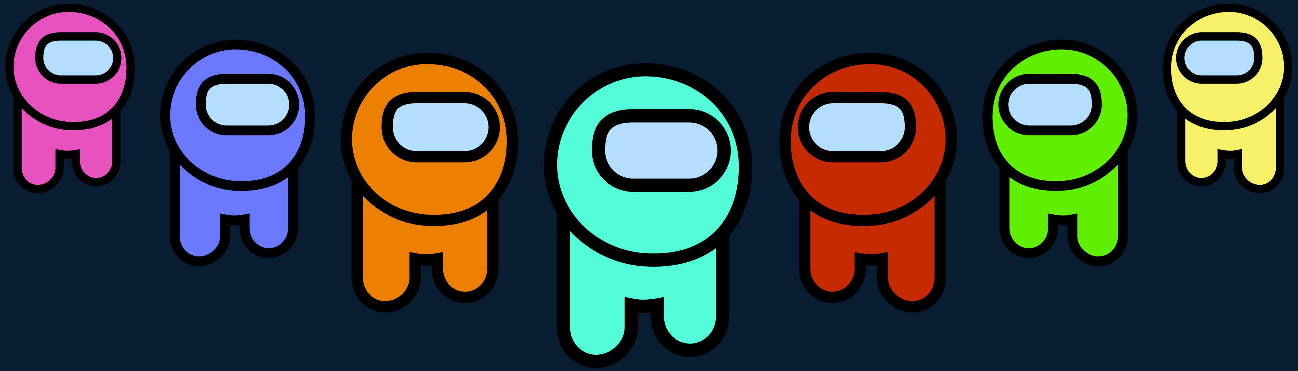
THOSE AMONG US:

The Insider Threat Facing Organizations



Presented by: Robert Sell
robert.sell@tracelabs.org

Introductions

Founder/President of Trace Labs

- NPO crowdsources OSINT to help find Missing Persons
- https://www.tracelabs.org

Search & Rescue Team Leader

- Over a decade
- Team Leader, Marine Rescue Technician, Tracker

Information Technology/Security

- Over two decades
- CISSP, CISM, etc.
- Operations to Incident Response
- Global teams

Email: robert.sell@tracelabs.org
Twitter: @robertesell

Search and Rescue Operations

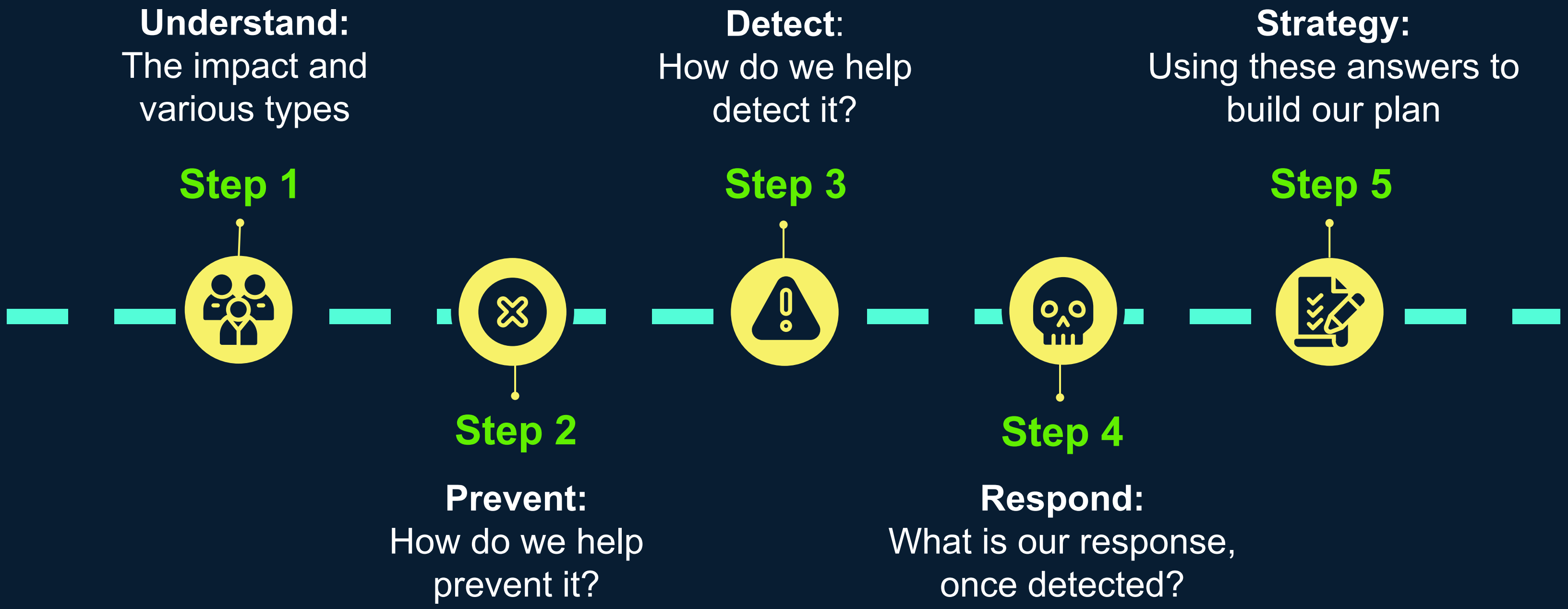
sky news
NewsDay
HACKERS HUNTING DOWN MISSING PEOPLE
MELWED 15°
HEADLINES AN ENERGY COMPANY IS CRITICISING THE FEDERAL REGULATOR

National Missing Persons Hackathon
Australian News

Disclaimer

- Opinions are my own and in no way representative of any of my past/present/future employers.
- All details presented here are for lawful use only.
- All information presented here is categorized as Public – TLP: White.
- This presentation does not cover all scenarios or situations.

Todays Journey



Step 1

Understand:
The impact and various types

Step 2

Prevent:
How do we help prevent it?

Step 3

Detect:
How do we help detect it?

Step 4

Respond:
What is our response, once detected?

Step 5

Strategy:
Using these answers to build our plan

UNDERSTAND

What Is Insider Threat?

Bad Definition

“One or more individuals with the access or inside knowledge of an organization, that would allow them to exploit the vulnerabilities of that entity’s security, systems, services, products or faculties with the intent to cause harm.”
- The National Infrastructure Advisory Council’s first report and recommendations on the insider threat to critical infrastructures, April 2008

Good Definition

“Insider threat is the potential for an insider to use their authorized access or understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities.”

