Cisco Talos and CNI
Lessons learned from Ukraine

Vanja Svajcer, Technical Leader, Cisco Talos

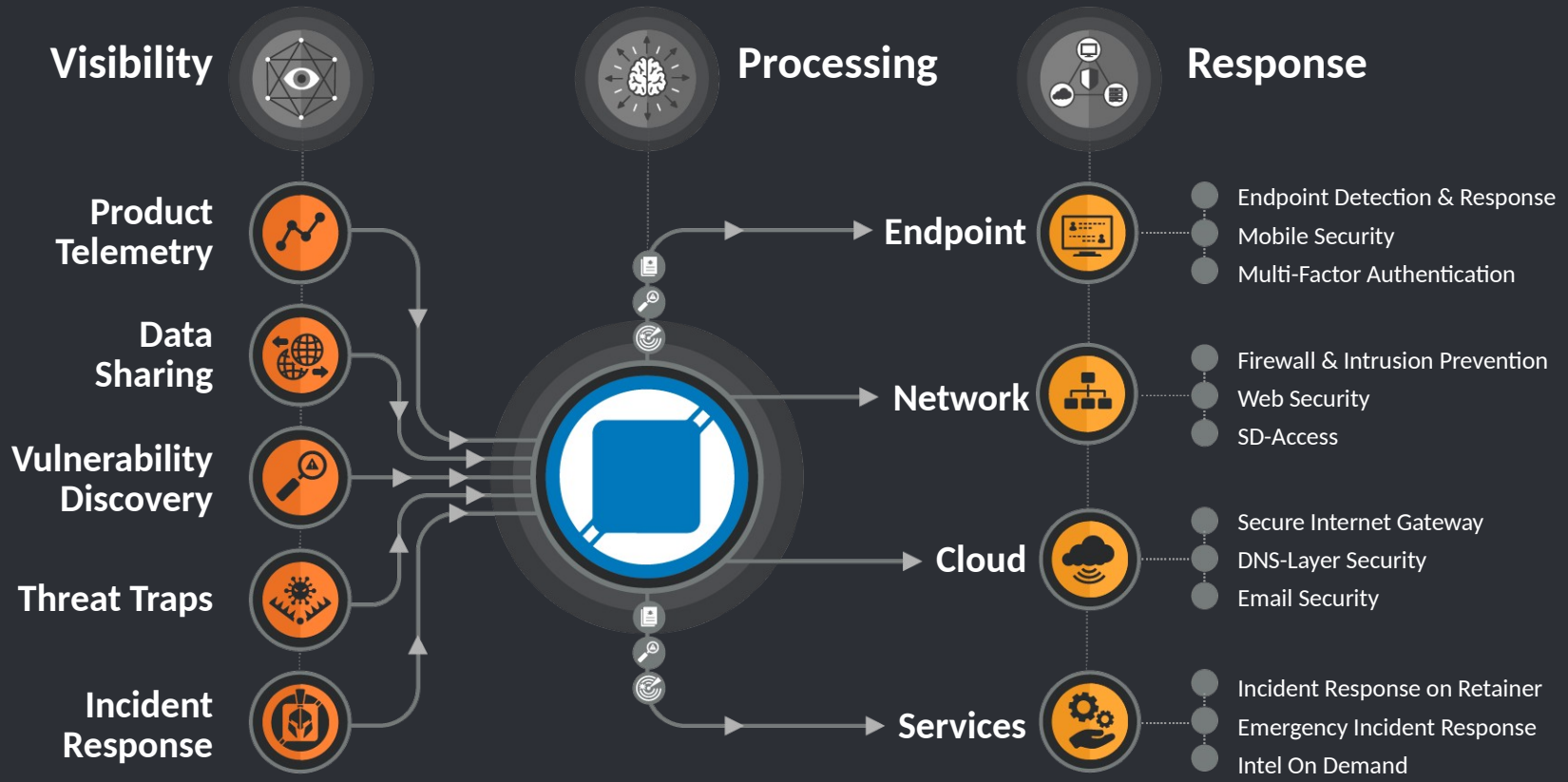
NOG.hr conference, April 2024

Talos
Cisco Security Research

Sadržaj

CISCO TALOS

From unknown to understood



Talos
Cisco Security Research

Cisco Talos & Ukraine

Previous assistance

- Six years in region
- On the ground during NotPetya
- Assisted with forensic analysis multiple events
- Assisted in monitoring of election infrastructure during 2019 presidential election

Partnerships

- State Special Communications Service of Ukraine (SSSCIP)
- Cyberpolice Department of the National Police of Ukraine
- National Coordination Center for Cybersecurity (NCCC at the NSDC of Ukraine)

Current assistance

- Providing defensive guidance
- Assisting with forensic analysis
- Providing intelligence
- Assisting in hunting activities

TALOS
Cisco Security Research

APTs: Russia Summary

Threats from Russian state-sponsored or state-aligned advanced persistent threats (APTs) remain a mainstay in our threat tracking and research efforts this year.

