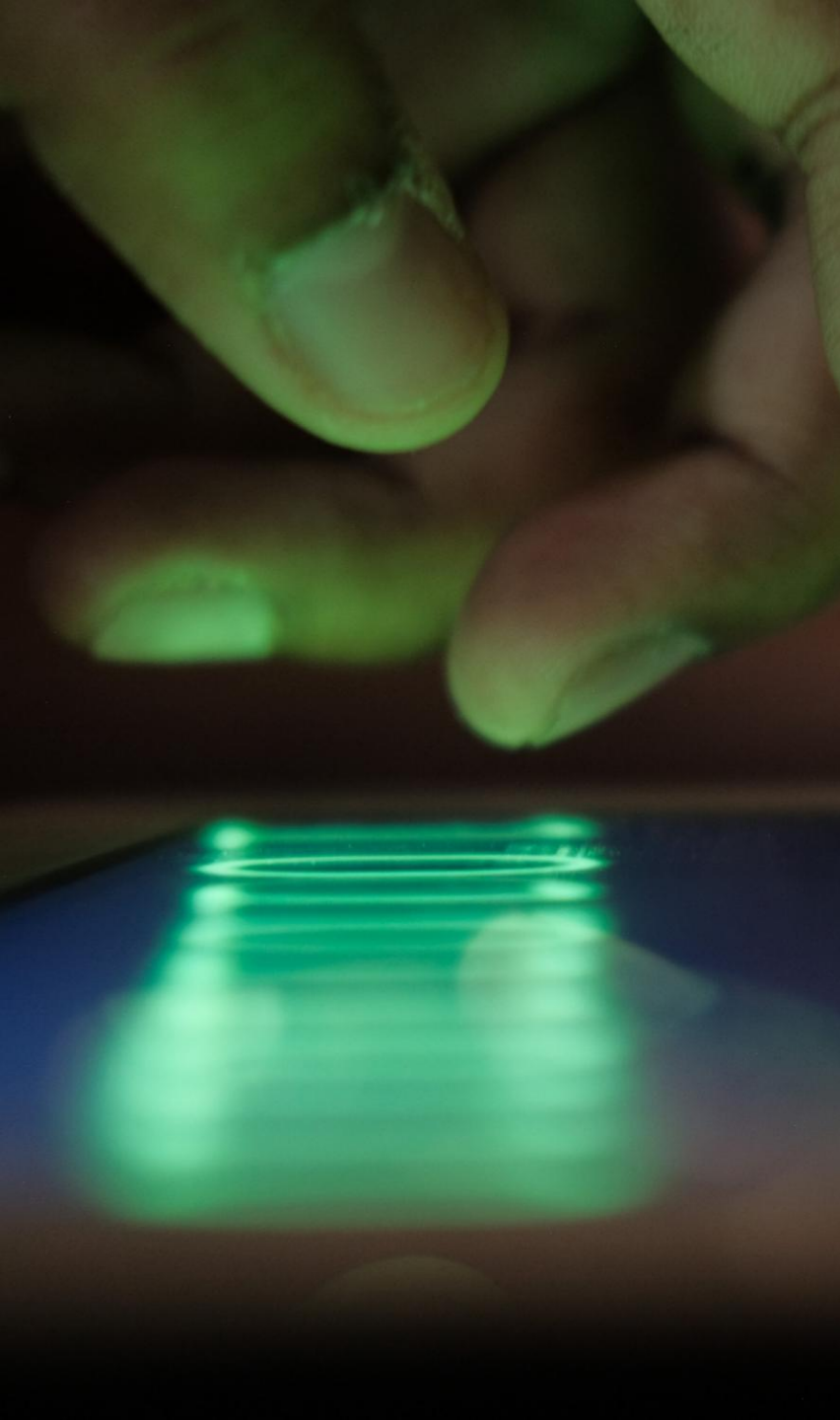


A scenic background image showing a sunset over a city. The sun is low on the horizon, casting a warm orange glow across the sky and reflecting on the water. The city skyline is visible in the distance, with various buildings and structures. In the foreground, there are dense evergreen trees and some autumn-colored foliage. The overall atmosphere is peaceful and scenic.

You're Lucky I'm One of the Good Guys

An Insider's View on Security Vulnerabilities

ITE Western District Annual Meeting
June 2026 - Bellevue, WA



Outline

1. The Challenge
2. Threats Actors
3. Threat Scenarios

Transportation networks are vulnerable

- Transportation systems are ubiquitous and poorly secured
- Cabinets and other street side infrastructure is widely dispersed and poorly monitored
- Communications protocols are dated, insecure, and well documented
- Traffic networks are often flat with little or no segmentation
- Culturally our industry has avoided, rather than embraced security



