
DRAGOS
Virtual ICS Conference
16 July 2020
Co-Sponsored by
EIG

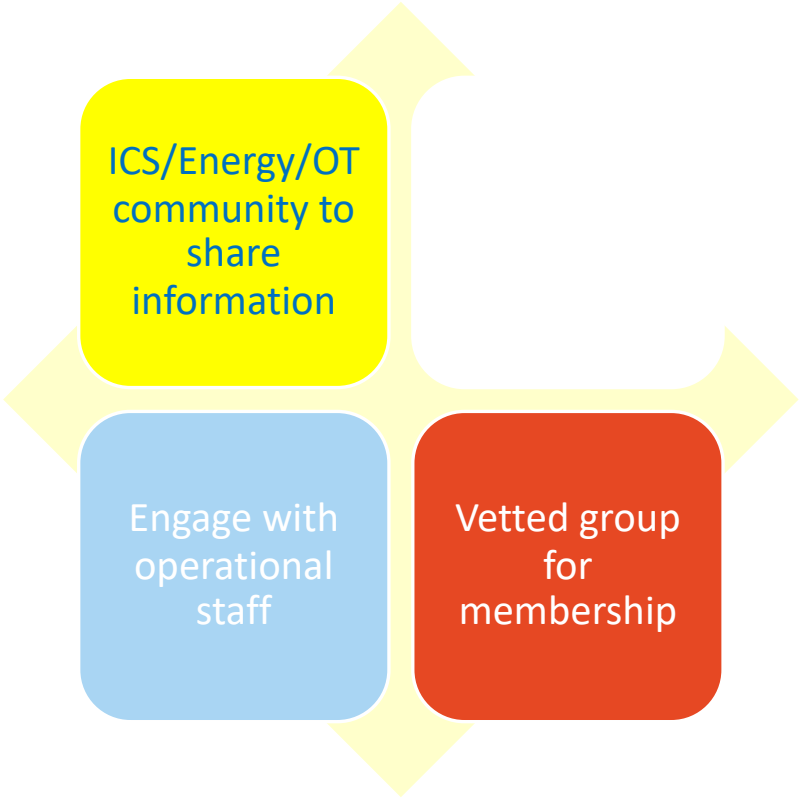
Today's Agenda

- 8:30-8:45am: **Welcome & Introductions** Warren Meikle, Dragos Senior Account Executive and Ben May, Energy Intelligence Group
- 8:45-9:25am: **Simple Wins During Slowdowns**
  Austin Scott, Principal Industrial Penetration Tester, Dragos
- 9:25-10:05am: **Adversary OSINT Collection Threats**, Casey Brooks, Sr. Adversary Hunter, Dragos
- 5 min Break!
- 10:10-10:45am: **The Rising Tide of Ransomware in Industrial and Critical Infrastructure Network**, Joe Slowik, Principal Adversary Hunter, Dragos
- 10:45-11:20am: **Industrial Threat Hunting - The When, Where and How**, Julian Gutmanis, Principal Industrial Incident Responder, Dragos
- 11:20-11:30am: **Wrap Up Remarks,** Warren Meikle

DRAGOS

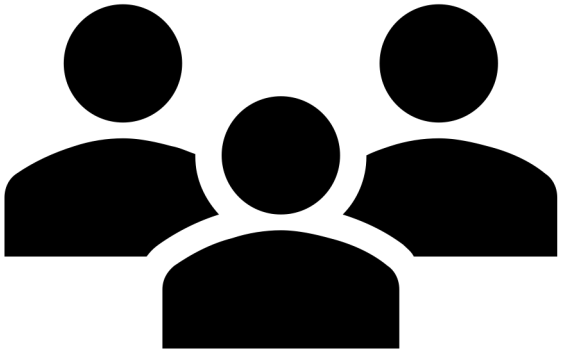
Energy Intel Group

JULY 2020



Overview – Energy Intel Group

Membership - Enquiries



- Reach out to admin@energyintelgroup.com

Dragos Virtual Conference

5 Quick Wins for Improving your ICS Cybersecurity Posture

Austin Scott (GICSP, CISSP, OSCP)
Dragos ICS Penetration Testing Principal

C:\>whoami

Austin Scott
Principal Industrial Penetration Tester
Dragos Professional Services

@Austin_m_Scott
https://www.linkedin.com/in/synergist/

019 DRAGOS YEAR IN REVIEW

81 Limited or no visibility into ICS/OT network

54 lacked separate IT and OT user management systems

76 organizations could not detect Dragos' Red Team activities

90 incidents involved shared credentials for lateral movement

100 routable network connections into their operational environments

71 have poor security perimeters

66 adversaries directly accessing the ICS

A THREAT-BASED APPROACH

KYBERITE

CAPABILITIES

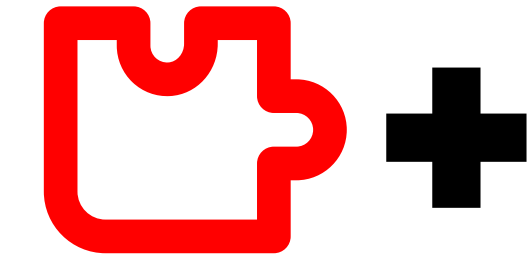
ICS Expertise, AV/EDR Evasion, PSExec, XOML Bypass, Fileless Execution

VICTIMOLOGY

Global ICS Assets

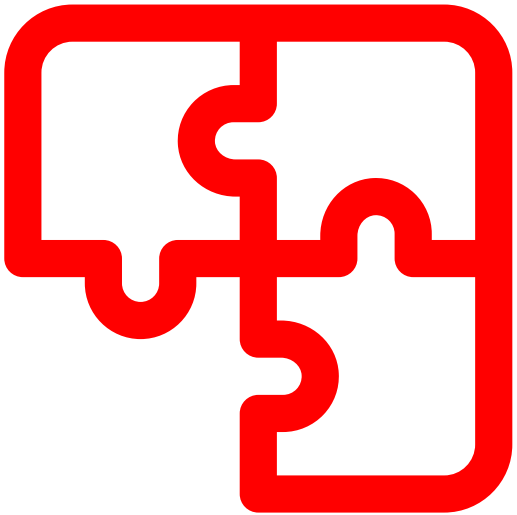
ICS SECURITY IS NOT ONE SIZE FITS ALL

TTPs



ATT&CK™

Environment



Windows?
Active Directory?
Security Controls?
Internet Accessible?
Industrial Vendor?
Firewall Rules?
Network Segments?

2019 TOP 5 ICS ASSESSMENT FINDINGS

1. FIREWALL RULES
2. ACCESS MANAGEMENT
3. HARDENING
4. LOGGING
5. NETWORK VISIBILITY

ICS FIREWALL RULES

WHAT WE SEE

- ICS Access from Corporate network
- Temporary rules
- Vendor solution dictated rules
- Vendor access rules

WHAT TO DO

- Use Firewall Browser and Identify: SSH, Telnet, Remote Desktop, VNC, WMI, PowerShell RM, RPC, SMB (PSEXEC)

CYBER RISK IMPACT

Reduce interactive protocol traversal points.

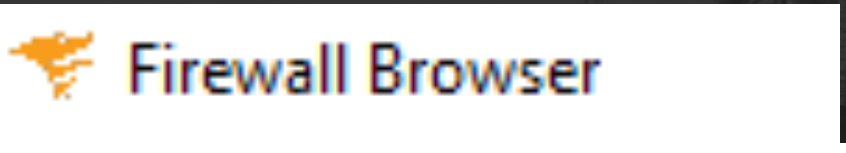
OPERATIONAL RISK

Medium – Verify firewall rule changes with ICS Vendors.

TOOLS REQUIRED

Solar Winds FREE Firewall Browser

FIREWALL BROWSER DEMO



Line No.	Source	Destination	Services	Action	ACL Name
1990	192.168.0.1/32	any	udp/snmp-snmptrap	accept	prod2-access
1991	192.168.0.1/32	any	udp/ntp	accept	prod2-access
1992	192.168.0.10		tcp/ftp-data-telnet	accept	prod2-access
1993	192.168.0.1/32		tcp/3389	accept	prod2-access
1994	192.168.0.1/32		tcp/3389	accept	prod2-access
1996		any	any	accept	prod2-access
1997		any	any	accept	prod2-access

ACCESS MANAGEMENT

WHAT WE SEE

- Domain Admins Galore
- Overprivileged Service Accounts
- Numerous Paths to Domain Admin

WHAT TO DO

- Download and Run BloodHound
- Review Paths to Admins
- Review Overprivileged Accounts

CYBER RISK IMPACT

Increase difficulties in gaining access to Domain Administrator accounts.

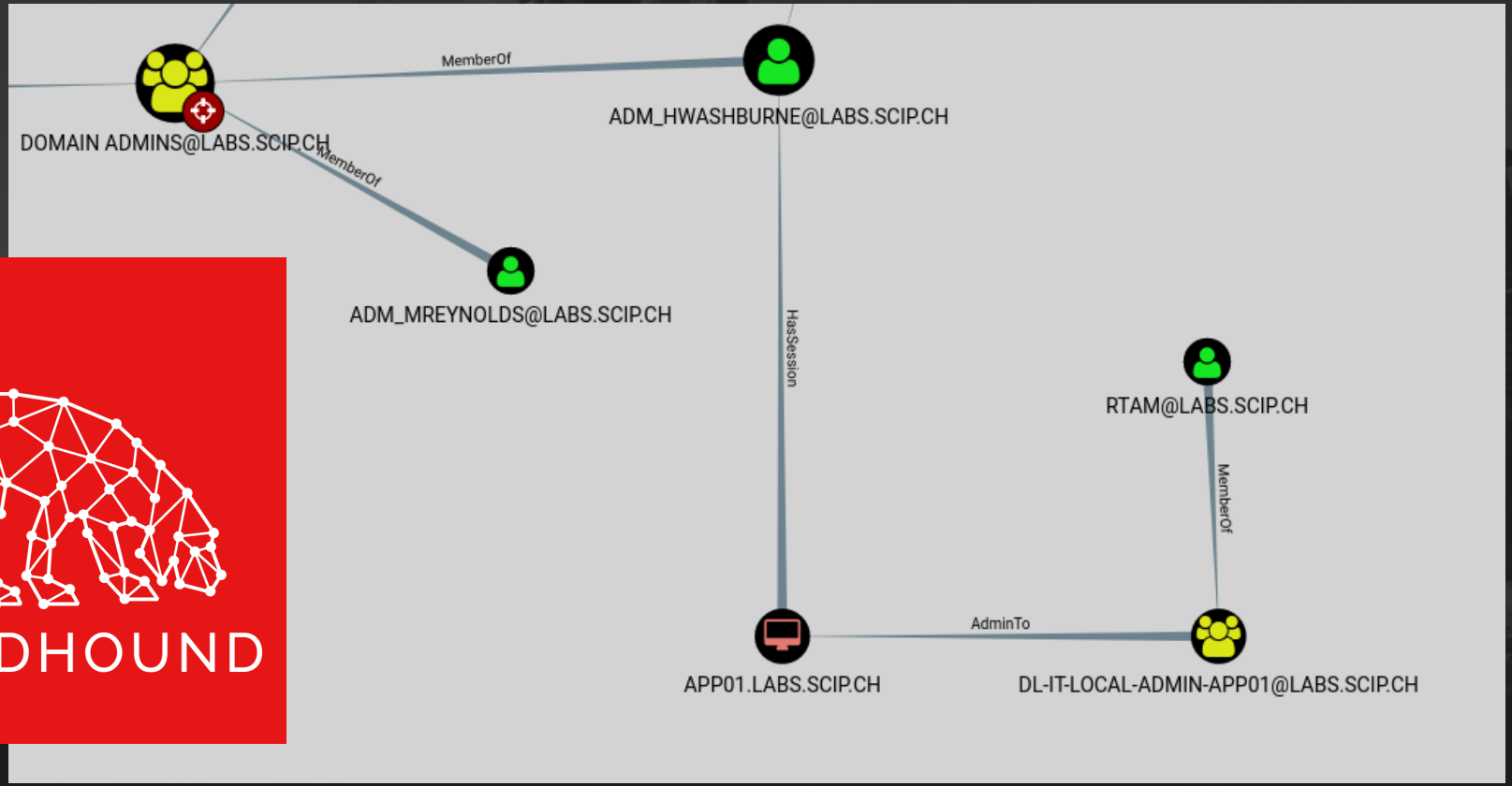
OPERATIONAL RISK

Very Low

TOOLS REQUIRED

Bloodhound, Active Directory Enum Script

BLOODHOUND DEMO



BLOODHOUND

ACCESS MANAGEMENT #2

WHAT WE SEE

- We almost always find Credentials
- We often find default Credentials
- We often find Credentials that are stored and not properly encrypted.

WHAT TO DO

- Understand where and how Credentials are stored.
- Implement Access Management.

CYBER RISK IMPACT

Increase the level of effort required to obtain credentials.

