SANS DFIR Webcast Series

DIGITAL FORENSICS & INCIDENT RESPONSE

THE WEBCAST WILL BEGIN SHORTLY

Analyzing the DHS/FBI's GRIZZLY STEPPE Report

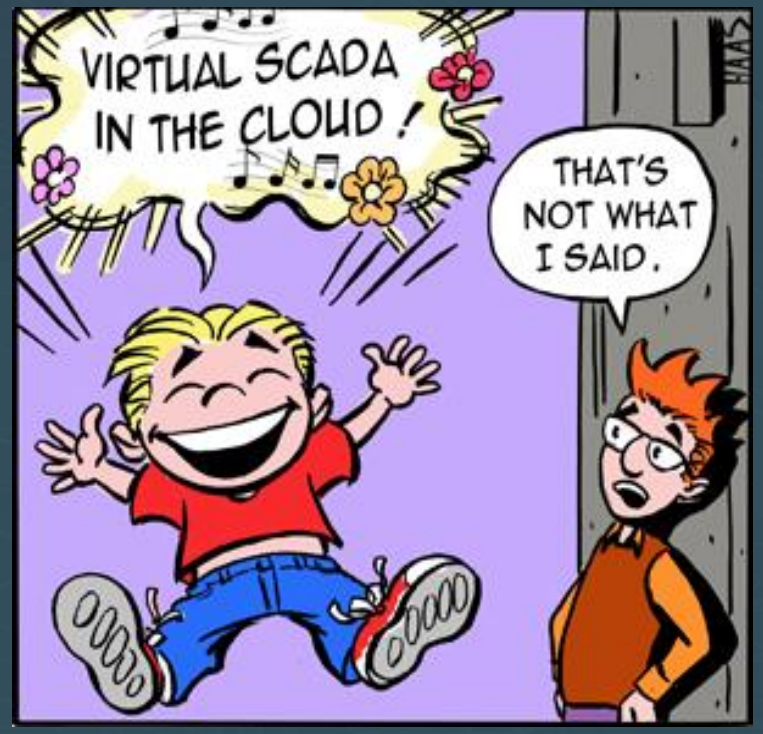
Robert M. Lee @RobertMLee

SANS Webcast

Analyzing the DHS/FBI's GRIZZLY STEPPE Report

DRAGOS

Robert M. Lee



- Current:
  - CEO and Founder, Dragos, Inc.
  - SANS Institute Certified Instructor and Course Author (FOR578 & ICS515)
  - Non-resident National Cybersecurity Fellow, New America
  - PhD Candidate, Kings College London
  - Writer, Little Bobby

Today's Four Intermingled Topics

- Attribution and the Democratic National Committee (DNC) hack
- Obama Administration's messaging to the public and Russian government
- DHS/FBI's GRIZZLY STEPPE Joint Analysis Report (JAR)
- Burlington Electric (Vermont electric utility) and info sharing impacts

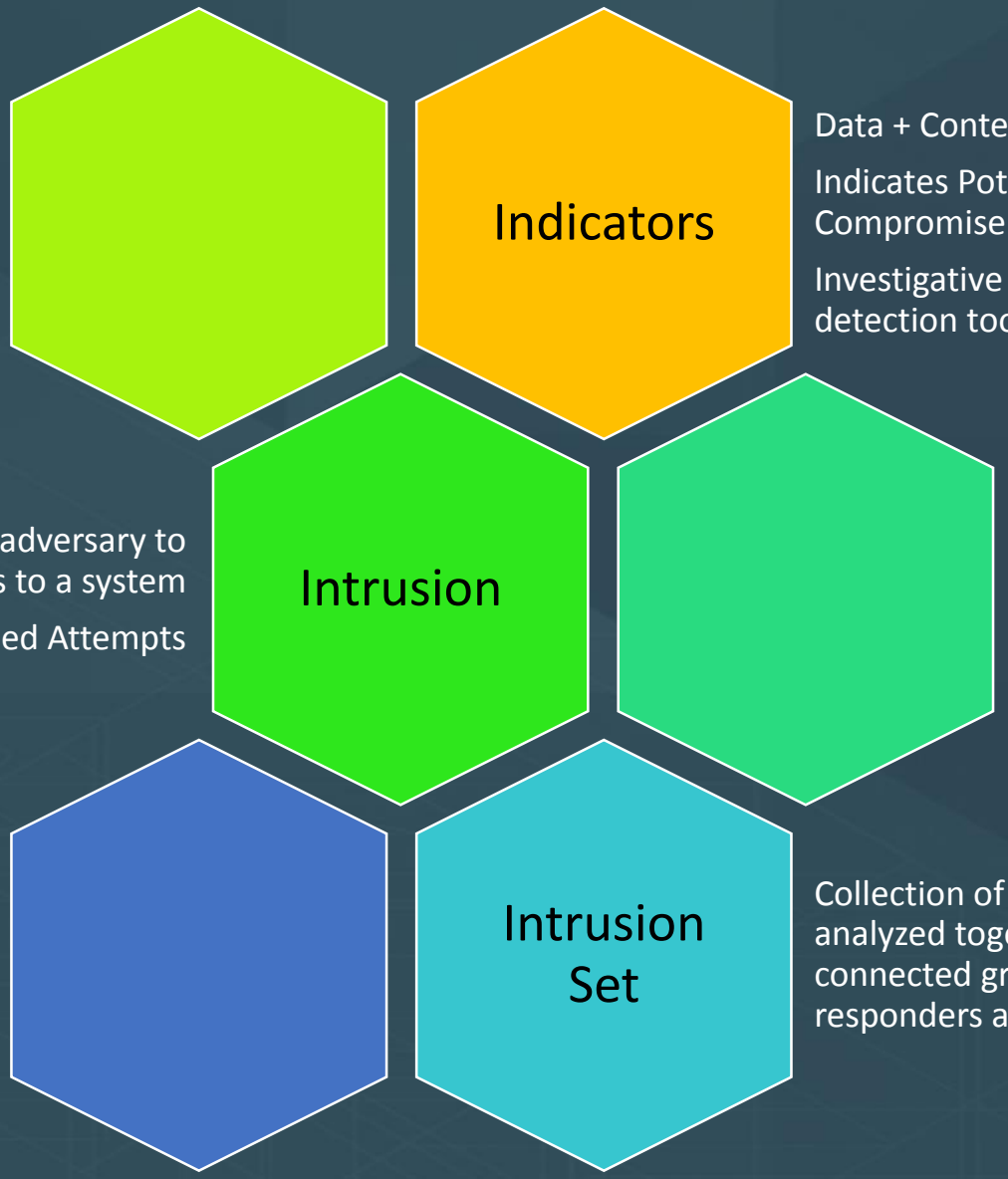
My Goals

- Analyze the GRIZZLY STEPPE report based on the stated intentions
- Frame the GRIZZLY STEPPE report in the context of the DNC hack
- Explore the impact to Burlington Electric and others
- Identify where the GRIZZLY STEPPE JAR could have been better
- Provide the audience with context and the tools/info to do research

