Anatomy of an Attack

Chris Hankin

Emerging Topics in ICS Security

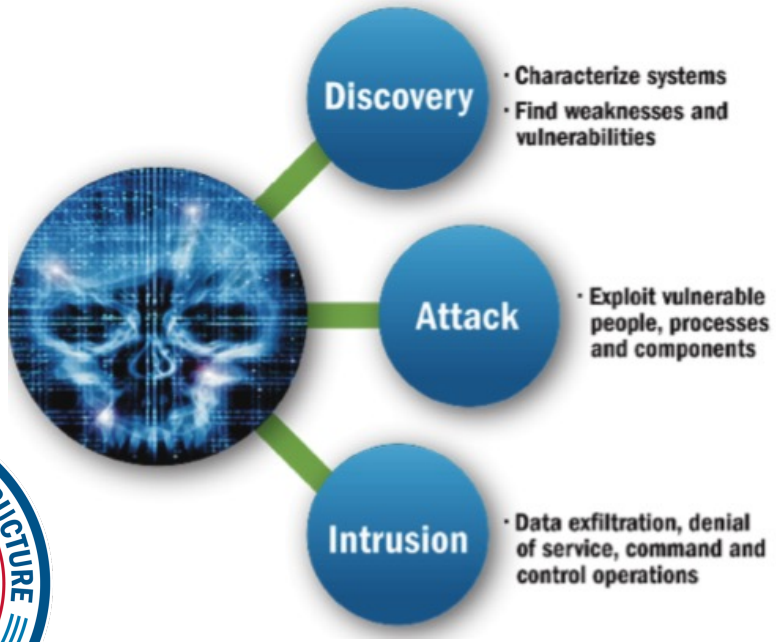
- Bring Your Own Device (BYOD)
- Virtual Machine Technologies
- Security Monitoring in an ICS environment
- ICS Intrusion Detection and Prevention Systems
- Security Information and Event Management (SIEM) technologies
- ICS Supply Chain Management
- Managed Services and Outsourcing
- Leveraging Cloud Services in ICS

Basis for ICS Security Controls

- Identification and Characterization of Risk
- Criticality-Based Asset Inventory
- Understanding Company Risk Appetite
- Implementation of Tailored Security Controls
- Using Communications Monitoring
- Physical Security Controls
- ICS Network Architecture
- Network Security Architecture

ICS Attack Methods

- Exploiting Weak Authentication
- Network Scanning/Probing
- Removable Media
- Brute Force Intrusion
- Abuse of Access Authority
- Spear Phishing
- SQL Injection



NCCIC

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

FY 2017 Most Prevalent Weaknesses

Area of Weakness	Rank	Risk
Boundary Protection	1	• Undetected unauthorized activity in critical systems • Weaker boundaries between ICS and enterprise networks
Identification and Authentication (Organizational Users)	2	• Lack of accountability and traceability for user actions if an account is compromised • Increased difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access
Allocation of Resources	3	• No backup or alternate personnel to fill position if primary is unable to work • Loss of critical knowledge of control systems
Physical Access Control	4	• Unauthorized physical access to field equipment and locations provides increased opportunity to: ○ Maliciously modify, delete, or copy device programs and firmware ○ Access the ICS network ○ Steal or vandalize cyber assets ○ Add rogue devices to capture and retransmit network traffic
Account Management	5	• Compromised unsecured password communications • Password compromise could allow trusted unauthorized access to systems
Least Functionality	6	• Increased vectors for malicious party access to critical systems • Rogue internal access established

CISA ASSESSMENTS: FISCAL YEAR 2019 MOST PREVALENT IT AND OT WEAKNESSES AND RISKS

Boundary Protection

RISK
Undetected unauthorized activity in critical systems

RISK
Weaker boundaries between ICS and enterprise systems

Principle of Least Functionality

RISK
Increased vectors for malicious party access to critical systems

RISK
Opportunity for rogue internal access to be established

Identification and Authentication

RISK
Lack of accountability and traceability for user actions if an account is compromised

RISK
Increased difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access

Physical Access Control

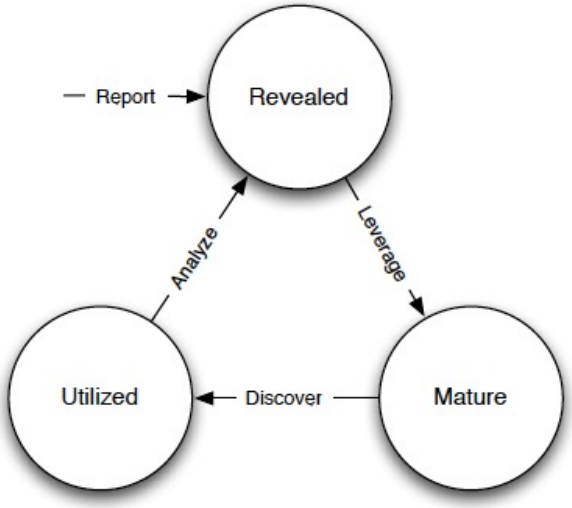
RISK
Unauthorized physical access to field equipment provides increased opportunity to:
- Maliciously modify, delete, or copy device programs and firmware
- Access the ICS network
- Steal or vandalize cyber assets
- Add rogue devices to capture and retransmit network traffic

Account Management

RISK
Increased opportunity for unapproved system access from shared or system accounts

Lockheed Martin Cyber Kill Chain™

- Atomic, Computed and Behavioural indicators



- Military doctrine: F2T2EA – find, fix, track, target, engage, assess

Courses of Action

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

From: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, by Hutchins et al, Lockheed Martin Corporation

Reconnaissance

- Research, identification and selection of targets
- Physical surveillance
- Internet presence
- Social media
- Family and close acquaintances of potential targets

Weaponization

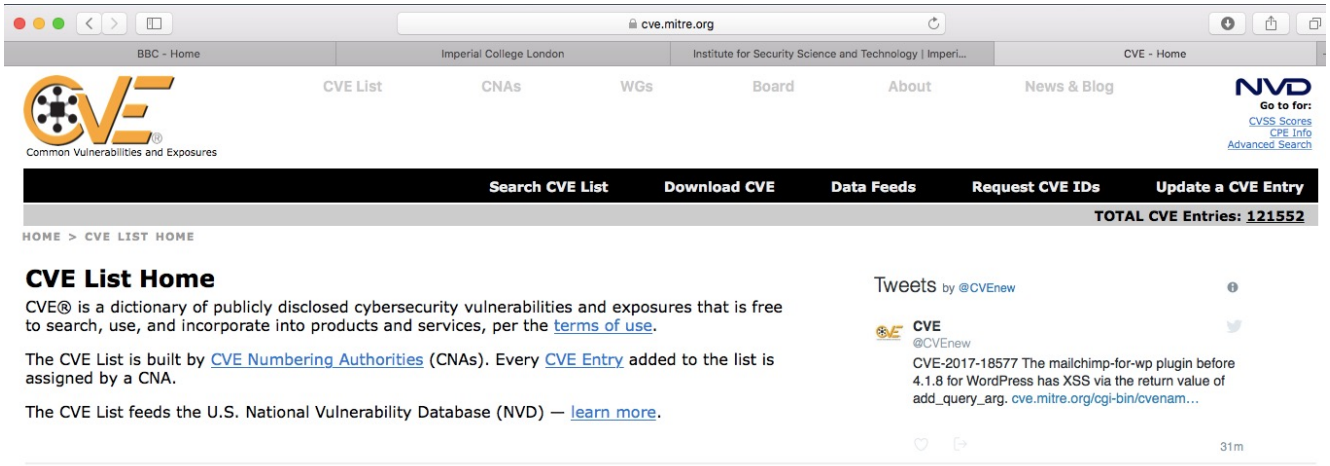
- Embedding of malware into delivery mechanism
- Typically a remote access trojan (RAT)
- Adobe PDF
- Microsoft Office Document

Delivery

- Removable Media (USB)
- E-mail attachment
- Website

Exploitation

- Exploit Vulnerability in application software or operating system



- Exploit user behavior
- Exploit auto-execution facility

Installation

- RAT or backdoor installed on the target system to allow persistent access.

