CSLAC Random Access

A Brief Update

October 2021

Big Data Threat– Russian Federation Campaign SolarWinds

The Most Critical Cybersecurity Threat Ever Experienced

grcotter@comcast.net

Not a New Random Access Cybersecurity Talk…….

CSLAC 2018 - The Rest of the Dragonfly Story

CSLAC 2019 - Vulnerabilities vs. Threats – 2016 Election

CSLAC 2020 – "Hidden" Cybersecurity Vulnerabilities

Background

Simultaneous Russian Federation Supply Chain Attacks

- Major Network Vendor SolarWinds Network System
- Major Cloud Infrastructure Vendors-Microsoft, IBM, Amazon
- Multiple Security Vendors Supporting Cloud-based Industry

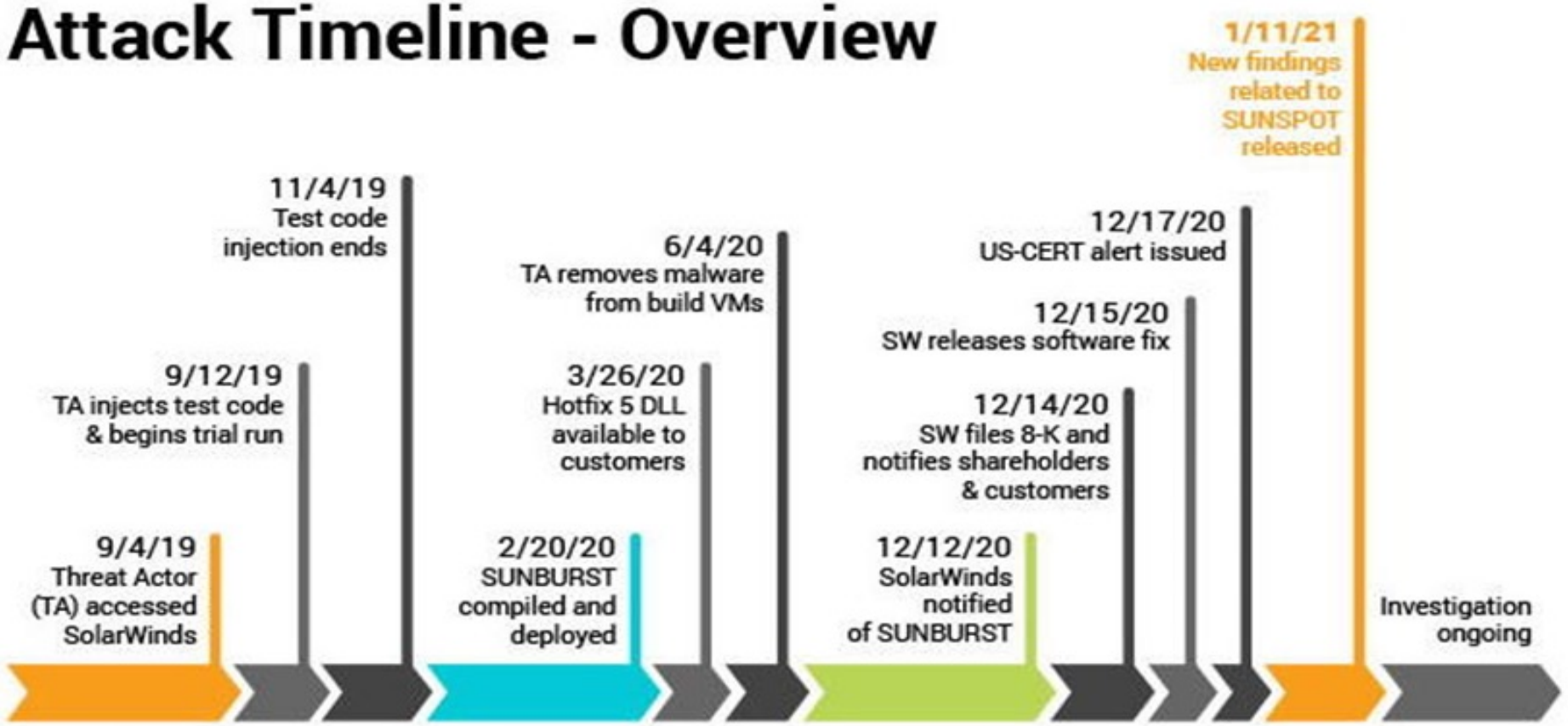
Revealed by FireEye Dec 13th, 2020, Backdated to Early 2019

Attribution: SVU APT29 (more likely FSB/SVU, Aligns With Federation DOE)

