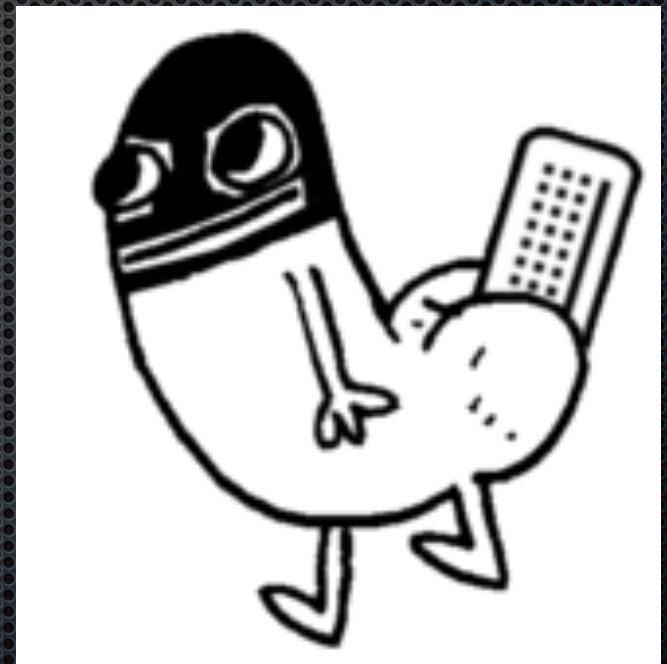


Know the enemy



Thanks OWASP Aarhus !

- Dennis Perto & Conscia
- Rob Lee (Dragos / SANS) & Ted Gutierrez (SANS ICS) for allowing me to share their work
- & all others shown, but not directly mentioned, thanks!



whoami

- current headspace = ICS Security
- @grumpy4n6
- ICS Security Analyst
- <https://www.linkedin.com/in/mitchellimpey/>

“

**DON'T
DEPEND
ON THE ENEMY NOT
COMING; DEPEND
RATHER ON BEING
READY
FOR HIM.**

”

-SUN-TZU

Why make a presentation ?

- introducing a new way to attack ?
- introducing a new way to defend ?
- created a new tool that does one of the above?
- describe a technique that works for you ?
- interesting pov / technique to improve InfoSec ?

<https://danielmiessler.com/blog/fixing-the-culture-of-infosec-presentations/>

Enough - get started ! :)

- ▀ Once upon a time...
- ▀ ... I had to make a report

CONTEXT

- these are *my* comments
- not classic “IT Security” talk (C,I,A)
- about ICS/SCADA security (A,I,C)
- priority = (Safety first) + Keeping things running
- ICS (industrial control systems) includes SCADA*
(supervisory control and data acquisition)

* https://en.wikipedia.org/wiki/Industrial_control_system



ATT&CK™

A screenshot of the JPCERT Coordination Center website. The header includes the JPCERT logo (a red 'J' inside a circle), the text 'JPCERT Coordination Center', and a navigation bar with icons for back, forward, search, and home. Below the header is a banner with the text 'Towards a safer cyber space without incident'. The main content area features the 'JPCERT CC' logo (with a registered trademark symbol) and the text 'Japan Computer Emergency Response Team Coordination Center' in English and Japanese ('JPCERT コーディネーションセンター').

kaspersky

DRAGOS

The ESET logo, consisting of the word 'eset' in a white, lowercase, sans-serif font inside a teal rounded rectangle.