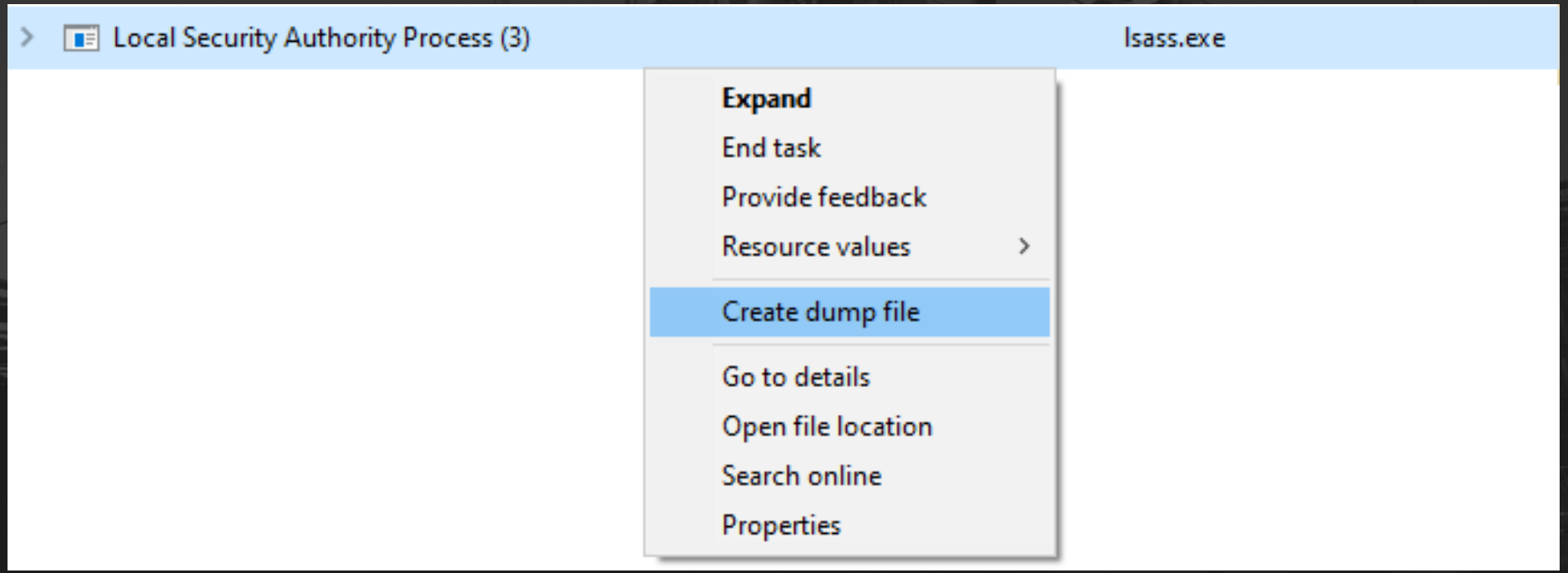
OPERATIONAL RISK

Very low

TOOLS REQUIRED

Session Gopher, LSASS Dump and Mimikatz, Mimikittenz, Nirsoft.net Password Utils

MIMIKATZ CREDENTIAL HUNT DEMO



MIMIKATZ CREDENTIAL HUNT DEMO

```
mimikatz(commandline) # sekurlsa::minidump c:\temp\lsass.dmp
Switch to MINIDUMP : 'c:\temp\lsass.dmp'

mimikatz(commandline) # sekurlsa::logonpasswords
Opening : 'c:\temp\lsass.dmp' file for minidump...

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : ADSDC02$
Domain            : ADSECLAB
Logon Server      : (null)
Logon Time        : 5/30/2015 10:14:48 PM
SID               : S-1-5-20
        msv :
         [00000003] Primary
         * Username : ADSDC02$
         * Domain   : ADSECLAB
         * NTLM     : ec2fa78dd1efe24d9780561f245c69c0
         * SHA1     : 48bbe93e4acc70bff740c717cf782b0f6c77653e
```

SESSION GOPHER CREDENTIAL HUNT DEMO

```
[+] Digging on WIN7-CLIENT01...
Microsoft Remote Desktop (RDP) Sessions


Source    : WIN7-CLIENT01\Bruce.Wayne
Hostname  : 10.181.73.202
Username  : CORP\Bruce.Wayne

Source    : WIN7-CLIENT01\Bruce.Wayne
Hostname  : dc01
Username  : CORP\ProfessorX

WinSCP Sessions


Source    : WIN-VV1VV5267KH\Brandon Arvanaghi
Session   : admin-anthony@198.273.212.334
Hostname  : 198.273.212.334
Username  : admin-anthony
Password  : Super*p@ssw0rd
```

HARDENING

WHAT WE SEE

- Common system hardening issues allow for hash reflecting, passing and clear-text password recovery.

WHAT TO DO

- Windows - Run CHAPS
- Linux - Run Linux Bash script

CYBER RISK IMPACT

Greatly increase the difficulty for adversaries to escalate privileges and move laterally.

OPERATIONAL RISK

Medium – Verify system hardening changes with ICS vendor.

TOOLS REQUIRED

- Configuration Hardening Assessment PowerShell Script (CHAPS)
- Microsoft Security Compliance Toolkit
- CIS tools
- STIG tools

CHAPS HARDENING DEMO

```
PS C:\CHAPS> . .\chaps.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\CHAPS\chaps.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (default is "D"): R


    Directory: C:\Users\0x00\AppData\Local\Temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        11/5/2019   6:54 AM                chaps-20191105-065441
[*] Start Date/Time: 20191105T06544201-05
[-] You do not have Administrator rights. Some checks will not succeed. Note warnings.
[*] Dumping System Info to seperate file\n
```

CHAPS HARDENING DEMO

[+] = TEST PASS

[-] = TEST FAIL

```
[*] Testing if WDigest is disabled.
[-] WDigest UseLogonCredential key does not exist.
[*] Testing if LLMNR is disabled.
[-] DNSClient.EnableMulticast is enabled:
[*] Testing if Computer Browser service is disabled.
[-] Computer Browser service is: Running
[*] Testing Lanman Authentication for NoLmHash.
[-] NoLmHash registry key is configured: 0
[*] Testing if PowerShell Version 2 is permitted
[-] PowerShell Version 2 is permitted.
```

LOGGING

WHAT WE SEE

- Not Logging the Right Stuff
- Lack of Centralized Logging

WHAT TO DO

- Run CHAPS
- Implement Centralized Logging
- Validate Event Logging

CYBER RISK IMPACT

Improve Threat Detection Capability
Improve Incident Response Capability

OPERATIONAL RISK

Low – Centralized logging can increase network traffic within ICS environment

TOOLS REQUIRED

Configuration Hardening Assessment PowerShell Script (CHAPS)

CHAPS WINDOWS EVENT LOG CONFIG DEMO

```
[*] Testing if PowerShell Moduling is Enabled
[-] EnableModuleLogging Is Not Set
[*] Testing if PowerShell EnableScriptBlockLogging is Enabled
[-] EnableScriptBlockLogging Is Not Set
[*] Testing if PowerShell EnableScriptBlockInvocationLogging is Enabled
[-] EnableScriptBlockInvocationLogging Is Not Set
[*] Testing if PowerShell EnableTranscripting is Enabled
[-] EnableTranscripting Is Not Set
[*] Testing if PowerShell EnableInvocationHeader is Enabled
[-] EnableInvocationHeader Is Not Set
[*] Testing if PowerShell ProtectedEventLogging is Enabled
[-] EnableProtectedEventLogging Is Not Set
[*] Event logs settings defaults are too small. Test that max sizes have been increased.
[x] Testing Microsoft-Windows-SMBServer/Audit log size failed.
[x] Testing Security log size failed.
[-] Microsoft-Windows-PowerShell/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-Pow
[-] Microsoft-Windows-TaskScheduler/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-
[-] Microsoft-Windows-WinRM/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-WinRM/Op
[-] Microsoft-Windows-Security-Netlogon/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Wind
[-] Microsoft-Windows-WMI-Activity/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-W
[-] Windows PowerShell max log size is smaller than System.Collections.Hashtable[Windows PowerShell] GB: 0.015 GB
[-] System max log size is smaller than System.Collections.Hashtable[System] GB: 0.02 GB
[-] Application max log size is smaller than System.Collections.Hashtable[Application] GB: 0.02 GB
[-] Microsoft-Windows-TerminalServices-LocalSessionManager/Operational max log size is smaller than System.Collections.Hasht
```

NETWORK VISIBILITY

WHAT WE SEE

- Operate in ICS networks undetected
- Maintain perpetual access
- Do not know what is on networks

WHAT TO DO

- Identify SPAN ports for monitoring
- Create procedure for collecting network packet captures
- Use a free tool to view them

CYBER RISK IMPACT

Improve Threat Detection Capability
Improve Threat Hunting Capability
Improve Incident Response Capability

OPERATIONAL RISK

Low – Connecting to SPAN ports is nonroutable – BUT CPU usage of switches should be monitored.

TOOLS REQUIRED

Dragos Community Tools
Network Miner - $$

Two Free (FOREVER) Community ICS Network Visibility Products from Dragos

The Dragos Platform

ICS CYBERSECURITY *RAPID* SELF-CHECK

Take ownership of understanding Cyber Risk in your environment.

OPERATIONALIZED RAPID SELF-CHECK


THANK YOU
DRAGOS

Adversary OSINT Collection Threats

Casey Brooks, Senior Adversary Hunter

Table of Contents

OSINT Collection Risk Assessment

OSINT Collection Risk and Vulnerability Matrix	Information is of Low Relevance/Importance for Intelligence Collection	Information is of Medium Relevance/Importance for Intelligence Collection	Information is of High Relevance/Importance for Intelligence Collection
Adversary utilization requires little to no analytical effort for operational integration.	2	3	3
Adversary utilization requires moderate to specialized analytical effort for operational integration.	1	2	3
Adversary utilization requires highly technical analytical effort for operational integration.	1	2	2

XENOTIME Accessed Documents

Victim-provided links to the following documents accessed by XENOTIME:

- System Separation Incident.pdf
- Trip of 275kV No1 Busbar.pdf
- A CSV that contained information about generator locations, production, etc.

System Separation Incident.pdf

- This document offers an end-to-end summary of an incident and how the grid reacted to unexpected stimulus.

- This information is invaluable to attackers because it sheds light on how the system reacts to an event impacting grid stability, how the victim and their constituency reacts to an islanding event, and how to affect the overall National Electricity Market (NEM).

- By seeing the production of each region and the flow between them at the time of Under Frequency Load Shedding (UFLS) rebalancing, attackers can piece together which interconnects are most vital and how much load will need to be shed to achieve a disruption event.

Trip of 275kV No1.pdf

- This document is valuable to an adversary because it is an engineering diagram of the substation.
- This is the information sophisticated attackers look for during target development, especially in military operations, because of its detailed nature.
- The company that is doing the work and owns the substation (Powerlink) is disclosed publicly, giving an adversary a target.
- Recreating the event in a cybersecurity manner may lead to cognitive biases (i.e. the assumption the event was mechanical) that would lead restoration teams to possibly overlook cyber as a cause.

Generators.csv

- A list of generation stations and renewables can be easily graphed to build a picture of the Australian grid system.
- Latitude and longitude locations are provided along with the amount of possible power generation, ramp up/down numbers, and fuel type that can provide attackers with useful data to plan scenarios.
- An attacker can incorporate this information with real-life documented incidents (like the SA separation event) to create a model for generation/demand and start exploring scenarios for creating islanding events.

OSINT Collection Risk Assessment

Document	Risk Assessment	Explanation
Preliminary report Qld SA System Separation 25 August 2018.pdf	3	Document has high value and relevance for adversary collection and requires specialized analytical effort for intelligence value for the adversary.
Trip of Wurdong 275kV No1 Busbar on 14 June 2018.pdf	3	Document has a high value and relevance for adversary collection and requires specialized analytical effort for intelligence value for the adversary.
Generators.csv	3	Document has a high value and relevance for adversary collection and requires specialized analytical effort for intelligence value for the adversary.
Map visualizations page	3	Webpage has a high value and relevance for adversary collection and requires specialized analytical effort for intelligence value for the adversary.
Realtime-outages.csv	3	Document has a high value and relevance for adversary collection and requires specialized analytical effort for intelligence value for the adversary.

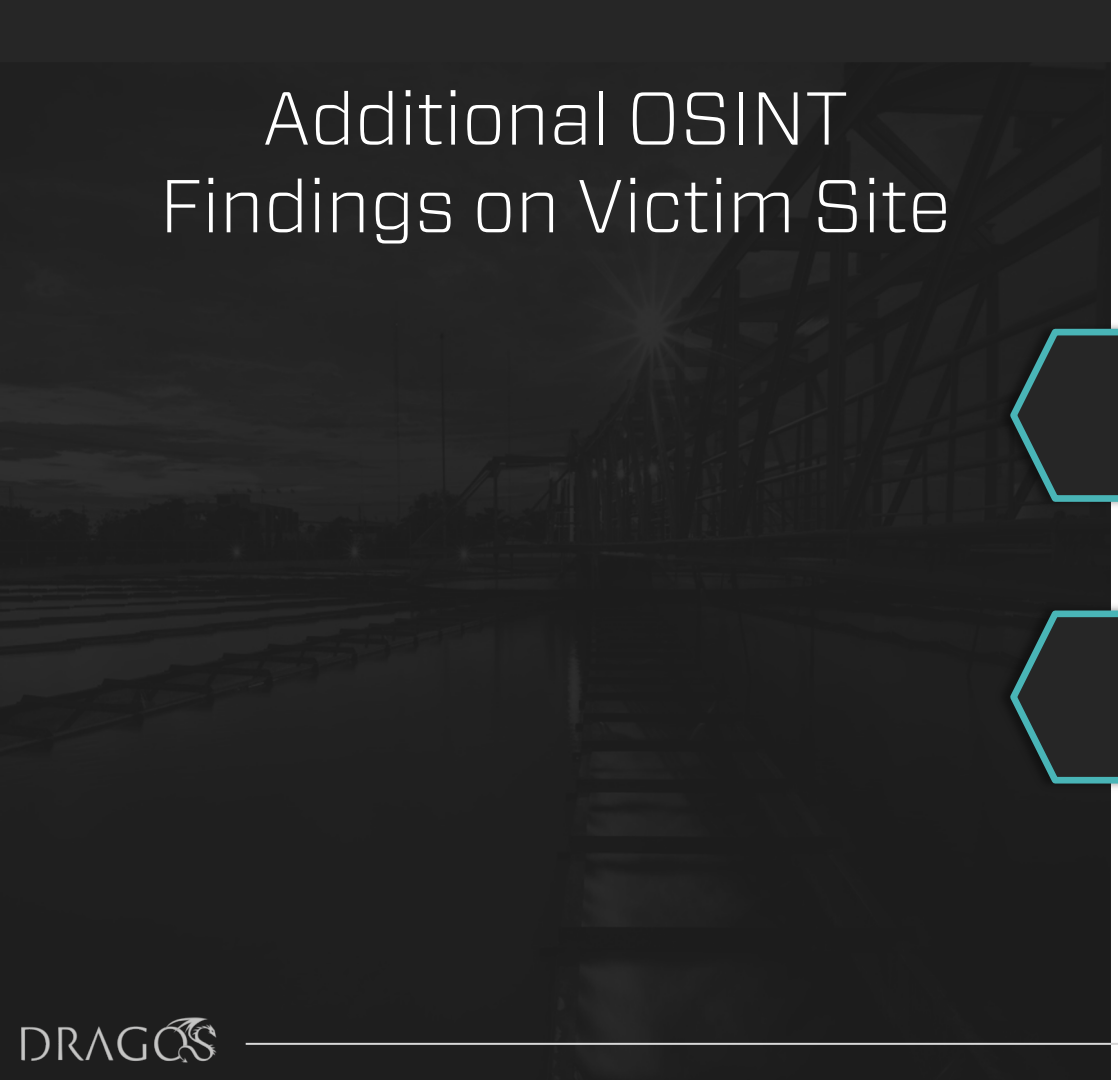
OSINT Collection Risk Assessment

Document	Risk Assessment	Explanation
Generation_Scheduled_Capacities.csv	2	Document has a high relevance for collection but requires highly technical analytical effort to operationalize the information for XENOTIME operations.
Generation_Summary.csv	2	Document has a high relevance for collection but requires highly technical analytical effort to operationalize the information for XENOTIME operations.
PoC Industry Management Plan – Risk and Issues.pdf	1	Document has little value and relevance for adversary collection and requires little analytical effort for intelligence value for the adversary.
WEB_STTM_PRICE_AND_DEMAND.csv	1	Document has little to no operational or intelligence value to the adversary and would require specialized analytical effort for intelligence value

ICS Impact

Dragos assesses with medium confidence XENOTIME collected AEMO-related material related to energy production and energy production facility locations to plan disruptions, enable targeting for attacks, and predict defender response to disruptions enabling them to increase the scale and length of an attack.