Not My Goal:

- Convince anyone of any position

Terminology



Data + Context

Indicates Potential Compromise

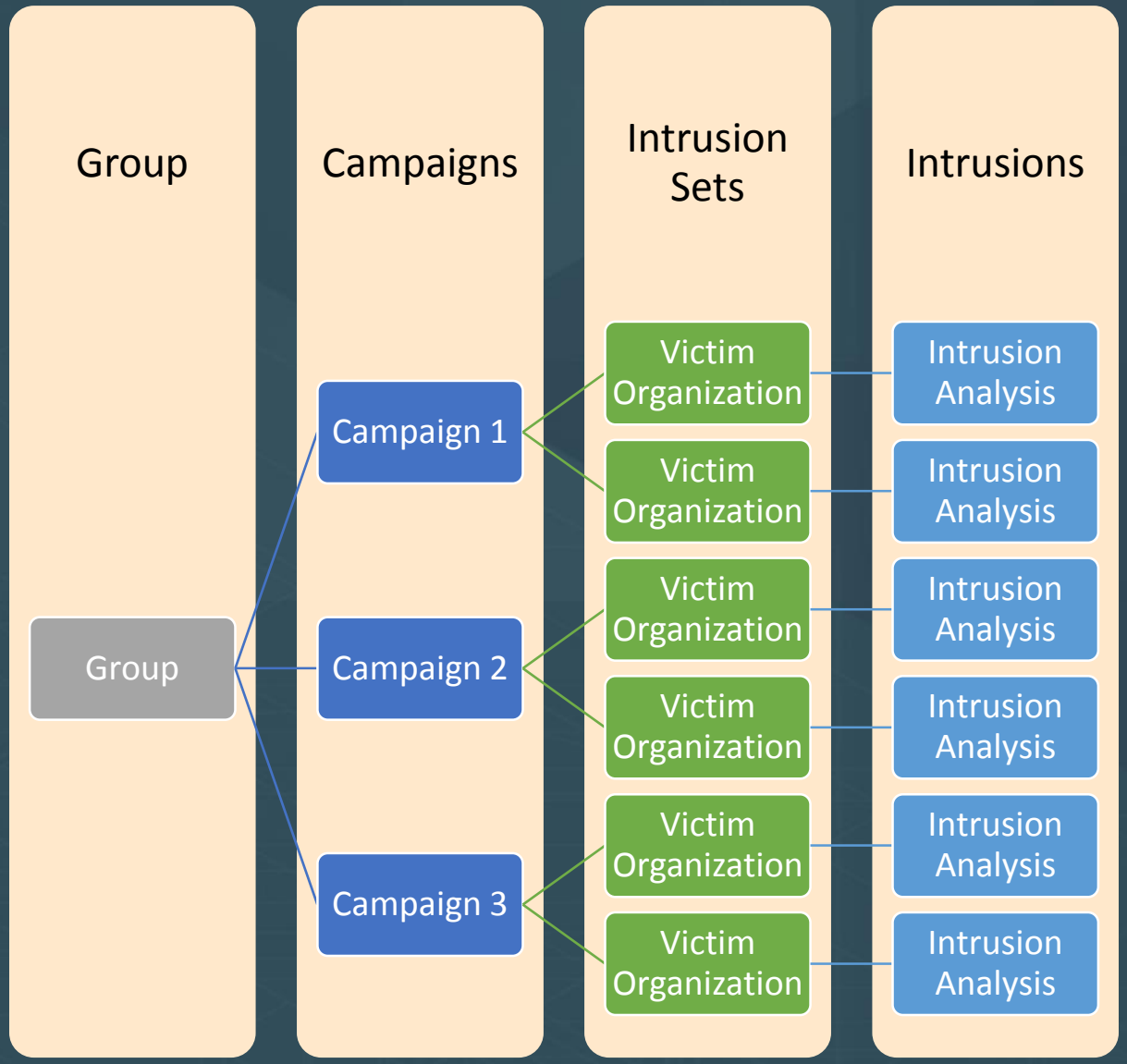
Investigative tool not detection tool

Attempts by an adversary to gain access to a system

Successful or Failed Attempts

Collection of intrusions analyzed together as a connected group to aid responders and defenders