Gamaredon

Broadly suspected to be a team of Russian government-supported actors based in Crimea, the group in recent months has concentrated their efforts on cyberespionage against Ukrainian entities.

Turla

Conducts long-term espionage and data exfiltration operations that are in line with Russian intelligence priorities that the U.S. government attributes to a unit within the FSB.

Turla's Snake

For nearly 20 years, APT Turla deployed Snake to steal and exfiltrate data from targeted systems through numerous relay nodes scattered around the world.

Internal Task Unit

We've continued monitoring suspicious activity in endpoint telemetry for nearly three dozen Ukrainian partners across critical infrastructure sectors, including government, utilities, financial services, health care, and transportation.

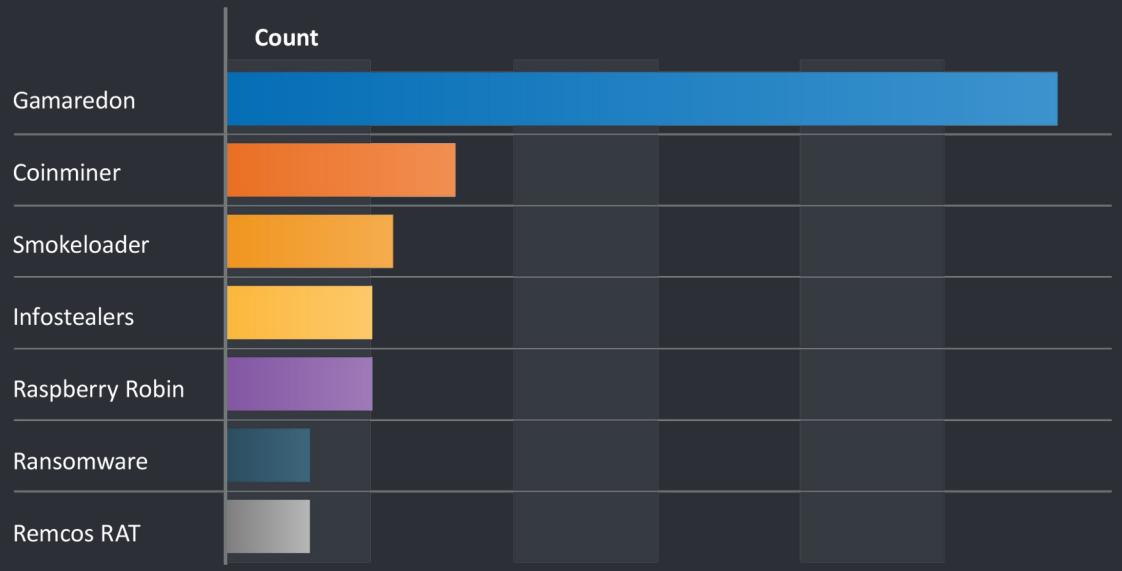
Russia-Ukraine war

The task unit has continuously responded to a myriad of cyber threats since the onset of the Russia-Ukraine war, the observed activity in 2023 was far less sophisticated than what is typically associated with the sophisticated adversaries.

SmokeLoader Malware

We observed a spike in SmokeLoader activity in late April and early May, aligning with CERT-UA's reporting of mass distribution of SmokeLoader targeting Ukrainian entities.

Top threats in Ukraine task force investigations



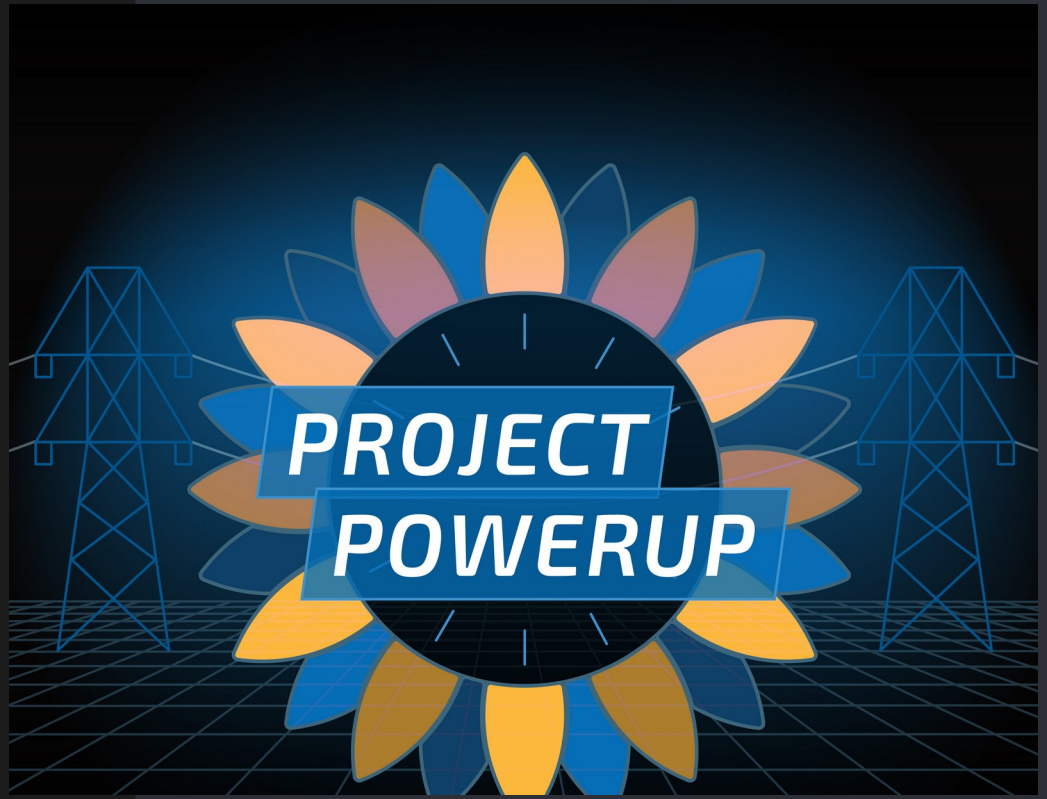
- Gamaredon is the most dominant threat to Ukraine that our task force responded to
- The group has historically targeted predominantly Ukrainian entities — particularly those responsible for the country's defense, diplomacy and internal security