TREND MICRO™

Command and Control (C2)

- F-Secure found that the HAVEX RAT used compromised web-sites as C2 servers:

```
abainternationaltoursandtravel.com
adultfriendgermany.com
africancranesafaris.com
alexvernigor.com
al-mashkoor.com
alpikaclub.com
antibioticsdrugstore.com
arsch-anus.com
artem.sataev.com
artsepid.com
ask.az
atampy.com
aziaone.com
```

Action on Objectives

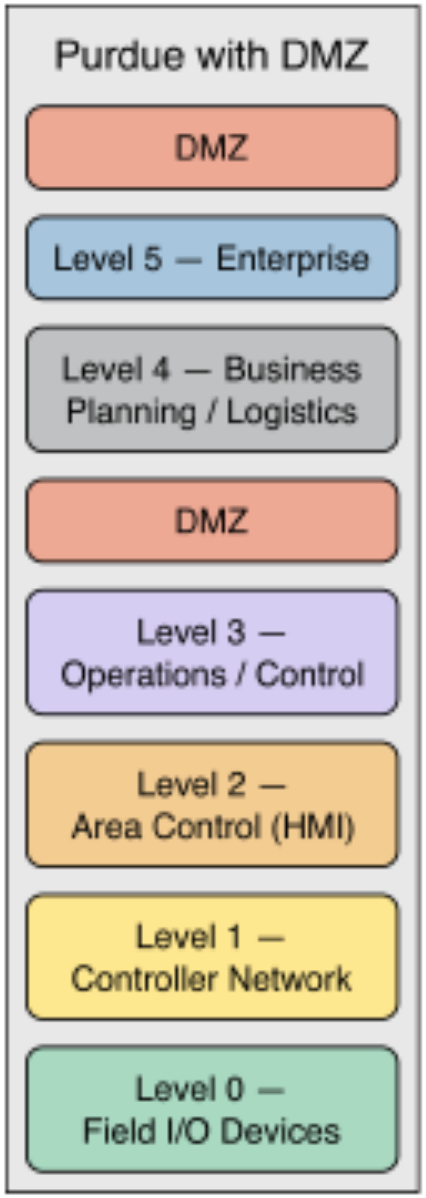
- Data exfiltration
- Data integrity
- Data availability

- Hopping off point

Courses of Action

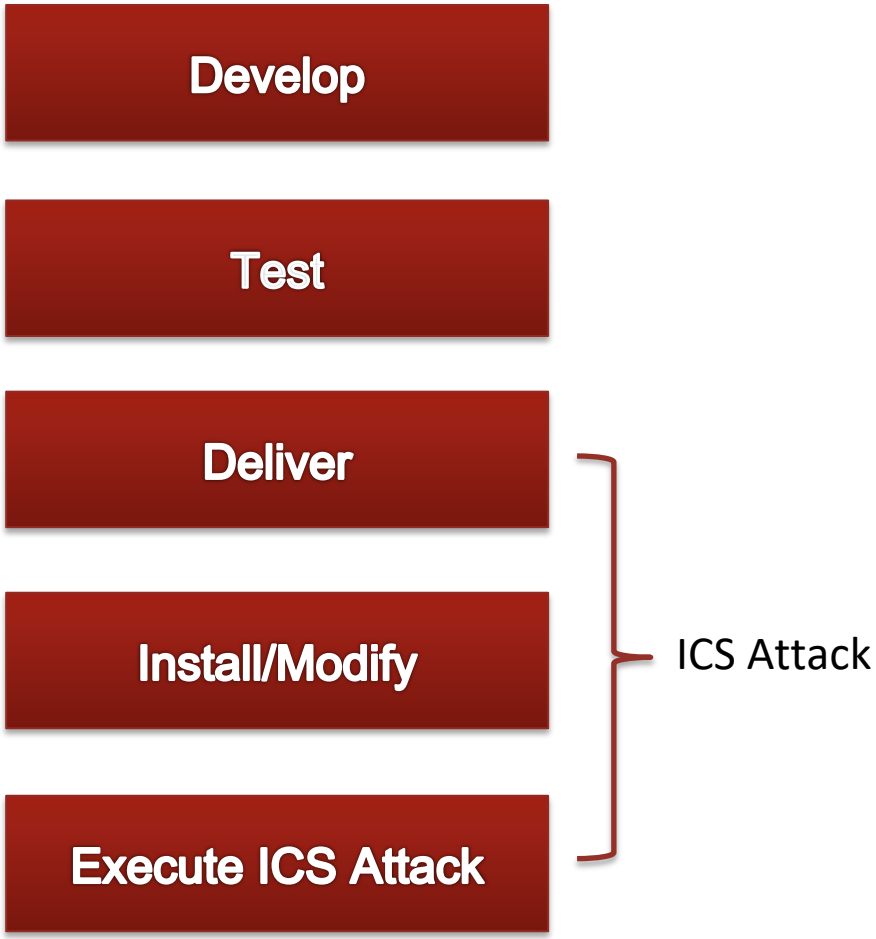
Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

From: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, by Hutchins et al, Lockheed Martin Corporation