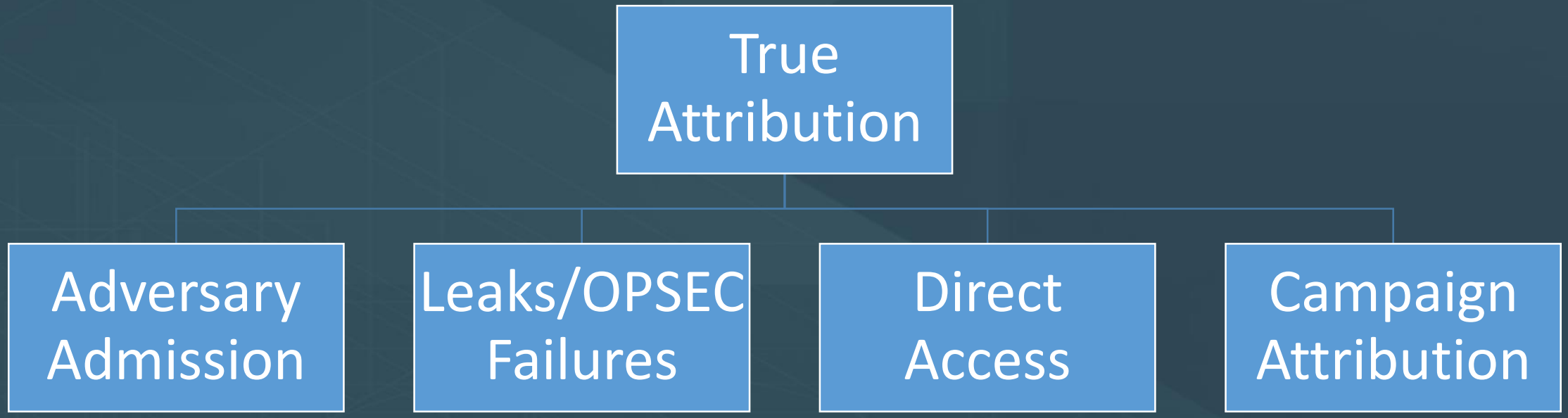
The Making of an Adversary Group



True Attribution vs. Campaign Attribution

- True Attribution can include:
  - Country Responsible (e.g. Russia)
  - Organizations Responsible (e.g. FSB)
  - People Responsible (e.g. Military and Intelligence members)
  - Supporting Organizations (e.g. training, exploit, and contractor companies)
- Campaign Attribution:
  - Analysis of intrusions to identify focus areas of adversaries and group them together
  - Much more useful than true attribution for network defense
  - Helps defenders identify, group, and investigate activity faster

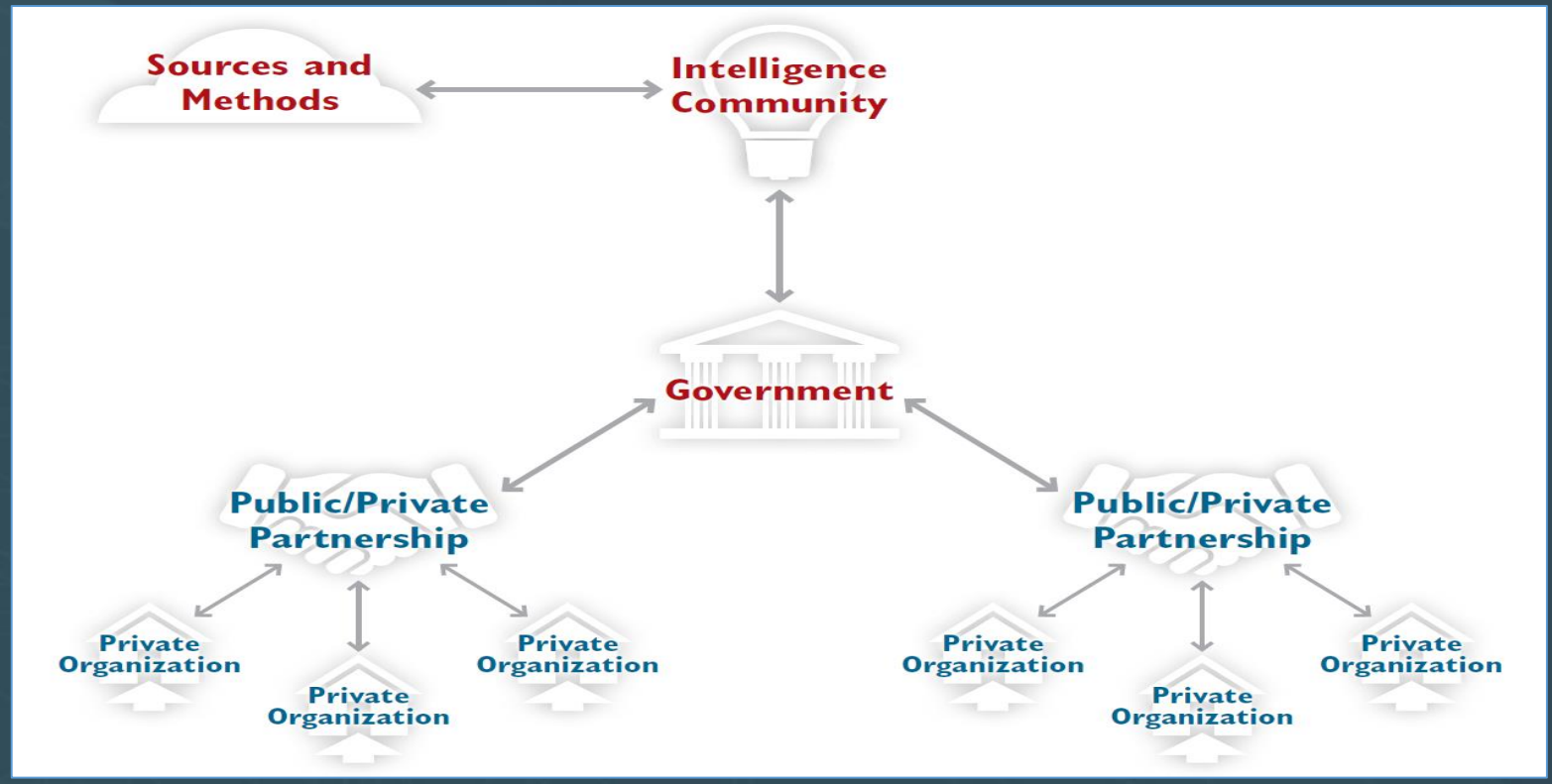
Roads to Attribution



Not All Data Types Are Created Equal

- How would you get true attribution?
  - Government hacks into foreign government computers or uses satellites, human assets, and other traditional intelligence capabilities
- What is best for network defense?
  - Private sector has better collection of intrusions, security operations, and incident response data required to properly analyze and defend against cyber threats

Private + Public Sector = Success



Common Misconceptions

- “Advanced threats wouldn’t use old malware or basic tactics”
- “Attribution isn’t doable”
- “If it looks like Russia it’s not Russia”
- “I could route my traffic through Russia and pretend to be them”
- “It’s all a false flag attack”
- “This indicator showed that it was Russia”
- There is a set of “evidence” to show in a simple way to prove attribution

An Abbreviated History of Russian Group Attribution

Moonlight Maze

- Reporting circa 1998
- Activity seen since 1996
- Source: U.S. Government (FBI)

The Dukes

- Reporting circa 2014
- Activity seen since 2008
- Source: F-Secure

Sofacy

- Reporting circa 2014
- Activity seen since 2008
- Source: Kaspersky Labs

APT28 and APT29

- Reporting circa 2014
- Activity seen since 2010
- Source: FireEye

COZYBEAR and FANCYBEAR

- Reporting circa 2014
- Activity seen since 2012
- Source: CrowdStrike

STRONTIUM

- Reporting circa 2015
- Activity seen since unknown
- Source: Microsoft

Bundestag Breach

- Reporting circa 2015
- Activity seen since 2014
- Source: German government

Raising Awareness About Russian Malicious Cyber Activity

The Department of Homeland Security and Federal Bureau of Investigation are releasing a Joint Analysis Report (JAR) that contains declassified technical information on Russian civilian and military intelligence services' malicious cyber activity, to better help network defenders in the United States and abroad identify, detect, and disrupt Russia's global campaign of malicious cyber activities.