THE CYBER KILL CHAIN®

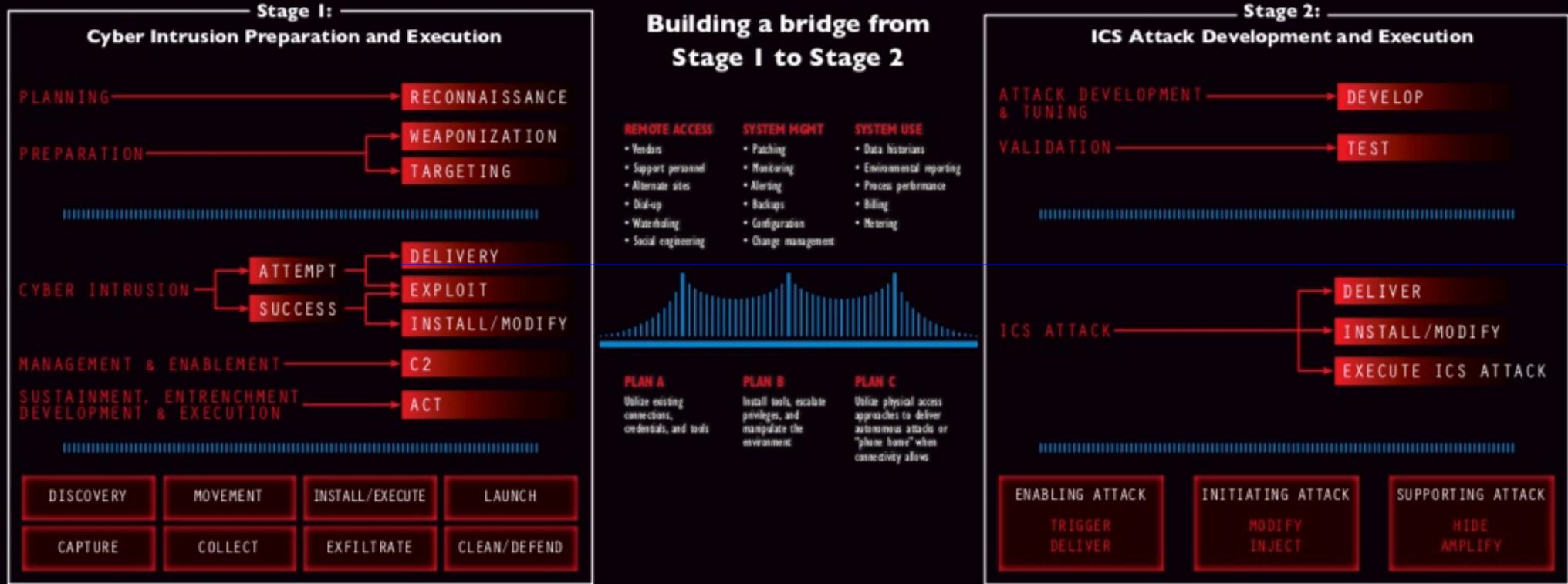
ICS Cyber Kill Chain



REFERENCE/CITATION: Michael J. Assante & Robert M. Lee [The Industrial Control System Cyber Kill Chain](#) / SANS Institute InfoSec Reading Room / October 2015



ADVERSARY METHODS



Stage 1 is based on the Cyber Kill Chain® model from Lockheed Martin

<https://www.sans.org/security-resources/posters/industrial-control-systems/perspective-cyber-attack-140>