Additional OSINT Findings on Victim Site



- Realtime-outages.csv
- Map visualizations page-

Realtime-outages.csv

RECONNAISSANCE

Dragos performed additional reconnaissance on the AEMO website and identified a page for Real Time Outages in Western Australia.

SITE

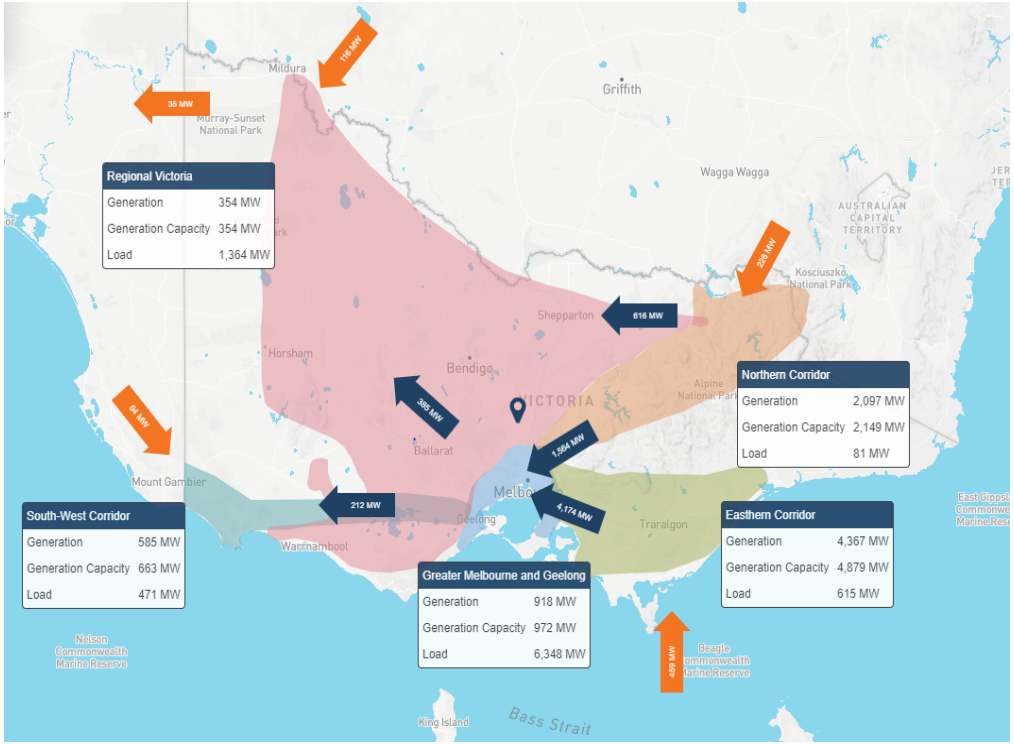
The site provides useful documents and explanations. The outage document contains information about the actual causes for the outage and remediation steps.

ATTACK

An attacker could use this data to sync a cyber-enabled event with a real world one, making response difficult and possibly causing conflation of issues.

Map visualizations page-

- A prime example is the VAPR overlay.
- The map contains historical information, including an overlay for “maximum demand” that yields detailed map and power flow data sets.



Attack Scenarios

- Disruption Event
- Power Price Manipulations
- Tangential Targeting

Disruption Event

- An attacker could recreate a frequency disruption event by mimicking the QLD/SA separation event and use the visualization maps to find each hop along the line. In this case, compromising a substation in the SWQ or NNS regions could begin replication of the event.
- Additional modeling should be done in respect to natural events.
- Each area of operation/territory poses different challenges and risk ratings.

Power Price Manipulation

- During islanding events, power prices can fall or surge to abnormal levels.
- If these events are not rectified quickly and reliability re-established, a wholesale power producer in a power-needy region could make substantial profits if they are able to increase to meet demands.

Tangential Targeting

- Companies could be used for a follow-on objective of disrupting an operation.
- Australia is home to four different aluminum smelters, concentrated in Eastern and Southern Australia.

Recommendations

MONITOR

Enable monitoring and logging of indicators where possible to identify XENOTIME reconnaissance activity.

AUTHENTICATE

Ensure that information about operations requires an authentication gateway to prevent automated scraping of webpages.

IDENTIFY

Identify information collected by the adversary, assess its potential use for adversary operations, and document for historical reference.

MODEL

Model and practice adversarial actions against response plans during disruption.

Conclusion

ASSESSMENT

Dragos assesses that the reconnaissance activity conducted by XENOTIME was likely early information gathering in the adversary's planning stages.

Asset owners and operators should review public information for attack enablement potential.

Information that is a requirement for public disclosure by policy, either corporate or governmental, should be determined if it is a necessity

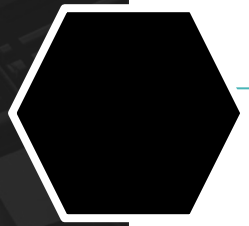
XENOTIME

The information gathered by XENOTIME provides valuable information for targeting electrical facilities operated by AEMO and gives insight about response actions.


THANK YOU
DRAGOS


DRAGOS
INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY
VISIBILITY. DETECTION. RESPONSE.

The Past and Future of Ransomware in Industrial Environments



Joe Slowik

Principal Adversary Hunter

WHOAMI

AGENDA

- ❑ Ransomware Overview
- ❑ Worms and Spreading
- ❑ Industrial Targeting
- ❑ State-Sponsored Ransomware

RANSOMWARE DEFINED

HISTORY

LEXICO

Powered by OXFORD

US DICTIONARY ransomware

Home › US English › ransomware

Definition of ransomware in English:

ransomware

Pronunciation /ˈransəmˌwer/ /ˈrænsəmˌwɛr/

NOUN

A type of malicious software designed to block access to a computer system until a sum of money is paid.

'although ransomware is usually aimed at individuals, it's only a matter of time before business is targeted as well'

+ More example sentences

OLDER THAN YOU THINK

HISTORY

Popular Latest

The Atlantic

TECHNOLOGY

The Computer Virus That Haunted Early AIDS Researchers

The first-ever ransomware attack was delivered on a floppy disk.

KAVEH WADDELL MAY 10, 2016

MORE STO

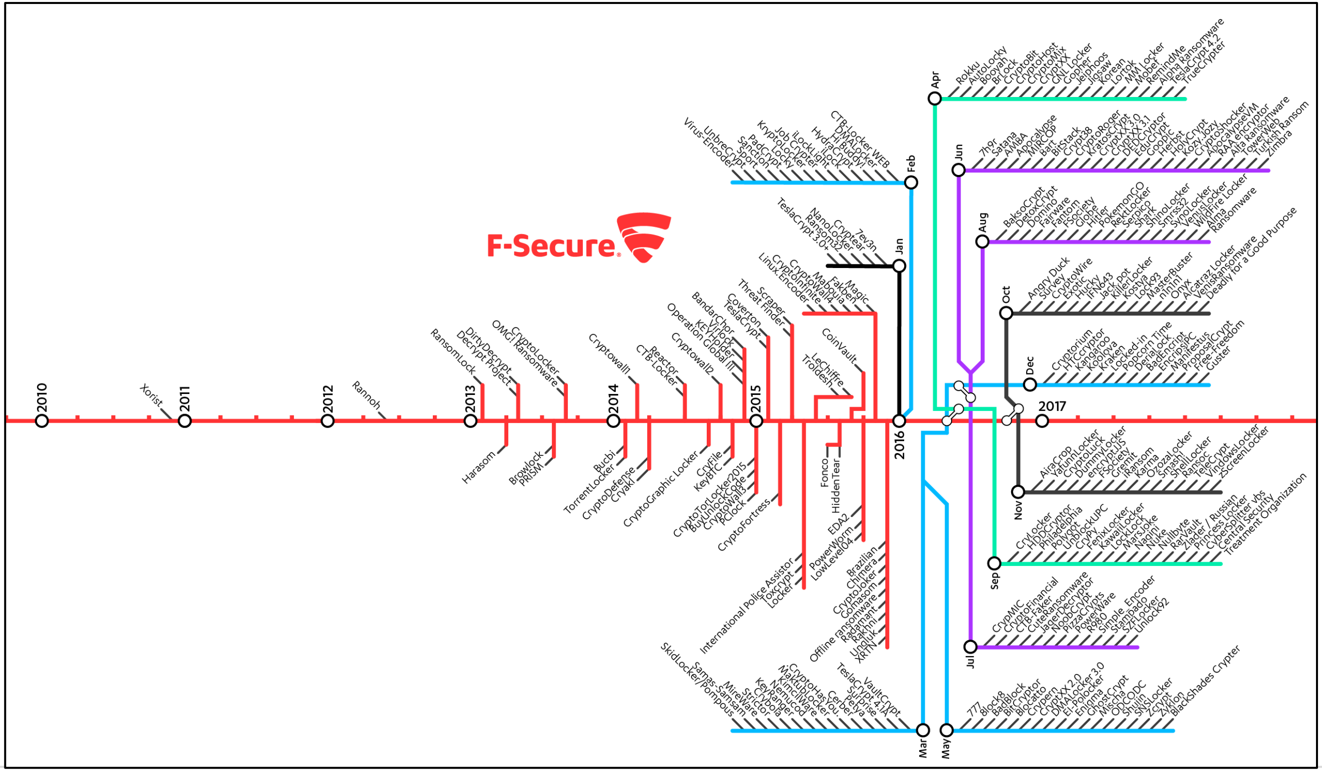
How to Murder H

KAITLYN TIFFANY

'Pure Poison' for a Career

RANSOMWARE PROLIFERATION

HISTORY



BEHAVIORAL SHIFTS OVER TIME

SPREADING

Pre-2017

- Primary targeting via phishing, malicious websites
- Single victim, single machine focus

2017-2018

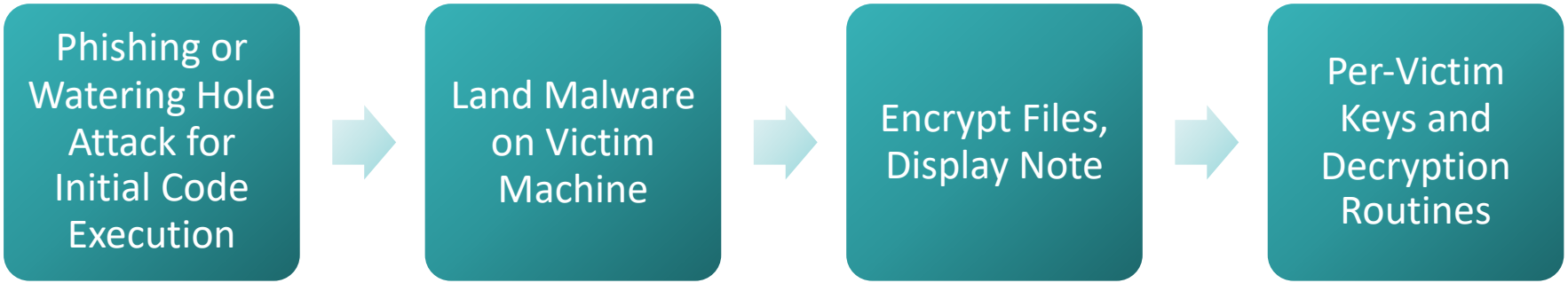
- Rise of the worms: MS17-010, dynamic credential capture
- Single victim machine, opportunistic targeting

2018-Present

- Interactive operations to attack corporate networks
- Hold entire networks hostage

PER-USER TARGETING

SPREADING



RISE OF THE WORMS

SPREADING

https://images.theconversation.com/files/169334/original/file-20170515-6987-lw7ou2.png?ixlib=rb-1.1.0&q=45&auto=format&w=926&fit=clip

RISE OF THE WORMS

SPREADING

MS17-010 Vulnerability

Hybrid Credential Re-Use + MS17-010

Pure Credential Capture and Replay

NETWORK-WIDE ATTACKS

SPREADING

CROWDSTRIKE | BLOG

Featured

Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware

January 10, 2019 Alexander Hanel Research & Threat Intel

BLEEPINGCOMPUTER

Search Site

NEWS DOWNLOADS VIRUS REMOVAL GUIDES TUTORIALS DEALS

Home > News > Security > New LockerGoga Ransomware Allegedly Used in Altran Attack

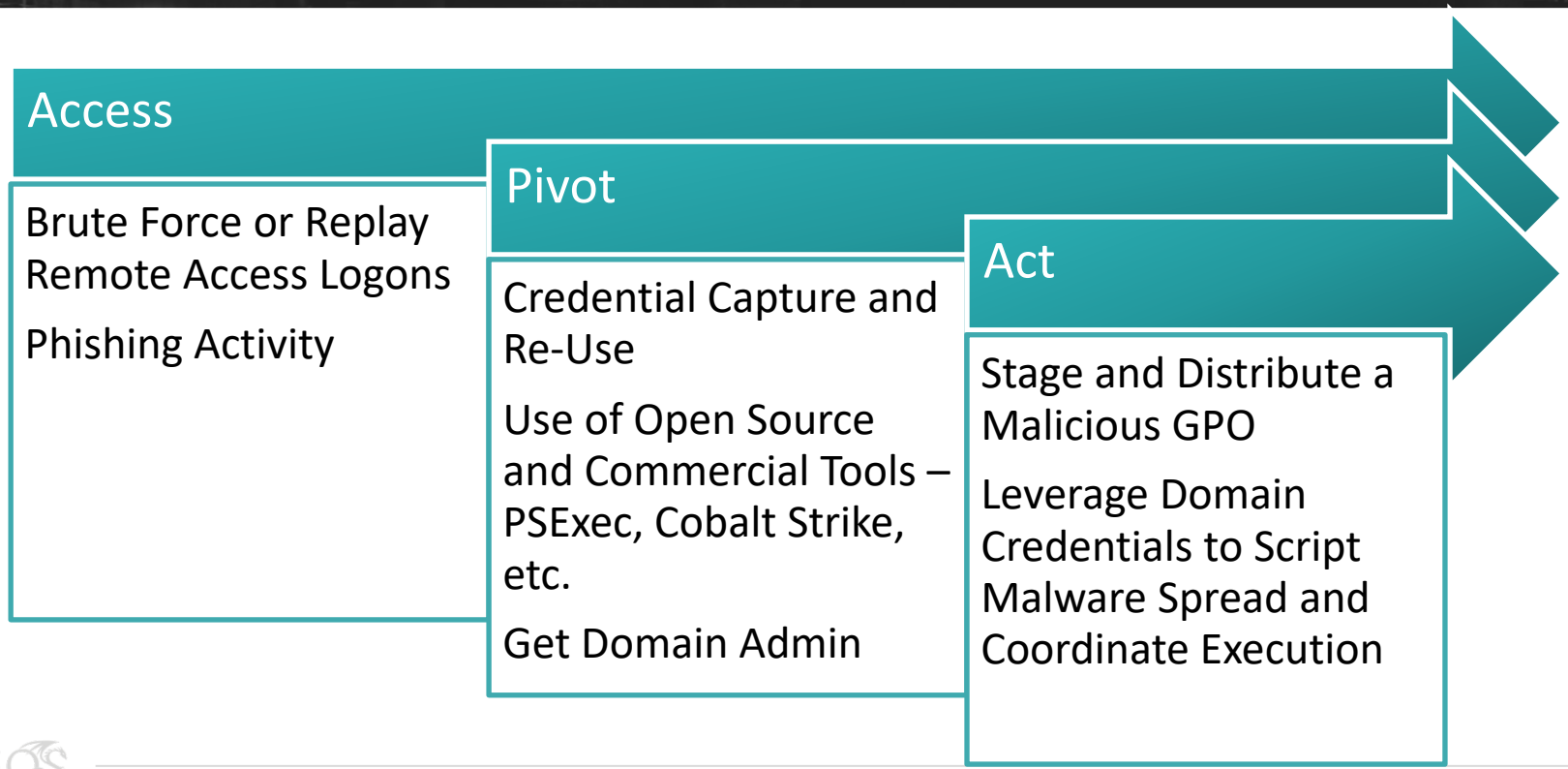
New LockerGoga Ransomware Allegedly Used in Altran Attack

By Ionut Ilascu January 30, 2019 03:03 AM 2

Hackers have infected the systems of Altran Technologies with malware that spread through the company network, affecting operations in some European countries. To protect client data and their own assets, Altran decided to shut down its network and applications.