2023 Top Insights
Source: Ukraine Task Unit

Cisco Security Research

Project Power Up

Helping to keep the lights on in Ukraine in the face of electronic warfare



Talos
Cisco Security Research

Nothing in the world compares to Ukraine’s CI issues

- 25,000 km of high KV lines
- 120+ HV substations
- 40 super critical transmission substations
- 6 have been destroyed
- Triple threat:
    - Cyber attacks
    - Kinetic strikes
    - Electronic warfare
- Let’s talk about electronic warfare…..

Cisco Security Research

The Ukrainian EW reality

- Electronic Warfare is disrupting transmission grid operation
- GNSS time (GPS) is vital to power grid operations
- **GPS is *super easy* to jam!**
- The Ukrainians are struggling to deal with grid time sync which GPS enables
- Already had one significant black out due to GNSS visibility

Wait, why even jam GPS to begin with?

- **It is a tactical and strategic imperative to have access to GPS**
- Modern warfare relies *heavily* on GPS.
    - Drones
    - Guided munitions
    - Combat coordination
    - Did I mention drones?

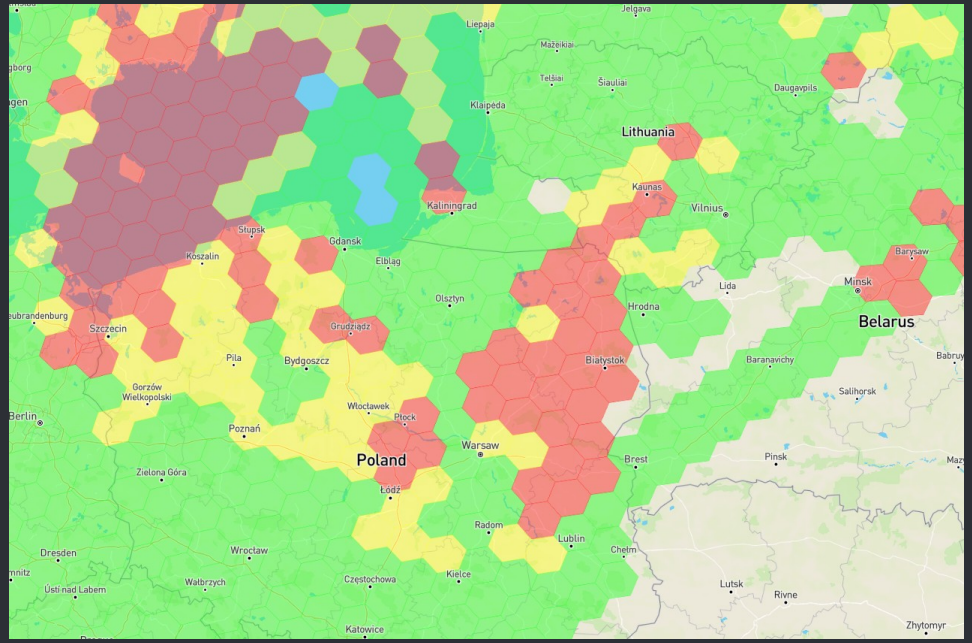
Wait, GPS is easy to jam?!

"There is only one man would give me the raspberry!"