- https://www.cisa.gov/defining-insider-threats

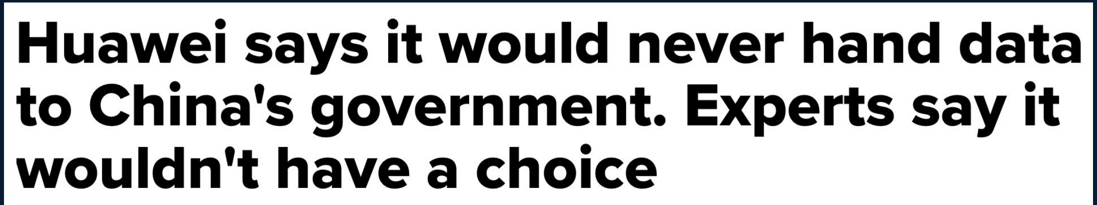
Insider Threat Impact

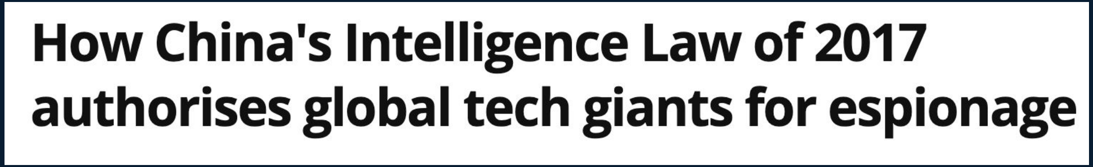
Relevant Statistics

- Businesses in the US encounter approximately 2,500 internal security breaches daily.
- More than 34% of businesses around the globe are affected by insider threats yearly.
- Over the last two years, the number of insider incidents has increased by 47%.
- Average cost of insider threats has gone up 31% from 2017 ($8.76M) to 2019 ($11.45M).

Sources:
https://techjury.net/blog/insider-threat-statistics/
https://www.isdecisions.com/insider-threat/statistics.htm

Insider Threat Impact


Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice


How China's Intelligence Law of 2017 authorises global tech giants for espionage

The New Nation State Threat

In 2017, China passed the new National Intelligence Law – Article 14:
“National intelligence work institutions, when carrying out intelligence work according to laws, may ask relevant institutions, organizations and citizens to provide necessary support, assistance and cooperation.”

The state now has the right to turn any of its citizens or organizations into spies.

Sources:
https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html
https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html
https://www.indiatoday.in/news-analysis/story/china-national-intelligence-law-2017-authorise-companies-espionage-india-1705033-2020-07-27

Types of Insider Threat

Category	Type	Intent	Triggered	Sophistication
Pawn	Accidental	No	Yes	Low
Pawn	Lazy	No	Yes	Low
Turncloak	Career	No	Yes	Low
Turncloak	Disgruntled	Yes	Yes	Medium
Imposter	Malicious	Yes	No	Medium
Imposter	Pirates	Yes	No	Medium/High
Imposter	Espionage	Yes	No	High

Types of Insider Threat

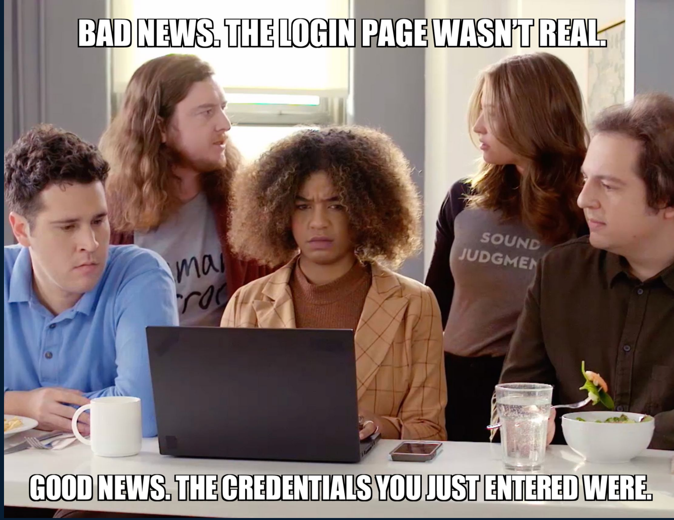
Pawns

- The pawn category often comes with an element of innocence.
- The employee may accidently cause harm through a mistake.
- Likely even regret what they did.
- Pawns are often as much a victim of the situation as the company is.

- Pawns may also just be lazy and not care about security procedures or policies.
- Either way, their intent isn’t damage to the organization.

- Always a trigger event which could be a phishing email or a missed promotion.

Types of Insider Threat


BAD NEWS. THE LOGIN PAGE WASN'T REAL.
GOOD NEWS. THE CREDENTIALS YOU JUST ENTERED WERE.