And they're critical

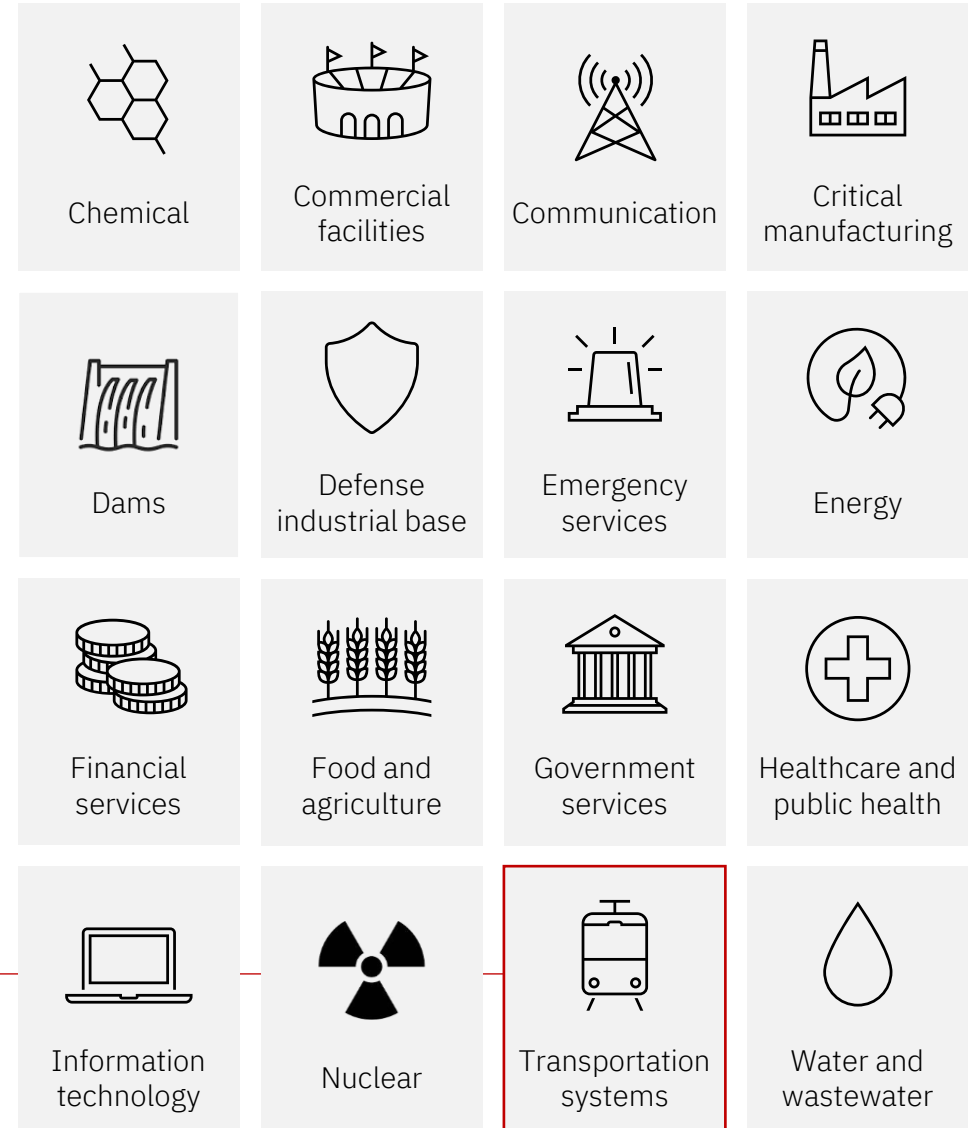
Transportation systems sector

One of 16 critical infrastructures

- Aviation
- Highway and motor carrier
- Maritime transportation system
- Mass transit and passenger rail
- Pipeline systems
- Freight rail
- Postal and shipping

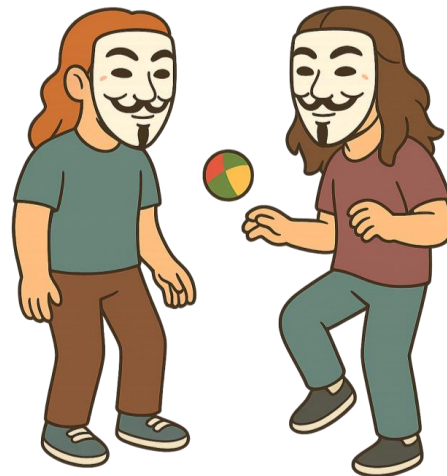
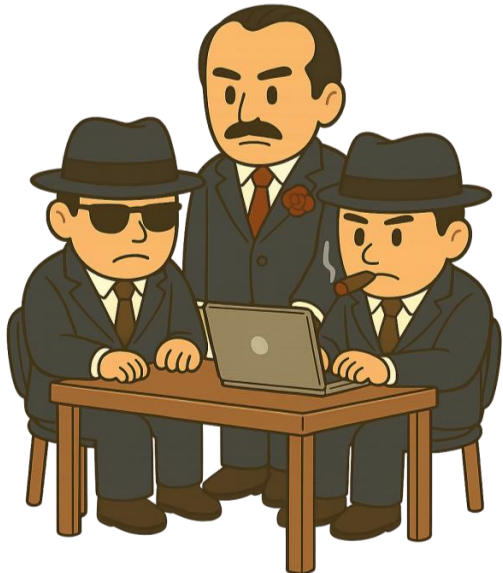


America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE



Threat Actors

- Script Kiddies
- Insider Threats
- Organized Cybercrime Groups
- Hacktivists
- Hostile Nation-State Actors
- Cyber Terrorists



Scenario One:

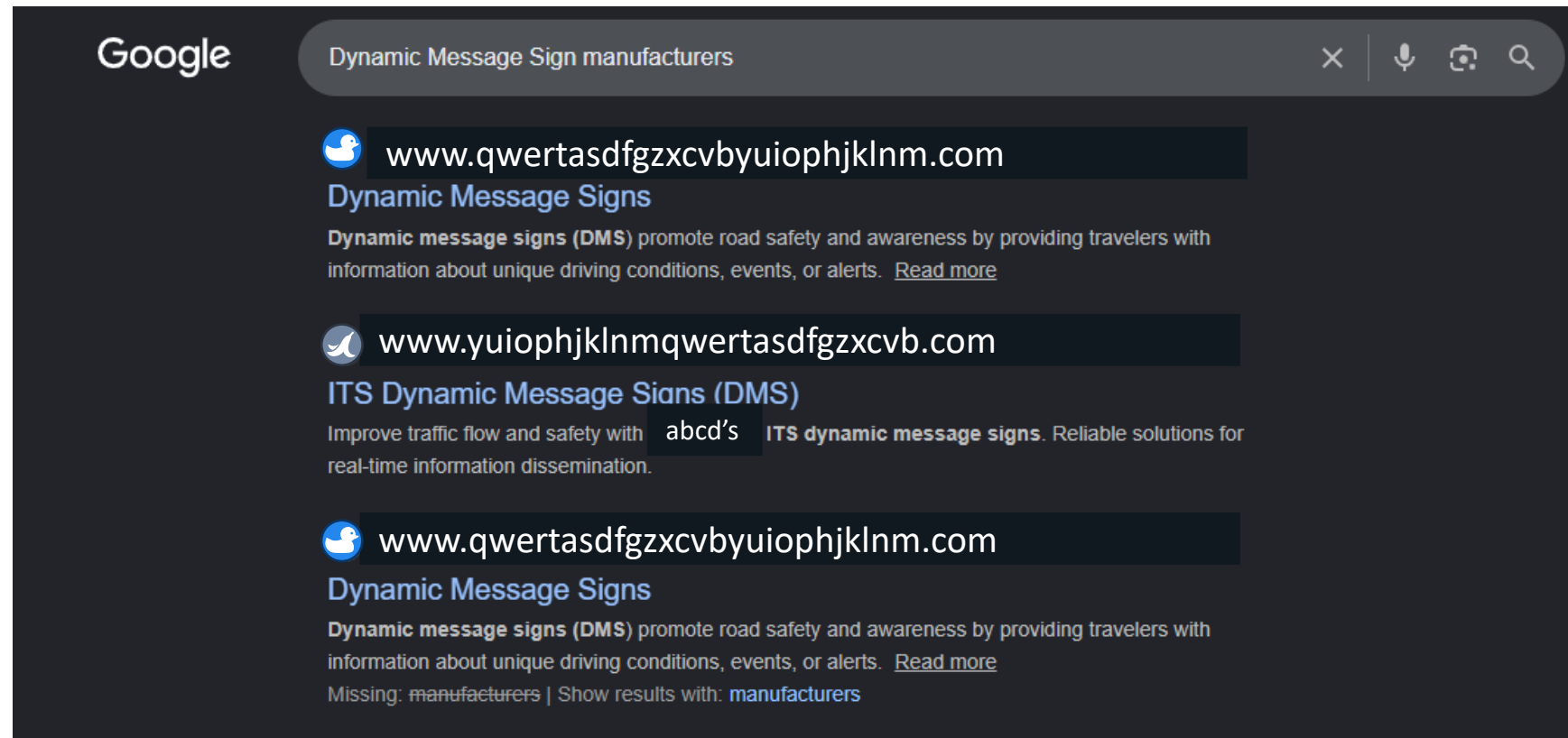


Joey is a high school student and script kiddie hears about how easy it is to hack dynamic message signs

He decides to give it a try...

