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?

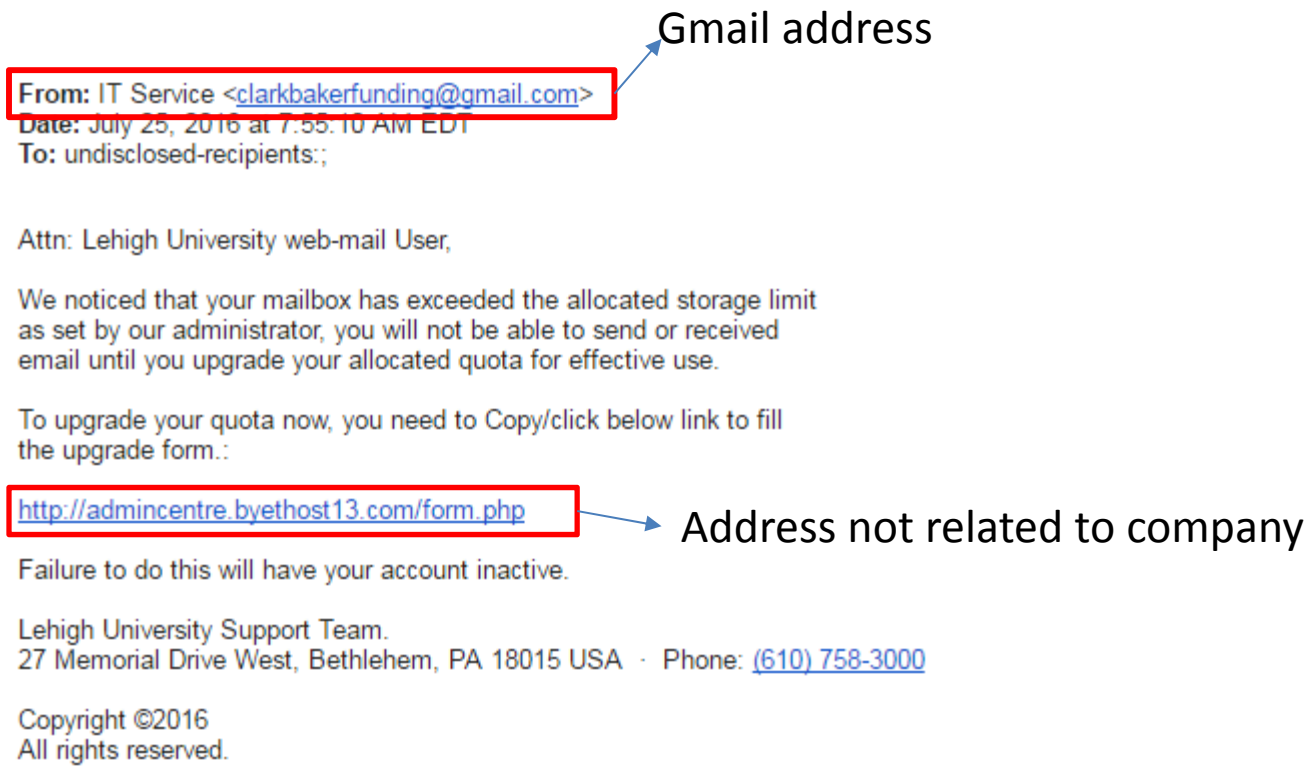
Has anyone performed any analysis based upon the Release or Jar?

Vulnerabilities

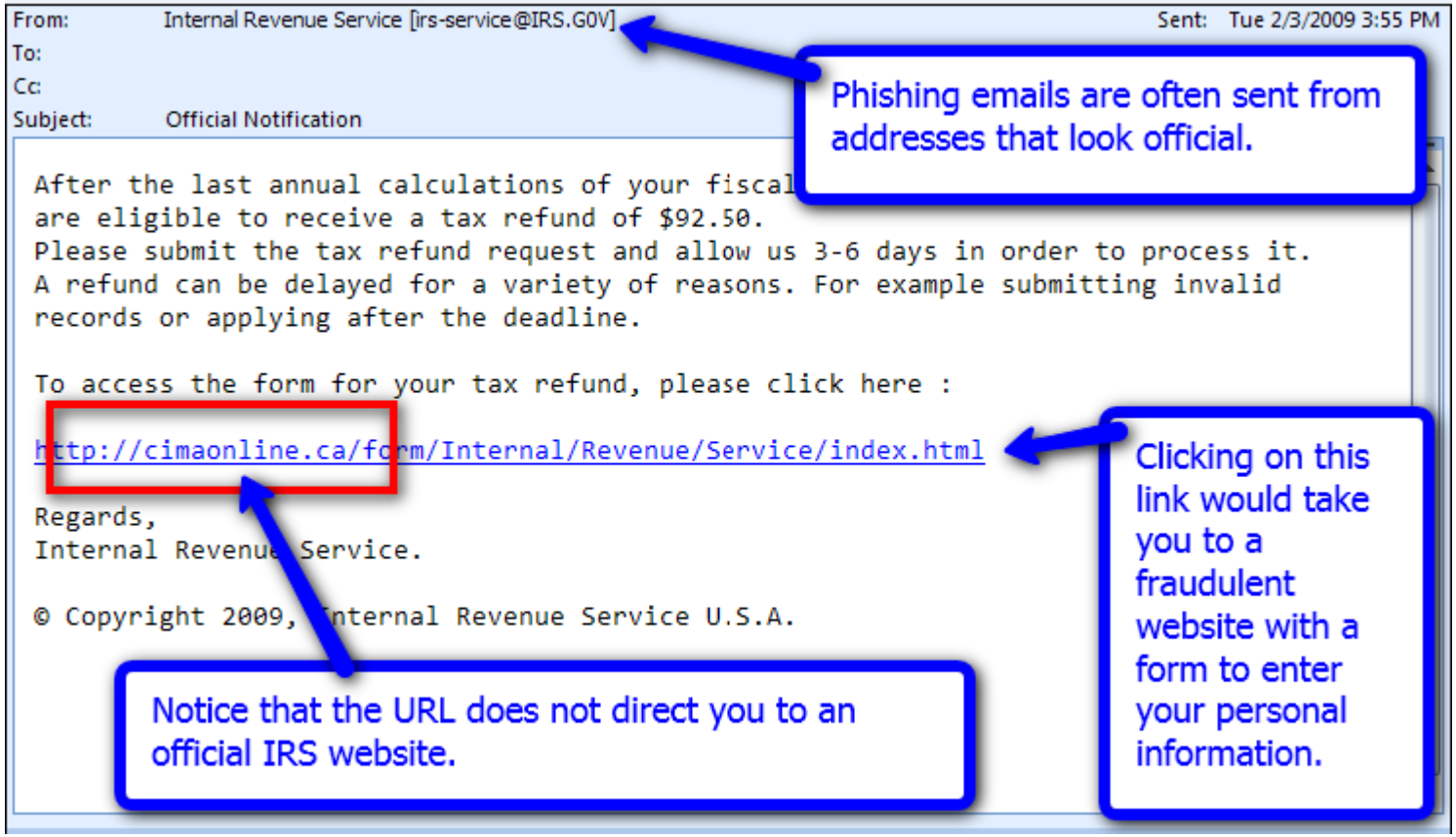
- Websites – Certain websites will deposit viruses on your system