THE NEW NORMAL

SPREADING



INCREASED INDUSTRIAL TARGETING

INDUSTRIAL

EKANS Ransomware and ICS Operations

Feb 3, 2020 | Blog, Industry News

Dragos Professional Services and the Dragos Platform regularly detect and respond to ransomware

NNT
SECURITY THROUGH SYSTEM INTEGRITY

Products | Solutions | Services | Re:

NNT ▸ Products ▸ Change Tracker™ Gen7 R2 ▸ Blog ▸ NotPetya Attack Disrupts Merck's Q2 Global

NOTPETYA ATTACK DISRUPTS MERCK'S Q2 GLOBAL OPERATIONS

Category: Change Tracker Enterprise

Pharmaceutical manufacturer, Merck, has revealed in its financial summary for the second quarter of 2017 that a devastating cyber-attack has disturbed its global operations, including manufacturing, research, and sales.

The attack in particular was not detailed, but it's believed the attack in reference is the NotPetya malware attack that took place in June. The **NotPetya** malware outbreak impacted tens of thousands of victims across 65 different countries, targeting massive organizations like the Ukraine's central bank, WPP, DLA Piper, and AP Moller-Maersk.

PROGRESSION OF INDUSTRIAL ATTACKS

INDUSTRIAL

CHANGE IN INDUSTRY TARGETING

INDUSTRIAL

2018-2019	• Focus on Manufacturing • LockerGoga, Ryuk, MegaCortex
2019-2020	• Shift to Increasing Oil & Gas Operations • Events in US, Mexico, Persian Gulf
2020-Present	• Continued Manufacturing, Addition of Electric Utilities • Multiple Phases of Operations Targeted • Risk Appetite Appears to Have Increased

UTILITY-TARGETED RANSOMWARE

INDUSTRIAL

CBC | MENU

COVID-19 Local updates Live video COVID-19 tracker Subscribe to newsletter

NEWS Top Stories Local The National Opinion World Canad

North

NTPC confirms 'cyber attack' from unknown source on Thursday, RCMP investigating

Northwest Territories Power Corporation website and email servi temporarily

Walter Strong · CBC News · Posted: Apr 30, 2020 5:32 PM CT | Last Updated: May 1

```
Hi!
Your files are encrypted by Netwalker.
All encrypted files for this computer has extension: .7469d7

--
If for some reason you read this text before the encryption
this can be understood by the fact that the computer slows d
and your heart rate has increased due to the ability to turn
then we recommend that you move away from the computer and a
Rebooting/shutdown will cause you to lose files without the
```

SC MEDIA UK | SC US — The Cyber-Security source

HOME | NEWS & FEATURES | BUYER'S GUIDE | OPINION | EVENTS | EXPERT REPORTS

Snake ransomware attack hits power company Enel Group

Jun 12, 2020
NEWS by Andrew McCorkell

The Enel Group was hit by a ransomware attack from EKANS (SNAKE) ransomware operators that affected its internal network, according to reports.

PEi POWER ENGINEERING INTERNATIONAL

Industry Sectors Regions Resources Magazine Events Engage Newsletter Part

Digitalization Cybersecurity World Regions Europe News

Energy giant EDP hit with costly ransomware attack

April 17, 2020 · 0

PROCESS-TARGETING RANSOMWARE

INDUSTRIAL

Most-Important Industrial Processes are Constantly Running – So Dependent Files are Programmatically Locked

Encrypting Vital Files – Historian Records, License Keys, Etc. – Requires Removing File Locks

Since 2019, Multiple Malware Families have Integrated Process Termination to Extend Encryption in Industrial-Specific Contexts

PROCESS-TARGETING RANSOMWARE

INDUSTRIAL

FIREEYE

Solutions Services Customers

Home > FireEye Blogs > Threat Research > **Ransomware Against the Machine: How Adversaries ar...**

Threat Research

Ransomware Against the Machine: How Adversarie Learning to Disrupt Industrial Production by Targe and OT

February 24, 2020 | by Daniel Kapellmann Zafra, Keith Lunden, Nathan Brubaker, Jeremy Kennelly

RANSOMWARE ICS CYBERCRIME

Since at least 2017, there has been a significant increase in public disclosures of ransomware incident industrial production and critical infrastructure organizations. Well-known ransomware families like V LockerGoga, MegaCortex, Ryuk, Maze, and now SNAKEHOSE (a.k.a. Snake / Ekans), have cost victim variety of industry verticals many millions of dollars in ransom and collateral costs. These incidents h resulted in significant disruptions and delays to the physical processes that enable organizations to p deliver goods and services.

CYBER ADVISORY

Technical Analysis of **MegaCortex Version 2** Ransomware

accenturesecurity

EKANS Ransomware and ICS Operations

Feb 3, 2020 | Blog, Industry News

Dragos Professional Services and the Dragos Platform regularly detect and respond to ransomware

PROCESS-TARGETING RANSOMWARE

INDUSTRIAL

```
taskkill /im wrsa.exe /f
taskkill /im lmon.exe /f
net stop TPVCGateway /y
taskkill /im dwrcst.exe /f
taskkill /im rasupd.exe /f
taskkill /im kis.exe /f
sc config MSSQLFDLauncher$SYSTEM_BGC start= disabled
sc config MSSQLSERVER start= disabled
sc config mozyprobackup start= disabled
taskkill /im bdagent.exe /f
sc config EPProtectedService start= disable
taskkill /im mcsvhost.exe /f
taskkill /im macmnsvc.exe /f
taskkill /im trjscan.exe /f
taskkill /im coreframeworkhost.exe /f
taskkill /im ehttpsrv.exe /f
sc config sacsvr start= disabled
sc config MSOLAP$TPS start= disabled
taskkill /im console.exe /f
taskkill /im cappactiveprotection.exe /f
taskkill /im proficyclient.exe4 /f
taskkill /im zillya.exe /f
taskkill /im proficysts.exe /f
sc config VeeamRESTSvc start= disabled
net stop VeeamBrokerSvc /y
sc config epag start= disable
taskkill /im dwnetfilter.exe /f
taskkill /im nd2svc.exe /f
```

RANSOMWARE AS WIPER

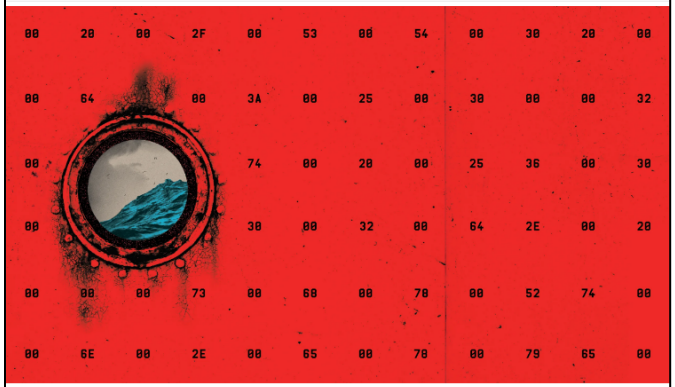
WIPER

Ransomware is inherently disruptive – can this be used to hide deliberate destruction?

NOTPETYA AND SANDWORM

WIPER

WIRED BUSINESS CULTURE GEAR MORE SIGN IN SUBSCRIBE



MIKE MCQUADE

ANDY GREENBERG SECURITY 08.22.2018 05:00 AM

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

STATEMENTS & RELEASES

Statement from the Press Secretary

FOREIGN POLICY | Issued on: February 15, 2018

★ ★ ★

In June 2017, the Russian military launched the most destructive and costly cyber-attack in history.

The attack, dubbed "NotPetya," quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. It was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences.

NOTPETYA FAILURES

WIPER

- Likely Spread too Far, Collateral Damage
- NotPetya not a Credible Ransomware Example
- Unmasked as State-Directed Disruption Operation

NOTPETYA REVISED

WIPER

More Plausible Encryption Method

- Possibility of recovery exists
- More authentic ransomware behavior

More Focused Spreading Mechanism

- Initial delivery via MEDoc resulted in unexpected victims
- Subsequent spreading produced significant collateral damage

Evade Attribution

- Better ‘blending in’ produces plausible deniability
- Avoids possible repercussions, responses

LOCKERGOGA AND NORSK HYDRO

WIPER

WEDNESDAY, MARCH 20, 2019

Ransomware or Wiper? LockerGoga Straddles the Line

EXECUTIVE SUMMARY

Ransomware attacks have been in the news with increased frequency over the past few years. This type of malware can be extremely disruptive and even cause operational impacts in critical systems that may be infected. LockerGoga is yet another example of this sort of malware. It is a ransomware variant that, while lacking in sophistication, can still cause extensive damage when leveraged against

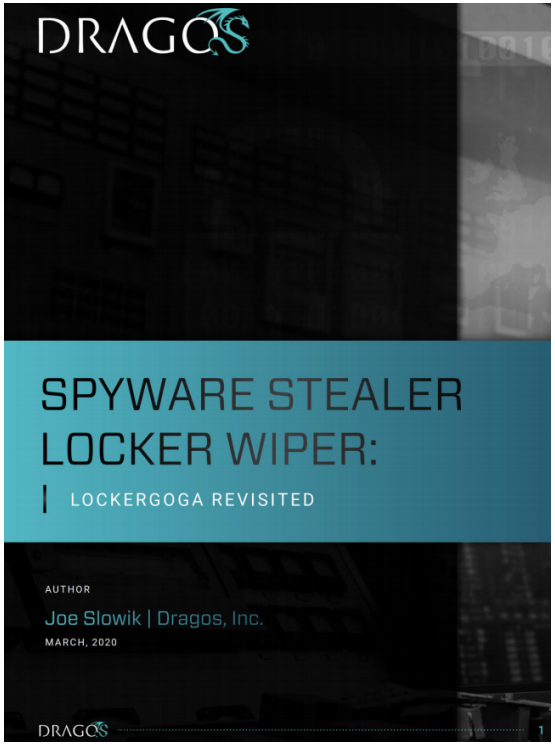
threatpost

ASUS Patches Live Update Bug That Allowed APT to Infect Thou... Cybercriminals Hav...

Ransomware Behind Norsk Hydro Attack Takes On Wiper-Like Capabilities

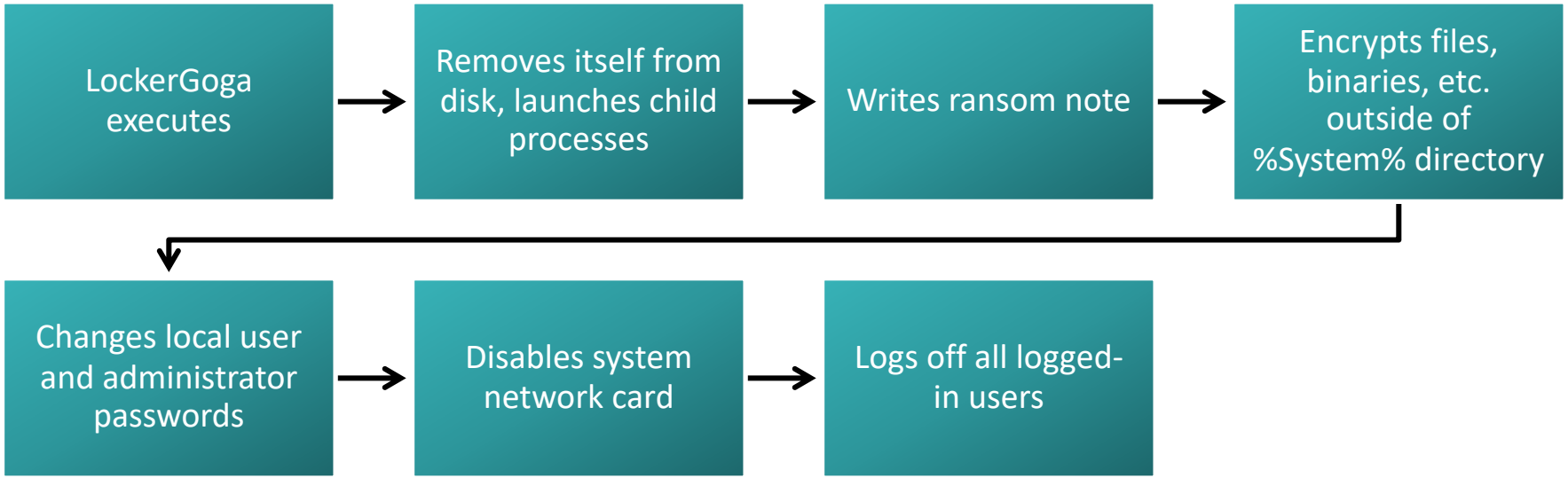
LOCKERGOGA AND NORSK HYDRO

WIPER



LOCKERGOGA AND NORSK HYDRO

WIPER



LOCKERGOGA SINCE HYDRO

WIPER

No Publicly-Identified LockerGoga Incidents since Norsk Hydro

Analysis and Government Reporting Indicates other Norwegian Entities likely Targeted for Roughly Simultaneous Effect

Although Investigations are Ongoing in Multiple Countries, no Criminal Charges or Suspects At this Time

WINNTI AND COLDLOCK

WIPER

TREND MICRO | SECURITY INTELLIGENCE Blog
SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

Home | Categories

Home » Malware » Targeted Ransomware Attack Hits Taiwanese Organizations

Targeted Ransomware Attack Hits Taiwanese Organizations

Posted on: May 6, 2020 at 5:00 am **Posted in:** Malware **Author:** Trend Micro

Updated on May 6, 2020, 7:20 Pacific Time with further details regarding directories targeted for encryption.

A new targeted attack has infected several organizations in Taiwan with a new ransomware family, which we have dubbed ColdLock. This attack is potentially destructive as the ransomware appears to target databases and email servers for encryption.