Scenario One:

He googles it:



Scenario One:

He takes that to Shodan:



Shodan
Maps
Images
Monitor
Developer
More...



SHODAN

ABC MFG



Login

TOTAL RESULTS
2

 View Report

 View on Map

 Advanced Search

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to.](#)

166. XXX.XXX.XXX

2026-05-14T16:14:22.964049

Verizon Business

 United States, San Jose

SNMP:

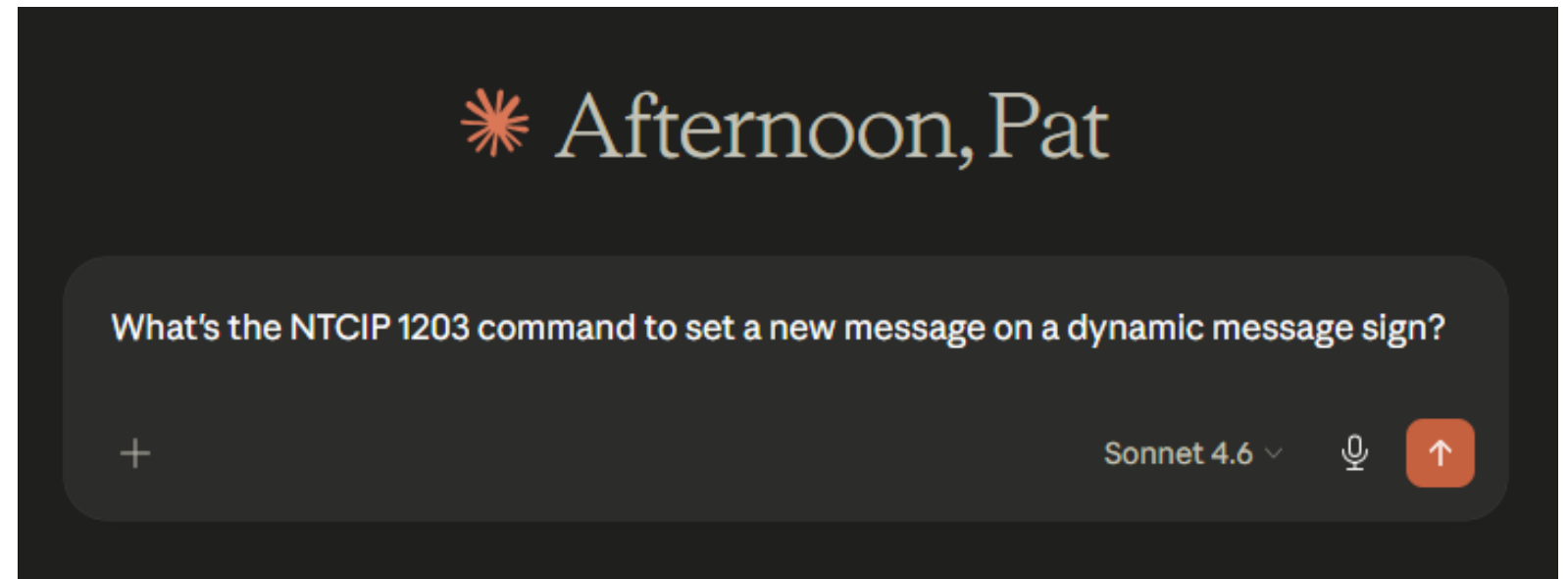
Description: ABC MFG DMS

Versions:

1

Scenario One:

Add a dash of free AI:



Scenario One:

And a couple prompts later:



3. SNMP SETs to Send

Assuming:

- Changeable message slot 1
- Your management station IP: 192.168.1.100
- Community string: public

Step 1 — Write the message

```
snmpset -v1 -c public 192.168.1.50 \  
  1.3.6.1.4.1.1206.4.2.3.5.8.1.3.3.1 s "Pat is Awesome"  
  1.3.6.1.4.1.1206.4.2.3.5.8.1.6.3.1 i 255  
  1.3.6.1.4.1.1206.4.2.3.5.8.1.7.3.1 i 0
```

OID

Object

Value

.5.8.1.3.3.1

dmsMessageMultiString

"Pat is Awesome"

Hacked road signs in Southern California city display explicit messages

by: [Wiley Jawhary](#)

Posted: Nov 20, 2025 / 04:52 PM PST

Updated: Nov 20, 2025 / 05:34 PM PST

SHARE



ENCINITAS, Calif. ([FOX 5/KUSI](#)) — Electronic signs installed across Encinitas to encourage safer driving are now at the center of a disturbing issue after several were hacked to display explicit messages and graphic images.

But instead of warnings to slow down or watch for pedestrians, residents say some signs have been reprogrammed with profanity, hate speech and inappropriate images.

“They’re really easy to hack,” said Encinitas resident Brad Lefkowitz, who first noticed photos circulating in neighborhood group chats. “We’ve been getting text messages where someone puts an obscene message or even an obscene image on the signs.”



ELECTRONIC TRAFFIC SIGNS HACKED

KUSI
NEWS

63°

5:09

<https://fox5sandiego.com/news/local-news/encinitas-hacked-road-signs/>



Mitigations:

1. Better network hygiene
2. Move towards better, encrypted and authenticated, protocols
3. Don't use from default passwords/community strings

Scenario Two:

Bruce is a signal tech has had it up to here with the management at the City, and in fact Cities all together.

He quits his job to move off grid...



Scenario Two:

But as a trained electrician, he's not living with out power. So, he goes shopping...



**Aluminum
Ladder
\$140**



**Safety Vest
\$20**



**Angle Grinder
\$60**

**White Truck
for a Day
\$150**

Current Selection

Large Pickup

Ram 2500 Big Horn or similar



Scenario Two:

Steeling you way to energy independence?

Priceless!



PORTLAND

ODOT out \$200K after copper stolen from lights on I-84 near Exit 7

by: [Joey Vacca](#)

Posted: Mar 5, 2026 / 05:55 PM PST

Updated: Mar 6, 2026 / 10:44 AM PST

SHARE



PORTLAND, Ore. (KGIN) – Copper thieves knocked out [60 light fixtures near exit 7 of I-84](#), according to ODOT. The hit is creating an unexpected cost for an agency already strapped for cash.

ODOT has to dig even deeper into its maintenance budget after falling victim to copper thieves. They are still staring down a shortfall of more than \$240 million, and are now faced with an estimated \$200 thousand repair cost. A dark interstate is a serious safety issue, so fixing the lights is a top priority. But financial pressure on the agency is not letting up.

“We need to delay other kinds of maintenance, graffiti cleanup, things like that,” ODOT spokesperson David House said. “And we need to continue to hold our hiring down, and make other efforts again to save money so that we have more money available.”