The Purdue Model

The ICS Kill Chain

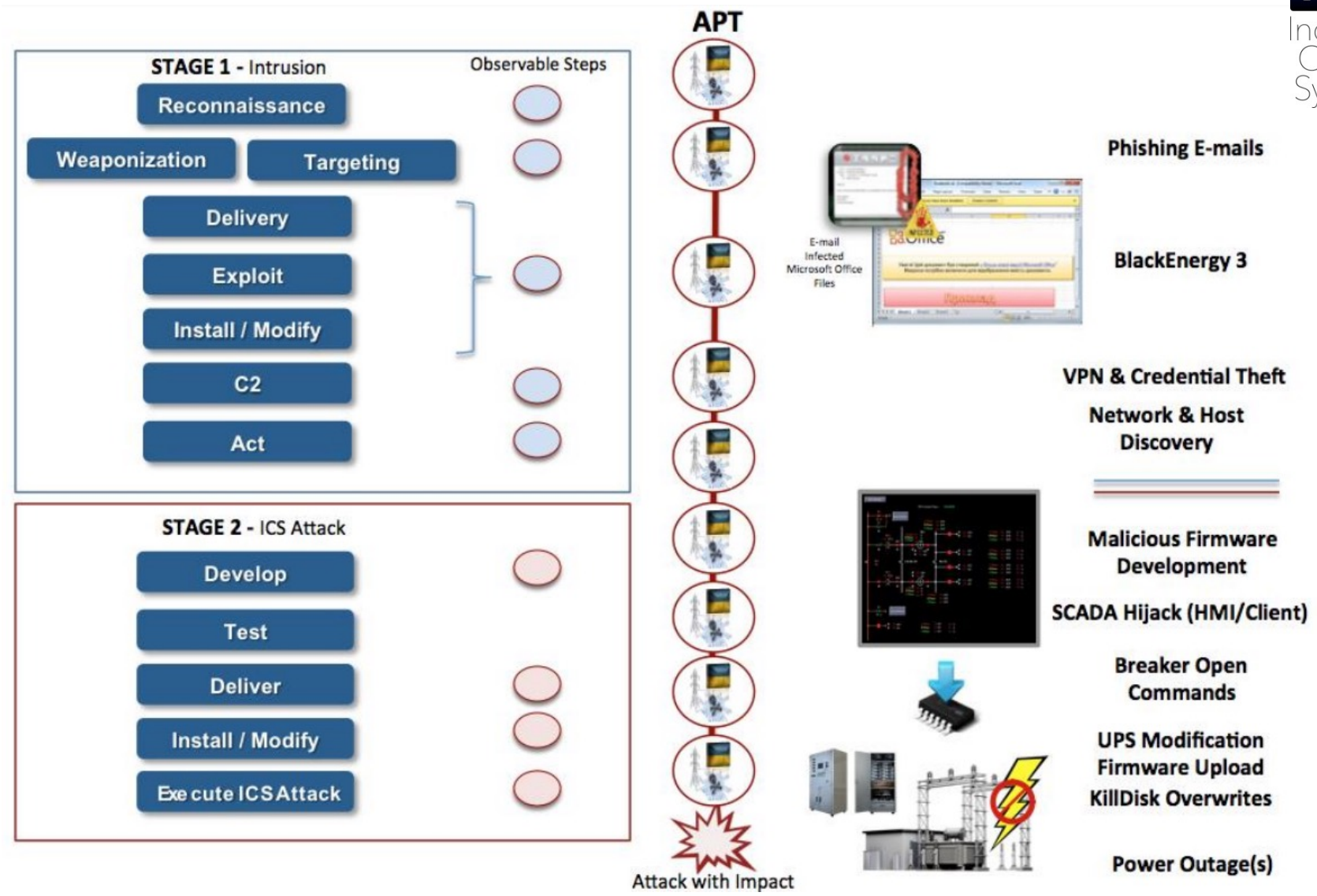


Validation

- Testing on target system
- Construction of testbed facilities

Cyber Attack on the Ukrainian Power Grid

SANS ICS Industrial Control Systems



Completion of Stage 1 of the ICS Cyber Kill Chain:

Identify and gain access to a system able to communicate with target SIS.

Stage 2 Develop:

Identify target SIS type and develop TRISIS with replacement logic and loader

Stage 2 Test:

Ensure TRISIS works as intended, likely off network in the adversary environment

Stage 2 Deliver:

Transfer TRISIS to the SIS which contains the 'loader' module for the new logic and support binaries that provide the new logic

Stage 2 Install/Modify:

Upon running the TRISIS executable, disguised as Triconex software for analyzing SIS logs, the malicious software utilizes the embedded binary files to identify the appropriate location in memory on the controller for logic replacement and uploads the 'initializing code' (4-byte sequence)

Stage 2 Execute ICS Attack:

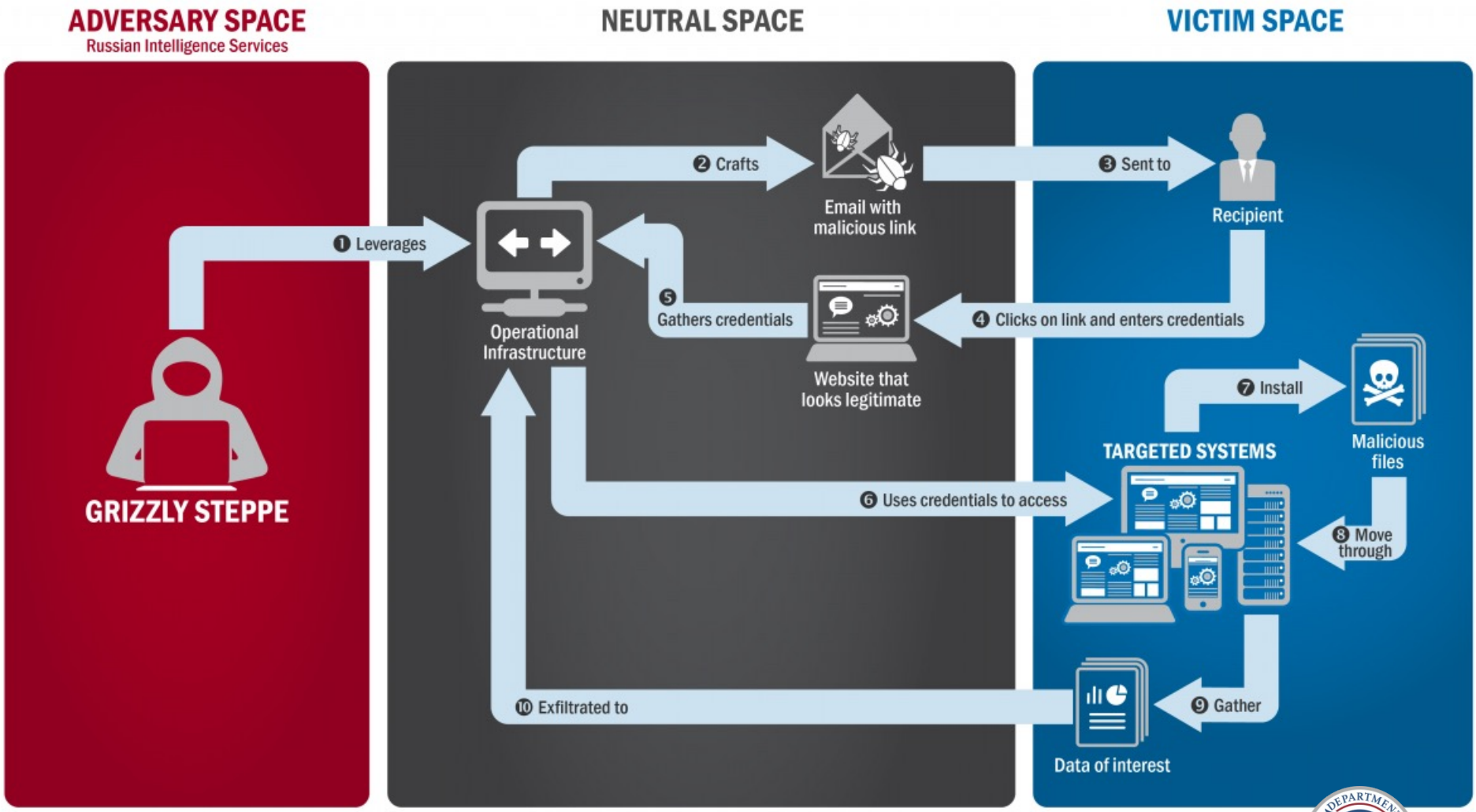
TRISIS verifies the success of the previous step and then uploads new ladder logic to SIS