The information we gathered indicates that this attack started hitting organizations in early May. Analysis of the malware points to similarities between ColdLock and two previously known ransomware families, specifically Lockergoga, Freezing, and the EDA2 "educational" ransomware kit. There have been no indications that this attack has hit any other organization outside of

TAIPEI 台北時報 TIMES

Front Page | Taiwan News | Business | Editorials | Sports | World News | Features

Home / Taiwan News

Sun, May 17, 2020 page2

Bureau names ransomware culprits

Staff writer, with CNA

Hackers known as the Winnti Group were behind ransomware attacks on Taiwan's two largest fuel suppliers, the Ministry of Justice Investigation Bureau said on Friday, adding that similar attacks on 10 domestic companies are likely in the next few days.

On May 4, state-run CPC Corp, Taiwan announced that its computer system had been infected with ransomware, causing payment issues at gas stations.

Formosa Petrochemical Corp reported similar issues the following day, and shut down its computer systems.

Powertech Technology Inc, a Hsinchu-based semiconductor firm, also reported a ransomware attack on May 5.

Mos

1 Pe pe

2 U

3 Mi ex

4 Ja

5 M

COLDLOCK PROFILE

WIPER

Specific Execution Profile with Timing Cues, Reflective Loading

Extends Encryption through Database and Email Targeting

But Scattershot Directory and File Selection for Encryption

COLDLOCK PROFILE

WIPER

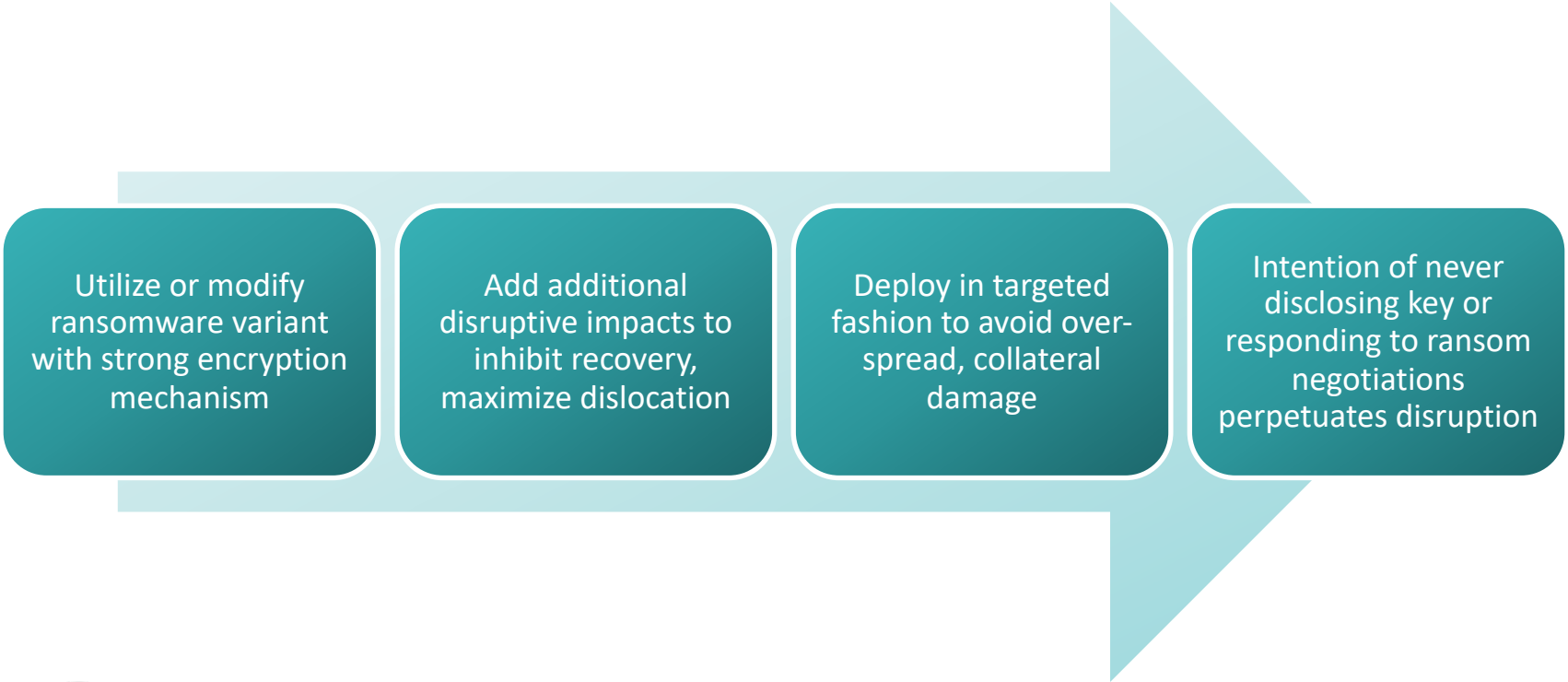
All Known ColdLock Victims are in Taiwan

Victims Included Only Oil Refining and Distribution Companies in Taiwan, Taiwan Chip Sector

ColdLock Has Not Been Seen Since Taiwan Events

RANSOMWARE AS CYBERWEAPON

WIPER



RANSOMWARE ADVANTAGES

WIPER

Plausible Deniability

Effective Disruption

Blends in to 'Criminal' Behavior

Tools Available for Purchase, Modification

No Need to Disclose Sensitive Capabilities

DEFENSE AND DETECTION

- Standard ransomware defense still applies
- Need to identify mechanisms to facilitate information sharing
- Greater law enforcement efforts against criminal ransomware can reduce the scope for state-sponsored entities to mimic

REFERENCES AND RESOURCES

- The Computer Virus that Haunted Early AIDS Reearchers – Kaveh Waddell, The Atlantic (https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/)
- State of Cyber Security 2017 – F-Secure (https://www.f-secure.com/documents/996508/1030743/cyber-security-report-2017)
- ExPetr/Petya/NotPetya is a wiper, Not Ransomware – Anton Ivanov & Orkhan Mamedov, Kaspersky (https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/)
- Petya.2017 is a Wiper not A Ransomware – Matt Suiche, Comae (https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b)
- Spyware, Stealer, Locker, Wiper: LockerGoga Revisited – Joe Slowik, Dragos (https://dragos.com/resource/spyware-stealer-locker-wiper-lockergoga-revisited/)


THANK YOU
DRAGOS

INDUSTRIAL THREAT HUNTING

JULIAN GUTMANIS

PRINCIPAL INDUSTRIAL INCIDENT RESPONDER

Western Australia Based

@Dragos ~18 months

Ex-Saudi Aramco, Ex-San Diego Gas & Electric

Background and Collateral

- Dragos provides a 5 day course in Assessing and Defending ICS. **One full day** is dedicated to Threat Hunting.

- Great background material on Dragos' website: https://www.dragos.com/white-papers/
  - Hunting with Rigor (Dan Gunter)
  - Collection Management Frameworks (Rob M. Lee, Ben Miller, Mark Stacey)
  - Four Types of Threat Detection (Sergio Caltagirone, Rob Lee)
  - Mapping Industrial Threats to ATT&CK for ICS
  - Generating Hypothesis for Successful Threat Hunting (Rob M. Lee, David Bianco)

Homework

- Threat hunting is beneficial in all stages of maturity, however **preparation will make you more successful**
  - Understand your **operations**
  - Understand your **architecture**
  - Obtain visibility into your **assets**
  - Identify **collection points and log sources**
    - https://www.dragos.com/resource/collection-management-frameworks-beyond-asset-inventories-for-preparing-for-and-responding-to-cyber-threats/
  - Gain **trust**

Threat Hunting

“A focused and iterative approach to searching out, identifying and understanding adversaries internal to the defender’s networks.”

Hunt to: Reduce our ‘friction’ and increase the adversaries ‘friction’

When to Hunt

- What is the catalyst for the hunt?
  - Periodic
  - Intelligence Initiated
  - Neighbour Network Events
  - Vendors / Third-party Events
  - Operations Events

Adding Structure: Threat Hunt Model

Purpose: Goals, Objectives, Outcomes

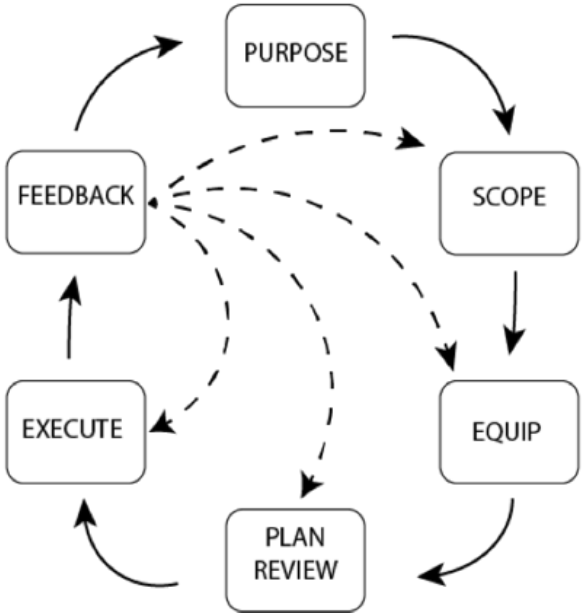
Scope: Location, Hypothesis Generation

Equip: Collection Management Framework, Resource Allocation

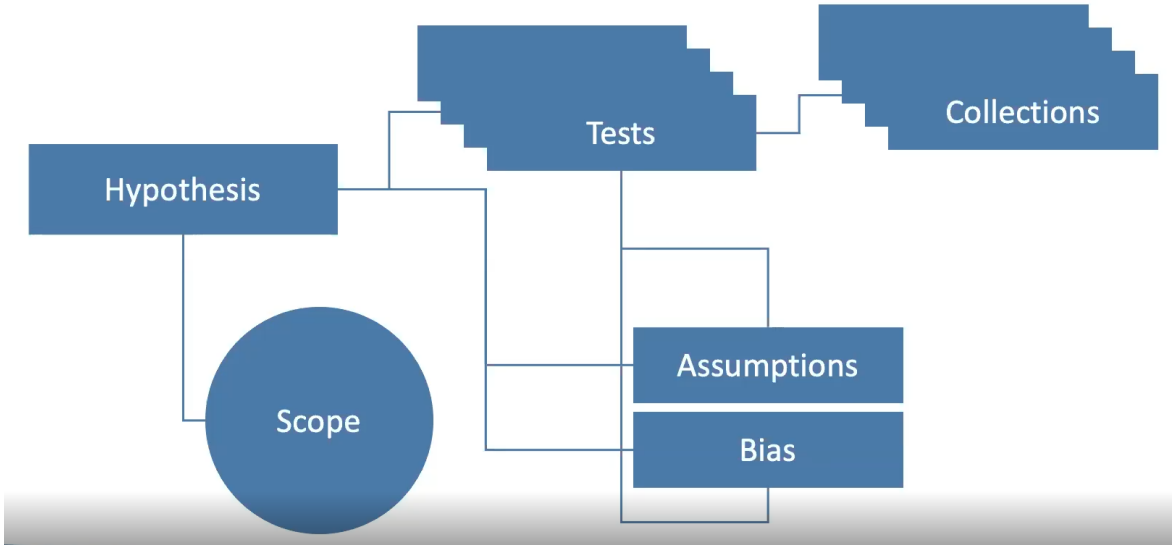
Plan Review: Final Checks

Execute: Do the Hunt!

Feedback: "How can we improve / automate / become more efficient?"

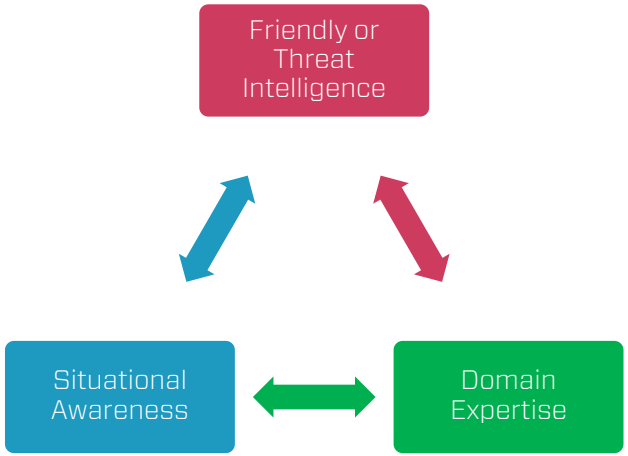


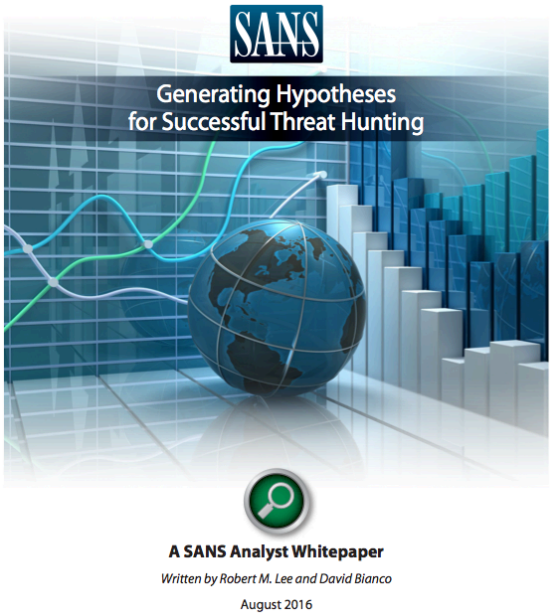
Make it actionable



Generating hypotheses

Hypotheses can be categorized into one or more of three methods:





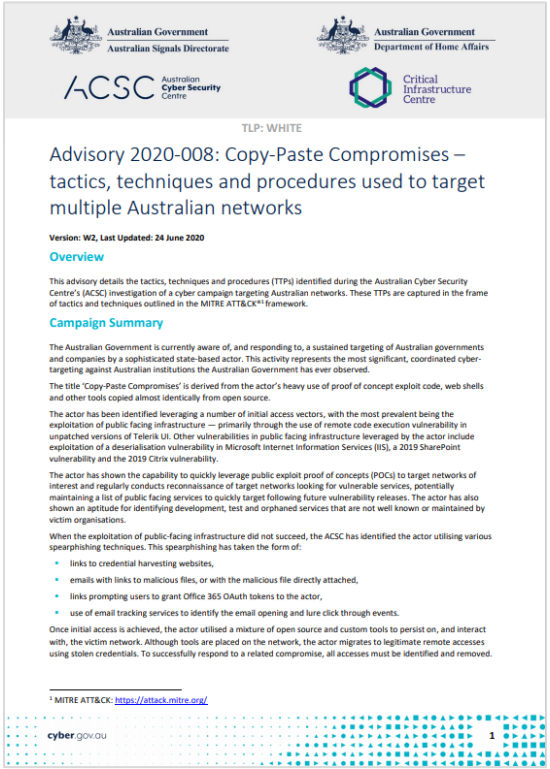
https://www.sans.org/reading-room/whitepapers/threats/generating-hypotheses-successful-threat-hunting-37172


INTEL DRIVEN HYPOTHESES
DRAGOS

Intel Driven Hypothesis

- “Awareness of threat intelligence, the use of indicators of compromise (**IOCs**) and knowledge of adversary tactics, techniques and procedures (**TTPs**)”

In Recent News



Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government
Department of Home Affairs

Critical Infrastructure Centre

TLP: WHITE

Advisory 2020-008: Copy-Paste Compromises – tactics, techniques and procedures used to target multiple Australian networks

Version: W2, Last Updated: 24 June 2020

Overview

This advisory details the tactics, techniques and procedures (TTPs) identified during the Australian Cyber Security Centre's (ACSC) investigation of a cyber campaign targeting Australian networks. These TTPs are captured in the frame of tactics and techniques outlined in the MITRE ATT&CK[1] framework.

