FORESCOUT

Automated Cybersecurity Across Your Digital Terrain

AN INNOVATIVE, AUTOMATED APPROACH TO LEVERAGING THREAT INTEL FOR MODERN THREAT DETECTION AND RESPONSE

Liran Chen , CISSP

VP Of Technical Services
and Operations

Agenda:

Manage Cyber Risk & Mitigate Threats

01 **The Threat Terrain**

Why are we here today?

02 **ICEFALL threat Intelligence**

The Embedded Risk.

03 **Hacktivist**

IoT/OT targets.

04 **MITRE ATT&CK**

Limitations of traditional security siloed solutions.

05 **Connecting Risk and threat**

Trends Impacting Your Digital Terrain

Visibility Lags Behind The Expanding Attack Surface

75%

OF ORGANIZATIONS REPORT **WIDENING VISIBILITY GAPS IN END-USER AND IOT ASSETS.**

Attackers Are Targeting Unmanaged Systems

35%

OF ORGANIZATIONS HAD IOT/OT DEVICES **TARGETED DIRECTLY** OR **AS PART OF A LARGER ATTACK.**

Fragmented Security Products Create Alert Fatigue

450

ALERTS PER HOUR THAT ANALYSTS MUST INVESTIGATE.

1. Cybersecurity Asset Management Trends 2021 – Enterprise Strategy Group | 2. The State of IoT/OT Cybersecurity in the Enterprise - Ponemon Institute | 3. Top Security and Risk Management Trends 2021 - Gartner

Vedere Labs Forescout Research Who Are We

The Focus

‘*Boutique*’ threat intel team

- ✓Focus on threats against unmanaged devices (IoT/IoMT/OT)
- ✓Focus on the network (rather than the endpoint as most other mainstream labs)
- ✓10+ years experience in the field

The Threat Intel

- ✓ Original vulnerability research activities (180+ CVEs in 18 months)
- ✓ Manual and automatic analysis of malware samples collected on the ground, over our own Adversary Engagement Platform or observed over the networks of Forescout customers

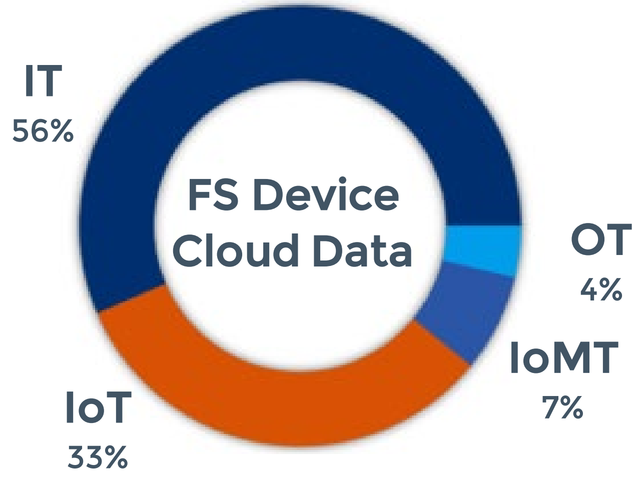
A Brief History of OT Attacks

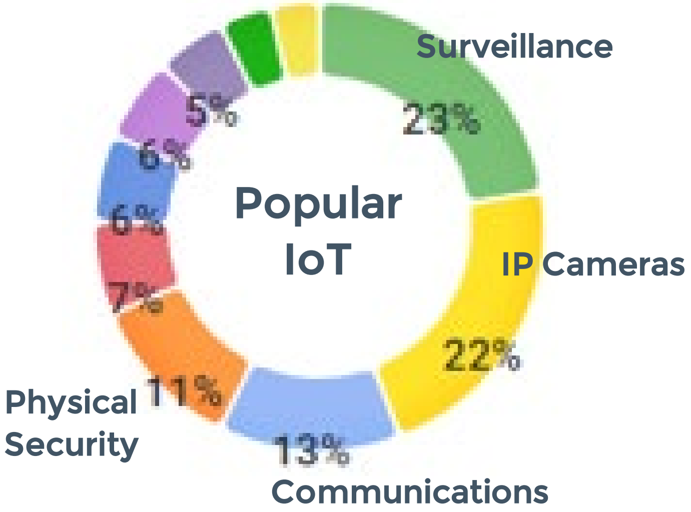
	Stuxnet 2010	Industroyer 1 (Crash Override) 2016	Triton 2017	Industroyer 2 2022	Ransomware (spills to OT) 2022
Description	First publicly known digital weapon developed	Fully automated malware that could detonate when the attackers wanted to	First attack to target Safety Instrumented System (SIS) controllers	Evolution of Industroyer 1. It focuses on IEC-104 protocol commonly used in the electric sector	Ransomware incidents impacting or reaching ICS systems (e.g., Colonial Pipeline, Water distribution)
Target	Sabotage nuclear enrichment facility in **Iran**	Cause an energy blackout in the **Ukrainian** capital, Kiev	A Saudi Arabian oil and gas facility. Attackers knew they could cause physical damage (even death)	(unsuccessful) cause a widespread power outages on April 8, 2022, in **Ukraine**	Medium Large organization in Services, Manufacturing and Retail
Threat Attribution	Gossip Girl, (a supra threat actor representing multiple countries, institutions or groups).	Sandworm APT, linked to the Russian GRU	A Russian government owned research center	Sandworm APT, linked to the Russian GRU	Conti, Revil, Clop (criminal gangs)
Main Features	Highly **sophisticated** Highly **targeted**	Low **sophistication** Multistage Automated	Highly **targeted** to a specific device (model and firmware version)	Low **sophistication** Less **targeted**	Non-targeted Opportunity driven **Cyber crime as a service**