Figure 4: TRISIS Attack Flow

Triton/Trisis

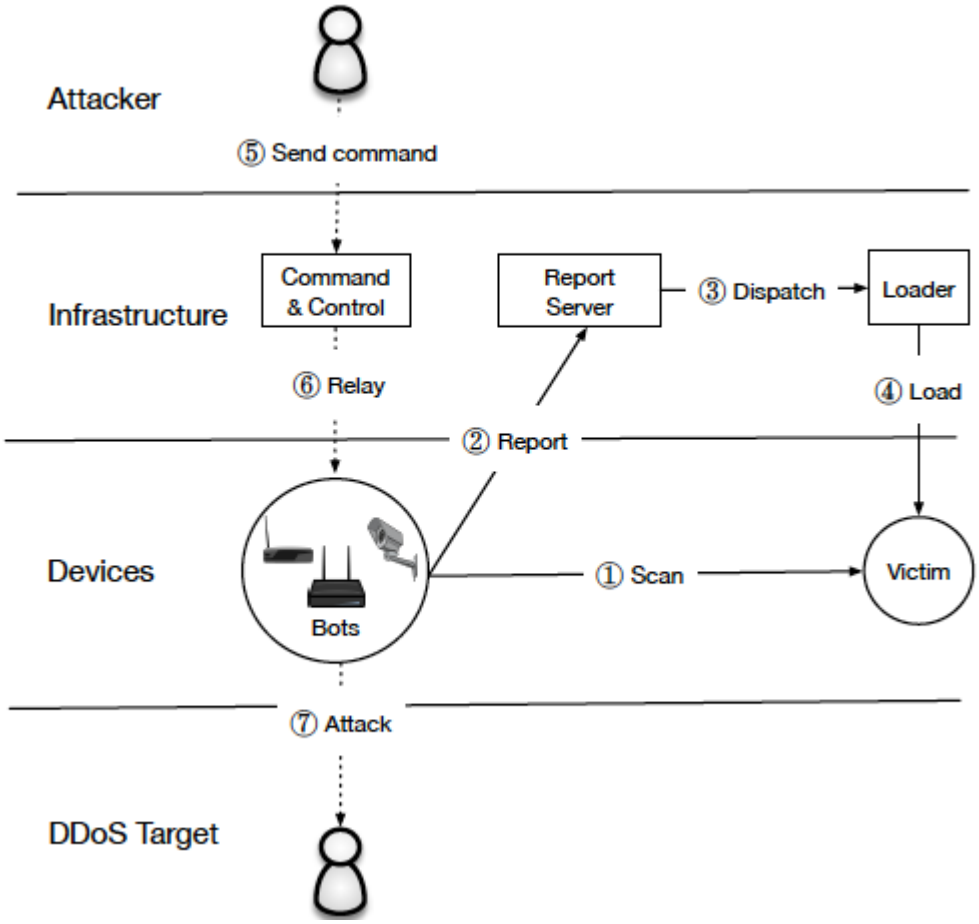
Source: Trisis Malware, Dragos

Vermont Electric Company



Other Attacks

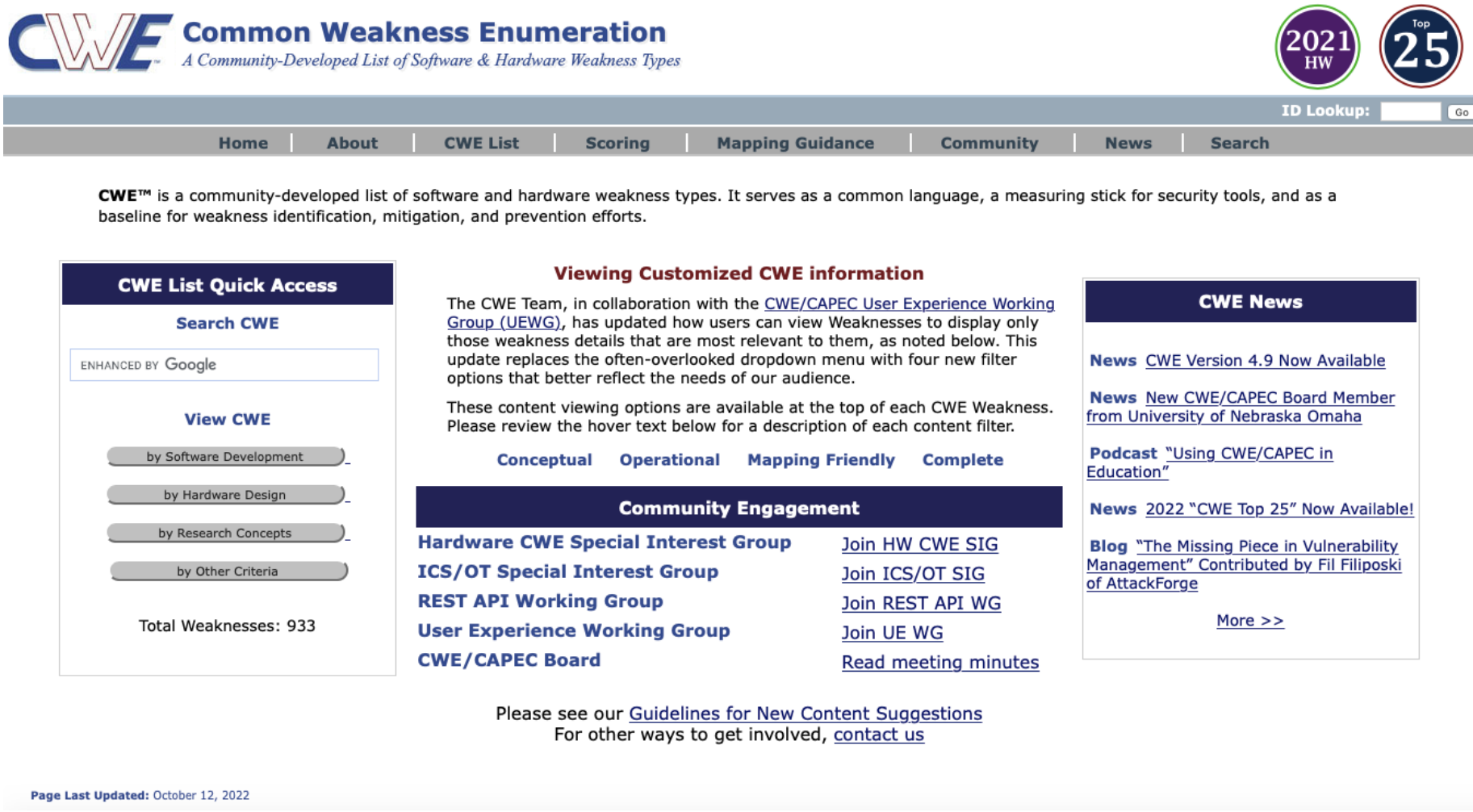
- Shamoon – wiper attack in Middle East; 2012 to 2018 (ongoing)
- Petya – ransomware using same EternalBlue exploit as WannaCry; 2016
- NOTPetya – masquerading as ransomware; 2017
- Mirai – IoT devices; 2016