Campaign Summary

The Australian Government is currently aware of, and responding to, a sustained targeting of Australian governments and companies by a sophisticated state-based actor. This activity represents the most significant, coordinated cyber-targeting against Australian institutions the Australian Government has ever observed.

The title 'Copy-Paste Compromises' is derived from the actor's heavy use of proof of concept exploit code, web shells and other tools copied almost identically from open source.

The actor has been identified leveraging a number of initial access vectors, with the most prevalent being the exploitation of public facing infrastructure — primarily through the use of remote code execution vulnerability in unpatched versions of Telerik UI. Other vulnerabilities in public facing infrastructure leveraged by the actor include exploitation of a deserialisation vulnerability in Microsoft Internet Information Services (IIS), a 2019 SharePoint vulnerability and the 2019 Citrix vulnerability.

The actor has shown the capability to quickly leverage public exploit proof of concepts (POCs) to target networks of interest and regularly conducts reconnaissance of target networks looking for vulnerable services, potentially maintaining a list of public facing services to quickly target following future vulnerability releases. The actor has also shown an aptitude for identifying development, test and orphaned services that are not well known or maintained by victim organisations.

When the exploitation of public-facing infrastructure did not succeed, the ACSC has identified the actor utilising various spearphishing techniques. This spearphishing has taken the form of:

- links to credential harvesting websites,
- emails with links to malicious files, or with the malicious file directly attached,
- links prompting users to grant Office 365 OAuth tokens to the actor,
- use of email tracking services to identify the email opening and lure click through events.

Once initial access is achieved, the actor utilised a mixture of open source and custom tools to persist on, and interact with, the victim network. Although tools are placed on the network, the actor migrates to legitimate remote accesses using stolen credentials. To successfully respond to a related compromise, all accesses must be identified and removed.

[1] MITRE ATT&CK: https://attack.mitre.org/

DRAGOS WorldView ICS Threat Intelligence PROPRIETARY AND CONFIDENTIAL

TLP: AMBER For Dragos Customers Only

THREAT INTELLIGENCE SUMMARY

TR-2020-31: Malicious Campaign Targets Australian Entities

16 June 2020

ICS Impact
Dragos learned of an ongoing campaign targeting Australian IT networks including critical infrastructure entities. The identified behaviors indicate possible PARISITE or CHRYSENE activities. At this time there is no indication of ICS-specific disruptive behavior.

Threat Analysis	Analyst Assessment
What is the threat classification?	IT Intrusion
What is the risk rating?	A limited threat, risk, or vulnerability requiring an applicability assessment before taking action
What is the targeted ICS industry vertical?	N/A
Which activity group is involved?	Possible PARISITE, CHRYSENE
To which stage on the ICS Cyber Kill Chain does this activity correlate?	Stage 1, Intrusion; Stage 1, Command and Control
How is the malware or attack delivered?	Exploitation of external-facing services and spearphishing techniques
How do you confirm a compromise?	Outbound communication to malicious infrastructure, PowerShell process communication to external IP addresses, remote logon activity from suspicious network space, changes in compromised user profiles.
What is the best course of action for remediation?	Compromised hosts should be rebuilt when possible and all related user accounts receive password resets.
What are the mitigations or countermeasures to stop it in the future?	Implement multi-factor authentication, limit the ability of certain programs to call scripting frameworks, limit scripting framework ability to communicate to outside resources.
Are IOCs available?	Yes

PARISITE

- Dragos tracks an active activity group known as “Parisite”, and has responded to incidents which have uncovered their activity.
- The group leverage emerging vulnerabilities, including vulnerabilities in Fortinet, PulseSecure and Palo Alto VPNs.
- Quite likely to leverage recent F5 Big-IP, Citrix Gateway vulnerabilities.

PARISITE - Hypothesis

THREAT HUNT WORKBOOK		
Hunt Catalyst	Public Threat Intelligence Reporting	
Context	Parisite Activity Group is targeting region with widespread compromises. Group is leveraging VPN exploits to gain unauthorized access to industrial organizations.	
Hypothesis	Parisite AG has obtained access to plant network via compromise of VPN infrastructure.	
Scope	**Window(s):** • Jan - July 2020	**Location(s):** • Perimeter VPN • Plant VPN • Engineering VPN

CVE-2019-1579

Palo Alto Networks Security Advisories / CVE-2019-1579

CVE-2019-1579 Remote Code Execution in GlobalProtect Portal/Gateway Interface

Severity 8.1 · HIGH

Attack Vector **NETWORK**

Attack Complexity **HIGH**

Privileges Required **NONE**

User Interaction **NONE**

Scope **UNCHANGED**

Confidentiality Impact **HIGH**

Integrity Impact **HIGH**

Availability Impact **HIGH**

NVD JSON

Published **2019-07-18**

Updated **2019-07-18**

Reference **PAN-SA-2019-0020**

```
admin@PA-VM> show admins

Admin                          From    Client Session-start      Idle-for
------------------------------------------------------------------------------
admin                     192.168.1.252      Web 07/12 22:16:32     00:17:01s
admin                     192.168.52.177     Web 07/12 21:45:11     00:03:14s
admin                     192.168.52.177     CLI 07/12 22:44:35     00:00:00s
```

```
admin@PA-VM# show mgt-config users
users {
  admin {
    phash fnRL/G5lXVMug;
    permissions {
      role-based {
        superuser yes;
      }
    }
  }
  parisite {
    phash $1$cemxsagl$vFjANNanFijGMcndp9sEt/;
  }
}
```

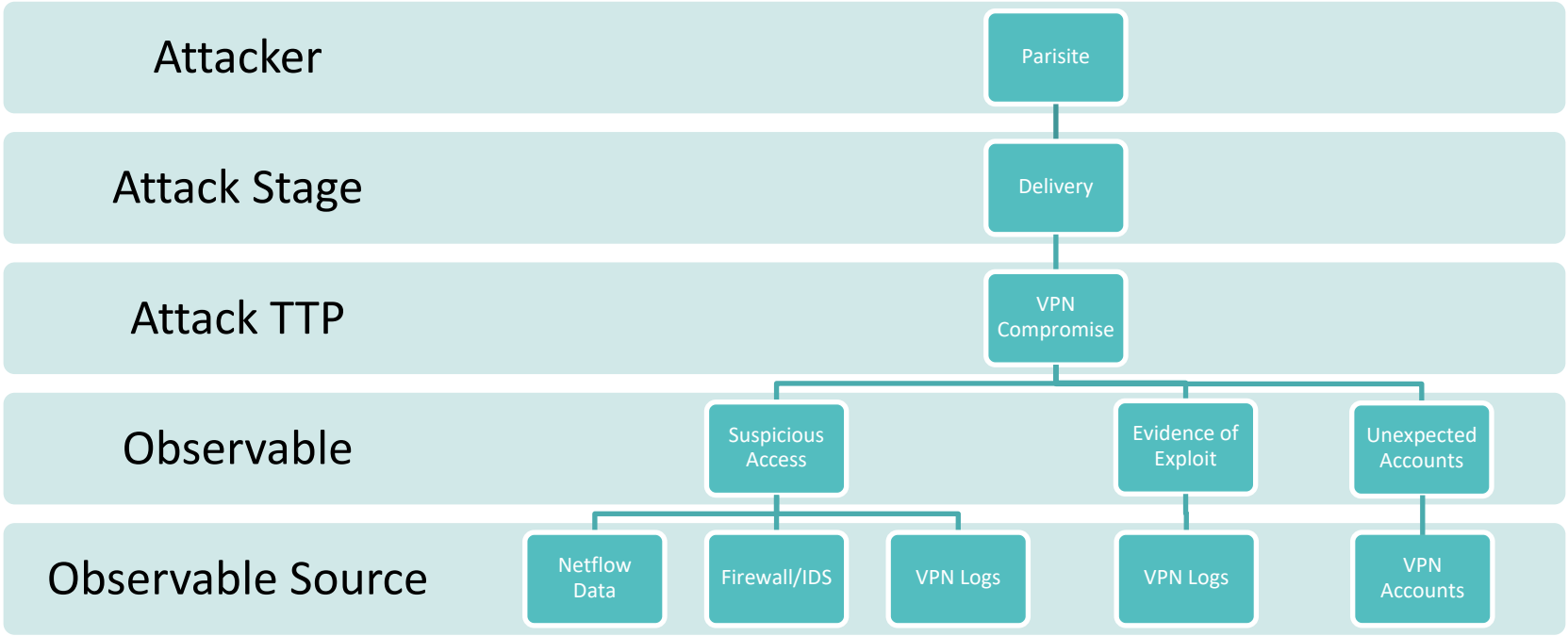
```
admin@PA-VM> show authentication local-user-db

                Vsys                User  Disabled
------------------------------------------------------
                shared              barry        no
                shared              garry        no
                shared              harry        no
                shared           parisite        no
```

```
$ time curl -s -d 'scep-profile-name=%9999999c' https://global-protect/sslmgr >/dev/null
real    0m1.721s
user    0m0.037s
sys     0m0.005s
$ time curl -s -d 'scep-profile-name=%99999999c' https://global-protect/sslmgr >/dev/null
real    0m2.051s
user    0m0.035s
sys     0m0.012s
$ time curl -s -d 'scep-profile-name=%999999999c' https://global-protect/sslmgr >/dev/null
real    0m5.324s
user    0m0.021s
sys     0m0.018s
```

```
admin@PA-VM> tail webserver-log sslvpn_access.log
192.168.1.252 15779 - 192.168.1.249 20077 [12/Jul/2020:23:19:18 -0700] "GET /global-protect/portal/images/favicon.ico HTTP/1.1" 200 1150 "https://192
Kit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 Edg/83.0.478.61" 1594621158.767 0.000 - 232
192.168.1.252 15779 - 192.168.1.249 20077 [12/Jul/2020:23:19:18 -0700] "GET /global-protect/login.esp HTTP/1.1" 200 11756 "https://192.168.1.249/" "M
3.0.4103.116 Safari/537.36 Edg/83.0.478.61" 1594621158.918 0.023 0.023 232
192.168.1.252 15779 - 192.168.1.249 20077 [12/Jul/2020:23:19:18 -0700] "GET /global-protect/portal/images/favicon.ico HTTP/1.1" 200 1150 "https://192
Kit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 Edg/83.0.478.61" 1594621158.956 0.000 - 232
192.168.1.252 15779 - 192.168.1.249 20077 [12/Jul/2020:23:19:19 -0700] "GET /global-protect/login.esp HTTP/1.1" 200 11756 "https://192.168.1.249/" "M
3.0.4103.116 Safari/537.36 Edg/83.0.478.61" 1594621159.095 0.023 0.023 232
192.168.1.252 15779 - 192.168.1.249 20077 [12/Jul/2020:23:19:19 -0700] "GET /global-protect/portal/images/favicon.ico HTTP/1.1" 200 1150 "https://192
Kit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 Edg/83.0.478.61" 1594621159.129 0.000 - 232
192.168.1.252 15779 - 192.168.1.249 20077 [12/Jul/2020:23:19:19 -0700] "GET /global-protect/login.esp HTTP/1.1" 200 11756 "https://192.168.1.249/" "M
3.0.4103.116 Safari/537.36 Edg/83.0.478.61" 1594621159.295 0.023 0.023 232
192.168.1.252 15779 - 192.168.1.249 20077 [12/Jul/2020:23:19:19 -0700] "GET /global-protect/portal/images/favicon.ico HTTP/1.1" 200 1150 "https://192
Kit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 Edg/83.0.478.61" 1594621159.330 0.000 - 232
192.168.1.252 15779 - 192.168.1.249 20077 [12/Jul/2020:23:19:19 -0700] "GET /global-protect/login.esp HTTP/1.1" 200 11756 "https://192.168.1.249/" "M
3.0.4103.116 Safari/537.36 Edg/83.0.478.61" 1594621159.486 0.023 0.023 232
192.168.1.252 15779 - 192.168.1.249 20077 [12/Jul/2020:23:19:19 -0700] "GET /global-protect/portal/images/favicon.ico HTTP/1.1" 200 1150 "https://192
Kit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 Edg/83.0.478.61" 1594621159.522 0.000 - 232
192.168.1.252 15782 - 192.168.1.249 20077 [12/Jul/2020:23:19:28 -0700] "POST /sslmgr HTTP/1.1" 200 145 "-" "curl/7.55.1" 1594621168.378 0.033 0.033 2
admin@PA-VM>
```

https://devco.re/blog/2019/07/17/attacking-ssl-vpn-part-1-PreAuth-RCE-on-Palo-Alto-GlobalProtect-with-Uber-as-case-study/

