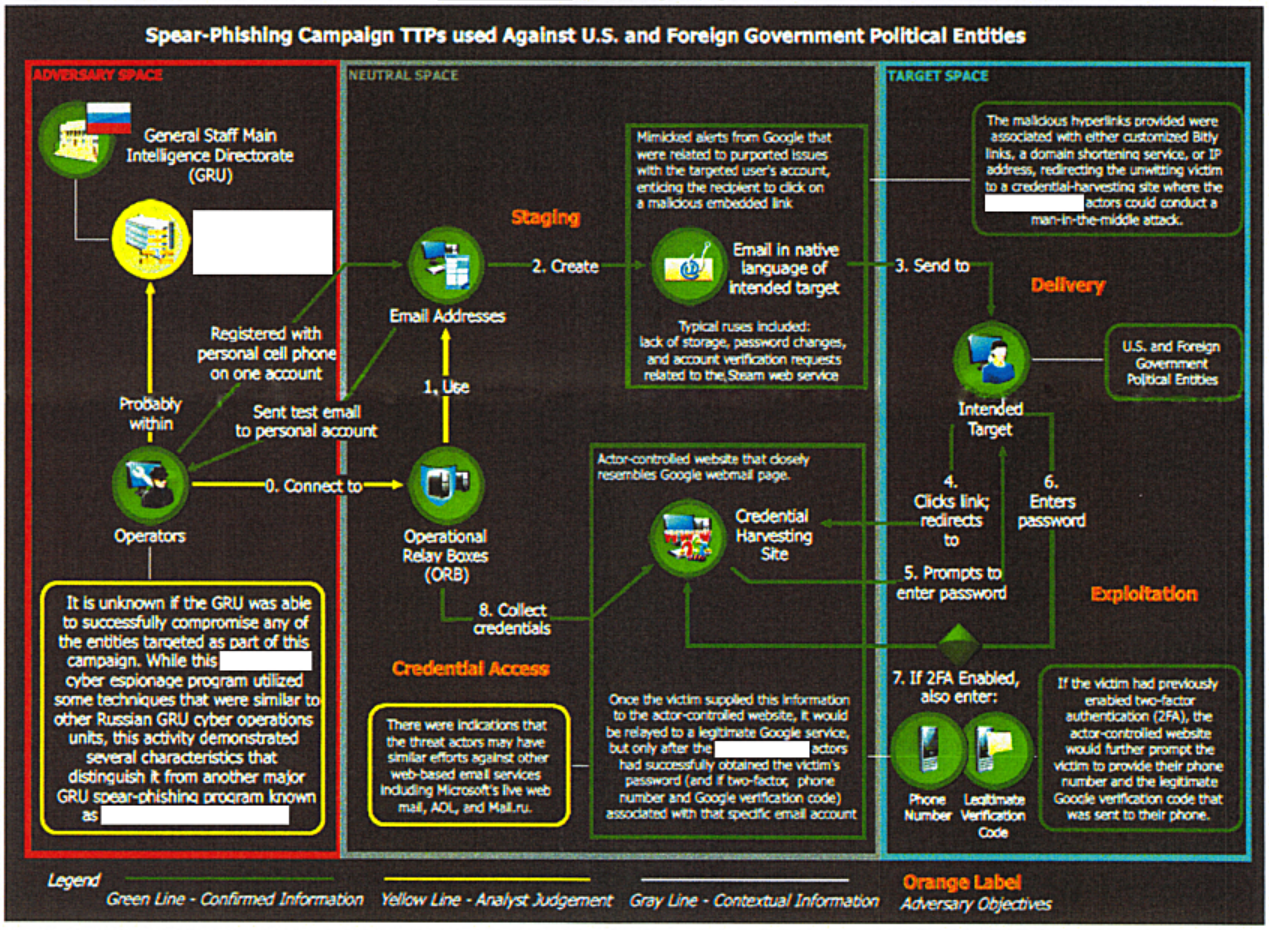
(TS//SI//OC/REL TO USA, FVEY/FISA) In parallel to the aforementioned campaign, the [redacted] cyber threat actors created another new operational email account elevationsystem@outlook.com on 19 October 2016. They then used this email address to send a test message to another known [redacted] operational email account. In that test email, which was written in English, the threat actors spoofed U.S. Company 2, and offered election-related products and services. All emails associated with this account were later deleted, and it was unknown if there was any targeting using this email account. (COMMENT: G iven that the email body was written in English and prepared less than 1 month before the 2016 U.S. Presidential election, it was likely intended for U.S.-based targets.)

**Spoofing Absentee Ballot Email Addresses (U//FOUO)**

(TS//SI//OC/REL TO USA, FVEY/FISA) Additionally, the [redacted] cyber threat actors sent what appeared to be a test email to two other accounts, requestabsentee@americansamoaelectionoffice.org and r-questabsentee@americansamoaelectionoffice.org. In both cases the actors received a response from the mail server on 18 October stating that the message failed to send, indicating that the two accounts did not exist.

> (TS//SI//REL TO USA, FVEY) COMMENT: Given that the test email did not contain any malicious links or attachments, it appeared the threat actors' intent was to create the email accounts rather than compromise them, presumably with the purpose of mimicking a legitimate absentee ballot-related service provider.

TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA [redacted] Spearphishing campaign






TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA

TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA

RUS

Примечание:

Автор настоятельно не рекомендует воспринимать данный доклад всерьёз так как описанными выше уязвимостями мог воспользоваться кто угодно.

Данный документ используется в качестве демонстрации возможностей применения стеганографических методов в принтерах.

ENG

Note:

The author strongly recommends not to take this report seriously, as the vulnerabilities described above could have been exploited by anyone.

This document is used as a demonstration of the possibilities of using steganography methods in printers.