Mirai Botnet

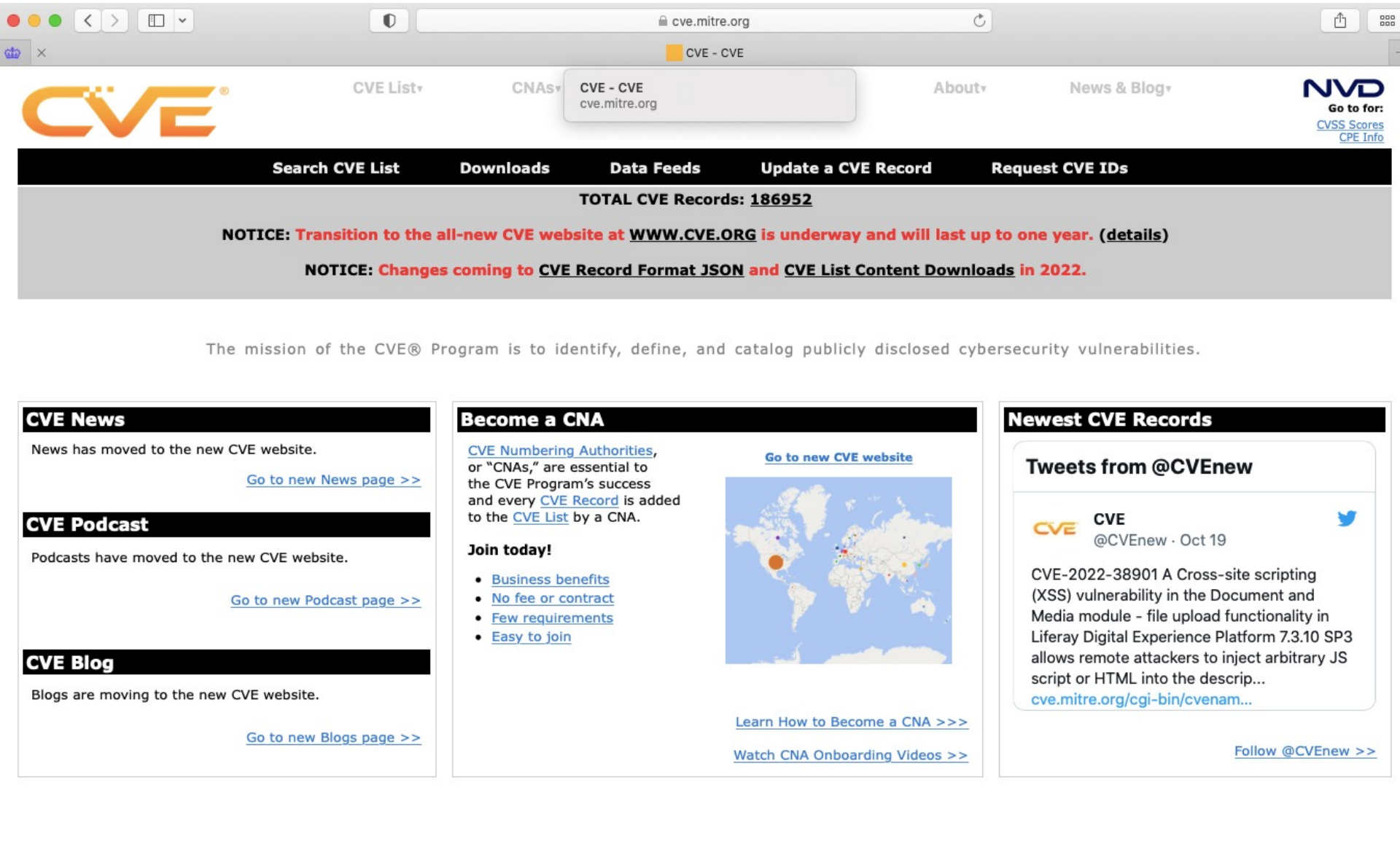
Understanding the Mirai Botnet, Antonakakis et al

CWE


Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types
2021 HW
Top 25
ID Lookup:
Go
Home
About
CWE List
Scoring
Mapping Guidance
Community
News
Search
CWE™ is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.
CWE List Quick Access
Search CWE
ENHANCED BY Google
View CWE
by Software Development
by Hardware Design
by Research Concepts
by Other Criteria
Total Weaknesses: 933
Viewing Customized CWE information
The CWE Team, in collaboration with the CWE/CAPEC User Experience Working Group (UEWG), has updated how users can view Weaknesses to display only those weakness details that are most relevant to them, as noted below. This update replaces the often-overlooked dropdown menu with four new filter options that better reflect the needs of our audience.
These content viewing options are available at the top of each CWE Weakness. Please review the hover text below for a description of each content filter.
Conceptual Operational Mapping Friendly Complete
Community Engagement
Hardware CWE Special Interest Group
Join HW CWE SIG
ICS/OT Special Interest Group
Join ICS/OT SIG
REST API Working Group
Join REST API WG
User Experience Working Group
Join UE WG
CWE/CAPEC Board
Read meeting minutes
CWE News
News CWE Version 4.9 Now Available
News New CWE/CAPEC Board Member from University of Nebraska Omaha
Podcast "Using CWE/CAPEC in Education"
News 2022 "CWE Top 25" Now Available!
Blog "The Missing Piece in Vulnerability Management" Contributed by Fil Filiposki of AttackForge
More >>
Please see our Guidelines for New Content Suggestions
For other ways to get involved, contact us
Page Last Updated: October 12, 2022

Rank	ID	Name	Score	KEV Count (CVEs)	Rank Change vs. 2021
1	CWE-787	Out-of-bounds Write	64.20	62	0
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.97	2	0
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22.11	7	+3 ▲
4	CWE-20	Improper Input Validation	20.63	20	0
5	CWE-125	Out-of-bounds Read	17.67	1	-2 ▼
6	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17.53	32	-1 ▼
7	CWE-416	Use After Free	15.50	28	0
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.08	19	0
9	CWE-352	Cross-Site Request Forgery (CSRF)	11.53	1	0
10	CWE-434	Unrestricted Upload of File with Dangerous Type	9.56	6	0
11	CWE-476	NULL Pointer Dereference	7.15	0	+4 ▲
12	CWE-502	Deserialization of Untrusted Data	6.68	7	+1 ▲
13	CWE-190	Integer Overflow or Wraparound	6.53	2	-1 ▼
14	CWE-287	Improper Authentication	6.35	4	0
15	CWE-798	Use of Hard-coded Credentials	5.66	0	+1 ▲
16	CWE-862	Missing Authorization	5.53	1	+2 ▲
17	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	5.42	5	+8 ▲
18	CWE-306	Missing Authentication for Critical Function	5.15	6	-7 ▼
19	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	4.85	6	-2 ▼
20	CWE-276	Incorrect Default Permissions	4.84	0	-1 ▼
21	CWE-918	Server-Side Request Forgery (SSRF)	4.27	8	+3 ▲
22	CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	3.57	6	+11 ▲
23	CWE-400	Uncontrolled Resource Consumption	3.56	2	+4 ▲
24	CWE-611	Improper Restriction of XML External Entity Reference	3.38	0	-1 ▼
25	CWE-94	Improper Control of Generation of Code ('Code Injection')	3.32	4	+3 ▲