Operationalising Intel – TTP Observables

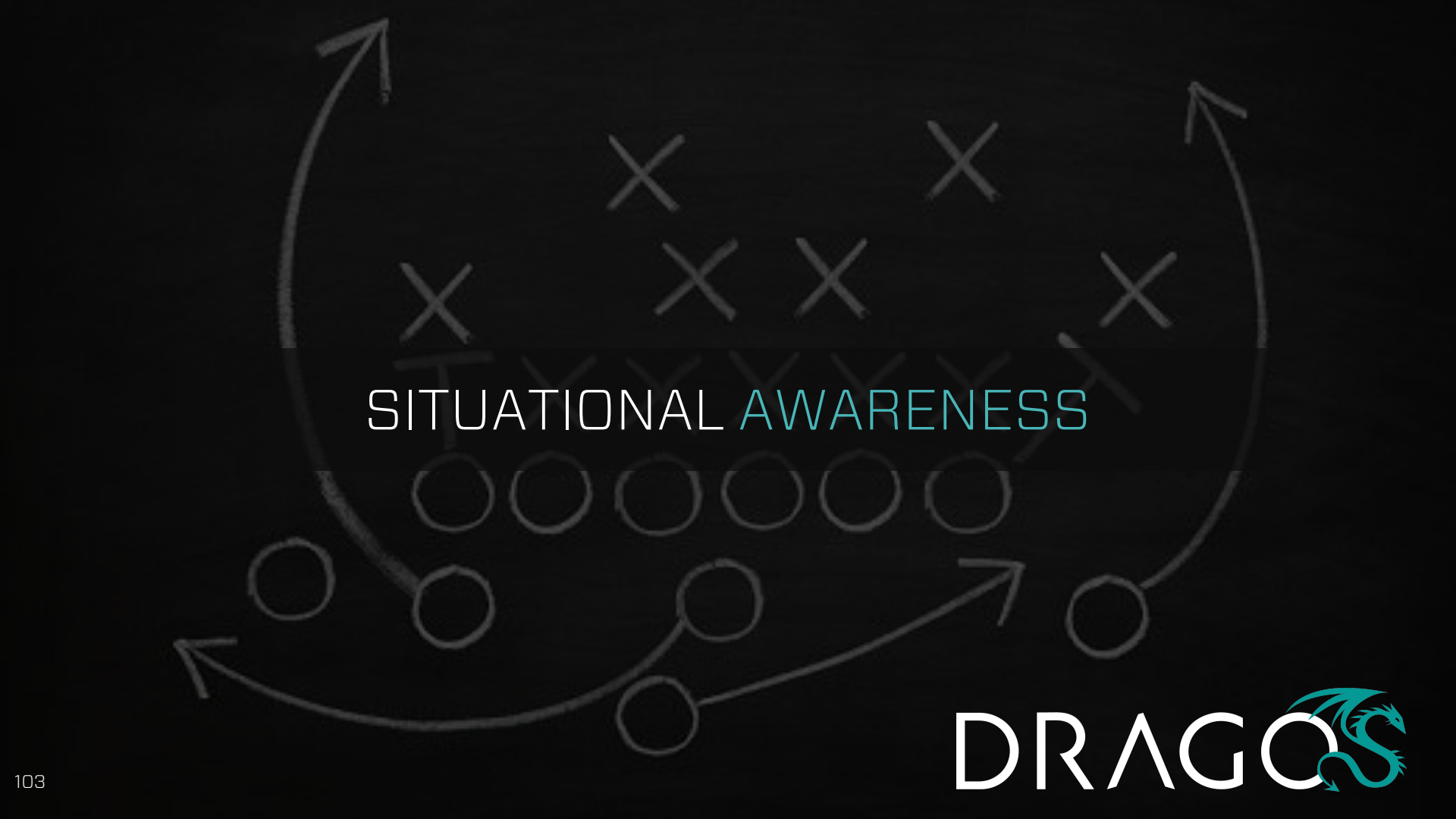


https://www.dragos.com/resource/hunting-with-rigor-quantifying-the-breadth-depth-and-threat-intelligence-coverage-of-a-threat-hunt-in-industrial-control-system-environments/

DRAGOS

PARISITE - Collections

THREAT HUNT WORKBOOK (CONT.)	
TESTS	**COLLECTIONS**
Identify suspicious access to /sslmgr	VPN Logs
Identify known bad connections (IOCS)	VPN Logs
Identify suspicious connections (unknowns/unexpected time, source, duration, frequency)	VPN Logs
Identify suspicious inbound traffic from VPN	VPN Logs, Router Netflow, Firewall Logs, IDS Logs
Identify unexpected VPN accounts	VPN Accounts (local and domain)
Identify suspicious 2FA mechanisms	Account 2FA configurations

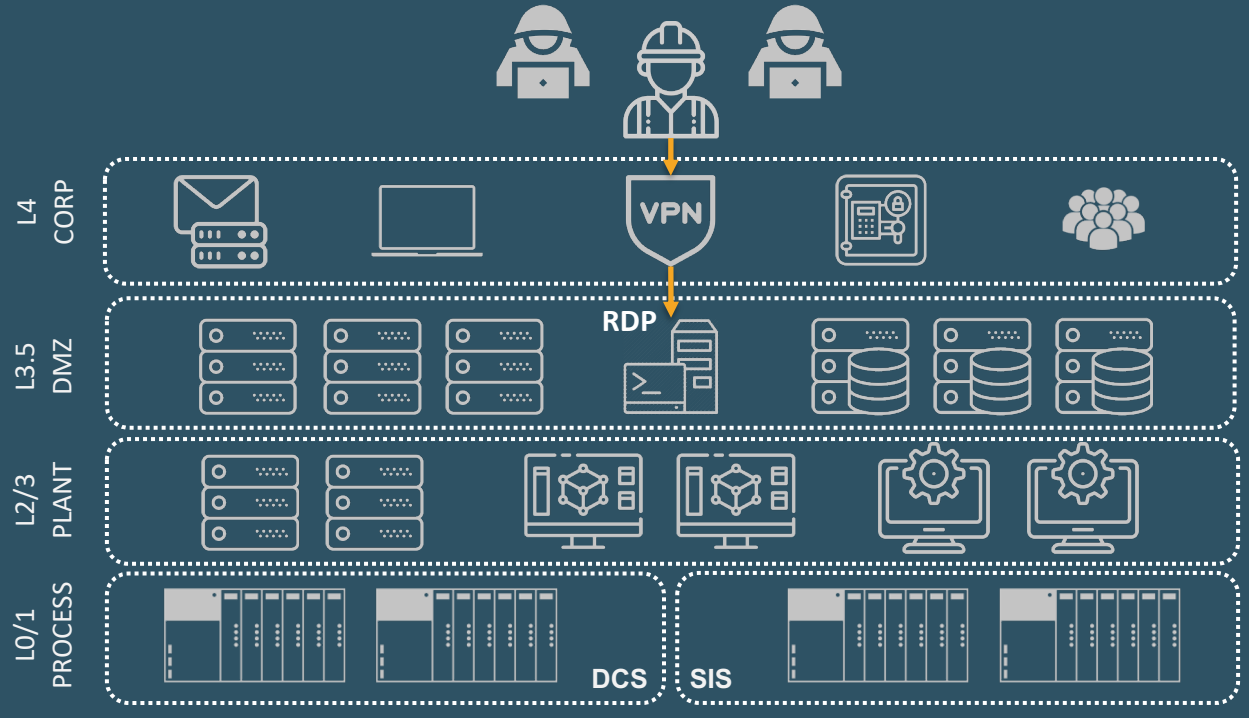


DRAGOS

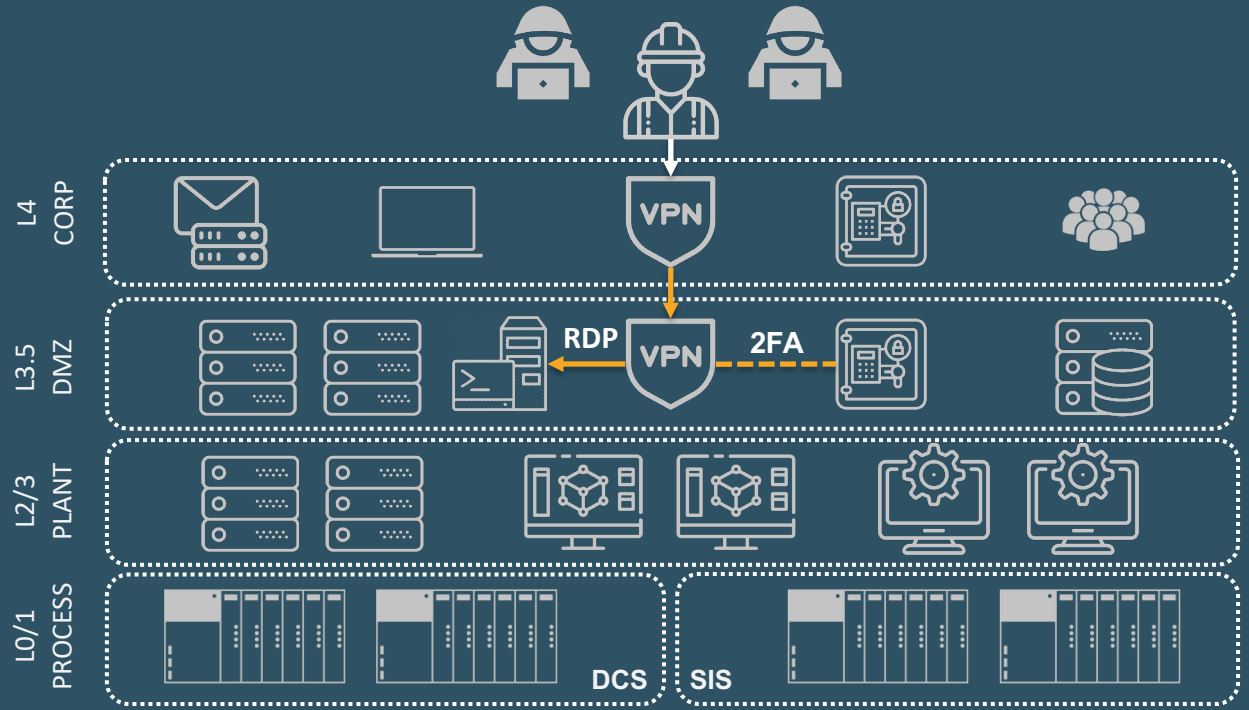
Situational Awareness Driven Hypotheses

- “Requires visibility into and understanding of networked environments and their individual elements”
- Focus on the most important assets and information (Crown Jewels Analysis (CJA))
- What an adversary might be looking for upon entering the network

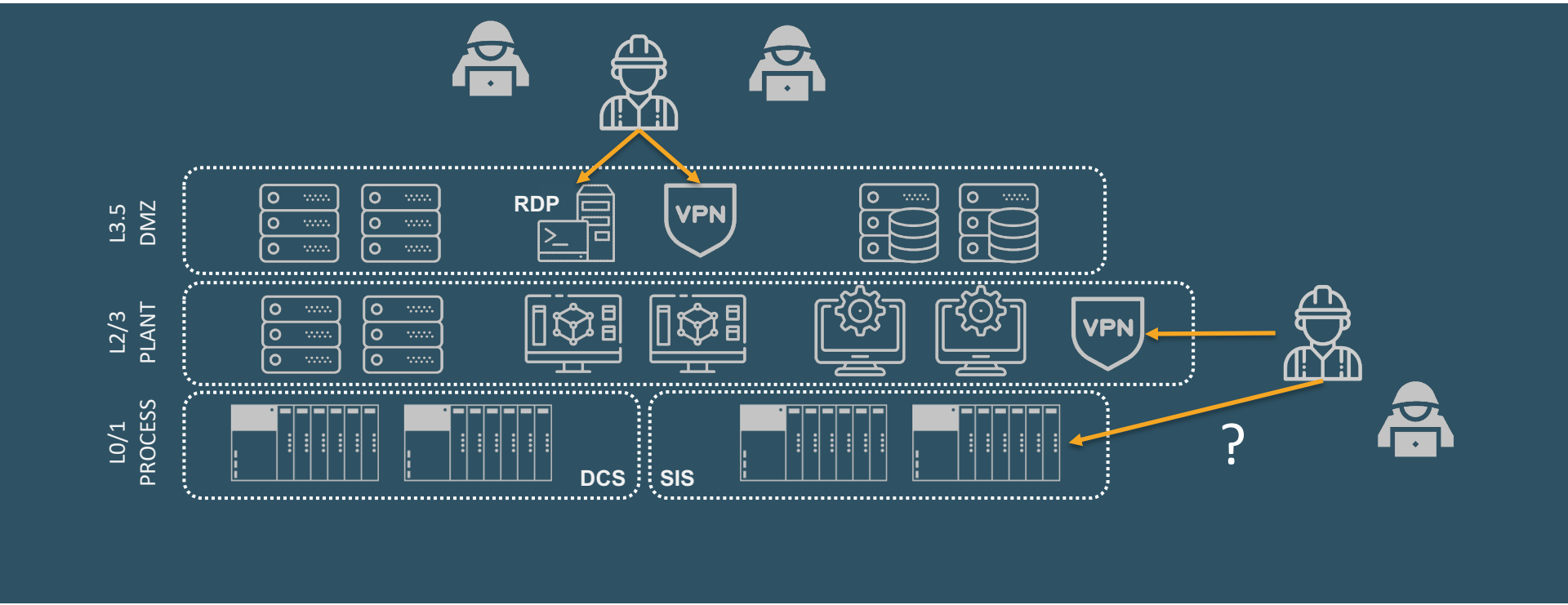
Common Architecture



Better Architecture



(Less)Common Architecture

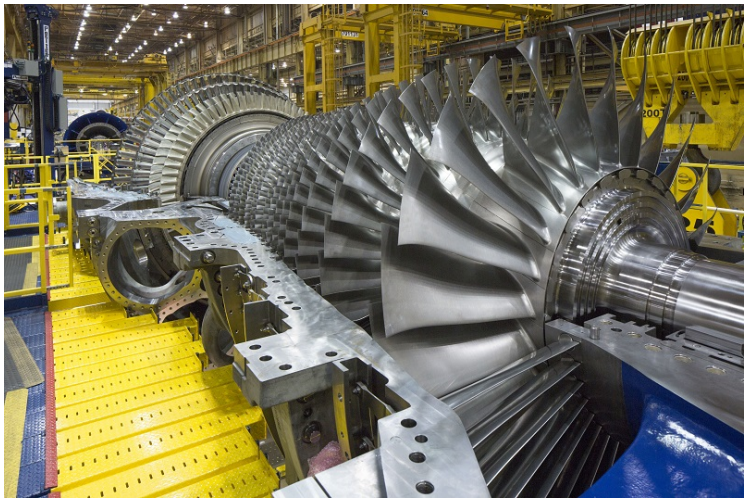


Examples – Vendor Infrastructure and Connections

GE Remote Monitoring and Diagnostics

"Every day, GE collects more than 30,000 operating hours of data from more than 1,600 globally deployed power generation assets, supplementing a 40 terabyte database representing more than 100 million fleet operating hours.

https://www.ge.com/content/dam/gepower-pgdp/global/en_US/documents/service/gas%20turbine%20services/monitoring-diagnostics-fact-sheet.pdf

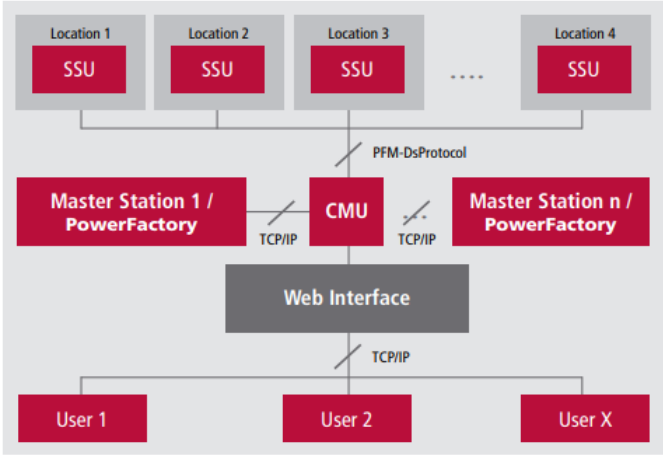


Examples – Vendor Infrastructure and Connections

NEM Power System Modelling

"The main commercial activity of DIgSILENT Pacific in Australia is to conduct power system studies for generators, transmission systems, distribution systems, mining and industrial systems. DIgSILENT Pacific uses a variety of software platforms as required by clients and as appropriate for specific tasks."