Category:	**Pawns**
Type:	**Accidental**
Intent:	**No**

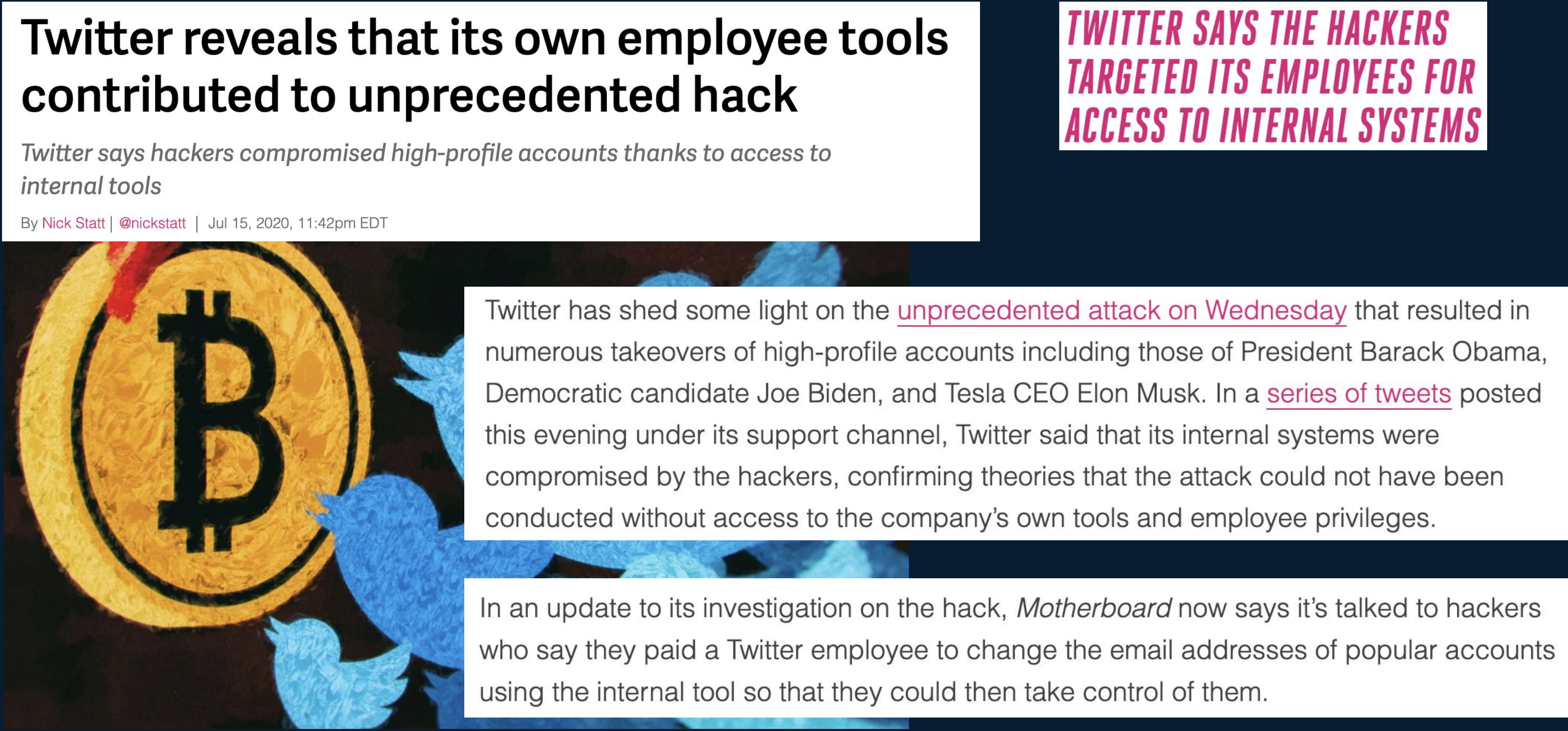
Profile:

- No intent to cause harm. Often the unknowing victim
- Very remorseful when made aware
- Often has poor judgement and easily tricked or distracted
- Often a social butterfly and using social media inappropriately
- Likely a target and victim of social engineering

Typical Scenario:

- Phishing links that make their computer a slave to external attackers

Example of Insider Threat – Type: Accidental



Twitter reveals that its own employee tools contributed to unprecedented hack

Twitter says hackers compromised high-profile accounts thanks to access to internal tools

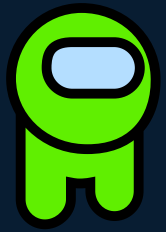
By Nick Statt | @nickstatt | Jul 15, 2020, 11:42pm EDT

TWITTER SAYS THE HACKERS TARGETED ITS EMPLOYEES FOR ACCESS TO INTERNAL SYSTEMS

Twitter has shed some light on the unprecedented attack on Wednesday that resulted in numerous takeovers of high-profile accounts including those of President Barack Obama, Democratic candidate Joe Biden, and Tesla CEO Elon Musk. In a series of tweets posted this evening under its support channel, Twitter said that its internal systems were compromised by the hackers, confirming theories that the attack could not have been conducted without access to the company's own tools and employee privileges.

In an update to its investigation on the hack, *Motherboard* now says it's talked to hackers who say they paid a Twitter employee to change the email addresses of popular accounts using the internal tool so that they could then take control of them.

Types of Insider Threat



Category:	**Pawns**
Type:	**Lazy (aka Negligent)**
Intent:	**No**

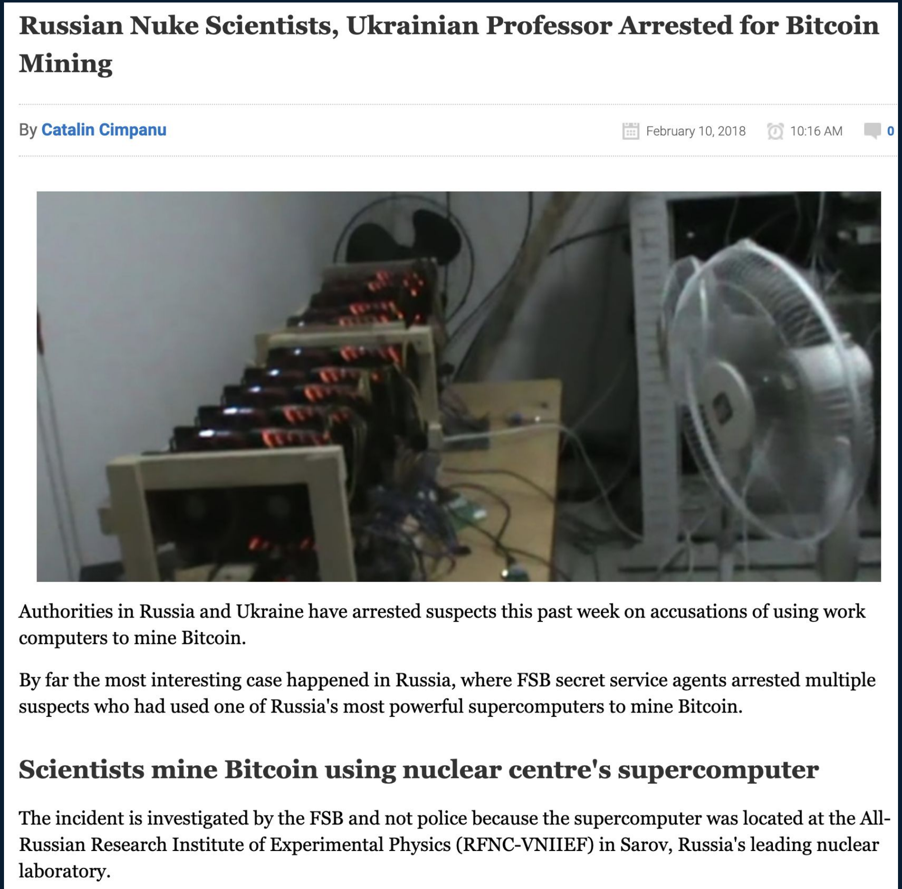
Profile:

- No intent to cause harm, just can't be bothered to be careful
- Unlike the Accidental type, Lazy does not typically feel much remorse
- Knows the rules and aware it's a violation but simply doesn't care
- Not motivated by greed or self gain as much as work avoidance
- Not interested in additional effort required to comply with policy

Typical Scenario:

- Leaves laptop or proprietary papers in public

Example of Insider Threat – Type: Lazy



Russian Nuke Scientists, Ukrainian Professor Arrested for Bitcoin Mining

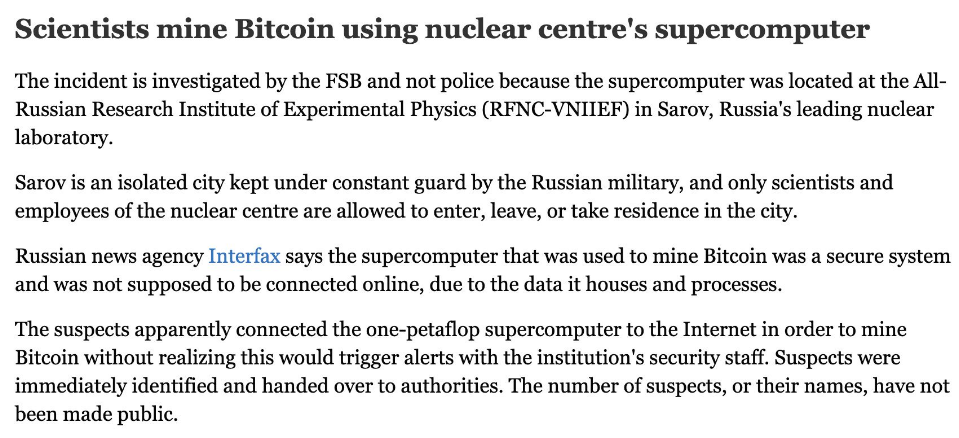
By Catalin Cimpanu February 10, 2018 10:16 AM 0

Authorities in Russia and Ukraine have arrested suspects this past week on accusations of using work computers to mine Bitcoin.

By far the most interesting case happened in Russia, where FSB secret service agents arrested multiple suspects who had used one of Russia's most powerful supercomputers to mine Bitcoin.

Scientists mine Bitcoin using nuclear centre's supercomputer

The incident is investigated by the FSB and not police because the supercomputer was located at the All-Russian Research Institute of Experimental Physics (RFNC-VNIIEF) in Sarov, Russia's leading nuclear laboratory.



Scientists mine Bitcoin using nuclear centre's supercomputer

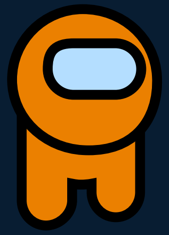
The incident is investigated by the FSB and not police because the supercomputer was located at the All-Russian Research Institute of Experimental Physics (RFNC-VNIIEF) in Sarov, Russia's leading nuclear laboratory.

Sarov is an isolated city kept under constant guard by the Russian military, and only scientists and employees of the nuclear centre are allowed to enter, leave, or take residence in the city.

Russian news agency Interfax says the supercomputer that was used to mine Bitcoin was a secure system and was not supposed to be connected online, due to the data it houses and processes.

The suspects apparently connected the one-petaflop supercomputer to the Internet in order to mine Bitcoin without realizing this would trigger alerts with the institution's security staff. Suspects were immediately identified and handed over to authorities. The number of suspects, or their names, have not been made public.

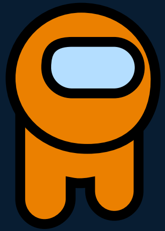
Types of Insider Threat



Turncloaks

- While the pawns are often victims, turncloaks are not
- The turncloaks are purposeful and sometimes acting with intent
- Will not show remorse, will not change their habits and will likely repeat
- Always a trigger event such as no policy enforcement or low employee engagement.

Types of Insider Threat



Category:	**Turncloak**
Type:	**Career**
Intent:	**No**

Profile:

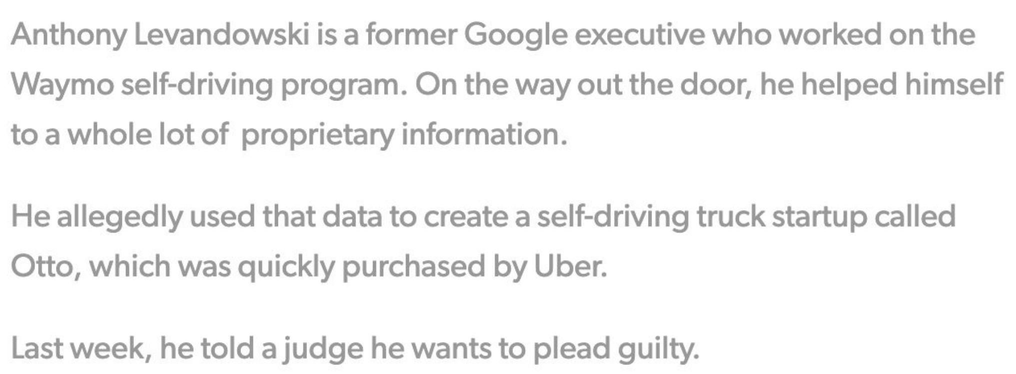
- No intent to cause harm however, intent to complete data exfil for career
- Little remorse when confronted and often pleads ignorance
- Conveniently forgets the rules and may take necessary actions to avoid detection
- Motivated by desire to retain digital work for personal career benefit
- May be ignorant of rules, pretend to be ignorant or just blatantly ignore rules

Typical Scenario:

- Exfiltrate their data and possibly group data via portable media or online storage

Example of Insider Threat – Type: Career

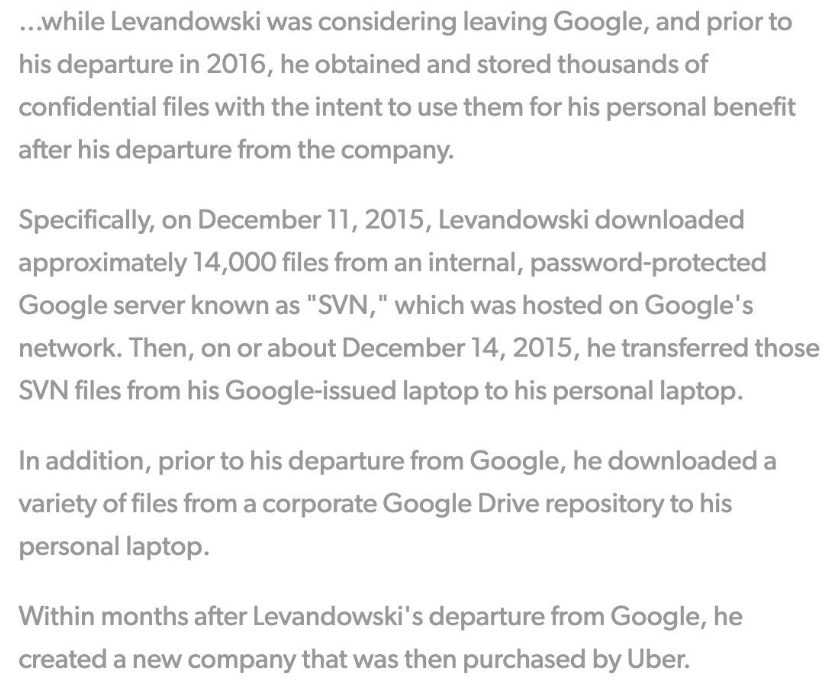
Google's Insider Threat Pleads Guilty



Anthony Levandowski is a former Google executive who worked on the Waymo self-driving program. On the way out the door, he helped himself to a whole lot of proprietary information.