- GPS L1 (1575.42 mhz) transmits at 27W (14.3 dBW)
- 31 SV fly at a medium earth orbit of 12,550 miles
- Given distance and normal interference, the GPS signal you receive is (hopefully) around -130/-160 dBW.
- Imagine the power of a 50 Watt bulb at 10,000+ miles away a GPS receiver
- Tl;dr – this is a super weak signal, easy to knock over

EW isn’t limited to just combat zones

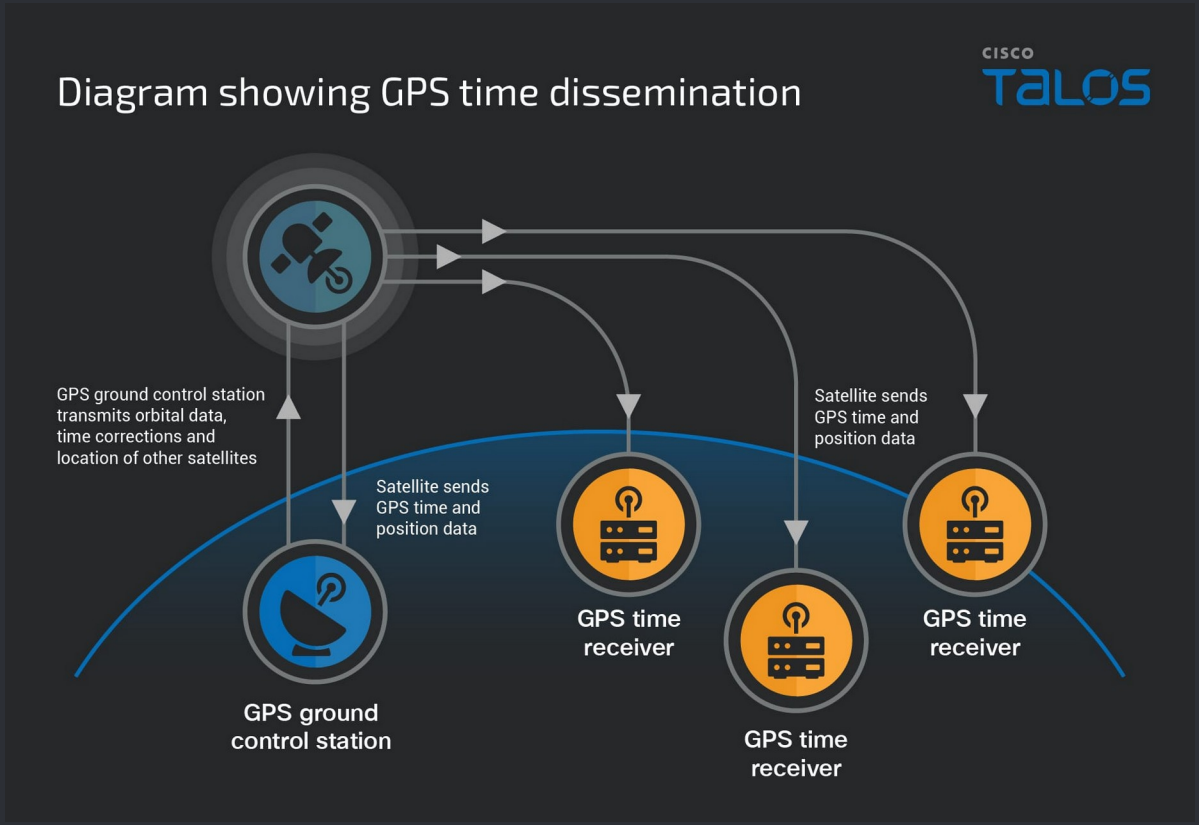
- GNSS disruption doesn’t know international borders
- This is a method of foreign power projection
- Civilian infrastructure pays the price
- Denial of PNT costs lives
- Let’s talk about the civilian impacts