source: https://cyberlaw.ccdcoe.org/wiki

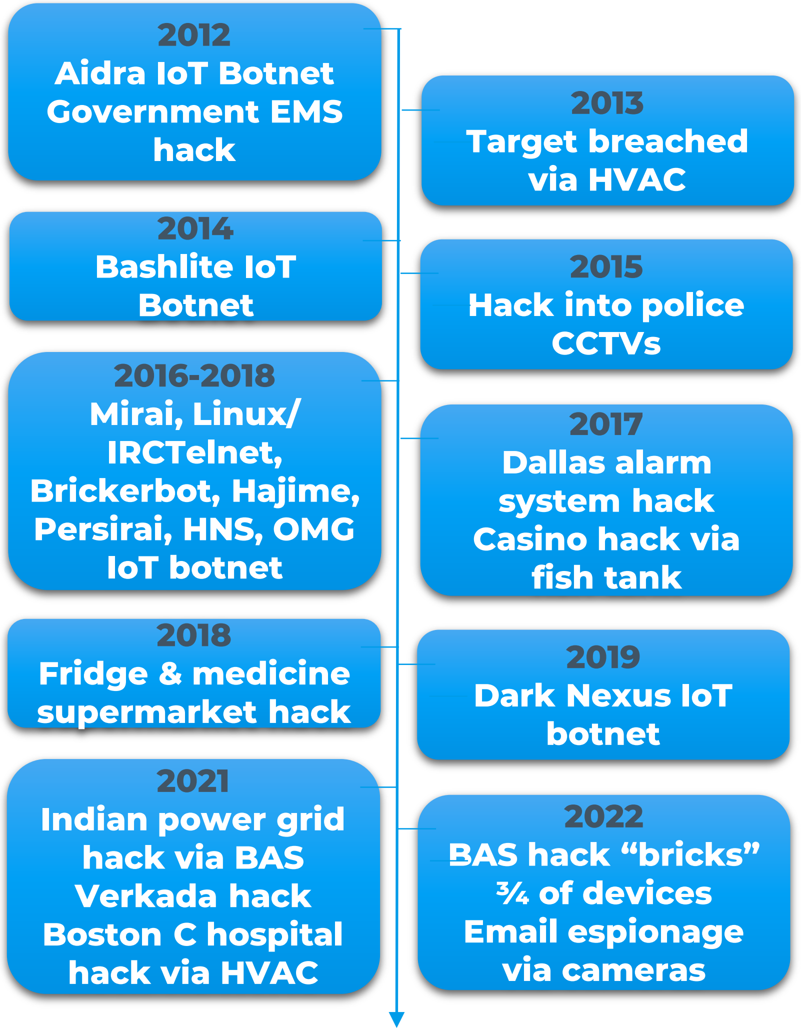
Key Current Trends

1. The device landscape is changing





2. IoT devices used as entry point for attacks



2012
Aidra IoT Botnet Government EMS hack

2013
Target breached via HVAC

2014
Bashlite IoT Botnet

2015
Hack into police CCTVs

2016-2018
Mirai, Linux/IRCTelnet, Brickerbot, Hajime, Persirai, HNS, OMG IoT botnet