When it comes to where the scrap metal goes next, metal buyers at Calbag Metals said it is not as simple as stopping into a shop, dropping off metal, and leaving with cash.



LIGHT POLES STRIPPED OF COPPER

ODOT SAYS THEFT REPAIRS COULD COST THOUSANDS



<https://www.koin.com/news/portland/odot-out-200k-after-copper-stolen-from-lights-on-i-84-near-exit-7/>



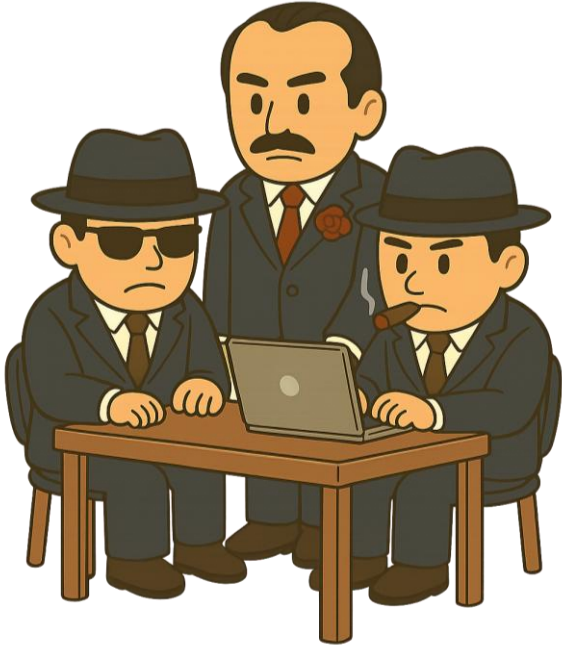
Mitigations:

- **Intrusion Detection**
 - Door Open Switches
 - Light/Temp Sensors
- **Active Monitoring**
- **Security Training**
 - See something, Say something
- **Better Locks**

Scenario Three:

Michael, Fredo, and Vito are running a successful and well organized (criminal) organization.

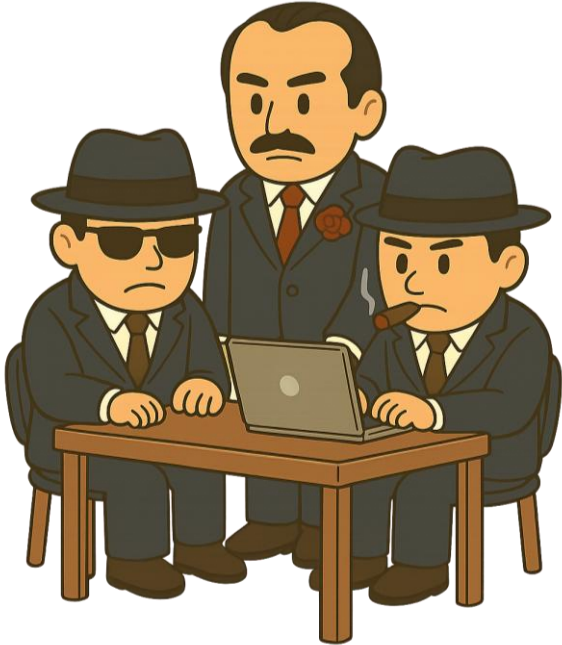
They aim to hit their annual EBITDA target by any means necessary...



Scenario Three:

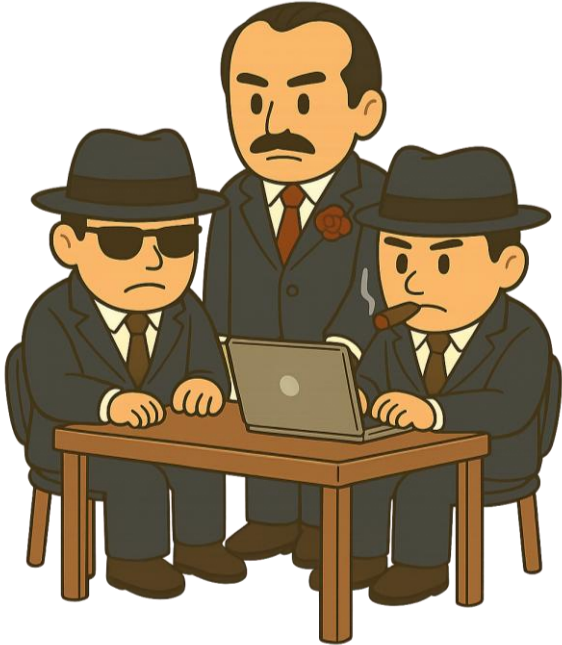
So, they make an investment...

...and they pay a disgruntled contractor for VPN and Service Account credentials.



Scenario Three:

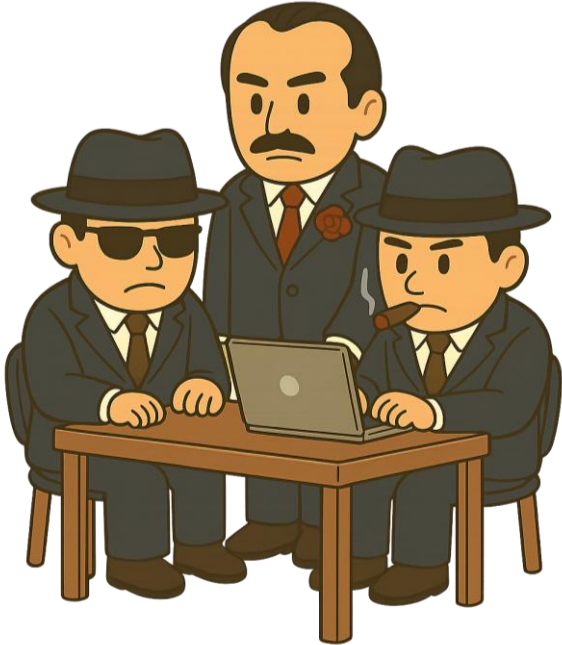
With convenient access and a satisfied teaming partner they spend weeks delivering their project...



Scenario Three:

Billing Milestone One: Encrypting your system

Billing Milestone Two: Selling the data they stole to another organization





KC Scout website, traffic cameras restored months after cyberattack

MoDOT, KDOT say 'full-service restoration efforts' still underway



Photo by: Kansas City Scout

By: Addi Weakley

Posted 7:49 AM, Jul 09, 2024 and last updated 7:53 AM, Jul 09, 2024

KANSAS CITY, Mo. — Months after a [cyberattack](#), the Kansas City Scout website, including live traffic cameras, was restored Tuesday.

The bi-state initiative between the Missouri Department of Transportation and Kansas Department of Transportation was hit [April 25](#).

[All systems were shut down](#) as a result of the cyberattack.

The [first phase](#) of restoration came [June 20](#) when digital message boards began displaying real-time information.