- Spearphishing – what is it and how does it catch you?
  - Looks are deceiving
    - Bad links
  - Attachments

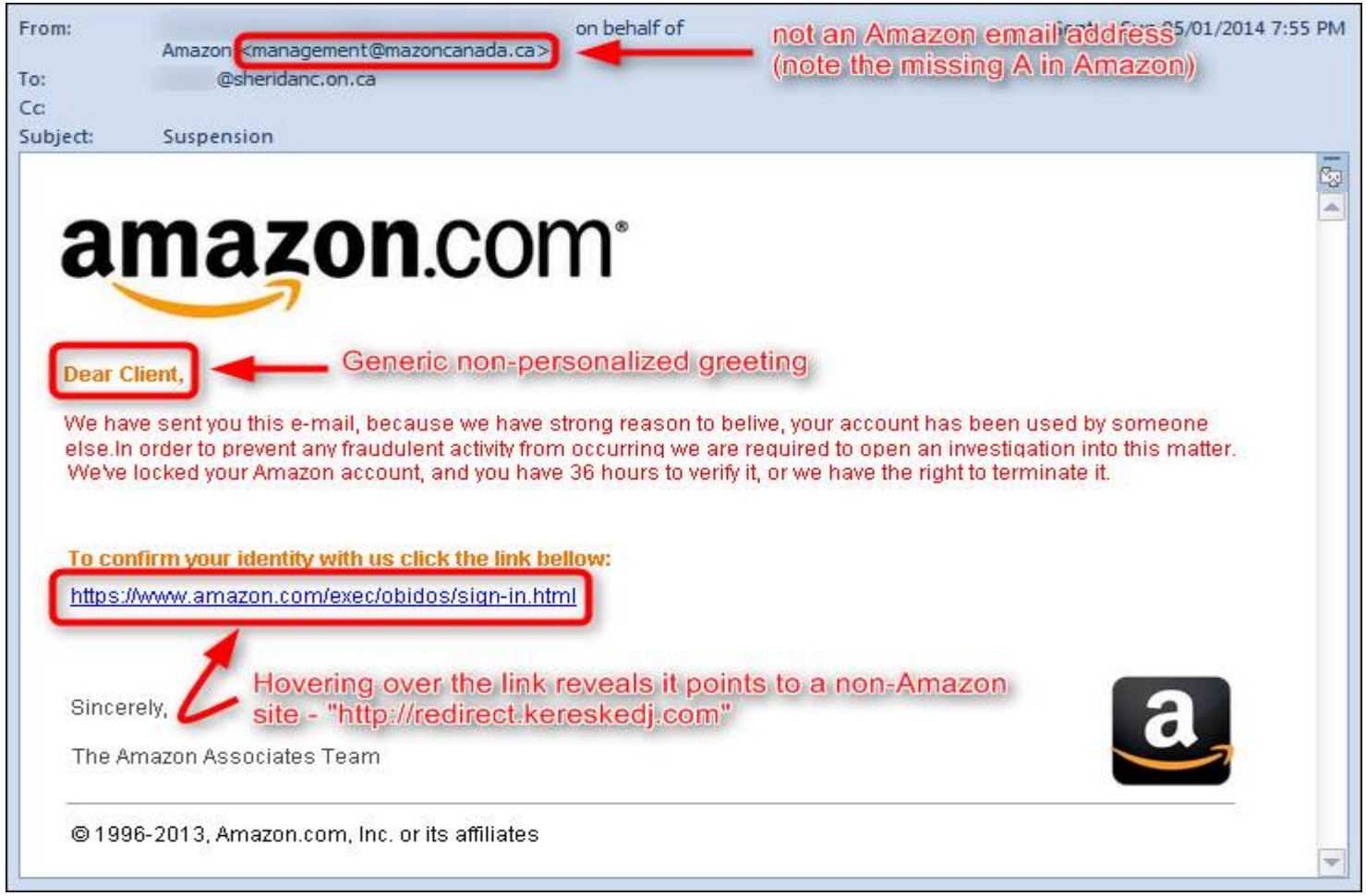
Spearphishing



Spearphishing



Spearphishing



Be Vigilant

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

Additional Questions?