2017
Dallas alarm system hack
Casino hack via fish tank

2018
Fridge & medicine supermarket hack

2019
Dark Nexus IoT botnet

2021
Indian power grid hack via BAS
Verkada hack
Boston C hospital hack via HVAC

2022
BAS hack "bricks" ¾ of devices
Email espionage via cameras

3. Attackers want money!

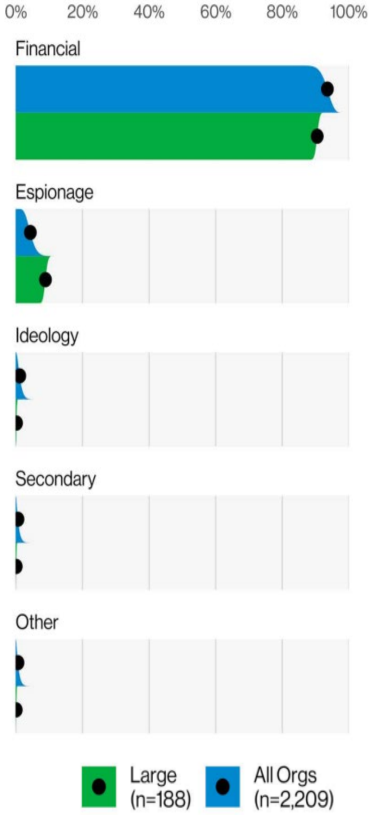


Figure 15. Motives in External actors by org size

https://www.verizon.com/business/resources/reports/dbir/

OT:ICEFALL

VEDERE LABS

How to Tackle a Decade of Insecure-by-Design Practices in OT

OT:ICEFALL Summary

Goals & Findings

- **Find and quantify** insecure-by-design vulnerabilities
- Discuss impact on OT **certification, risk management, supply chain, and offensive capabilities**
- **Public disclosure on June 21st:** 56 CVEs on 10 vendors

Impact & Mitigation

- Thousands of devices **exposed online**
- Devices often found on **critical infrastructure verticals** such as Oil & Gas, Power Generation & Distribution, Manufacturing, Water Treatment & Distribution, Building Automation
- Often no patches, but focus on **cyber hygiene**

Why Research Insecure-by-Design OT?

Past decade...

- Project Basecamp highlighted **insecure-by-design** critical OT devices and protocols

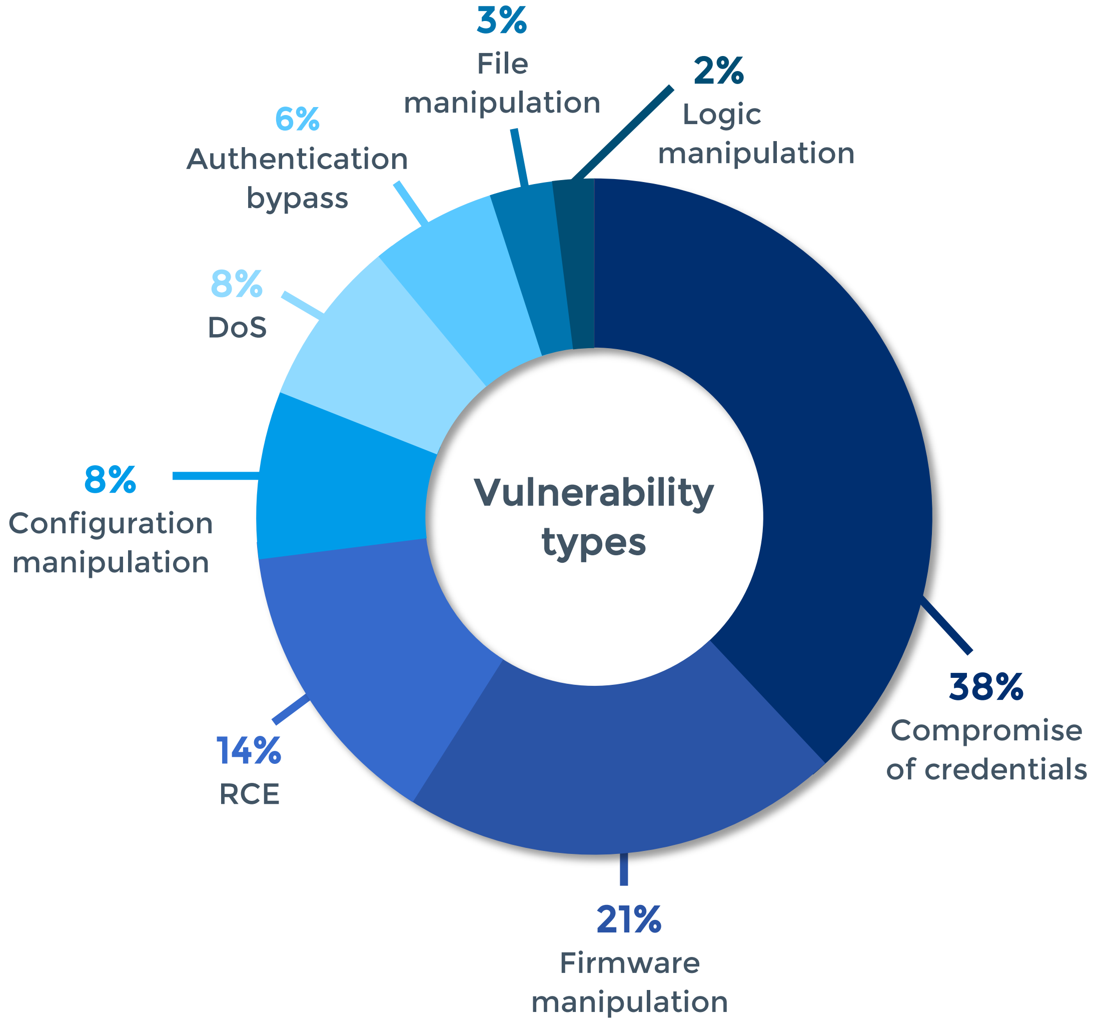
- **Real-world OT incidents** abusing insecure-by-design functionality such as:
  - Industroyer, TRITON, INCONTROLLER