- The JAR includes information on computers around the world that Russian intelligence services have co-opted without the knowledge of their owners in order to conduct their malicious activity in a way that makes it difficult to trace back to Russia. In some cases, the cybersecurity community was aware of this infrastructure, in other cases, this information is newly declassified by the U.S. government.
- The report also includes data that enables cybersecurity firms and other network defenders to identify certain malware that the Russian intelligence services use. Network defenders can use this information to identify and block Russian malware, forcing the Russian intelligence services to re-engineer their malware. This information is newly de-classified.
- Finally, the JAR includes information on how Russian intelligence services typically conduct their activities. This information can help network defenders better identify new tactics or techniques that a malicious actor might deploy or detect and disrupt an ongoing intrusion.

This information will allow network defenders to take specific steps that can often block new activity or disrupt on-going intrusions by Russian intelligence services. DHS and FBI are encouraging security companies and private sector owners and operators to use this JAR and look back within their network traffic for signs of malicious activity. DHS and FBI are also encouraging security companies and private sector owners and operators to leverage these indicators in proactive defense efforts to block malicious cyber activity before it occurs. DHS has already added these indicators to their Automated Indicator Sharing service.

White House Fact Sheet – Intention of JAR

- Sanctions and expulsion of diplomats was the first stage of responses
- Accompanied with the GRIZZLY STEPPE Joint Analysis Report (JAR)
  - The JAR was never intended to be proof of attribution
- The Four Goals of the JAR
  - Help network defenders but not provide technical evidence of attribution
  - Combine private sector & declassified govt data
  - Help defenders identify and block Russian malware w/ specifically declassified government data
  - Include new tradecraft and techniques used by the Russian intelligence services

Point 1: Help network defenders but not provide technical evidence of attribution

- 1 ½ page description focuses entirely on attribution
- Technical data provided is not descriptive of Russian activity
- A significant majority of the technical data is useless to defenders
- Of 800+ IPs roughly 300 were public infrastructure sites
- Lack of temporal info renders the data nearly useless

This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. The U.S. Government is referring to this malicious cyber activity by RIS as GRIZZLY STEPPE.

Previous JARs have not attributed malicious cyber activity to specific countries or threat actors. However, public attribution of these activities to RIS is supported by technical indicators from the U.S. Intelligence Community, DHS, FBI, the private sector, and other entities. This determination expands upon the Joint Statement released October 7, 2016, from the Department of Homeland Security and the Director of National Intelligence on Election Security.

Reported Russian Military and Civilian Intelligence Services (RIS)

Alternate Names
APT28
APT29
Agent.btz
BlackEnergy V3
BlackEnergy2 APT
CakeDuke
Carberp
CHOPSTICK
CloudDuke
CORESHELL
CosmicDuke
COZYBEAR
COZYCAR
COZYDUKE
CrouchingYeti
DIONIS
Dragonfly
Energetic Bear
EVILTOSS
Fancy Bear
GeminiDuke
GREY CLOUD
HammerDuke
HAMMERTOSS
Havex
MiniDionis
MiniDuke
OLDBAIT
OnionDuke
Operation Pawn Storm
PinchDuke
Powershell backdoor
Quedagh
Sandworm
SEADADDY
Seaduke
SEDKIT
SEDNIT
Skipper
Sofacy
SOURFACE
SYNful Knock
Tiny Baron
Tsar Team
twain_64.dll (64-bit X-Agent implant)
VmUpgradeHelper.exe (X-Tunnel implant)
Waterbug
X-Agent

The Technical Data

	A	B	C	D	E	F	G	H
1	INDICATOR_VALUE	TYPE	COMMEN	ROLE	ATTACK_P	OBSERVEC	HANDLING	DESCRIPTION
2	efax[.]pfdregistry[.]net/eFax/37486[.]ZIP	URL		URL WATCHLIST			TLP:WHITE	It is recommended that network administrators review traffic to/from the URL address to determine possible malicious activity.
3	private[.]directinvesting[.]com	FQDN		C2	C2		TLP:WHITE	The Remote Access Tool malware "8F154D23AC2071D7F179959AABA37AD5" attempts to use this C2.
4	www[.]cderlearn[.]com	FQDN		C2	C2		TLP:WHITE	The Remote Access Tool malware "AE7E3E531494B201FBF6021066DDD188" attempts to use this C2.
5	ritsoperrol[.]ru	FQDN					TLP:WHITE	It is recommended that network administrators review traffic to/from the domain to determine possible malicious activity.
6	littjohnwilhap[.]ru	FQDN					TLP:WHITE	It is recommended that network administrators review traffic to/from the domain to determine possible malicious activity.
7	wilcarobbe[.]com	FQDN					TLP:WHITE	It is recommended that network administrators review traffic to/from the domain to determine possible malicious activity.
8	one2shoppee[.]com	FQDN					TLP:WHITE	It is recommended that network administrators review traffic to/from the domain to determine possible malicious activity.
9	insta[.]reduct[.]ru	FQDN					TLP:WHITE	It is recommended that network administrators review traffic to/from the domain to determine possible malicious activity.
10	editprod[.]waterfilter[.]in[.]ua	FQDN					TLP:WHITE	It is recommended that network administrators review traffic to/from the domain to determine possible malicious activity.
11	mymodule[.]waterfilter[.]in[.]ua	FQDN					TLP:WHITE	It is recommended that network administrators review traffic to/from the domain to determine possible malicious activity.
12	efax[.]pfdregistry[.]net	FQDN					TLP:WHITE	It is recommended that network administrators review traffic to/from the IP address to determine possible malicious activity.
13	167[.]114[.]35[.]70	IPV4ADDR		IP_WATCH	C2		TLP:WHITE	This IP address is located in Canada.
14	185[.]12[.]46[.]178	IPV4ADDR		IP_WATCH	C2		TLP:WHITE	This IP address is located in Swaziland.

```
MacBook-Pro-6:~ jake$ nslookup watson.telemetry.microsoft.com
Server:         75.75.75.75
Address:        75.75.75.75#53

Non-authoritative answer:
watson.telemetry.microsoft.com  canonical name = modern.watson.data.microsoft.com.akadns.net.
Name:   modern.watson.data.microsoft.com.akadns.net
Address: 65.55.252.43
```

Jake Williams @MalwareJake · Jan 3

Before you act on JAR indicators, one of the IP's is 65.55.252.43. Bad #CTI is worse than none at all. Dr. Watson is a Russian operative.