He allegedly used that data to create a self-driving truck startup called Otto, which was quickly purchased by Uber.

Last week, he told a judge he wants to plead guilty.



...while Levandowski was considering leaving Google, and prior to his departure in 2016, he obtained and stored thousands of confidential files with the intent to use them for his personal benefit after his departure from the company.

Specifically, on December 11, 2015, Levandowski downloaded approximately 14,000 files from an internal, password-protected Google server known as "SVN," which was hosted on Google's network. Then, on or about December 14, 2015, he transferred those SVN files from his Google-issued laptop to his personal laptop.

In addition, prior to his departure from Google, he downloaded a variety of files from a corporate Google Drive repository to his personal laptop.

Within months after Levandowski's departure from Google, he created a new company that was then purchased by Uber.

Types of Insider Threat

I SWEAR TO GOD IF YOU TAKE MY STAPLER
I WILL SHOW YOU WHAT AN INSIDER THREAT LOOKS LIKE
imgflip.com

Category:	Turncloak
Type:	Disgruntled
Intent:	Yes

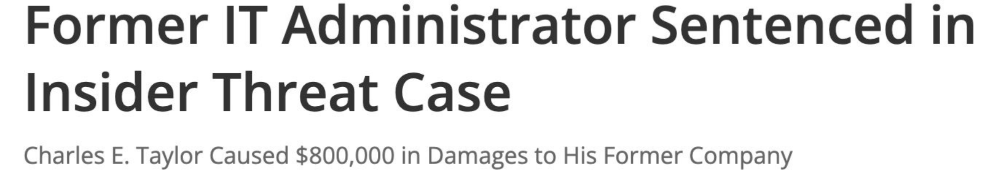
Profile:

- Intent to cause harm (i.e. damage)
- No remorse until emotionally satisfied
- Knows the rules and will take necessary actions to avoid detection
- Motivated by desire to retaliate from sense of personal wrongdoing
- May pretend to have interest to comply with policy but is secretly planning damage

Typical Scenario:

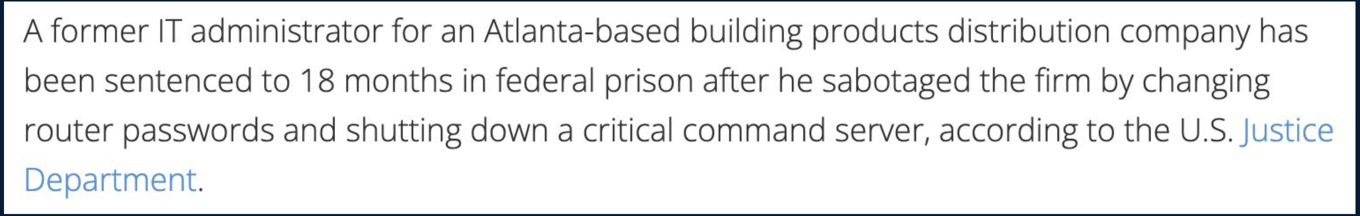
- Distract employees, encourage others to be unproductive, sabotage projects and introduce external threats such as ransomware.

Example of Insider Threat – Type: Disgruntled

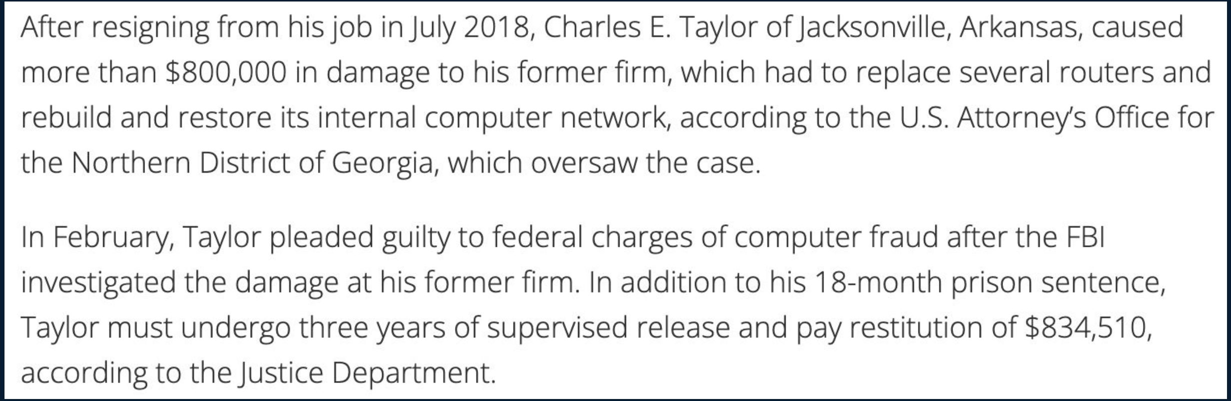


Former IT Administrator Sentenced in Insider Threat Case

Charles E. Taylor Caused $800,000 in Damages to His Former Company



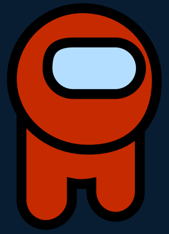
A former IT administrator for an Atlanta-based building products distribution company has been sentenced to 18 months in federal prison after he sabotaged the firm by changing router passwords and shutting down a critical command server, according to the U.S. Justice Department.



After resigning from his job in July 2018, Charles E. Taylor of Jacksonville, Arkansas, caused more than $800,000 in damage to his former firm, which had to replace several routers and rebuild and restore its internal computer network, according to the U.S. Attorney's Office for the Northern District of Georgia, which oversaw the case.

