



Grizzly Steppe – Does the Bear do Cyber?

January 4, 2017 12 n Eastern



Grizzly Steppe

- Agenda
 - What is Grizzly Steppe
 - NCCIC and JAR
 - What kinds of actions create the situation
 - Spearphishing
 - Websites
 - Questions



Grizzly Steppe

Joint Analysis Report (JAR)

- NCCIC, Department of Homeland Security (DHS)
- Federal Bureau of Investigation (FBI)

<https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity>

This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit.



Grizzly Steppe

This RIS activity is part of an ongoing campaign of cyber-enabled operations directed at the U.S. government and its citizens. These cyber operations have include spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations leading to the theft of information.



Grizzly Steppe

Actions to Take Using Indicators

DHS recommends that network administrators review the IP addresses, file hashes, and Yara signature provided and add the IPs to their watchlist to determine whether malicious activity has been observed within their organizations. The review of network perimeter netflow or firewall logs will assist in determining whether your network has experienced suspicious activity.



Grizzly Steppe

Caveat on JAR

- 900 Indicators provided
- under current reviewing and analyzing per the recommendations
- some of the Indicators are related to yahoo, google, and other known businesses
- related network traffic that is used in day to day business activity.



Grizzly Steppe

Reporting (suggested discussion points)

- *E-ISAC*
- *DOE OE-417*
- *NERC Reliability Standard EOP-004*
- *CIP-008 for High and Medium*
- *CIP-003 for Low Impact, Incidence Response*



Grizzly Steppe

Questions on the NCCIC Release or JAR documents?

Has anyone performed any analysis based upon the Release or Jar?



Vulnerabilities

- Websites – Certain websites will deposit viruses on your system
- Spearphishing – what is it and how does it catch you?
 - Looks are deceiving
 - Bad links
 - Attachments



Spearphishing

From: IT Service <clarkbakerfunding@gmail.com> Gmail address
Date: July 25, 2016 at 7:55:10 AM EDT
To: undisclosed-recipients;

Attn: Lehigh University web-mail User,

We noticed that your mailbox has exceeded the allocated storage limit as set by our administrator, you will not be able to send or received email until you upgrade your allocated quota for effective use.

To upgrade your quota now, you need to Copy/click below link to fill the upgrade form.:

<http://admincentre.byethost13.com/form.php> Address not related to company

Failure to do this will have your account inactive.

Lehigh University Support Team.
27 Memorial Drive West, Bethlehem, PA 18015 USA · Phone: [\(610\) 758-3000](tel:6107583000)

Copyright ©2016
All rights reserved.



Spearphishing

From: Internal Revenue Service [irs-service@IRS.GOV] Sent: Tue 2/3/2009 3:55 PM
To:
Cc:
Subject: Official Notification

After the last annual calculations of your fiscal are eligible to receive a tax refund of \$92.50. Please submit the tax refund request and allow us 3-6 days in order to process it. A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please click here :
<http://cimaonline.ca/form/Internal/Revenue/Service/index.html>

Regards,
Internal Revenue Service.

© Copyright 2009, Internal Revenue Service U.S.A.

Phishing emails are often sent from addresses that look official.

Clicking on this link would take you to a fraudulent website with a form to enter your personal information.

Notice that the URL does not direct you to an official IRS website.



Spearphishing

From: Amazon <management@mazoncanada.ca> on behalf of Amazon not an Amazon email address (note the missing A in Amazon) Jan 25, 2014 7:55 PM
To: @sheridanc.on.ca
Cc:
Subject: Suspension

amazon.com

Dear Client, ← Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to believe, your account has been used by someone else. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

<https://www.amazon.com/exec/obidos/sign-in.html> ← Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,
The Amazon Associates Team



© 1996-2013, Amazon.com, Inc. or its affiliates



Be Vigilant

- Keep raising awareness
- Conducting tests
- NERC CIP Versions 5+ Standards will help keep this moving



Additional Questions?