CVE

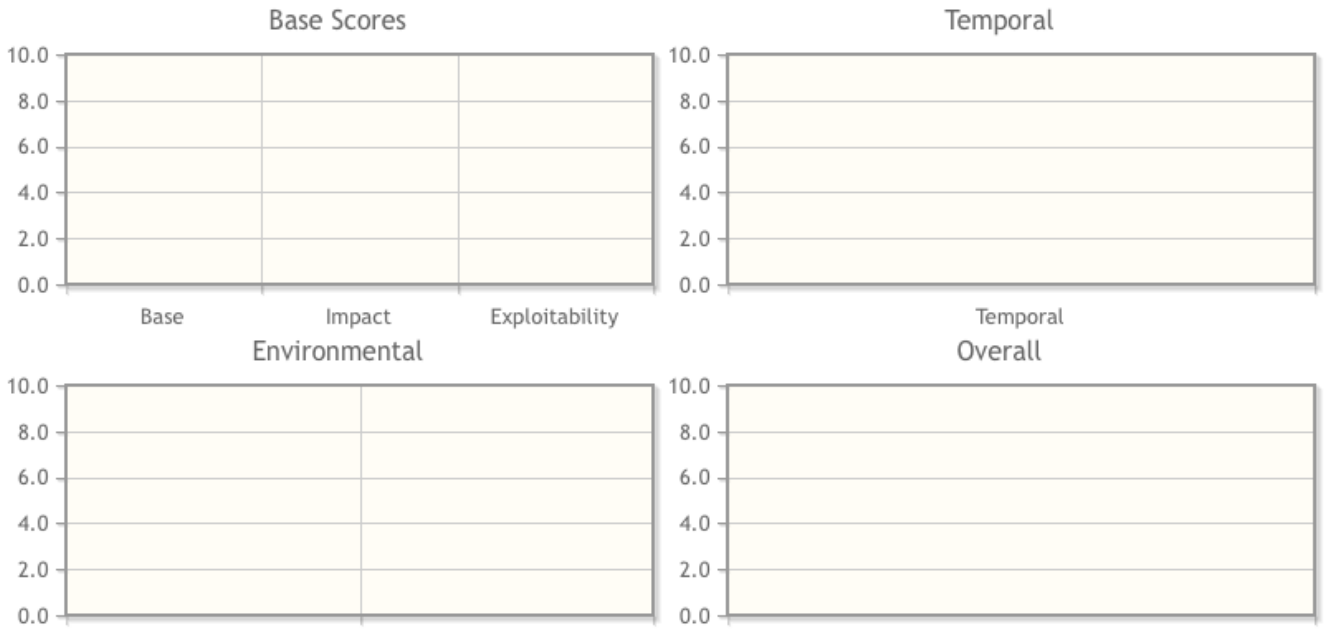

cve.mitre.org
CVE - CVE
CVE - CVE
cve.mitre.org
CVE List
CNAs
About
News & Blog
NVD
Go to for:
CVSS Scores
CPE Info
Search CVE List
Downloads
Data Feeds
Update a CVE Record
Request CVE IDs
TOTAL CVE Records: 186952
NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG is underway and will last up to one year. (details)
NOTICE: Changes coming to CVE Record Format JSON and CVE List Content Downloads in 2022.
The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.
CVE News
News has moved to the new CVE website.
Go to new News page >>
CVE Podcast
Podcasts have moved to the new CVE website.
Go to new Podcast page >>
CVE Blog
Blogs are moving to the new CVE website.
Go to new Blogs page >>
Become a CNA
CVE Numbering Authorities, or "CNAs," are essential to the CVE Program's success and every CVE Record is added to the CVE List by a CNA.
Join today!
Business benefits
No fee or contract
Few requirements
Easy to join
Go to new CVE website
Learn How to Become a CNA >>>
Watch CNA Onboarding Videos >>
Newest CVE Records
Tweets from @CVEnew
CVE
@CVEnew · Oct 19
CVE-2022-38901 A Cross-site scripting (XSS) vulnerability in the Document and Media module - file upload functionality in Liferay Digital Experience Platform 7.3.10 SP3 allows remote attackers to inject arbitrary JS script or HTML into the descrip...
cve.mitre.org/cgi-bin/cvenam...
Follow @CVEnew >>

CVSS

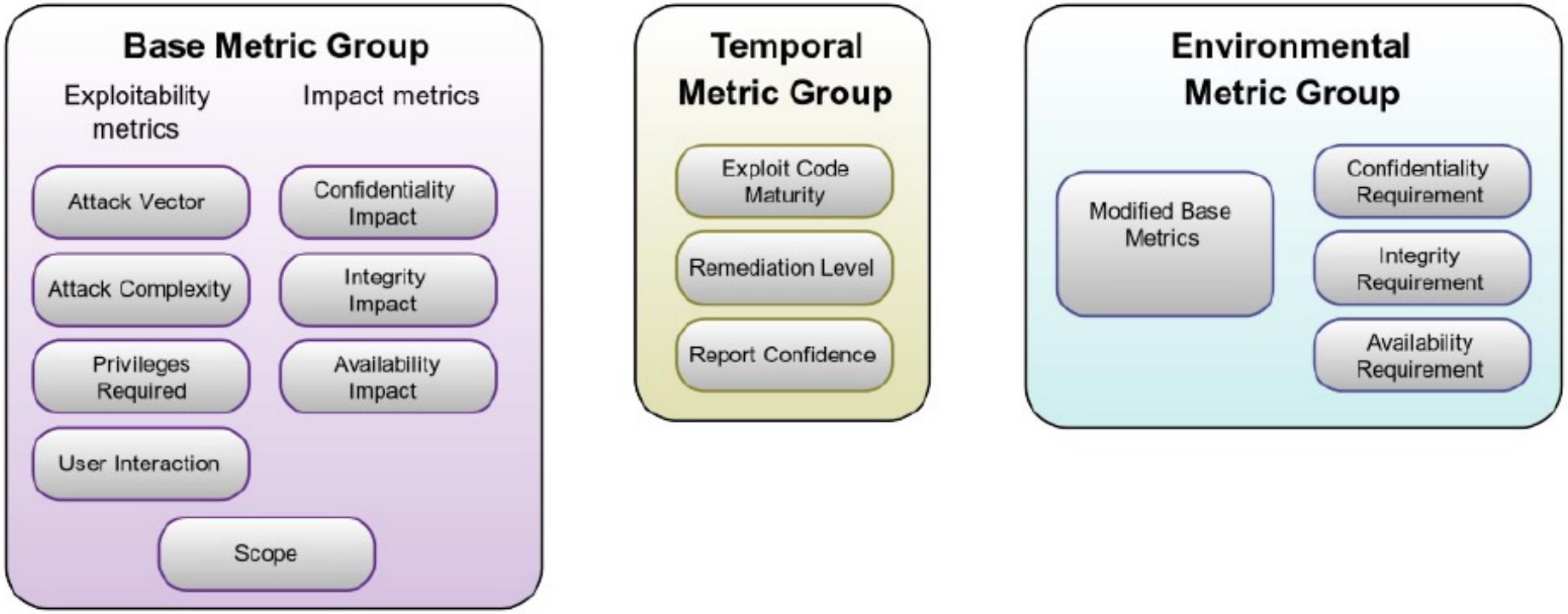
nvd.nist.gov

Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS continued



Common Vulnerability Scoring System Version 3.1 Calculator

Hover over metric group names, metric names and metric values for a summary of the information in the official CVSS v3.1 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, and notes on using this calculator (including its design and an XML representation for CVSS v3.1).