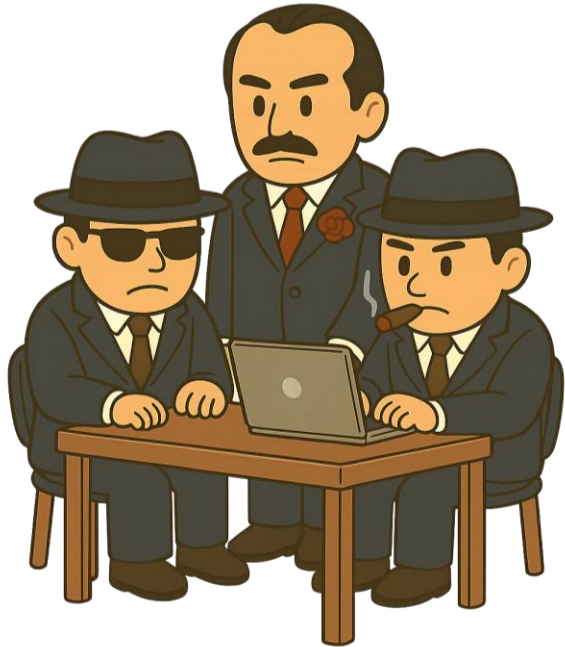
Even with the website back, MoDOT and KDOT said "full-service restoration efforts are still underway."

Access to the KC Scout mobile app, real-time cameras on the MoDOT Traveler Map, camera streaming for media partners and KDOT's traveler map ([KanDrive.gov](#)) have yet to be restored.



Fox 4 News https://youtu.be/Rrz_aFoOZyk?si=Y3NapeamMiogfHK8

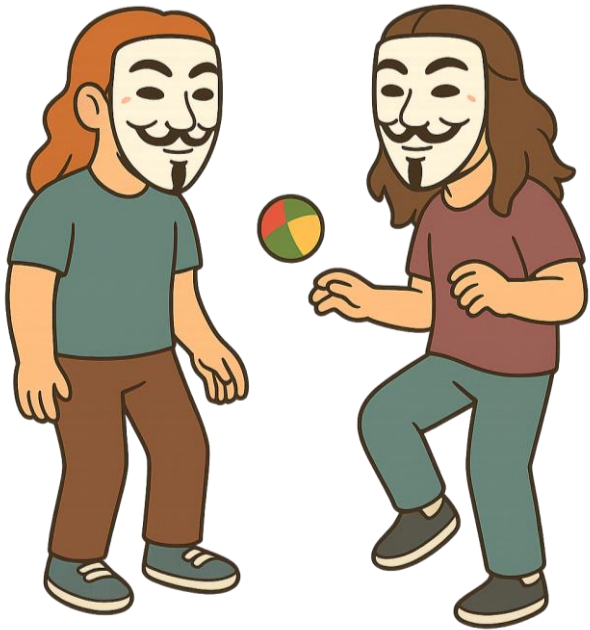
<https://www.kshb.com/news/local-news/transportation/kc-scout-website-traffic-cameras-restored-months-after-cyberattack>



Mitigations:

- Compliance Frameworks like SOC2 or NIST
- Zero Trust Models
- Eliminate long-lived credentials
- Profile use to detect stolen accounts
 - Odd login times
 - New IP addresses
 - Impossible travel schedules
 - Service accounts that are logging in like a user

Scenario Four:

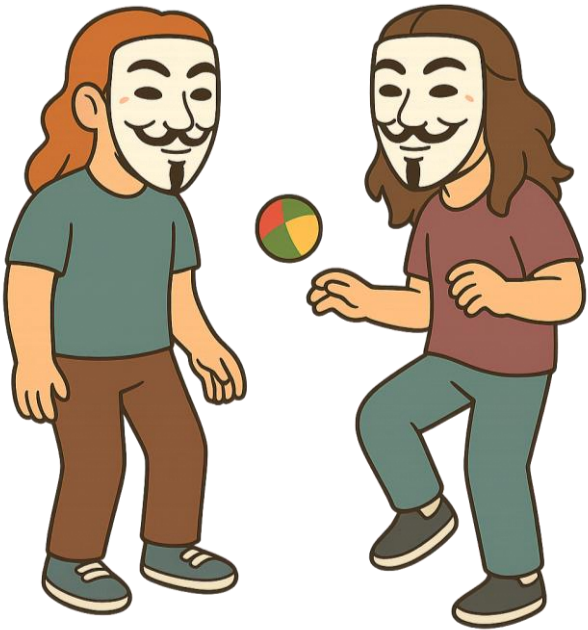


The Vegan's International League on Ecology (V.I.L.E.) is a hacktivism group looking to make a statement...

The pick a target the simultaneously epitomizes the industrial meat industry and the petrochemical depended transportation system...

Scenario Four:

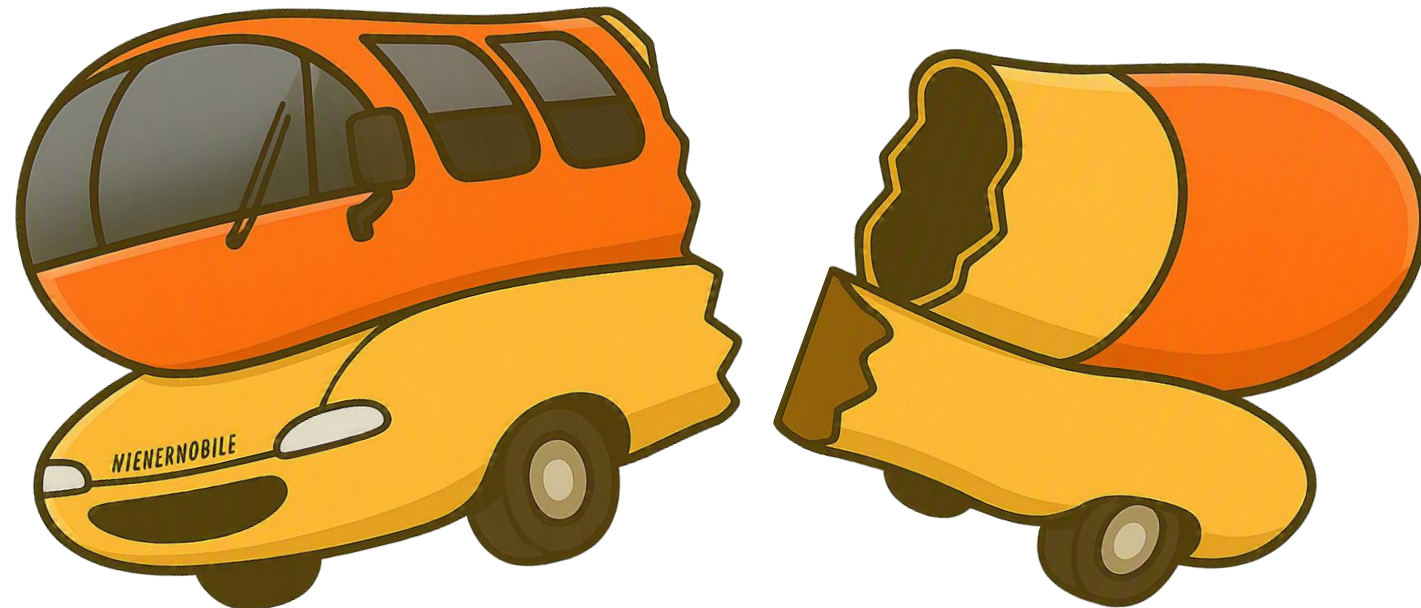
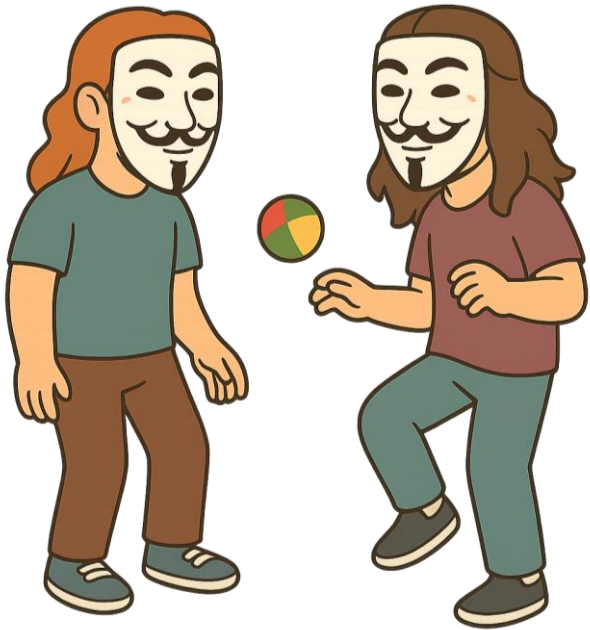
That's right, they plan to attack the Oscar Meyer Weiner Mobile.