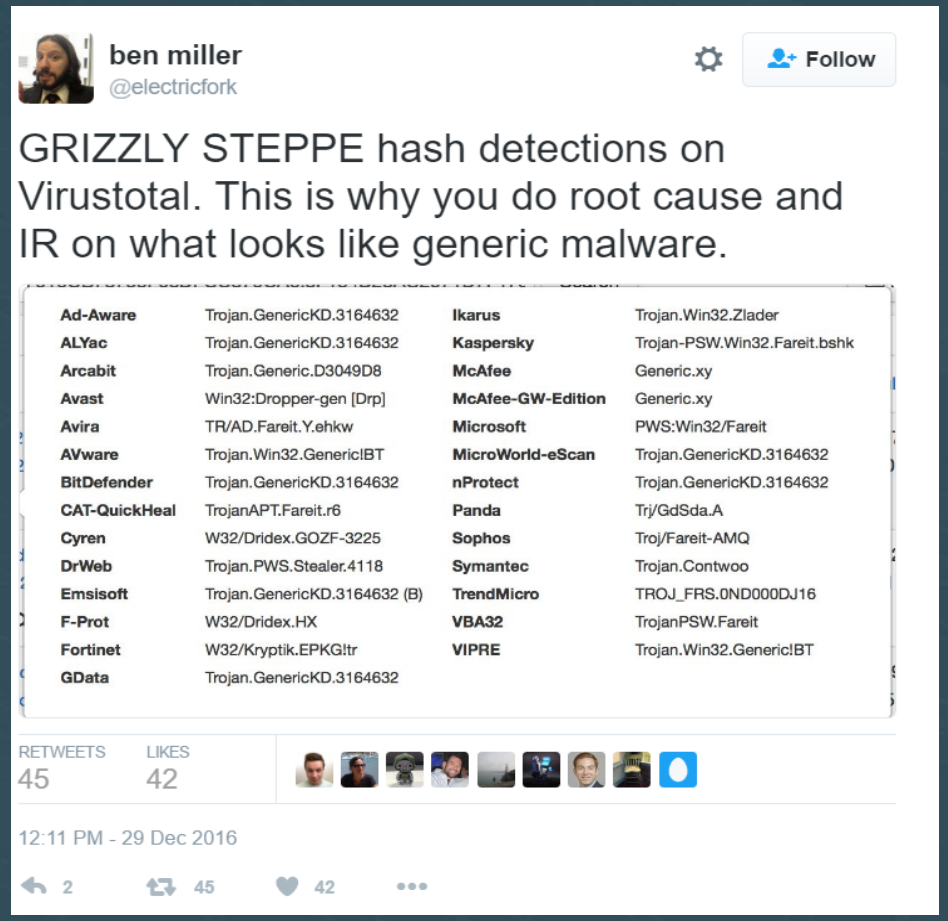
15 140 119 •••

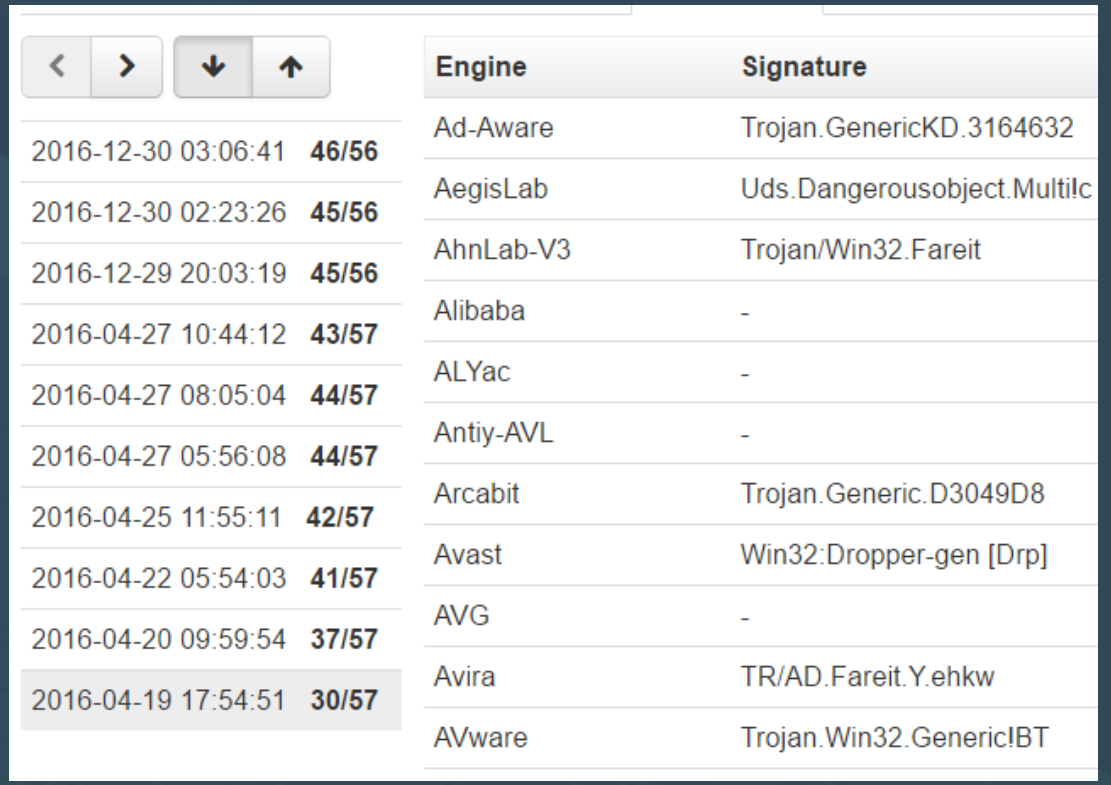
Point 2: Combine private sector & declassified govt data