Cisco Security Research

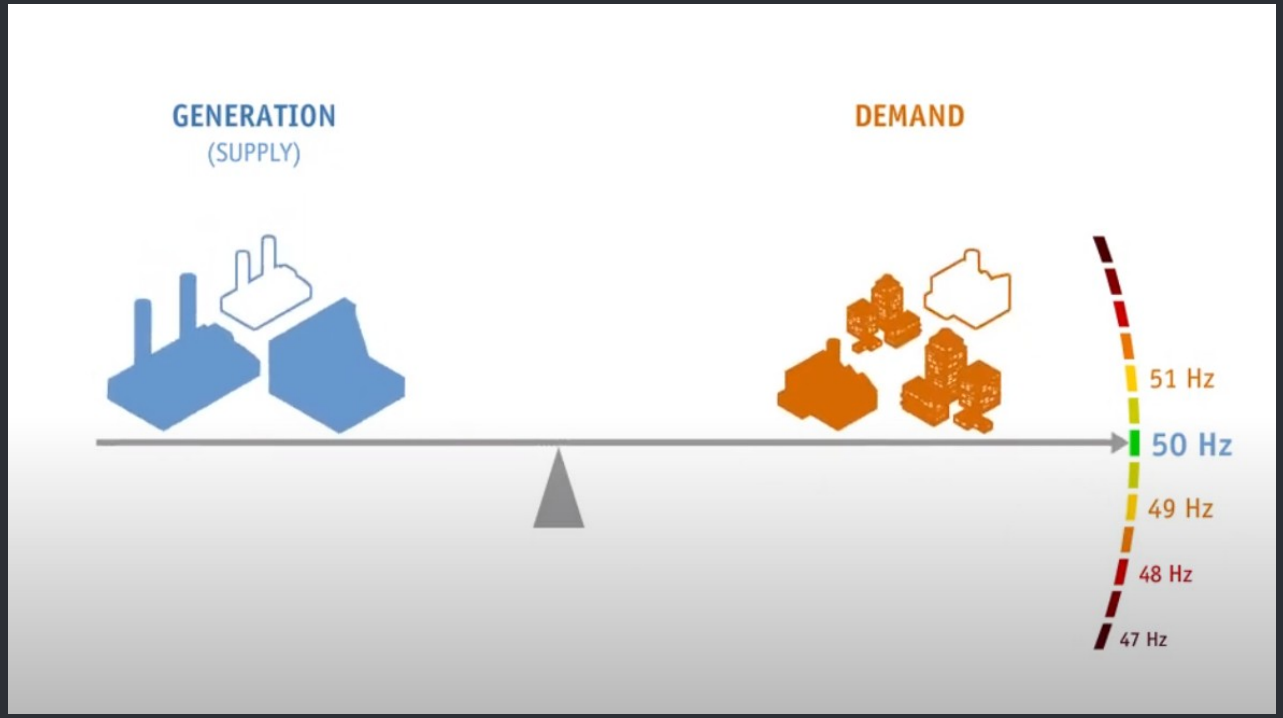
Why is GPS time so valuable?

PNT dissemination



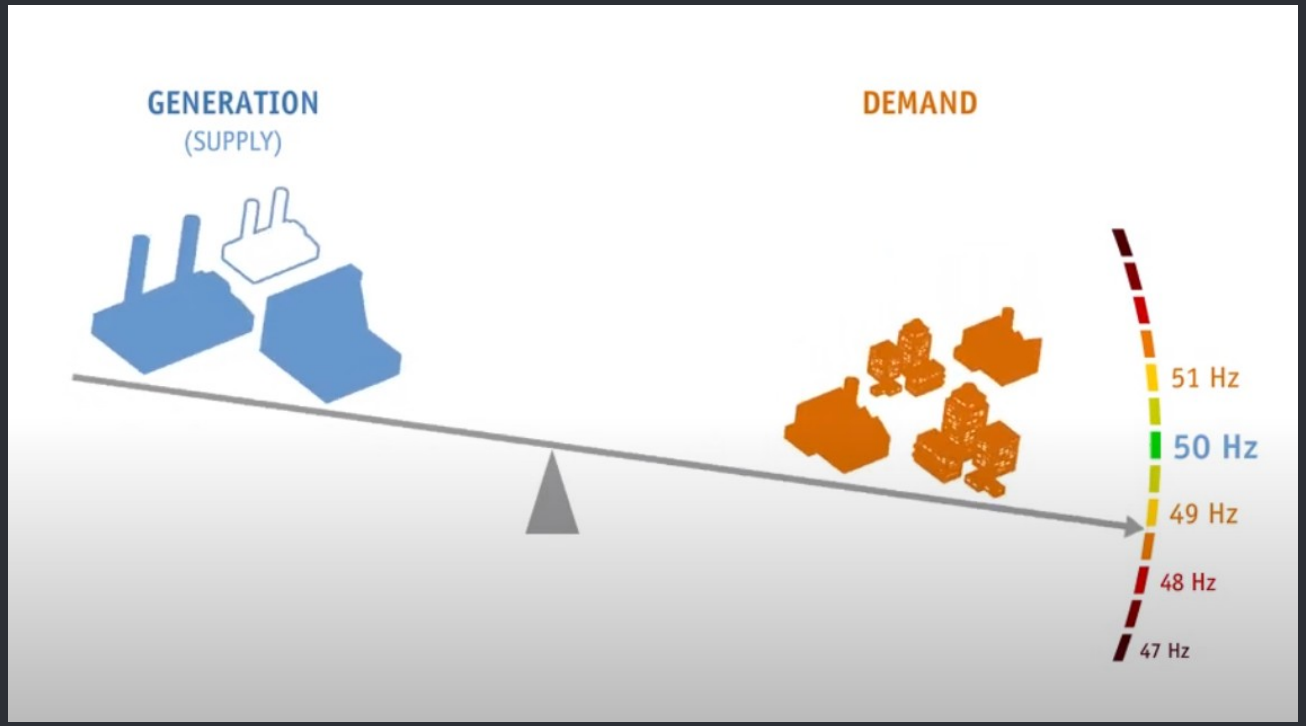
Why does it even matter?

The grid must always stay in balance



Bad things happen when it unbalances!

