Share / Email

Executive Summary of Grizzly Steppe Findings from Homeland Security Assistant Secretary for Public Affairs Todd Breasseale

Release Date: December 30, 2016

For Immediate Release
Office of the Press Secretary
Contact: 202-282-8010

WASHINGTON – Department of Homeland Security Assistant Secretary for Public Affairs Todd Breasseale issued an executive summary today of the U.S. government's findings of Russian malicious cyber activity known as Grizzly Steppe. The executive summary is below.

GRIZZLY STEPPE: Russian Malicious Cyber Activity

Russia's civilian and military intelligence services engaged in aggressive and sophisticated cyber-enabled operations targeting the U.S. government and its citizens. The U.S. Government refers to this activity as GRIZZLY STEPPE. These cyber operations included spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations, and theft of information from these organizations. This stolen information was later publicly released by third parties.

In operations targeting other countries, including U.S. allies and partners, Russian intelligence services (RIS) have undertaken damaging or disruptive cyber-attacks, including on critical infrastructure—in some cases masquerading as third parties or hiding behind false online personas designed to cause the victim to misattribute the source of the attack.

How Do Russian Intelligence Services Operate in Cyberspace?

RIS often uses spearphishing to gain access to targeted systems (see Figure 1 below). In one 2015–16 operation (detailed in our Joint Analysis Report (JAR)), Russian cyber actors conducted a spearphishing campaign to establish presence and persistence on a target network, obtain higher-level privileges, and steal (or “exfiltrate”) information.

These actors tricked recipients into changing their passwords through a fake website that was designed by the Russians cyber actors to appear legitimate. The actors then used those credentials—the username and password—to access the network as if they were legitimate users. They installed other malicious files, moved freely throughout the target network, gathered data and information, and exfiltrated it from the target network. Russian cyber actors continue to conduct spearphishing campaigns, including one launched as recently as November 2016, just days after the U.S. election.

What is the U.S. Government Doing?

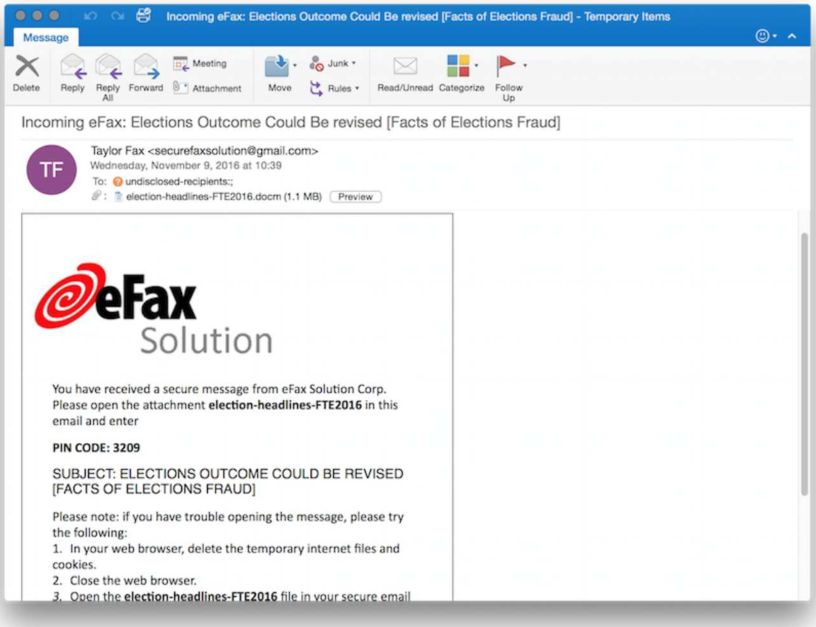
The Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) released a Joint Analysis Report (JAR), which provides details of the tools and infrastructure used by Russian intelligence services (RIS) to compromise and exploit networks and infrastructure associated with the recent U.S. election, as well as a range of U.S. government, political, and private sector entities. The JAR also arms network defenders with the tools they need to identify, detect, and disrupt Russia’s global campaign of malicious cyber activity. We urge users and administrators to use this information to better protect your networks.

What Is Spearphishing?

Spearphishing is the use of forged emails, texts, and other messages to manipulate users into opening malware or malicious software or clicking on malicious links.

Spearphishing attacks can lead to credential theft (e.g., passwords) or may act as an entry point for threat actors into an organization to steal or manipulate data and disrupt operations.

For more information, see the US CERT Tip on Avoiding Social Engineering and Phishing Attacks.



Incoming eFax: Elections Outcome Could Be revised [Facts of Elections Fraud]

TF

Taylor Fax <securefaxsolution@gmail.com>
Wednesday, November 9, 2016 at 10:39
To: undisclosed-recipients:;
: election-headlines-FTE2016.docm (1.1 MB)

You have received a secure message from eFax Solution Corp. Please open the attachment **election-headlines-FTE2016** in this email and enter