In February, Taylor pleaded guilty to federal charges of computer fraud after the FBI investigated the damage at his former firm. In addition to his 18-month prison sentence, Taylor must undergo three years of supervised release and pay restitution of $834,510, according to the Justice Department.

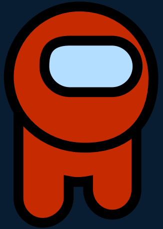
Types of Insider Threat



Imposters

- While pawn is accidental and turncloak has intent, the imposter is sophisticated.
- You likely won't even know they have an imposter within your ranks.
- The Imposter is a professional. A trained actor. Carefully planned strategy.
- Isn't emotional. Running like a business. If it takes them too long to get what they want, they may move on to the next victim.
- Unlike pawns or turncloaks, there is no trigger event with Imposters.

Types of Insider Threat



Category:	**Imposter**
Type:	**Malicious**
Intent:	**No**

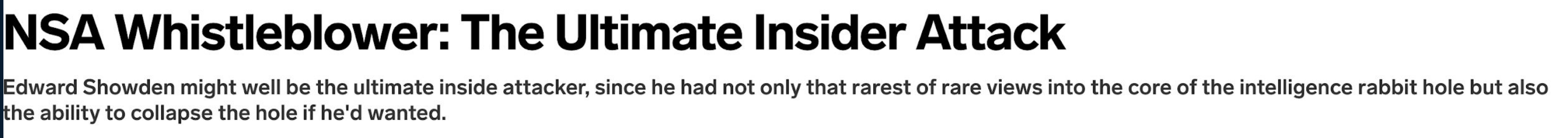
Profile:

- Fully intent on causing harm to the organization
- No remorse. Unlike the Disgruntled, Malicious wasn’t triggered
- Knows the rules and has likely taken adequate measures not to get caught
- Not necessarily motivated by greed or self gain but instead hurting the company
- Likely understand company rules and policy but willing to violate

Typical Scenario:

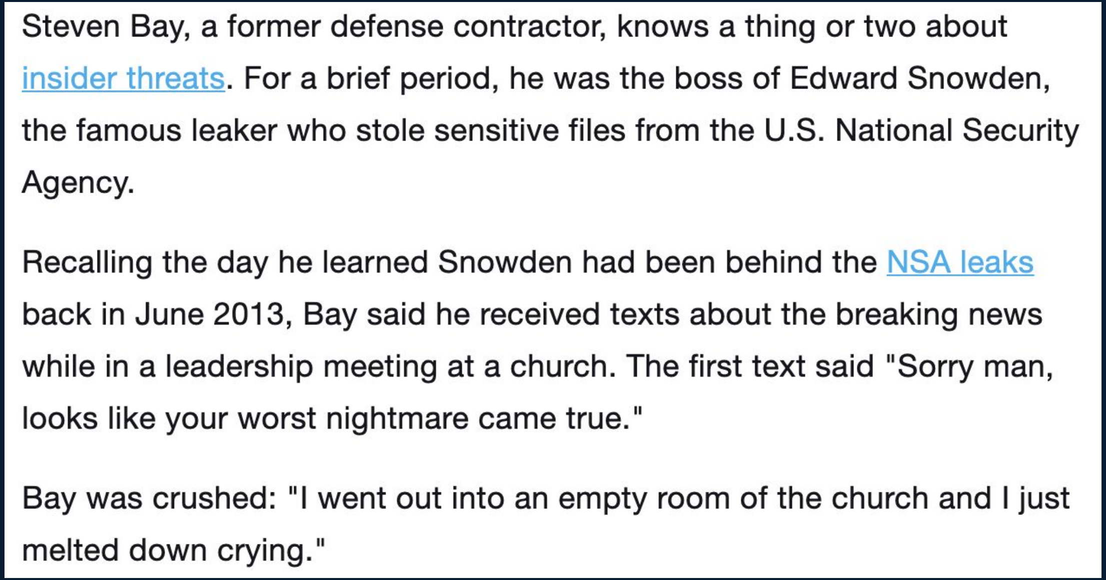
- Whistle blower or sabotage (i.e. Edward Snowden, Wikileaks, Anonymous)

Example of Insider Threat – Type: Malicious



NSA Whistleblower: The Ultimate Insider Attack

Edward Showden might well be the ultimate inside attacker, since he had not only that rarest of rare views into the core of the intelligence rabbit hole but also the ability to collapse the hole if he'd wanted.

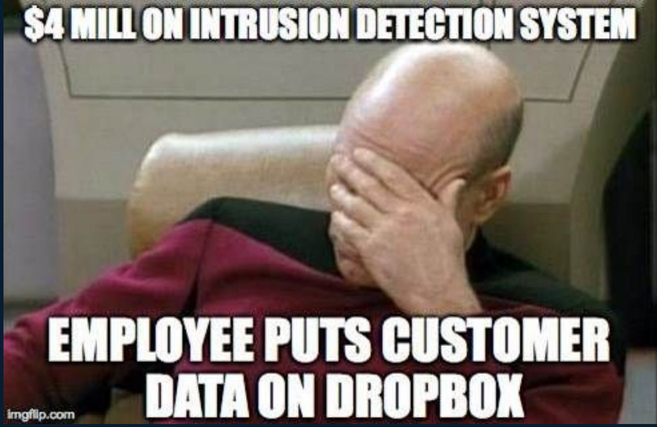


Steven Bay, a former defense contractor, knows a thing or two about insider threats. For a brief period, he was the boss of Edward Snowden, the famous leaker who stole sensitive files from the U.S. National Security Agency.

Recalling the day he learned Snowden had been behind the NSA leaks back in June 2013, Bay said he received texts about the breaking news while in a leadership meeting at a church. The first text said "Sorry man, looks like your worst nightmare came true."

Bay was crushed: "I went out into an empty room of the church and I just melted down crying."