And we must measure it very quickly all the time in multiple places to know!



Cisco Security Research

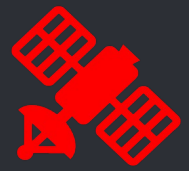
No PMU data? Things can start to get out control!

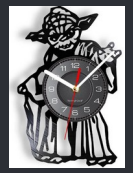
- **This is difficult enough to do normally, much less during a war**
- The spinning plates start to fall, we lose balance
- “We’ve lost telemetry to a PMU. Weather? Equipment failure? Destroyed?”

GPS Time in Ukraine (pre-Cisco)

How it’s supposed to work in Ukraine

Normal GPS to PMU clock sync behavior





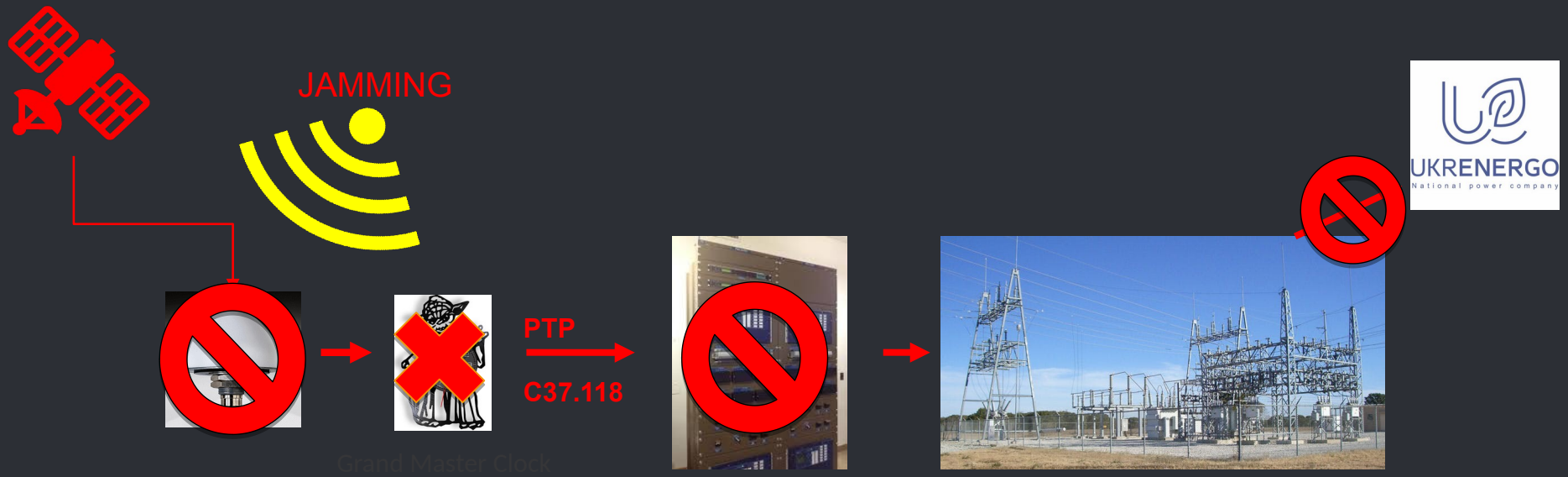
Grand Master Clock

PTP

C37.118

UKRENERGO
National power company

Enter the jamming



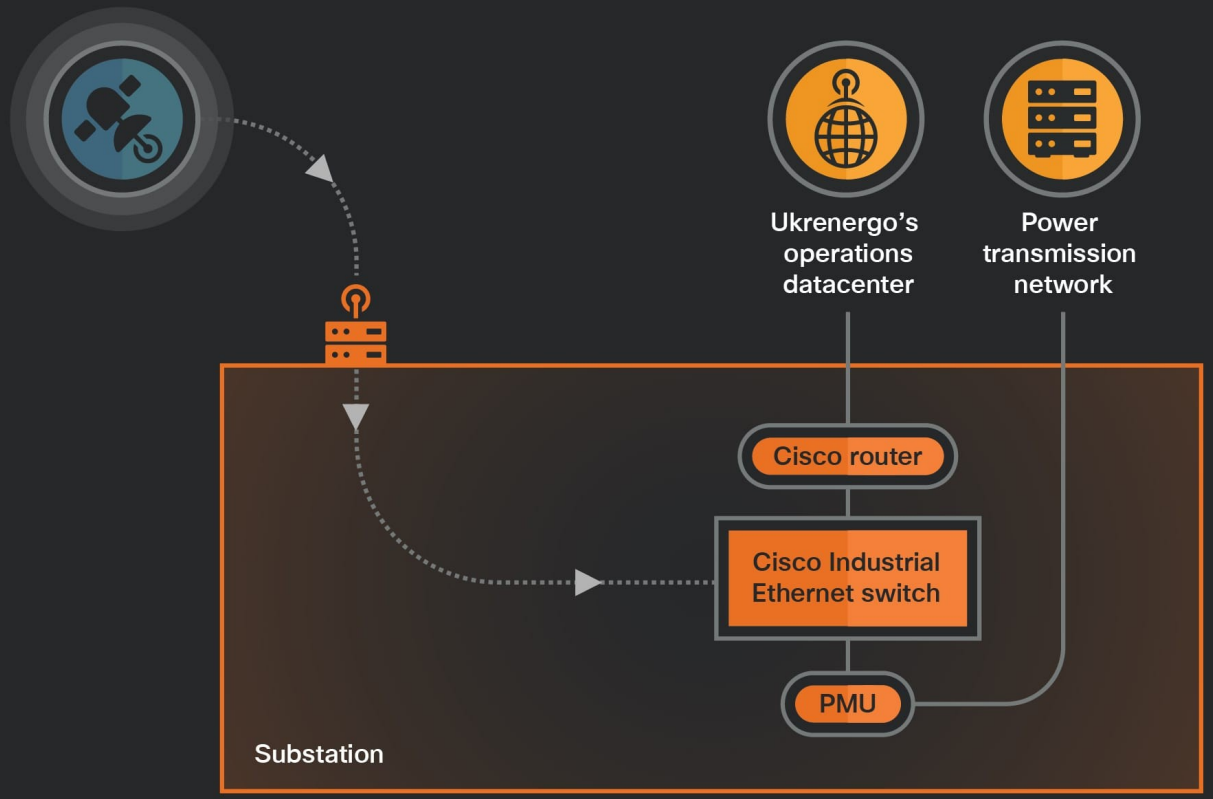
GPS Time in Ukraine with Cisco

Cisco Security Research

Enter: The humble IE5K

- Has a robust *good enough* internal clock? ✓
- Can be rapidly obtained? ✓
- Full business BU buy in? ✓
- Let's get it done! ✓

Diagram showing how the Cisco Industrial Ethernet switch is incorporated into Ukrenergo's infrastructure



In field failure pcap due to jamming

```
Time quality flags
    .0.. .... = Leap second direction: Delete
    ..0. .... = Leap second occurred: False
    ...0 .... = Leap second pending: False
    .... 0100 = Message Time Quality indicator code: Clock unlocked, time within 10^-6 s (0x4)
Fraction of second (raw): 468
Fraction of second: 780
Measurement data
    [Dissected using configuration from frame: 640691]
    Station: "XXXXXXXXXXXX    "
        Flags
            00.. .... .... .... = Data error: Good measurement data, no errors (0x0)
            ..1. .... .... .... = Time synchronized: Synchronization lost
                [Expert Info (Note/Response): PMU not sync flag set]
                    [PMU not sync flag set]
                    [Severity level: Note]
                    [Group: Response]
            ...0 .... .... .... = Data sorting: By timestamp
            .... 0... .... .... = Trigger detected: No trigger
            .... .0.. .... .... = Configuration changed: No
            .... ..0. .... .... = Data modified indicator: Data not modified
            .... ...0 10.. .... = PMU Time Quality: Estimated maximum time error < 1 µs (0x2)
            .... .... ..00 .... = Unlocked time: Locked or unlocked less than 10 s (0x0)
            .... .... .... 0000 = Trigger reason: Manual (0x0)
```