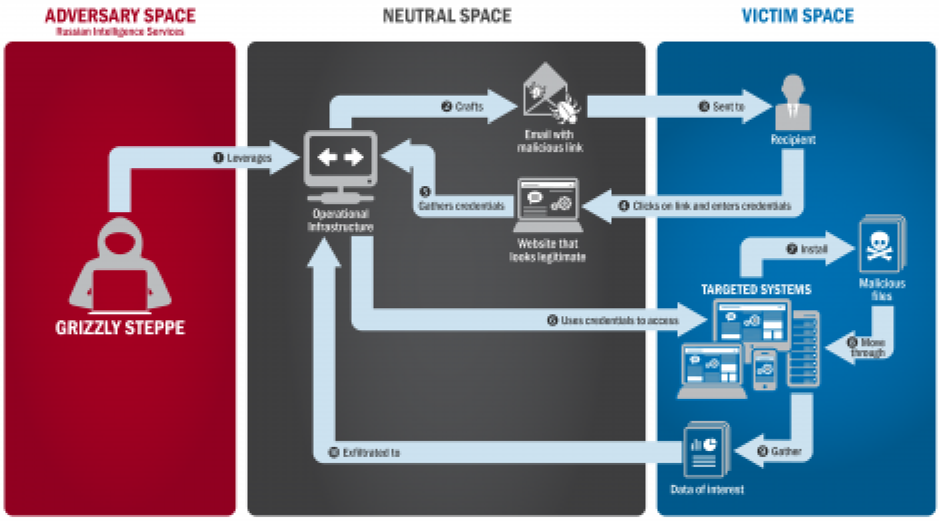
PIN CODE: 3209

SUBJECT: ELECTIONS OUTCOME COULD BE REVISED [FACTS OF ELECTIONS FRAUD]

Please note: if you have trouble opening the message, please try the following:

1. In your web browser, delete the temporary internet files and cookies.
2. Close the web browser.
3. Open the **election-headlines-FTE2016** file in your secure email

Figure 1: Sample of Russian Post-Election Spearphishing



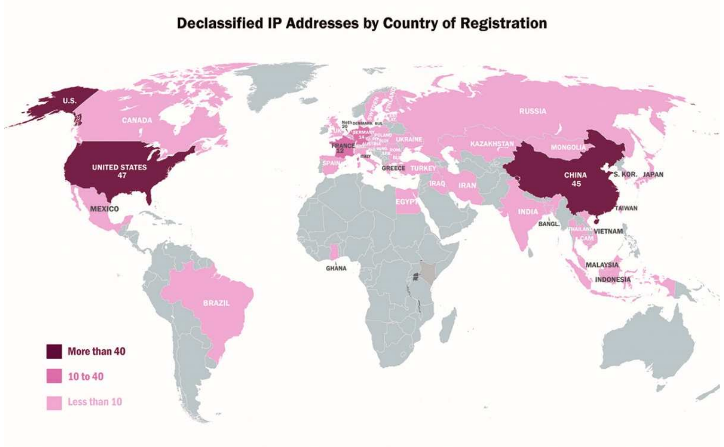
(/photo/lifecycle-successful-spearphishing-operation)

Figure 2: Lifecycle of Successful Spearphishing Operation

What Information is in the JAR?

The JAR includes information on computers, servers, and other devices around the world that RIS uses to conduct command-and-control activity between compromised devices, send spearphishing emails, and steal credentials.

The JAR identifies these devices by each one's Internet Protocol (IP) address, which is a set of numbers that serves as an "address" for each computer and is used to transmit data between computers. Because RIS is using other people's networks without their owners' knowledge to hide their malicious activity, the computers at these IP addresses typically also host legitimate websites or other Internet services. In some cases, the cybersecurity community was aware of this infrastructure. In other cases, this information has been newly declassified by the U.S. government. The map in Figure 3 shows the 60 countries in which newly declassified IP addresses are located. The JAR also includes information on how RIS typically conducts their activities. This information can help network defenders understand how this adversary operates and can help identify new activity or disrupt ongoing intrusions by RIS.



(/photo/declassified-ip-addressed-country-registration)

Figure 3: Declassified Worldwide Infrastructure Co-Opted by Russian Intelligence Services

How You Can Protect Yourself and Your Networks

A commitment to good cybersecurity and best practices is critical to protecting networks and systems. Here are some questions you may want to ask of your organization to help prevent and mitigate against attacks.

- **Backups:** Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
- **Risk Analysis:** Have we conducted a cybersecurity risk analysis of the organization?
- **Staff Training:** Have we trained staff on cybersecurity best practices?
- **Vulnerability Scanning and Patching:** Have we implemented regular scans of our networks and systems? Do we appropriately patch known system vulnerabilities?
- **Application Whitelisting:** Do we allow only approved programs to run on our networks?
- **Incident Response:** Do we have an incident response plan? Have we practiced it?
- **Business Continuity:** Are we able to sustain business operations without access to certain systems? For how long?
- **Penetration Testing:** Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

What to Do If You See Signs of Malicious Cyber Activity

If you find signs of malicious cyber activity, we encourage you report it to DHS's National Cybersecurity and Communications Integration Center (NCCICCustomerService@hq.dhs.gov (mailto:NCCICCustomerService@hq.dhs.gov) or 888-282-0870 (tel:888-282-0870)) or the FBI through your local field office or the FBI's Cyber Division (cywatch@ic.fbi.gov (mailto:cywatch@ic.fbi.gov) or 855-292-3937 (tel:855-292-3937)).

Topics: Combat Cyber Crime (/topics/combat-cyber-crime) , Cybersecurity (/topics/cyber-security)

Keywords: cyber security (/keywords/cyber-security) , Cybersecurity (/keywords/cybersecurity) , cybersecurity activity (/keywords/cybersecurity-activity) , Russia (/keywords/russia)

Last Published Date: December 30, 2016