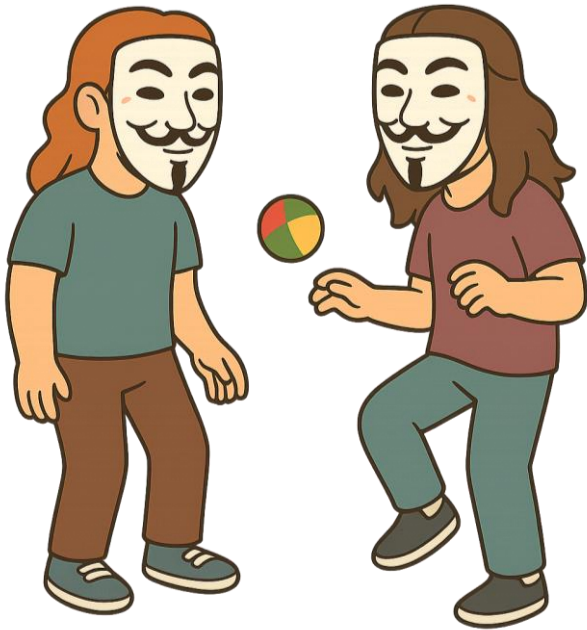
Scenario Four:

That's right, they plan to attack the Oscar Meyer Weiner Mobile...

And this time they are planning direct action.



Scenario Four:



**This is a radar sensor
it has an effective
range of 75 meters
and 16 detection
zones**

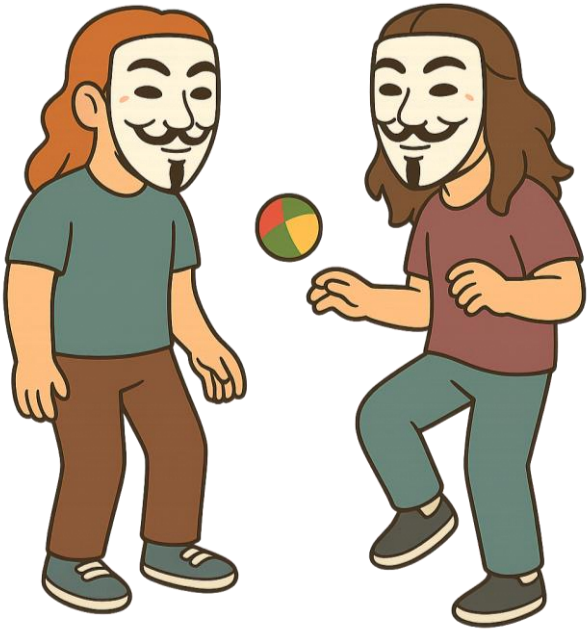


**This is a claymore mine
it has an effective range
of 50 meters and 700
steel ball bearings**

Scenario Four:

With a little modeling clay and spray paint they make a clandestine device

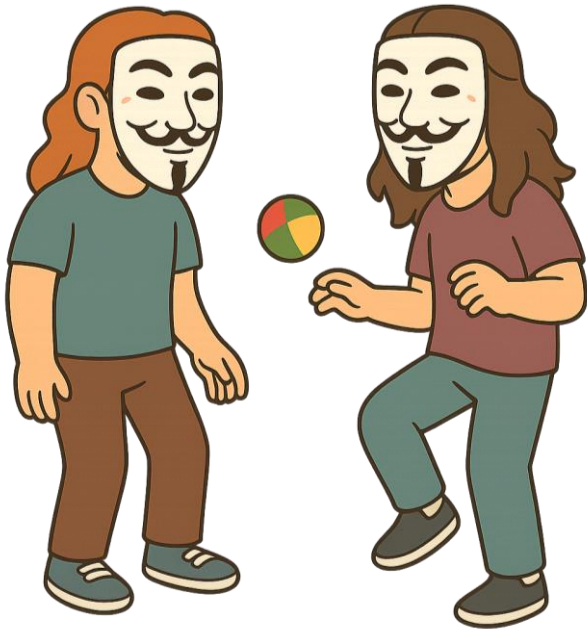
Wearing a yellow safety vest, they hid it in plane sight on a signal mast arm

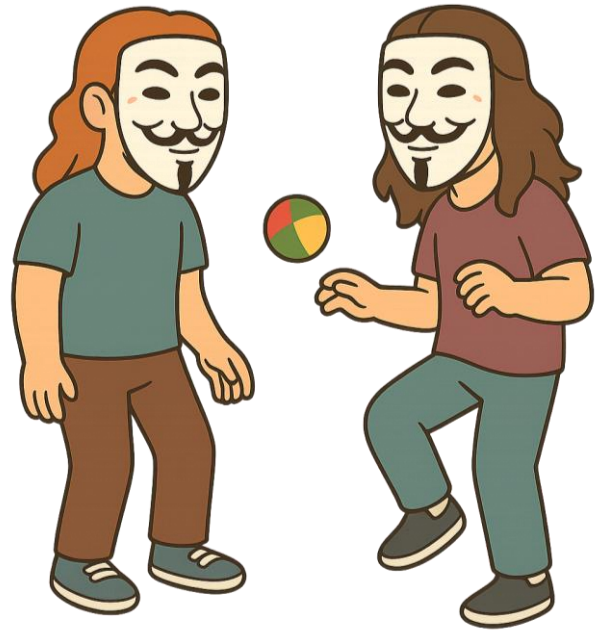


Scenario Four:

They wire it to an unused output on a 2070 C11 pin on the traffic controller

And while they are there, they compromise the PTZ camera



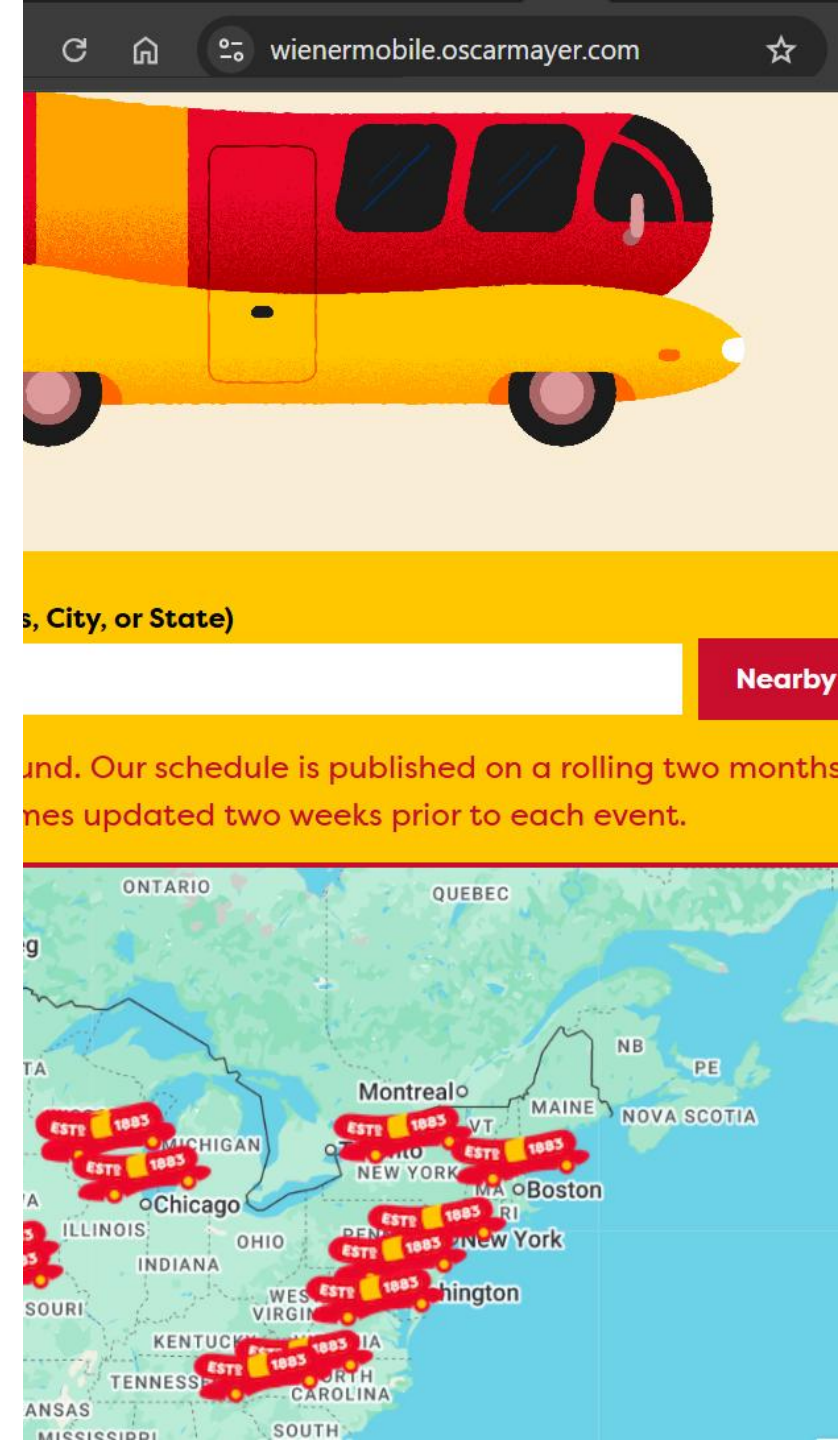


Scenario Four:

And when they know the target is in the area

They monitor and wait for the moment to trigger an output remotely

Output Points Status					
IO Module 1 ▼ Show All Output Points					
Output Point	Control	Status	Description	Output Control Type	Index
51	☐	●	C1-94	Channel Red Do Not Walk Driver	10
52	☐		C1-95	Channel Yellow Ped Clear Driver	10
53	☐		C1-96	Channel Green Walk Driver	10
54	☐	●	C1-97	Channel Red Do Not Walk Driver	9
55	☐		C1-98	Channel Yellow Ped Clear Driver	9
56	☐		C1-99	Channel Green Walk Driver	9
57	☒	●	C11-1	Not Active	0
58	☐		C11-2	Not Active	0



Ecoterrorism Suspected in House Fires in Seattle Suburb

Share full article



Homes being promoted as “green,” but criticized by some as ruining suburban Seattle wetlands, were severely damaged by fire.

Elaine Thompson/Associated Press

By **William Yardley**

March 4, 2008

MALTBY, Wash. Five luxury homes in a subdivision marketed as “built green” near here were destroyed or severely damaged by fire early Monday, and evidence at the scene suggested the fires might have been started by radical environmentalists who viewed the homes as violating rather than complementing the wooded wetlands in which they were built.

“Built green?” read letters spray-painted onto a bedsheet found hanging on a fence at the site, about 25 miles northeast of Seattle.

“Nope Black!

MORE

FBI

Q Se

History

History of the FBI

Directors, Then and Now

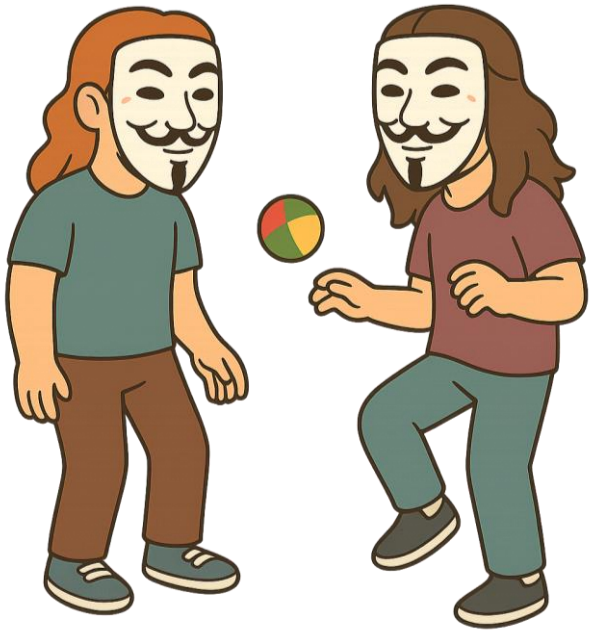
Cases and Criminals

More

Weather Underground Bombings



Three Weather Underground members were killed when a bomb they had built exploded in the basement of a townhouse in Greenwich Village on March 6, 1970. In the days following the explosion, police found 57 sticks of dynamite, four completed bombs, detonators, timing devices, and other bomb-making equipment. Bettmann/Corbis photo.