Base Score

Select values for all base metrics to generate score

Attack Vector (AV)

Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)

Low (L) | High (H)

Privileges Required (PR)

None (N) | Low (L) | High (H)

User Interaction (UI)

None (N) | Required (R)

Scope (S)

Unchanged (U) | Changed (C)

Confidentiality (C)

None (N) | Low (L) | High (H)

Integrity (I)

None (N) | Low (L) | High (H)

Availability (A)

None (N) | Low (L) | High (H)

Base Score

8.6
(High)

Attack Vector (AV)

Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)

Low (L) | High (H)

Privileges Required (PR)

None (N) | Low (L) | High (H)

User Interaction (UI)

None (N) | Required (R)

Scope (S)

Unchanged (U) | Changed (C)

Confidentiality (C)

None (N) | Low (L) | High (H)

Integrity (I)

None (N) | Low (L) | High (H)

Availability (A)

None (N) | Low (L) | High (H)

Vector String -

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Temporal Score

Select values for all base metrics to generate score

Exploit Code Maturity (E)

Not Defined (X) | Unproven (U) | Proof-of-Concept (P) | Functional (F) | High (H)

Remediation Level (RL)

Not Defined (X) | Official Fix (O) | Temporary Fix (T) | Workaround (W) | Unavailable (U)

Report Confidence (RC)

Not Defined (X) | Unknown (U) | Reasonable (R) | Confirmed (C)

Environmental Score

Select values for all base metrics to generate score

Confidentiality Requirement (CR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Integrity Requirement (IR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Availability Requirement (AR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Modified Attack Vector (MAV)

Not Defined (X) | Network | Adjacent Network | Local | Physical

Modified Attack Complexity (MAC)

Not Defined (X) | Low | High

Modified Privileges Required (MPR)

Not Defined (X) | None | Low | High

Modified User Interaction (MUI)

Not Defined (X) | None | Required

Modified Scope (MS)

Not Defined (X) | Unchanged | Changed

Modified Confidentiality (MC)

Not Defined (X) | None | Low | High

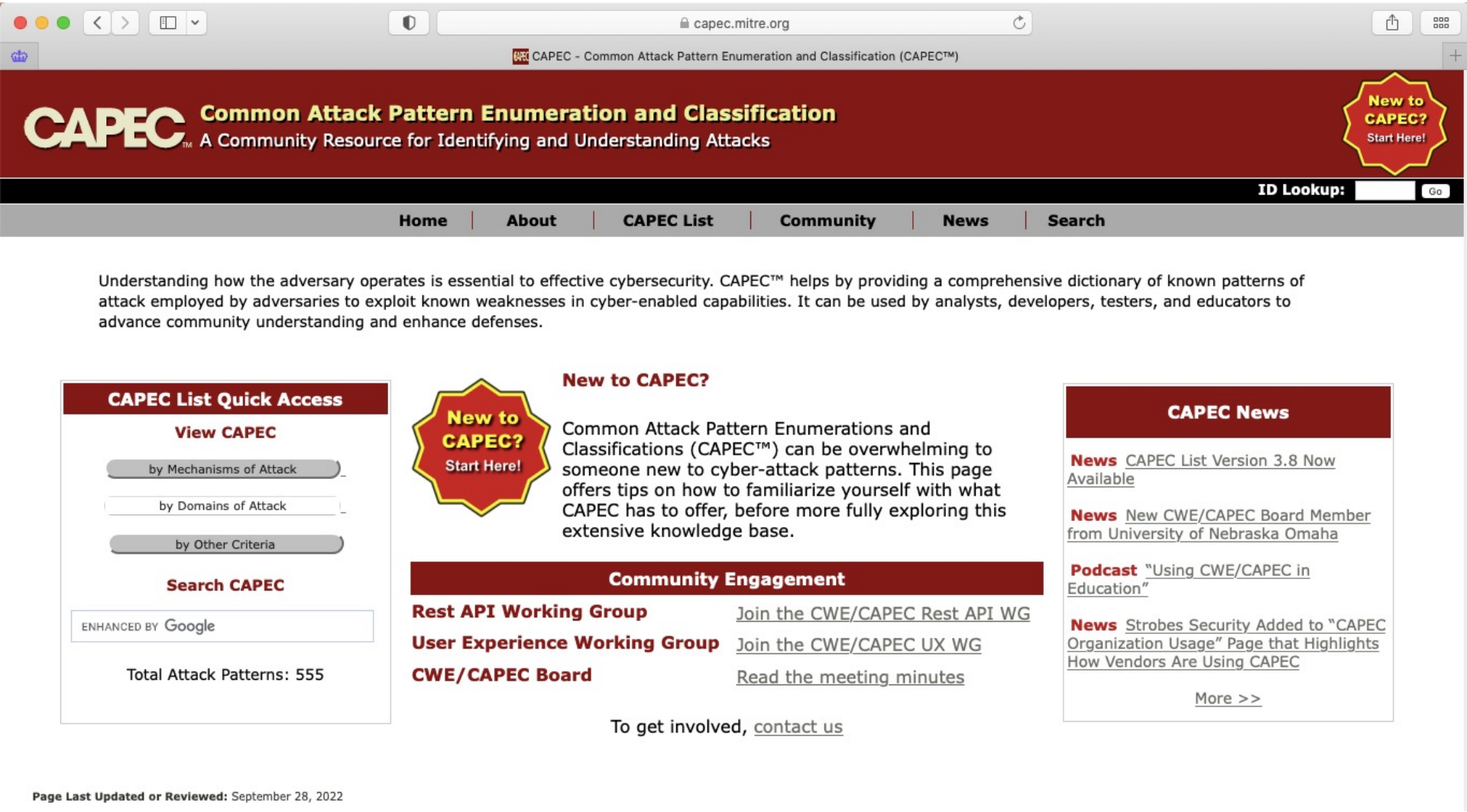
Modified Integrity (MI)

Not Defined (X) | None | Low | High

Modified Availability (MA)