- There were no indications of previously classified government data
- The data was not sourced (what was government vs. private sector)
- Cannot properly evaluate this point
  - If any of this data was previously classified it was likely over classified and already public

Point 3: Help defenders identify and block Russian malware w/ specifically declassified government data

- Again no context to the malware was given
- Generic malware can be interesting but needs tied to campaigns which it was not
  - Further problematic since Russian intelligence was mixed with unrelated criminal elements
- This was not classified data or it was over classified



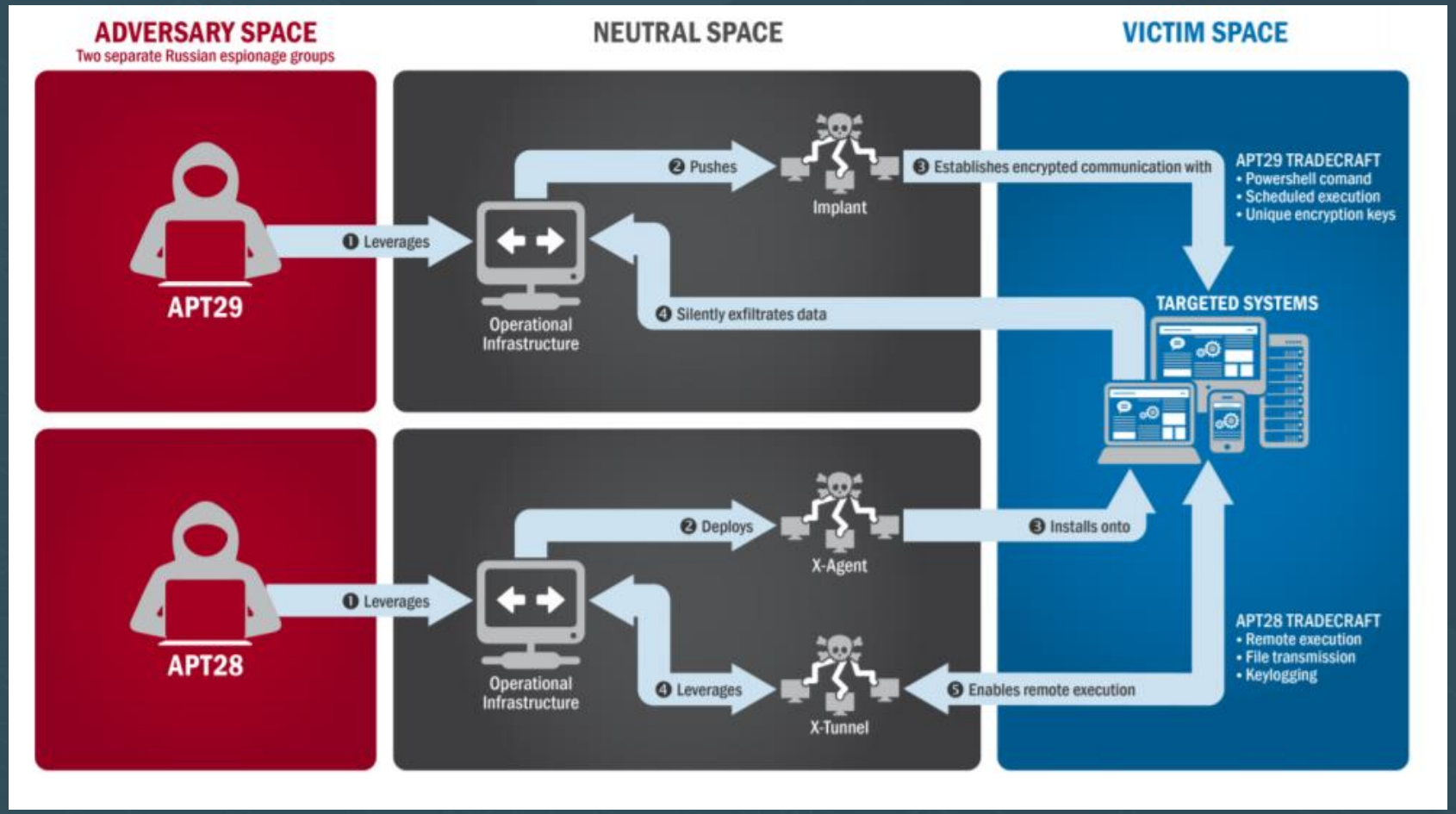


2016-12-30 03:06:41	**46/56**
2016-12-30 02:23:26	**45/56**
2016-12-29 20:03:19	**45/56**
2016-04-27 10:44:12	**43/57**
2016-04-27 08:05:04	**44/57**
2016-04-27 05:56:08	**44/57**
2016-04-25 11:55:11	**42/57**
2016-04-22 05:54:03	**41/57**
2016-04-20 09:59:54	**37/57**
2016-04-19 17:54:51	**30/57**

Engine	Signature
Ad-Aware	Trojan.GenericKD.3164632
AegisLab	Uds.Dangerousobject.Multi!c
AhnLab-V3	Trojan/Win32.Fareit
Alibaba	-
ALYac	-
Antiy-AVL	-
Arcabit	Trojan.Generic.D3049D8
Avast	Win32:Dropper-gen [Drp]
AVG	-
Avira	TR/AD.Fareit.Y.ehkw
AVware	Trojan.Win32.Generic!BT

Point 4: Include new tradecraft and techniques used by the Russian intelligence services