ICS Attack Difficulty

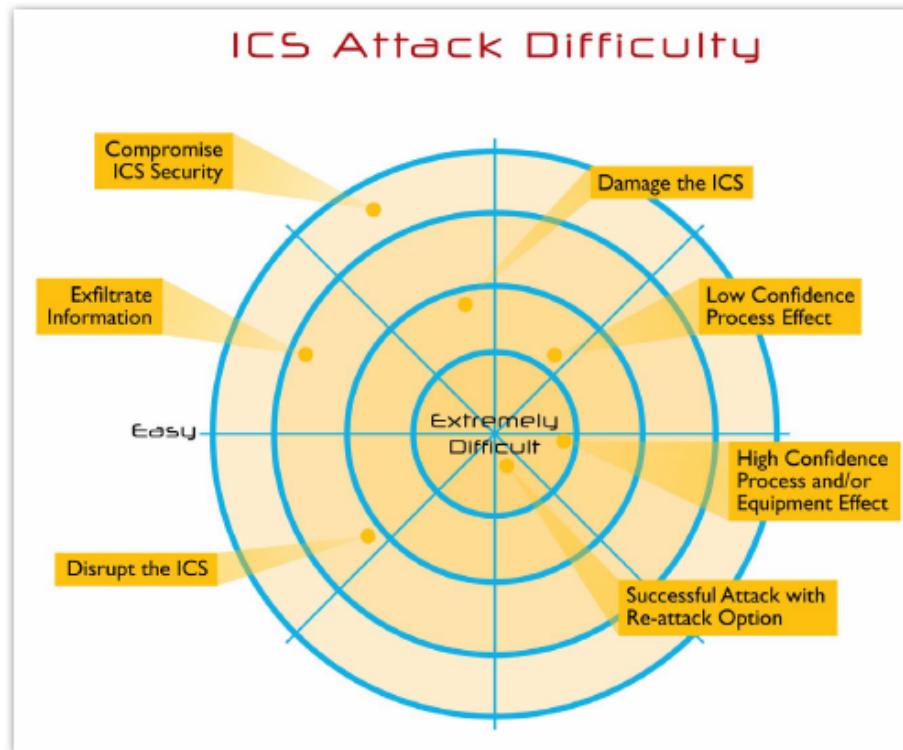


Figure 3. ICS Attack Difficulty Scale



... these are still NOT the reports I was looking for...





H_x HEXANE since 2018

➤ MODE OF OPERATION
IT compromise and information gathering against ICS entities

➤ CAPABILITIES
Embedded binaries in documents, C2 via DNS and HTTP, evasion techniques

➤ VICTIMOLOGY
Oil & Gas, Middle East, Central Asia, Africa

➤ LINKS
None

R_a RASPITE since 2017

➤ MODE OF OPERATION
IT network limited, information gathering on electric utilities with some similarities to CHRYSENE

➤ CAPABILITIES
Service installer malware designed to beacon out to adversary infrastructure

➤ VICTIMOLOGY
Electric Utilities, US, Saudi Arabia, Japan, Europe

➤ LINKS
LeafMiner

M_a MAGNALLIUM since 2016

➤ MODE OF OPERATION
IT network limited, information gathering against industrial orgs

➤ CAPABILITIES
STONEDRILL wiper, variants of TURNEDUP malware

➤ VICTIMOLOGY
Petrochemical, Aerospace, Saudi Arabia, UAE

➤ LINKS
APT133

D_y DYMALLOY since 2016

➤ MODE OF OPERATION
Deep ICS environment information gathering, operator credentials, industrial process details

➤ CAPABILITIES
GOODOR, DORSHEL, KARAGANY, Mimikatz

➤ VICTIMOLOGY
Turkey, Europe, US

➤ LINKS
Dragonfly2, Berserker Bear

E_L ELECTRUM since 2016

➤ MODE OF OPERATION
Electric grid disruption and long-term persistence

➤ CAPABILITIES
CRASHOVERRISE

➤ VICTIMOLOGY
Ukraine, Electric Utilities

➤ LINKS
Sandworm

C_o COVELLITE since 2017

➤ MODE OF OPERATION
IT compromise with hardened anti-analysis malware against industrial orgs

➤ CAPABILITIES
Encoded binaries in documents, evasion techniques

➤ VICTIMOLOGY
Electric Utilities, US

➤ LINKS
Lazarus, Hidden Cobra

X_t XENOTIME since 2014

➤ MODE OF OPERATION
Focused on physical destruction and long-term persistence

➤ CAPABILITIES
TRISS, custom credential harvesting, off the shelf tools

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

➤ LINKS
None

A_L ALLANITE since 2017

➤ MODE OF OPERATION
Watering-hole and phishing leading to ICS recon and screenshot collection

➤ CAPABILITIES
PowerShell scripts, THC Hydra, SecretStomp, Inveigh, PSExec

➤ VICTIMOLOGY
Electric utilities, US & UK

➤ LINKS
Palmetto Fusion

C_h CHRYSENE since 2017

➤ MODE OF OPERATION
IT compromise, information gathering and recon against industrial orgs

➤ CAPABILITIES
Watering holes, 64-bit malware, covert C2 via IPv6 DNS, ISMOOR

➤ VICTIMOLOGY
Oil & Gas, Manufacturing, Europe, MENA, N. America

➤ LINKS
OilRig, Greenbug

HEXANE



HEXANE
Since 2018

Mode of Operation

IT compromise and information gathering against ICS entities

Capabilities

Embedded binaries in documents, C2 via DNS and HTTP, evasion techniques

Victimology

Oil & Gas, Middle East, Central Asia, Africa

Links

None

New activity group targets oil and gas, telecommunications providers

Dragos identified a new activity group targeting industrial control systems (ICS) related entities: HEXANE. Dragos observed this group targeting oil and gas companies in the Middle East, including Kuwait as a primary operating region. Additionally, and unlike other activity groups Dragos tracks, HEXANE also targeted telecommunication providers in the greater Middle East, Central Asia, and Africa, potentially as a stepping stone to network-focused man-in-the-middle and related attacks.