Types of Insider Threat


$4 MILL ON INTRUSION DETECTION SYSTEM
EMPLOYEE PUTS CUSTOMER DATA ON DROPBOX
imgflip.com

Category:	**Imposter**
Type:	**Pirates**
Intent:	**Yes**

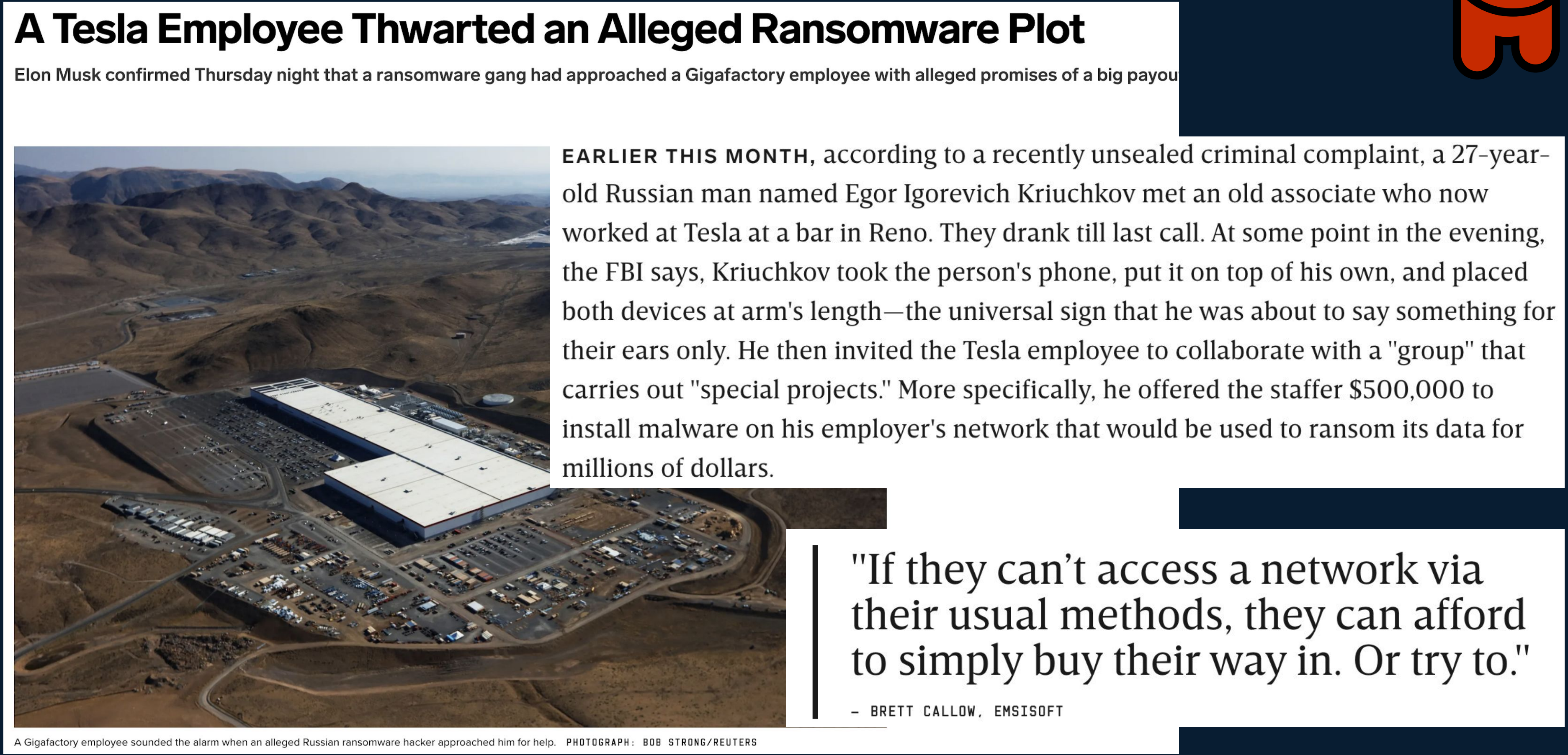
Profile:

- Fully intent on finding opportunities to profit (which they know will cause harm)
- No remorse. This is their standard MO.
- Knows the rules and work to obtain goal and exit before detection
- Will have excuses and back stories should they be questioned
- Motivated by greed and personal gain
- Not interested in complying with policy. In Fact, this is just a barrier to this person

Typical Scenario:

- Ransomware for payout. Selling of credentials or corporate data.

Example of Insider Threat – Type: Pirate



A Tesla Employee Thwarted an Alleged Ransomware Plot

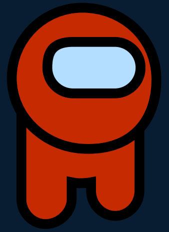
Elon Musk confirmed Thursday night that a ransomware gang had approached a Gigafactory employee with alleged promises of a big payou

EARLIER THIS MONTH, according to a recently unsealed criminal complaint, a 27-year-old Russian man named Egor Igorevich Kriuchkov met an old associate who now worked at Tesla at a bar in Reno. They drank till last call. At some point in the evening, the FBI says, Kriuchkov took the person's phone, put it on top of his own, and placed both devices at arm's length—the universal sign that he was about to say something for their ears only. He then invited the Tesla employee to collaborate with a "group" that carries out "special projects." More specifically, he offered the staffer $500,000 to install malware on his employer's network that would be used to ransom its data for millions of dollars.

> "If they can't access a network via their usual methods, they can afford to simply buy their way in. Or try to."
>
> – BRETT CALLOW, EMSISOFT

A Gigafactory employee sounded the alarm when an alleged Russian ransomware hacker approached him for help. PHOTOGRAPH: BOB STRONG/REUTERS

Types of Insider Threat



Category:	**Imposter**
Type:	**Espionage**
Intent:	**Yes**

Profile:

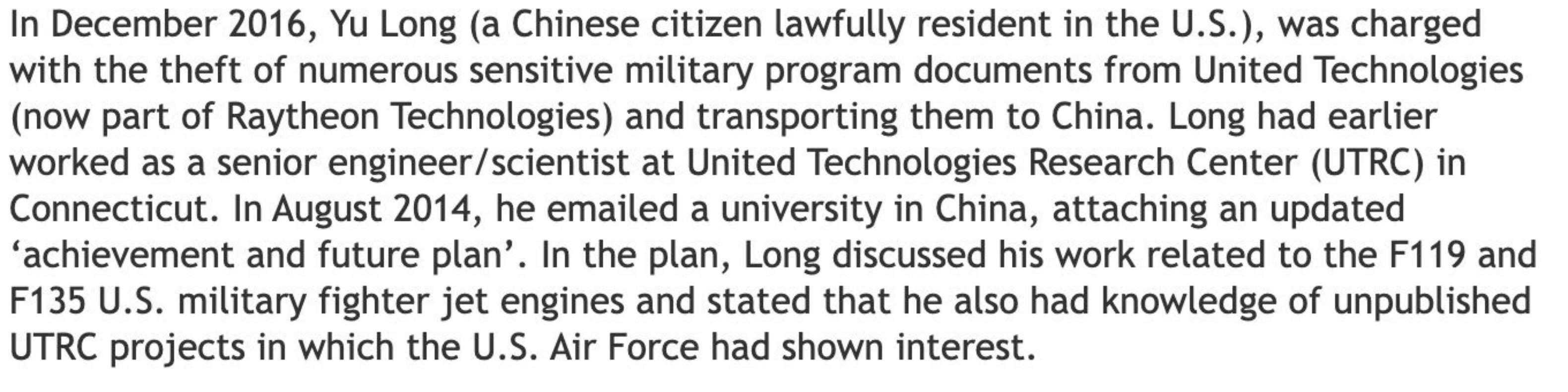
- Fully intent on carrying out their mission (which they know will cause harm)
- No remorse. Employed to infiltrate, escape & evade with data exfil
- Knows the rules and will be very careful to avoid violation detection
- Likely a nation state or corporate actor who does this professionally
- Will fake interest in compliance to fool security