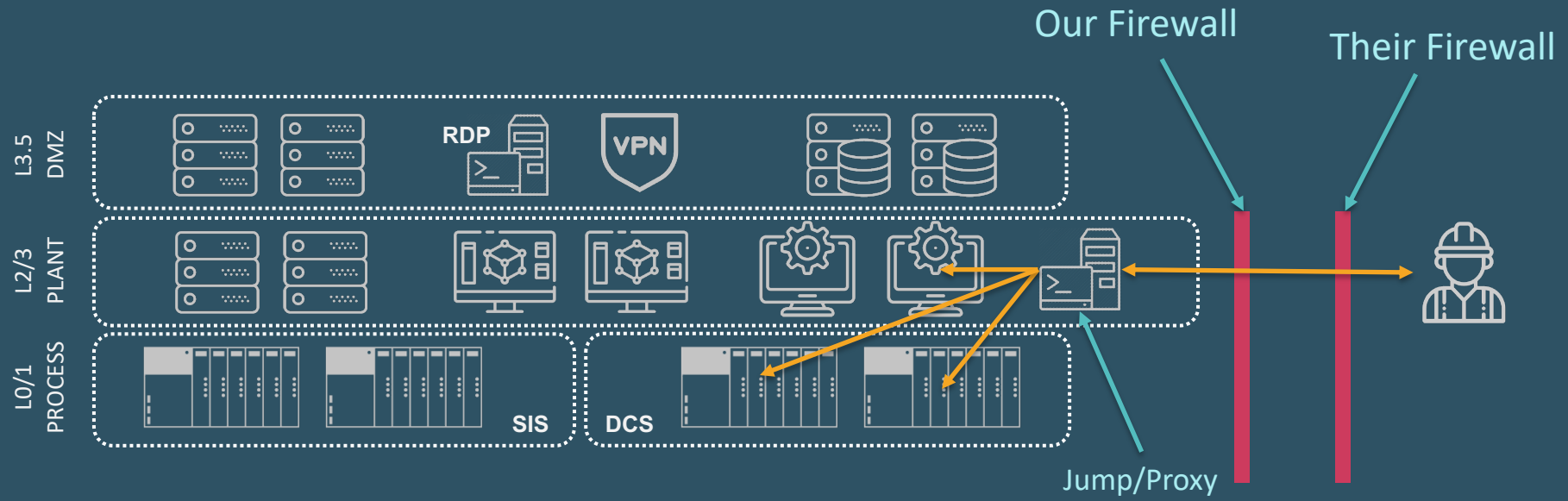
https://www.digsilent.com.au/publications/2018/papers/CommentsToDraftModelGuidelines.pdf
https://www.digsilent.com.au/pdf/PFMonitor_Brochure.pdf
https://aemo.com.au/-/media/Files/Electricity/NEM/Security_and_Reliability/System-Security-Market-Frameworks-Review/2018/Power_Systems_Model_Guidelines_PUBLISHED.pdf



Engineering Access - Hypothesis

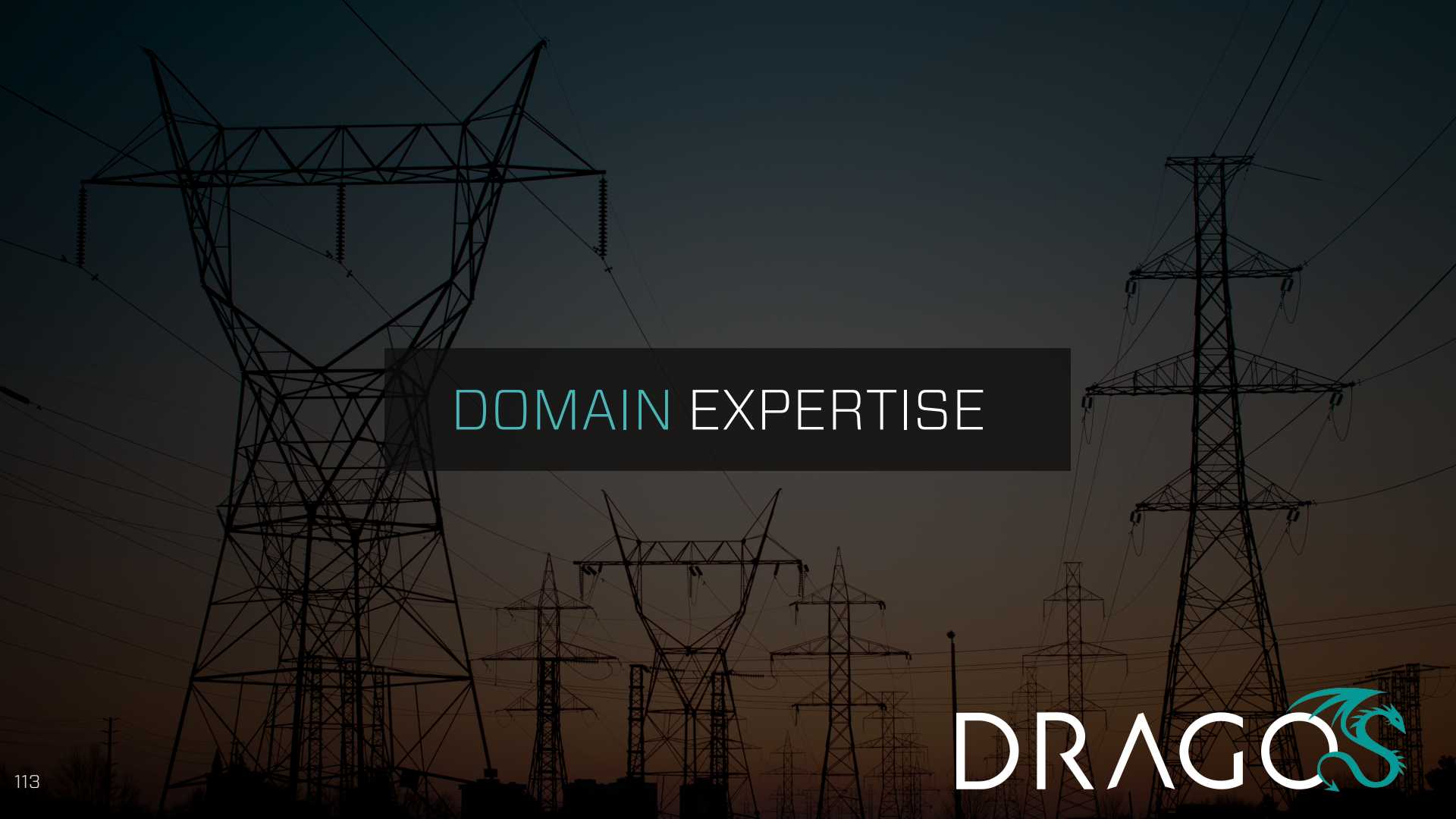
THREAT HUNT WORKBOOK		
Hunt Catalyst	Periodic – Situational Awareness	
Context	Power generation facility ABC leverages a gas powered turbine by vendor XYZ. The vendor maintains persistent access to the turbine for maintenance and diagnostic purposes.	
Hypothesis	An adversary has compromised our vendor and is accessing sensitive systems within the control network via the turbine diagnostics link.	
Scope	**Window(s):** • Jan - July 2020	**Location(s):** • Plant Control Network • Vendor Link

Likely (Optimistic) Scenario



Vendor - Collections

THREAT HUNT WORKBOOK (CONT.)	
TESTS	**COLLECTIONS**
Identify suspicious connections (unknowns/unexpected time, duration, frequency, targets)	Firewall/Router/Switch ACL Logs, PCAP
Identify suspicious behaviour (scanning, data exfil)	Firewall/Router/Switch ACL Logs, PCAP
Identify suspicious protocols / services (WinRM, WMI, SSH, RDP etc)	Firewall/Router/Switch ACL Logs, PCAP
Identify “High-Risk” communications (firmware modification, controller logic / program changes)	PCAP, Controller Logs


DOMAIN EXPERTISE
DRAGOS

Domain Expertise

- Bring knowledge gained from previous incidents and hunts, and those shared with us.
- Situational awareness and intelligence previously derived is no longer immediately relevant.
- Knowledge has shaped who the threat hunter is today.

Example: Operational Issues

- **TIP: Work your way into Engineering RCA**
- Conduct hybrid hunts / investigations on interesting or suspicious events
- Conduct periodic hunts on other systems, leveraging our past experiences

Unexpected Plant Shutdown

TRISIS SCENARIO

PetroChemical plant in Saudi Arabia experienced numerous unexpected shutdowns of the facility through “malfunctioning” safety controllers.

Subsequent investigation (threat hunt!) identified TRISIS malware on safety engineering workstations.

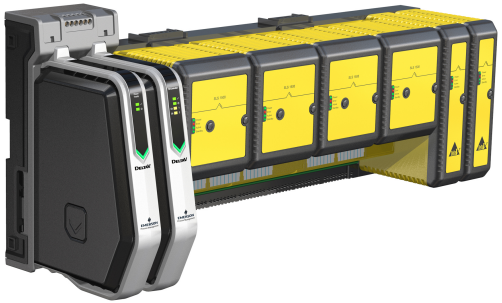
https://www.dragos.com/resource/analyzing-trisis/
https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf

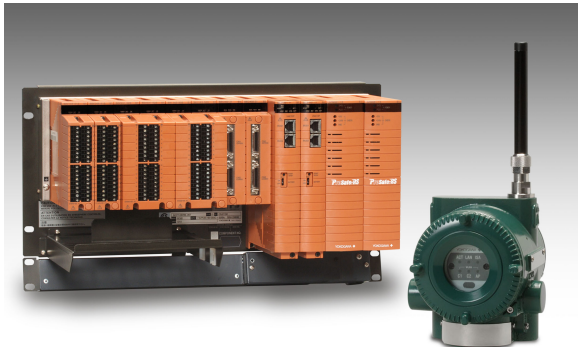
XENOTIME

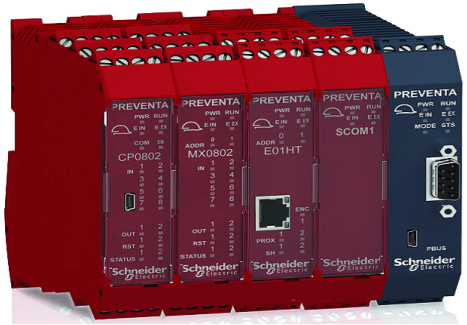
CAPABILITIES
TRISIS, custom credential harvesting, off the shelf tools

VICTIMOLOGY
Oil & Gas, Electric, Middle East, US, Europe, APAC

Same Techniques | Different Targets



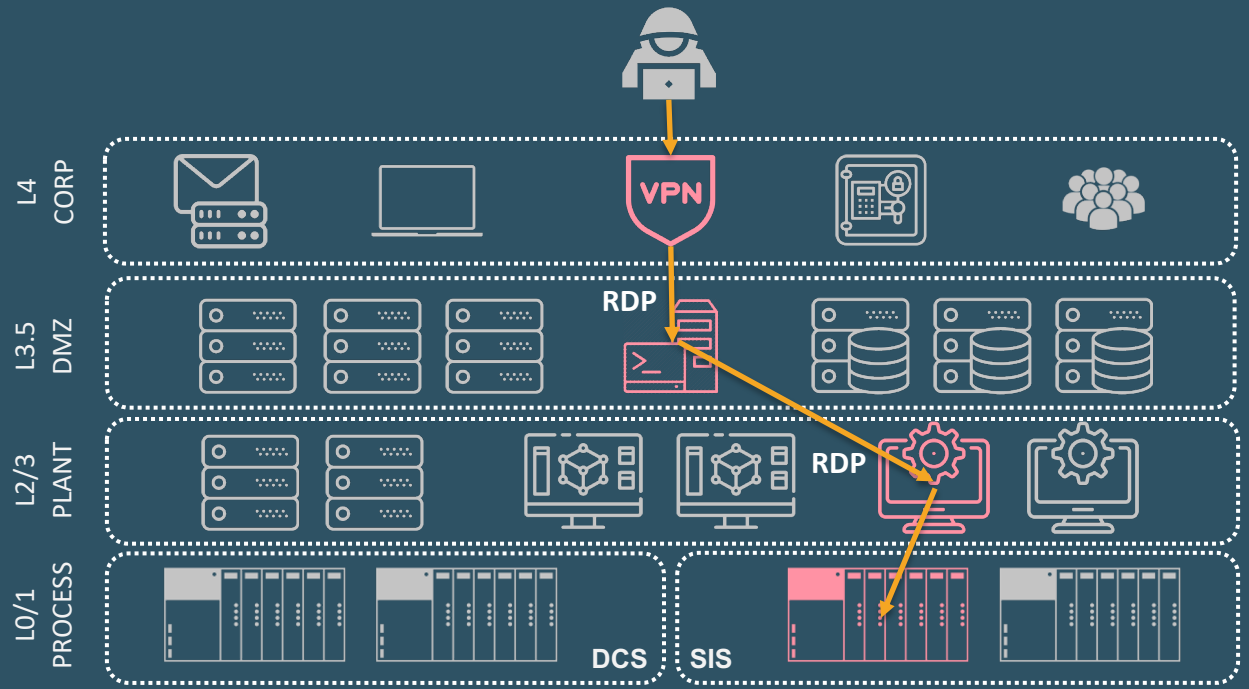




Sis Compromise - Hypothesis

THREAT HUNT WORKBOOK	
Hunt Catalyst	Operational Issues
Context	Plant XYZ has been experiencing operational irregularities within the stability of plant operations. The plant has experienced at least one unexpected shutdown caused by a malfunctioning safety controller. Similar events have occurred in the past, including the TRISIS incident at a Petrochemical facility in Saudi Arabia.
Hypothesis	An adversary has compromised the plant safety engineering workstations and is leveraging the systems to conduct unauthorized activities on safety controllers.
Scope	**Window(s):** • Jan - July 2020 **Location(s):** • Plant DMZ • SIS Engineering Workstations, SIS Controllers

XENOTIME Enumerated Attack Path



Sis Compromise - Collections

THREAT HUNT WORKBOOK (CONT.)	
TESTS	**COLLECTIONS**
Identify suspicious connections to engineering workstations (unexpected time, duration, frequency, protocols)	DMZ and Plant Firewall/Router/Switch ACL Logs, PCAP, Engineering Workstation Logs
Identify file creations and executions on Engineering Workstations	Host-based artifacts (MFT, Shellbags, Registry Hives etc)
Identify unexpected behaviour on Safety Controllers	Controller logs, SIS Engineering Application Logs

Findings and Actions

Document your findings, even if nothing is found.

Threat Findings

- Did we find any associated activity?

Initiate Incident Response

Environmental Findings

- Were we able to achieve objectives?
- Can we improve defences?

Automation

- Can we streamline the hunt for future?
- Can we automate the hunt for the SOC?


jgutmanis@dragos.com
DRAGOS

Thank you for participating!
Learn more:
dragos.com/resources/

DRAGOS