Cisco Security Research

Diagram of GPS testing equipment

CISCO TALOS

GPS Disciplined Atomic Clock

Provides accurate time references for comparison

PTP Packet Analyzer

Measures the time accuracy of the PTP packets

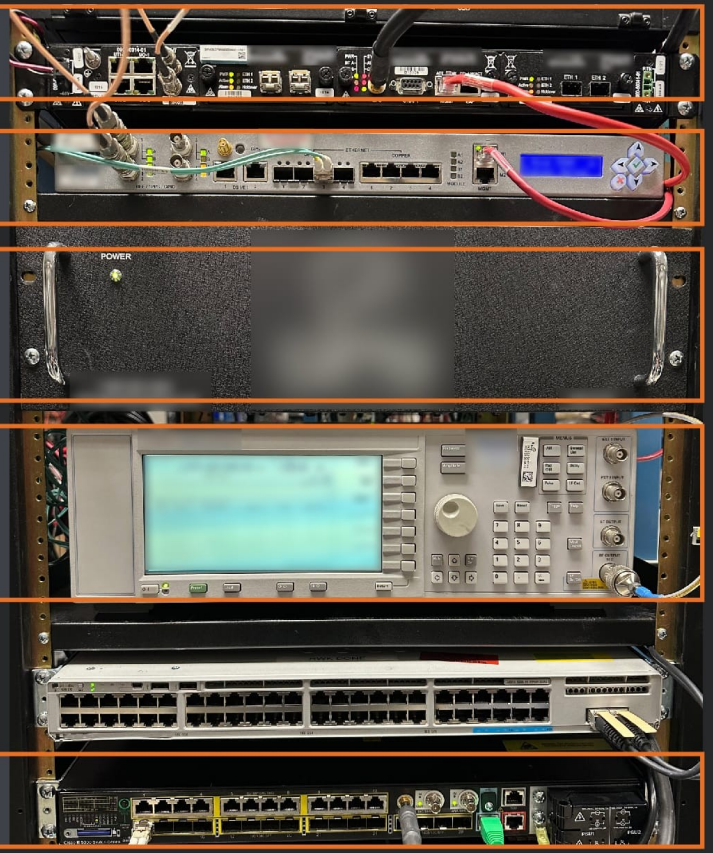
GPS Splitter

Sends the same RF GPS signal
to all the components in the setup

RF Signal Generator

Simulates the jamming signal

Industrial Ethernet Switch



Success!!!

With modifications to the IE5K, loss of GPS clock didn't cause the system to fail!

IEEE Std 1588™-2008	IEEE Std C37.118.2™-2011
Reason RT430	
FREQUENCY_TRACEABLE: True TIME_TRACEABLE: True PTP_UTC_REASONABLE: True grandmasterClockClass: 6 grandmasterClockAccuracy: The time is accurate to within 100 ns (0x21)	Message Time Quality indicator code: Normal operation, clock locked (0x0) Time synchronized: Clock is synchronized PMU Time Quality: Estimated maximum time error < 100 ns (0x1)
SEL-2488 (GPS antenna)PtPv2	
FREQUENCY_TRACEABLE: True TIME_TRACEABLE: True PTP_UTC_REASONABLE: True grandmasterClockClass: 6 grandmasterClockAccuracy: The time is accurate to within 100 ns (0x21)	Message Time Quality indicator code: Normal operation, clock locked (0x0) Time synchronized: Clock is synchronized PMU Time Quality: Estimated maximum time error < 100 ns (0x1)
SEL-2488 (GPS antenna)IRIG-B004	
	Message Time Quality indicator code: Normal operation, clock locked (0x0) Time synchronized: Clock is synchronized PMU Time Quality: Estimated maximum time error < 100 ns (0x1)
SEL ICON	
FREQUENCY_TRACEABLE: True TIME_TRACEABLE: True PTP_UTC_REASONABLE: True grandmasterClockClass: 6 grandmasterClockAccuracy: The time is accurate to within 250 ns (0x22)	Message Time Quality indicator code: Normal operation, clock locked (0x0) Time synchronized: Clock is synchronized PMU Time Quality: Estimated maximum time error < 100 ns (0x1)
Cisco ie5000-8hour-mz	
FREQUENCY_TRACEABLE: True TIME_TRACEABLE: True PTP_UTC_REASONABLE: True grandmasterClockClass: 6 grandmasterClockAccuracy: The time is accurate to within 250 ns (0x22)	Message Time Quality indicator code: Normal operation, clock locked (0x0) Time synchronized: Clock is synchronized PMU Time Quality: Estimated maximum time error < 100 ns (0x1)
Cisco ie5000-clkAcc250ns-mz	
FREQUENCY_TRACEABLE: True TIME_TRACEABLE: True PTP_UTC_REASONABLE: True grandmasterClockClass: 6 grandmasterClockAccuracy: The time is accurate to within 250 ns (0x22)	Message Time Quality indicator code: Normal operation, clock locked (0x0) Time synchronized: Clock is synchronized PMU Time Quality: Estimated maximum time error < 100 ns (0x1)
Cisco ie5000-clkAcc25us-mz	
FREQUENCY_TRACEABLE: True TIME_TRACEABLE: True PTP_UTC_REASONABLE: True grandmasterClockClass: 6 grandmasterClockAccuracy: The time is accurate to within 250 ns (0x22)	Message Time Quality indicator code: Normal operation, clock locked (0x0) Time synchronized: Clock is synchronized PMU Time Quality: Estimated maximum time error < 100 ns (0x1)
Cisco ie5000-clkCls6-mz	
FREQUENCY_TRACEABLE: True TIME_TRACEABLE: True PTP_UTC_REASONABLE: True grandmasterClockClass: 6 grandmasterClockAccuracy: The time is accurate to within 250 ns (0x22)	Message Time Quality indicator code: Normal operation, clock locked (0x0) Time synchronized: Clock is synchronized PMU Time Quality: Estimated maximum time error < 100 ns (0x1)

A massive team effort

Cisco Security Research

Stay Connected and Up To Date

Spreading security news, updates,
and other information to the public.

White papers, articles & other information
talosintelligence.com

ThreatSource Newsletter
cs.co/TalosUpdate

Talos Blog
blog.talosintelligence.com

Social Media Posts
X: @talossecurity

Videos
cs.co/talostube

Beers with Talos & Talos Takes
talosintelligence.com/podcasts

Talos publicly shares security information through numerous channels to help make the internet safer for everyone.

CISCO TALOS

CISCO

TALOS

TALOSINTELLIGENCE.COM