Typical Scenario:

- Data exfiltration without the company ever knowing it was lost

Examples of Insider Threat – Type: Espionage

Theft of U.S. IP is a fundamental part of China's stated intention to be the world leader in science and technology by 2050



In December 2016, Yu Long (a Chinese citizen lawfully resident in the U.S.), was charged with the theft of numerous sensitive military program documents from United Technologies (now part of Raytheon Technologies) and transporting them to China. Long had earlier worked as a senior engineer/scientist at United Technologies Research Center (UTRC) in Connecticut. In August 2014, he emailed a university in China, attaching an updated 'achievement and future plan'. In the plan, Long discussed his work related to the F119 and F135 U.S. military fighter jet engines and stated that he also had knowledge of unpublished UTRC projects in which the U.S. Air Force had shown interest.

Triggers & Intent

Category	Type	Intent	Triggered	Sophistication
Pawn	Accidental	No	Yes	Low
Pawn	Lazy	No	Yes	Low
Turncloak	Career	No	Yes	Low
Turncloak	Disgruntled	Yes	Yes	Medium
Imposter	Malicious	Yes	No	Medium
Imposter	Pirates	Yes	No	Medium/High
Imposter	Espionage	Yes	No	High

We can now see the patterns which can help build our defenses:

- Pawns and Turncloaks have triggers. An event occurs which allows them to be threats.
- Pawns and some Turncloaks do not have intent.
- Imposters are not triggered yet have intent.

Prevent

Preventing Pawns

Training

- User awareness training
- Social media appropriateness training
- Social engineering training
- Active phishing program
- Physical security training
- Reception training

Management

- Disciplinary action for policy violators

Corporate Culture

- Security Champion Program
- See Something, Say Something Program
- Separation of Duties
- Strict enforcement of security policies

Technical Controls

- Multifactor authentication

Preventing Turncloaks

Training

- Sensitive data training
- Employee legal responsibility training
- InfoSec penetration testing
- Physical penetration testing

Management

- Annual Non Disclosure Agreement (NDA)
- Monitor & remediate conflict
- Exit Interviews

Corporate Culture

- Employee engagement programs
- Technical Fellowship Program
- Open dialogue on Security

Technical Controls

- Whitelist specific corporate cloud storage
- Data Loss Prevention (DLP)
- Deny portable media
- No BYOD

Preventing Imposters

Training

- Espionage awareness training

Corporate Culture

- Security/Protectionism culture
- Visible SOC/SIEM/CCTV activity

Management

- Stringent background checks
- Compartmentalized departments
- Counter espionage team integration

Technical Controls

- Tamper proof card access
- Micro segmented network
- Micro segmented physical access
- Role based access control (RBAC)
- VPN all access
- Holistic monitoring analytics
- Predictive profiling

Detect

Detecting Insider Threats

Two detection methods:

1. Tools: Typical Information Security tools
2. Behaviors: Identifying Insider Threat IoCs

Ideally, dedicated Insider Threat team utilizes both of these in a holistic strategy.

However:

- Most companies don't utilize SIEM/SOC for insider threat detection.
- Even fewer companies have dedicated staff to work this.

The Solution: Corporate Culture: See Something, Say Something – Anonymous reporting.

Indicators of Compromise for Management

Behavioral Precursors

- Conflict (coworker or supervisor)
- Decline in performance or attendance
- Policy or rule violations
- Aggressive, angry or violent
- Substance abuse

Technical Precursors

- Creating backdoors, shares, accounts
- Disabling controls
- Malicious code or hacking tools
- Unnecessarily moving data

Socials

- Bad mouthing company
- Promoting competitors

Unmet Expectations

- Passed over for a promotion
- Demotion, transferred or perf management
- Disagreement over salary or benefits
- Lack of raise over prolonged period

Concealment

- Using backdoors, shares or accounts
- Modifying or deleting logs or backups
- Avoiding to record physical access

Criminal

- Tampering with access
- Modification or deleting critical data
- Planting ransomware
- Introducing malicious code

Indicators of Compromise for Employees

User Awareness training for employees should teach how and what to report:

- Working unusual hours
- Unusual computer use
- Attempted (or successful) access to unauthorized areas
- Unexplained income and/or spending
- Inappropriate use of social media
- Strange behaviors such as making personal issues public
- Disgruntled employee behavior such as discontent with supervisors
- Disloyalty to the organization
- Vague answers to specific questions on behavior

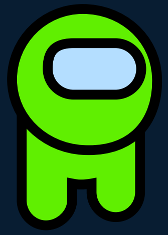
Respond

Responding to Insider Threats

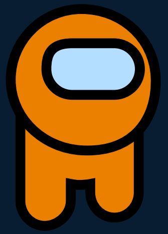
- Follow the formalized Insider Threat component in the Incident Response Plan.
- Understand the nature of the event – Do you fully understand what has happened and why?
- Response must be based on evidence. You may need to be patient.
- Must be a multi department effort that includes Human Resources and Legal.
- May require local LEA involvement if criminal activity is present (espionage).
- Response should be continual (in some form or fashion).

Strategy

Insider Threat Strategy

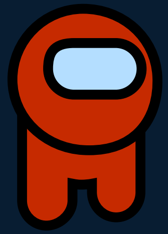


- Respond - Lack of response will encourage attackers (i.e. Career/Lazy type)
- Start easy – Control the internal influence



Custom approach for different types:

  - Pawns = Education – Can be cost effective and fun
  - Turncloaks = Company Culture – Motivate (and govern)
  - Imposters = Matured Controls – Holistic mix of technical and behavioral



- Collaborate early - internal groups like HR and external groups like local LEAs

Without adequate planning for insider threat, anyone producing innovation is simply a free R&D arm of those willing to take it.

Q&A