Not Defined (X) | None | Low | High

CAPEC


capec.mitre.org
CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC™)
CAPEC
Common Attack Pattern Enumeration and Classification
A Community Resource for Identifying and Understanding Attacks
New to CAPEC? Start Here!
ID Lookup:
Go
Home
About
CAPEC List
Community
News
Search
Understanding how the adversary operates is essential to effective cybersecurity. CAPEC™ helps by providing a comprehensive dictionary of known patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities. It can be used by analysts, developers, testers, and educators to advance community understanding and enhance defenses.
CAPEC List Quick Access
View CAPEC
by Mechanisms of Attack
by Domains of Attack
by Other Criteria
Search CAPEC
ENHANCED BY Google
Total Attack Patterns: 555
New to CAPEC? Start Here!
New to CAPEC?
Common Attack Pattern Enumerations and Classifications (CAPEC™) can be overwhelming to someone new to cyber-attack patterns. This page offers tips on how to familiarize yourself with what CAPEC has to offer, before more fully exploring this extensive knowledge base.
Community Engagement
Rest API Working Group
Join the CWE/CAPEC Rest API WG
User Experience Working Group
Join the CWE/CAPEC UX WG
CWE/CAPEC Board
Read the meeting minutes
To get involved, contact us
CAPEC News
News CAPEC List Version 3.8 Now Available
News New CWE/CAPEC Board Member from University of Nebraska Omaha
Podcast "Using CWE/CAPEC in Education"
News Strobes Security Added to "CAPEC Organization Usage" Page that Highlights How Vendors Are Using CAPEC
More >>
Page Last Updated or Reviewed: September 28, 2022

CAPEC VIEW: Mechanisms of Attack

View ID: 1000
Structure: Graph

Status: Stable

Downloads: Booklet | CSV | XML

Objective

This view organizes attack patterns hierarchically based on mechanisms that are frequently employed when exploiting a vulnerability. The categories that are members of this view represent the different techniques used to attack a system. They do not, however, represent the consequences or goals of the attacks. There exists the potential for some attack patterns to align with more than one category depending on one's perspective. To counter this, emphasis was placed such that attack patterns as presented within each category use a technique not sometimes, but without exception.

Relationships

The following graph shows the tree-like relationships between attack patterns that exist at different levels of abstraction. At the highest level, categories exist to group patterns that share a common characteristic. Within categories, meta level attack patterns are used to present a decidedly abstract characterization of a methodology or technique. Below these are standard and detailed level patterns that are focused on a specific methodology or technique used.

Show Details:

Expand All | Collapse All

1000 - Mechanisms of Attack

- Engage in Deceptive Interactions - *(156)*
- Abuse Existing Functionality - *(210)*
- Manipulate Data Structures - *(255)*
- Manipulate System Resources - *(262)*
- Inject Unexpected Items - *(152)*
- Employ Probabilistic Techniques - *(223)*
- Manipulate Timing and State - *(172)*
- Collect and Analyze Information - *(118)*
- Subvert Access Control - *(225)*

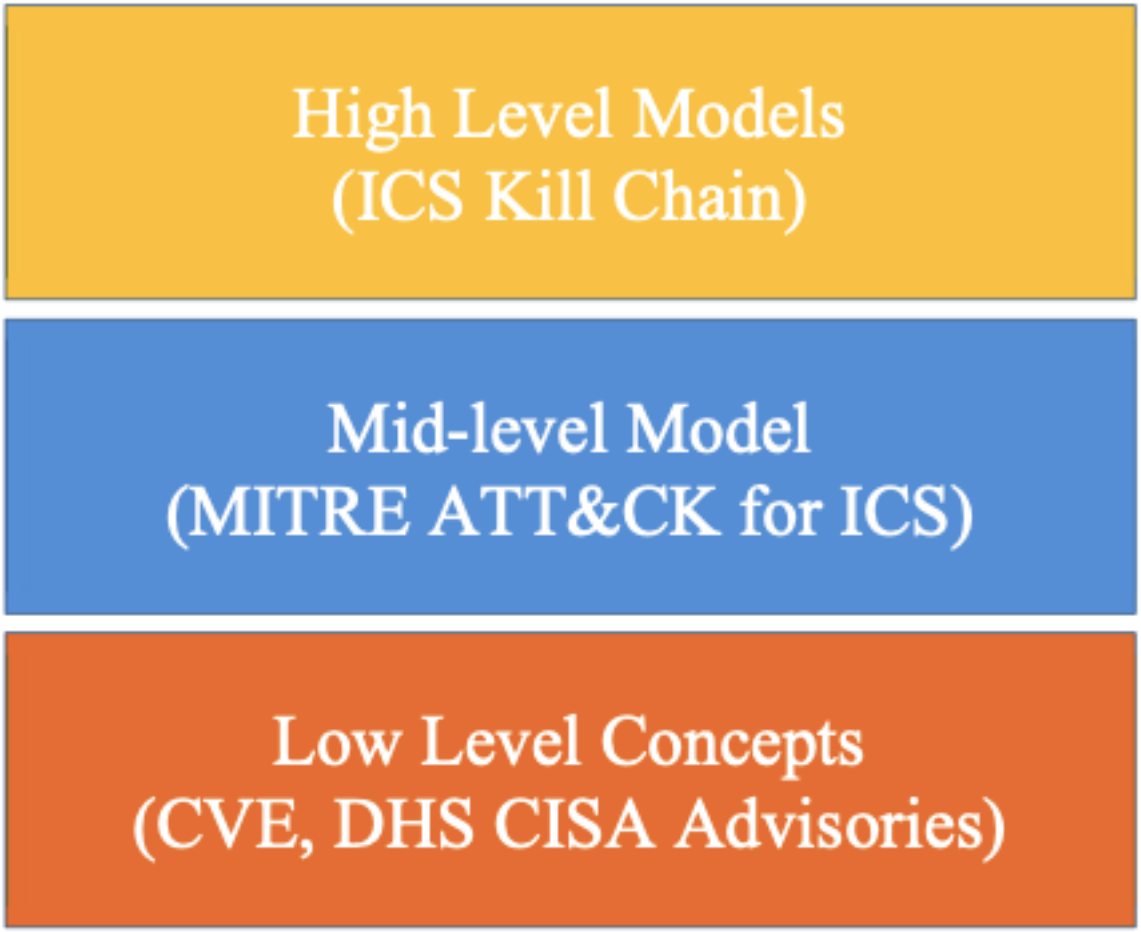
BACK TO TOP

View Metrics

	CAPECs in this view		Total CAPECs
Attack Patterns	517	out of	517
Categories	9	out of	49
Views	0	out of	9
Total	**526**	out of	575

MITRE ATT&CK For ICS

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		


High Level Models
(ICS Kill Chain)
Mid-level Model
(MITRE ATT&CK for ICS)
Low Level Concepts
(CVE, DHS CISA Advisories)

Comparison

- CAPEC is focused on application security
- ATT&CK is focused on network security:
  - Hunting for new threats
  - Enhancing threat intelligence
  - Adversary emulation

Summary

- Sophisticated attacks involve a long process, involving multiple phases – they are socio-technical
- Average time to detect a data breach currently 212 days and 75 days to fix (IBM)
- CWE, CVE focus on individual steps
- CAPEC, ATT&CK focus on whole attack
- Kill Chains and NIST provide more abstract view from attacker and defender perspectives.