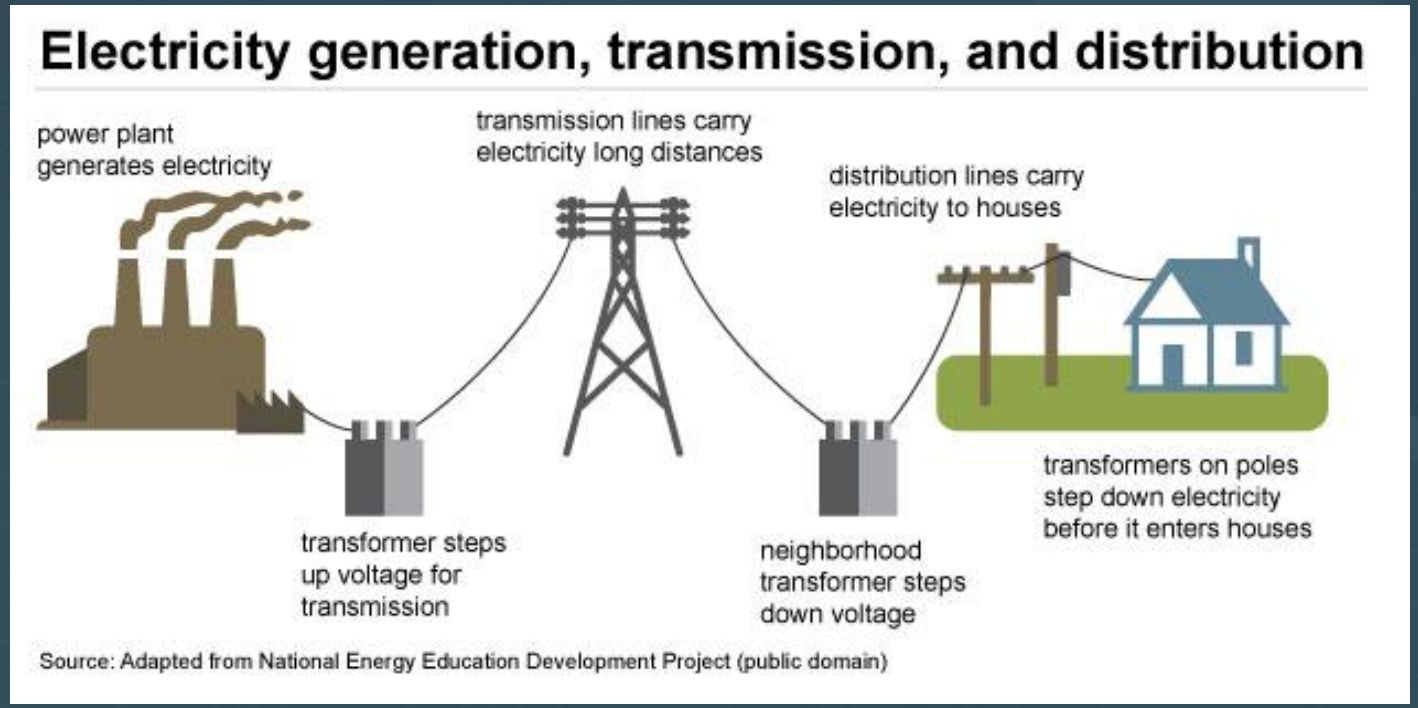
- Tradecraft and techniques were already known to the public
- None of the tradecraft or techniques were specific to Russian groups
- Tradecraft and techniques are difficult to obtain by the victim and hard to change for the adversary; they are ideal above indicators

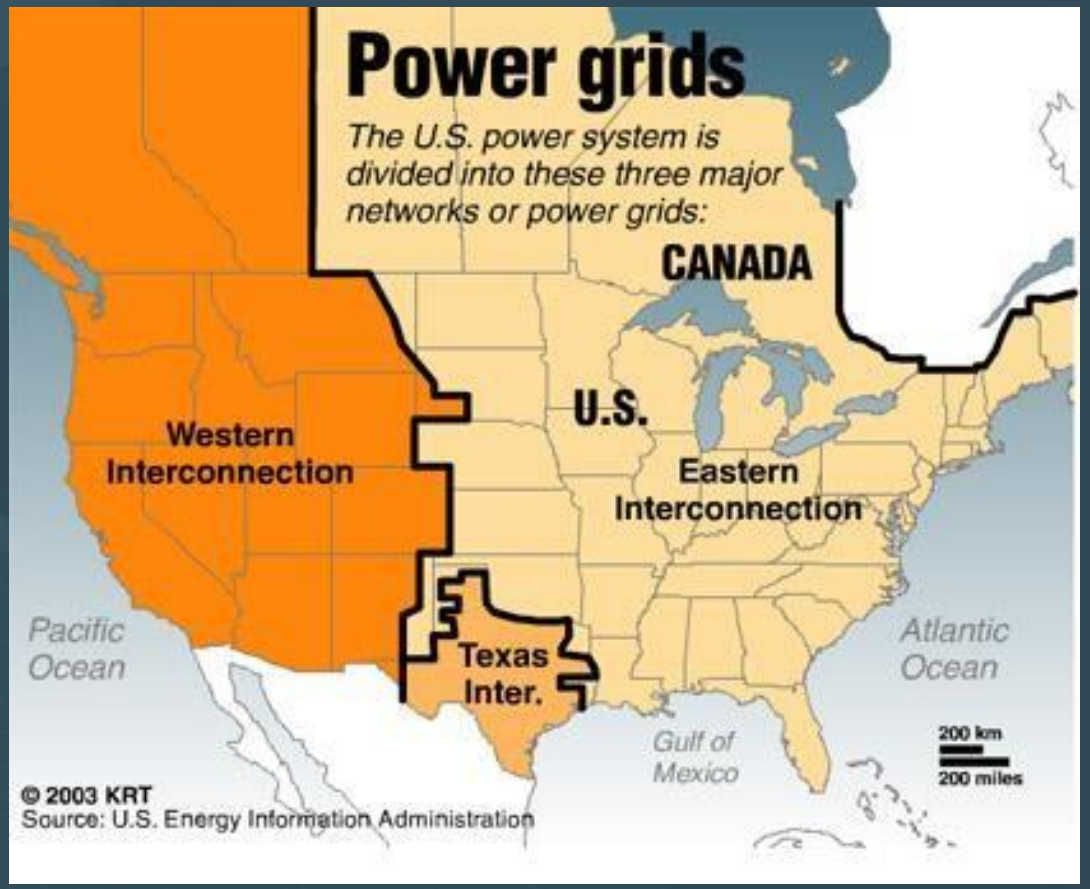


Opportunities for Improvement:

- Ensure the written report meets the guidance and expectations laid out
- When providing indicators such as IP addresses include at a minimum:
  - IP Address
  - Time Observed (First and Last observed if possible)
  - Activity Observed (e.g. delivered malware, command and control for malware, etc.)
  - Information Known (e.g. registrant information)
  - Source (e.g. observed directly or a specific 3rd party)
- Ensure audience knows how to use the information
  - Indicators are investigation tools not detection mechanisms
  - Indicators are not tools for attribution
- Source information provided including tradecraft
- Do not use reports as an effort to overly advertise your pet projects