Mitigations:

- **Cabinet Intrusion Detection**
 - Door Open Switches
 - Light/Temp Sensors
- **Active Monitoring**
 - Positive maintenance verification
- **Security Training**
 - See something, Say something
- **Better Locks**

Scenario Five:

The Peoples Republic of Omelas has created a team of hacker dedicated to creating Advanced Persistent Threats (APT) in US transportation networks



Scenario Five:



They infiltrate an agency's network using a stolen agency VPN account.

They find access to network of PTZ camera across a major metropolitan city...

Scenario Five:

And then they dig in...

And wait...

And wait...

And wait...



Scenario Five:

They are still waiting today for the moment to use the traffic camera to support a physical attack at a future date.





TEL AVIV, Israel (AP) — The role of Israel's hijacking of Iran's street cameras in the killing of the country's supreme leader underscores how surveillance systems are increasingly being targeted by adversaries in wartime.

Hundreds of millions of cameras have been installed above shops, in homes and on street corners across the world, many connected to the internet and poorly secured. Recent advances in artificial intelligence have enabled militaries and intelligence agencies to sift through vast amounts of surveillance footage and identify targets.

On Feb. 28, Israel vividly demonstrated the potential of such systems to be hacked and used against adversaries when Israel tracked down Iranian leader Ayatollah Ali Khamenei with the help of Tehran's own street cameras — despite repeated warnings that Iran's surveillance systems had been compromised, according to interviews and an Associated Press review of leaked data, public statements and news reports.

Iran built a vast camera network to control dissent. Israel used it to track targets, AP sources say

<https://www.pbs.org/newshour/world/iran-built-a-vast-camera-network-to-control-dissent-israel-used-it-to-track-targets-ap-sources-say>



Mitigations:

- Good network hygiene
- Well segmented networks
- Intrusion Detection System to profile normal traffic and identify anomalies
- Anonymizing or masking non-relevant video data

Scenario Six:

Grans Huber wants to cause havoc at the City of Nakatomi while they host a major sporting event

Using publicly available information and some social engineering, staff are identified and profiles for home addresses, social media accounts, cell phone numbers, etc.



Scenario Six:

With these details he sim-jacks an account to steal a phone number used for text message 2FA...

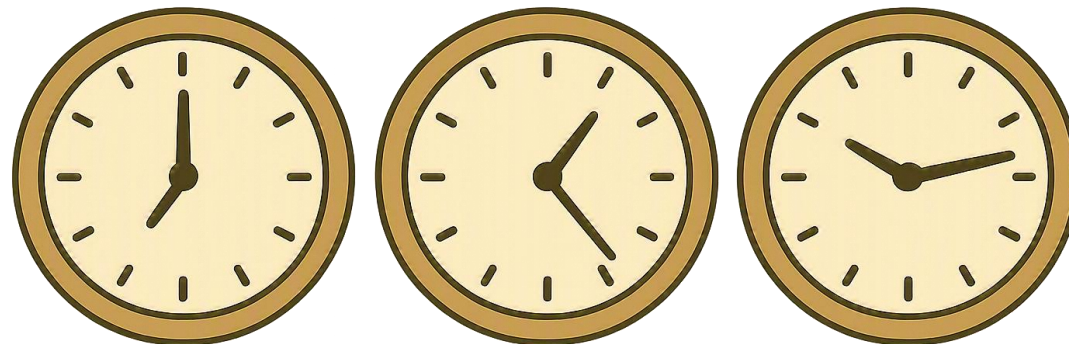
Basically, he called the phone company's support line with enough data to activate a new phone



Scenario Six:

From this foothold he works to escalate his privileges and identify additional vulnerabilities in the system.

The attacker creates a replacement DLL file. The replacement operates exactly as the current DLL does but send random NTCIP time set commands to devices.



Who said
we are
terrorists?



Scenario Six:

Once the attack is noticed by agency staff and a response is mounted, a ransomware payload is executed, and a financial demand is made.

ANDY GREENBERG EXCERPT SECURITY OCT 17, 2019 6:00 AM

The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History

How digital detectives unraveled the mystery of Olympic Destroyer—and why the next big attack will be even harder to crack.

SAVE THIS STORY

All products featured on WIRED are independently selected by our editors. However, we may receive compensation from retailers and/or from purchases of products through these links. [Learn more.](#)

JUST BEFORE 8 pm on February 9, 2018, high in the northeastern mountains of South Korea, Sang-jin Oh was sitting on a plastic chair a few dozen rows up from the floor of Pyeongchang's vast, pentagonal Olympic Stadium. He wore a gray and red official Olympics jacket that kept him warm despite the near-freezing weather, and his seat, behind the press section, had a clear view of the raised, circular stage a few hundred feet in front of him. The 2018 Winter Olympics opening ceremony was about to start.

As the lights darkened around the roofless structure, anticipation buzzed through the 35,000-person crowd, the glow of their phone screens floating like fireflies around the stadium. Few felt that anticipation more intensely than Oh. For years



<https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/>



Mitigations:

- Employee training on phishing and social engineering
- Social media information discipline
- Avoid SMS based 2FA
- Software Bills of Materials (BOMs)

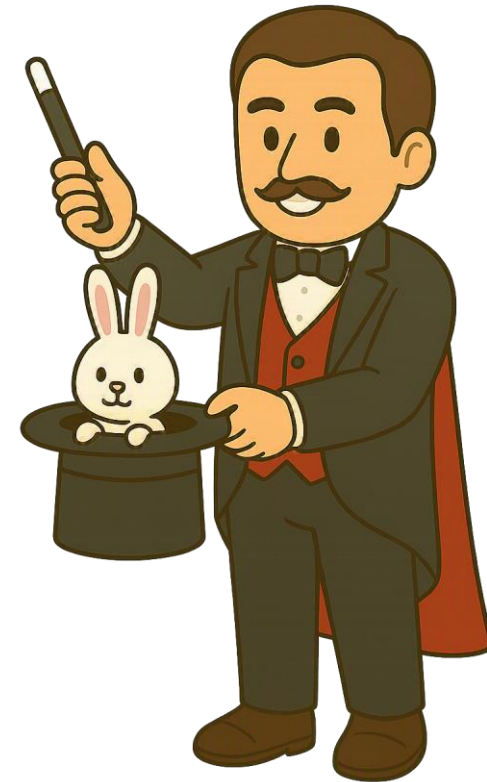
Closing Thoughts

Hacking is like magic...

It's impressive until you know the trick...

And once you know the trick, it's usually simple and ugly.

But, unlike magic, we need to talk about the tricks!





Contact us

PATRICK MARNELL

VP of Product

✉ patrick.marnell@q-free.com

☎ (541) 758-8529

🌐 www.q-free.com



@qfreeasa | #liveqfree