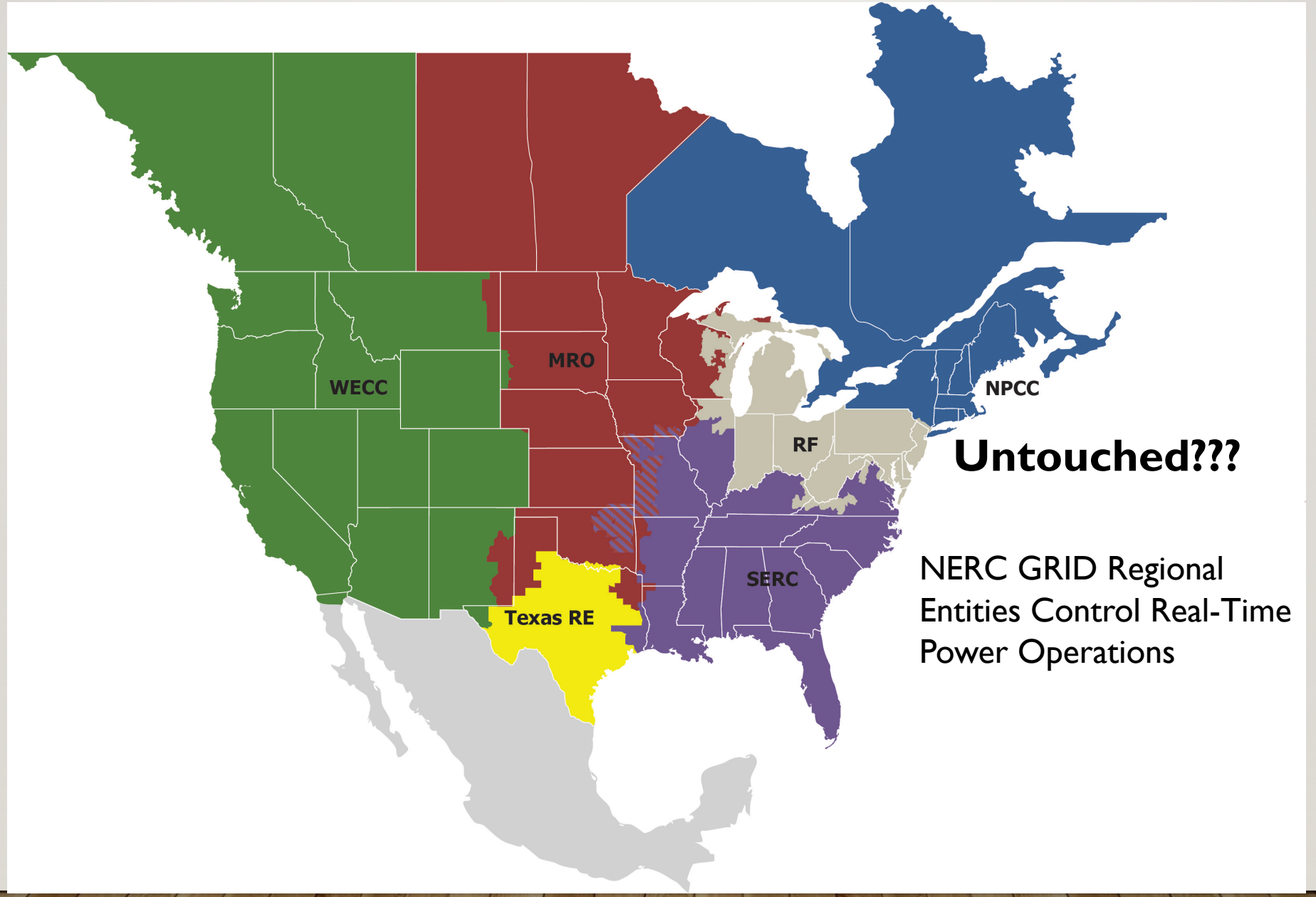
Victims: Highly Selective, Government, Grid Regulators, Major IT Services, Security Vendors, Other Intelligence and Critical Infrastructure Targets

My View: Persistent Differentiating between Espionage and More Malicious Objecives is a Serious Mistake but Endemic in IT and Security Industry (and the Energy Industry).

Attack Timeline - Overview



All events, dates & times approximate and subject to change pending completed investigation



Untouched???

NERC GRID Regional Entities Control Real-Time Power Operations

Synchrophasor Sites In The North American Electric Grid

Russia FSB & MOD GRU

Industroyer ICS Malware

IEC61850-based attack can disable targeted ICS cyber assets at Transmission and Distribution Synchrophasor (PMU) equipped sites

U.S. /RUSSIA CYBER STATUS POST BIDEN-PUTIN SUMMIT

- Issue: Biden Ultimatum on Critical Infrastructures, incl. Election, Pipelines
- Russian Active Measures Abated; e.g., JBS Hackers Disbanded. Active Grid Measures Also?
- U.S. Sanctions Levied but NSA/CyberCommand Threats Quieted
- WH Cybersecurity Policy Actions Have Slowed, Follow ups to EO's
- Importantly, Further SolarWinds Policy Responses Now Appear Uncertain
- My Question – Does this Suggest Understanding That Direct Attacks on Critical Infrastructures are "Off-Limits"?

SOLARWINDS "WOKE" THREAT ASSESSMENT SUMMARY

Unprecedented Attack – Analogies to 9/11, a Cyber Pearl Harbor, Impact Highest in Cyber History

Complexity -- Years in the Making, Most Sophisticated, 1000+ Developers, Massively Breeched Security Industry, Stealth a Primary Factor, Broadly-based but Highly Selective,

OPSec -- Some of the Best (FireEye), Beyond "Defense" as Practiced e.g., Diagnostics, Disguising Infections and Avoiding Detection; Six Specific Security Firms of Concern

Objectives – Full Spectrum (Reece thru Destruction), Persistence and Longevity, High Value Targets Particularly (in Cloud Environments) ….and…."to demonstrate it could be done with minimum retaliation."

Victims – 18,000 Initially Infected, Over 300 Reported Secondary Attacks, Each Custom Tailored, Hand Executed; 4720 Intrusions Reported by Swiss Firm, Prodaft.

Caution: US Fragmentation, Objectivity, and Absence of Any Deep, Thorough Analysis Creates Much Uncertainty in Predicting Where Federation Will Take This Strategy

MY RECOMMENDATIONS

- Take Federation Campaign Very Seriously, Keep up with all Advisories; NSA/CyberCommand, CISA, FBI, IC, Mitre, Industry, etc.
- Unless Immune to Effects, Get Assured, Affordable, Professional Cybersecuriity Help
- Please Note: Security Firms Reported Product Penetrations: Fidelis, FireEye, Microsoft, Minecast, Palo Alto Networks, Qualys,
- Seriously Embrace Concept of ***Zero Trust*** for Your Environment, e.g., **Cloud Zero Trust**. Treat it as a Journey, not a Destination