HEXANE intrusion activity includes malicious documents that drop malware to establish footholds for follow-on activity. Although the group appears operational since at least mid-2018, activity accelerated in early- to mid-2019. This timeline, targeting, and increase of operations coincides with an escalation of tensions within Middle East, a current area of political and military conflict.

HEXANE's telecommunications targeting appears to follow a trend demonstrated by other activity groups. ICS adversaries are increasingly targeting third-party organizations along the supply chains of potential targets. For instance, in 2018, Dragos identified the activity group XENOTIME targeting several industrial original equipment manufacturers (OEMs), and hardware and software suppliers. By compromising devices, firmware, or telecommunications networks used by targets within ICS, malicious activity could potentially enter the victim environment through a trusted vendor, bypassing much of the entity's security stack.

HEXANE demonstrates similarities to the activity groups MAGNALLIUM and CHRYSENE. All are ICS-targeting activities focusing largely on oil and gas, and some of the behaviors and recently observed tactics, techniques, and procedures (TTPs) are similar. Like

HEXANE, MAGNALLIUM also increased its activity in early- to mid-2019. Dragos identified recent MAGNALLIUM activity targeting US government and financial organizations as well as oil and gas companies, attempting to gain access to computers at target organizations.

Name	Targets	Where	Damage ICS	Steal Credentials Compromise Website	Since
XENOTIME	E, O	ME, NA, EU, APAC	SIS	Y / Y	2014
ELECTRUM	E	Ukraine	Y	Y / ?	2016
RASPITE	E	US, Saudi, Japan, EU	N	Y / Y	2017
MAGNALLIUM	A, P	Saudi, UAE	N	Y / Y	2016
DYMALLOY	ICS	EU, US, Turkey	N	Y / Y	2017
COVELLITE	E	EU, East Asia, US	N	Y / N	2017
ALLANITE	E, ICS	US, UK	N	Y / Y	2017
CHRYSENE	E, M, O, P	NA, EU, ME	N	Y / Y	2017
HEXANE	O, T	ME, Asia, Africa	N	Y / Y	2018

Based on information from <https://dragos.com/adversaries/>

A = Aerospace E = Electrical Utilities ICS = Industrial Control Systems

M = Manufacturing O = Oil + Gas P = Petrochemical T = Telecom

Greatly simplifying the DRAGOS material previously mentioned

<https://energinet.dk/energisystem fullscreen>

RUSSIAN NEWS AGENCY
TASS

f t



A photograph of a control room at the Beloyarskaya nuclear power plant. In the foreground, an operator wearing a light-colored uniform is seated at a desk, working on multiple computer monitors displaying various data and control panels. Behind the operator is a massive, long control console filled with numerous analog and digital control panels, each with its own set of knobs, switches, and displays. A large, illuminated digital screen above the console shows a complex network diagram or map. On the wall to the right, there is a large round clock. The ceiling is white with a grid of recessed lights.

© Donat Sorokin/TASS

MOSCOW, August 18. /TASS/. A power unit of the Beloyarskaya nuclear plant in Russia's Urals Sverdlovsk region was shut down on Sunday due to a false activation of the nuclear safety protection system, Rosenergoatom, an operator of Russia's nuclear plants, said on its website.

Summary

- Stop making Stage 1 so damn easy !
- limit value of credentials by using unique logins + passwords; use multi factor authentication
- enable logs, collect, analyze, + monitor logons/logins of all internal/external access (start by noticing!)
- understand how they break in; add appropriate IT controls based on your threat/risk analysis
- measure your progress (<https://www.cyber.gov.au/publications/essential-eight-maturity-model>)

Links of possible interest

- ✖ <https://danielmiessler.com/>
- ✖ <https://scadahacker.com/training.html>
- ✖ <https://www.sans.org/cyber-security-summit/archives/ics>
- ✖ activeresponse.org/diamond-model-kill-chain
- ✖ <http://www.robertmlee.org/a-collection-of-resources-for-getting-started-in-icsscada-cybersecurity/>
- ✖ <https://www.langner.com/resources/>



the summary slide - Rob M. Lee in Kuwait