Power Grids 101





Burlington Electric – In the News

National Security

Russian hackers penetrated U.S. electricity grid through a utility in Vermont, U.S. officials say

The headquarters of FSB, grey building at center, in downtown Moscow, Russia on Friday, Dec. 30, 2016. FSB is a Russian spy agency named by the administration as being behind the Grizzly Steppe operation. (Alexander Zemlianichenko/AP)

By Juliet Eilperin and Adam Entous December 30 at 7:55 PM

Most Read

1 Russian hackers penetrated U.S. electricity grid through a utility in Vermont

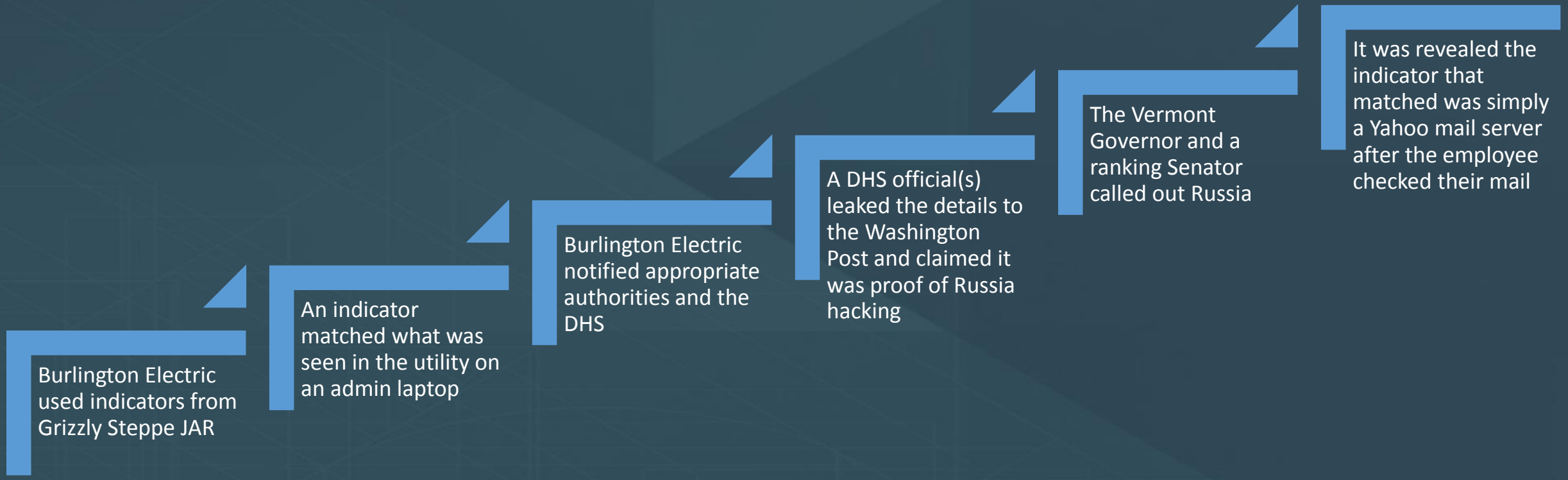
National Security

Russian operation hacked a Vermont utility, showing risk to U.S. electrical grid security, officials say

National Security

Russian government hackers do not appear to have targeted Vermont utility, say people close to investigation

Burlington Electric – What Happened



Report Impacts

Summarized FAQ

- Can true attribution be done?
  - Yes, it's time consuming and costly though w/ little to no impact on network defense
- Did a Russian government hack the DNC?
  - Yes, the COZYBEAR and FANCYBEAR groups have been tracked for years prior to the DNC hack by man leading security firms. The DNC is just another example of their activity
- Did the Russian government hack the vote/influence the election?
  - No and/or uncertain. No evidence has been presented technically to say the vote was manipulated. The influence of the election is a discussion for policy not cyber threat intel
- Was the DHS/FBI GRIZZLY STEPPE report meant to be proof of Russian hacking?
  - No, it was confusing based off their narrative but it was never intended to be about attribution. It was a document to help network defenders.
- Did the GRIZZLY STEPPE report help network defenders?
  - No, it failed to achieve the goals it laid out for itself and defenders who used the data from the report are more likely to do their organizations harm in terms of resource cost
- Is the DHS/FBI incompetent?
  - No, the report was just not a good representation of the good work being done

Things to Come – The Intelligence Community's Report

Russian Motivations

- Clapper has stated there are multiple motivations
- Intercepted communications were used to assess this

Sources and Methods

- Rarely given but Clapper indicated he will "push the envelope"
- Congressmen and Senators have expressed concern in revealing too much

Proof

- Not sure what would help
- Technical proof is already available

DNC Data

- Misconceptions about the FBI's investigation of this
- No one involved in the investigation is speaking on this matter

My Expectations

- Timeline of events clearly intermingling Intelligence Community intercepts with public technical evidence

Parting Thoughts: Things that are Troubling to Me

- The perception and suggestion that the Intelligence Community is skewed towards a specific political party or are subject to politics in their analysis
  - Wholly damaging to move from “healthy skepticism” to disparagement or distrust
- The politicizing of intelligence through out of context quotes by media
- Technical experts commenting on cases that they have zero experience
- Technical experts not involved in a specific case speaking out of turn
- The expectation of sending out data more timely instead of more accurately
- That people will see a single report as representative of the larger effort

Suggested Reading

- MOONLIGHT MAZE
  - https://sipa.columbia.edu/system/files/Cyber_Workshop_Attributing%20cyber%20attacks.pdf
  - https://medium.com/@chris_doman/the-first-sophistiated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7#.yz6u097v1
- Pawn Storm
  - http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf
- APT28
  - https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf
- DNC Coverage by Thomas Rid
  - http://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/
- The Dukes
  - https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf
- FANCYBEAR
  - https://www.crowdstrike.com/resources/crowdcasts/bear-hunting-history-and-attribution-of-russian-intelligence-operations/

Thanks for Coming

Stay in Touch:
www.RobertMLee.org
@RobertMLee

SANS DFIR Webcast Series

DIGITAL FORENSICS & INCIDENT RESPONSE

THANK YOU FOR ATTENDING

Analyzing the DHS/FBI's GRIZZLY STEPPE Report

Robert M. Lee @RobertMLee