Biggest issues facing OT security

- Persistent lack of **basic security controls**
- Opaque and proprietary nature of these systems

Vulnerabilities

Disclosure on June 21st



Impact of vulnerabilities

- Set of 56 CVEs demonstrating insecure-by-design practices in OT

4 main categories of vulnerabilities:

- Insecure engineering protocols
- Weak cryptography or broken authentication
- Insecure firmware updates
- Remote code execution

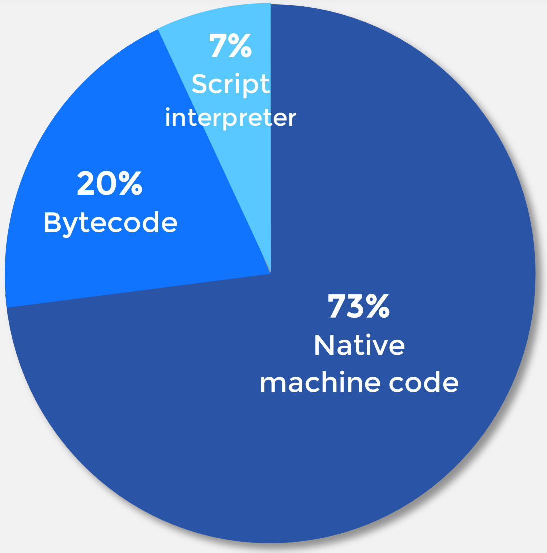
Affecting 10 vendors:

OMRON, Bently Nevada (a Baker Hughes business), EMERSON, Honeywell, JTEKT 株式会社ジェイテクト, SIEMENS, PHOENIX CONTACT, motorola, YOKOGAWA

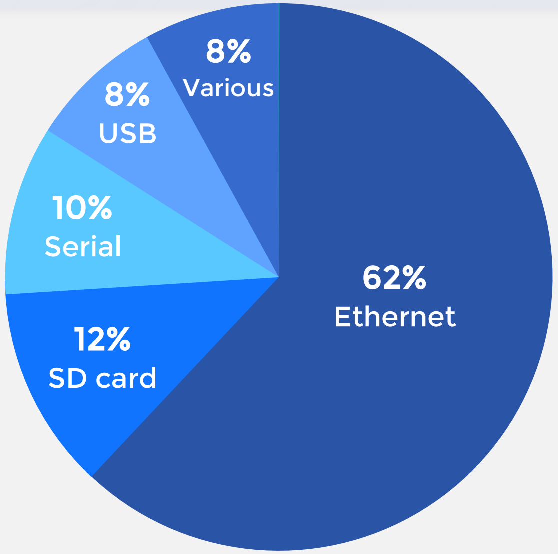
Not All Insecure Designs are Equal

Three main pathways to gaining RCE on level 1 devices via native functionality:

Logic downloads

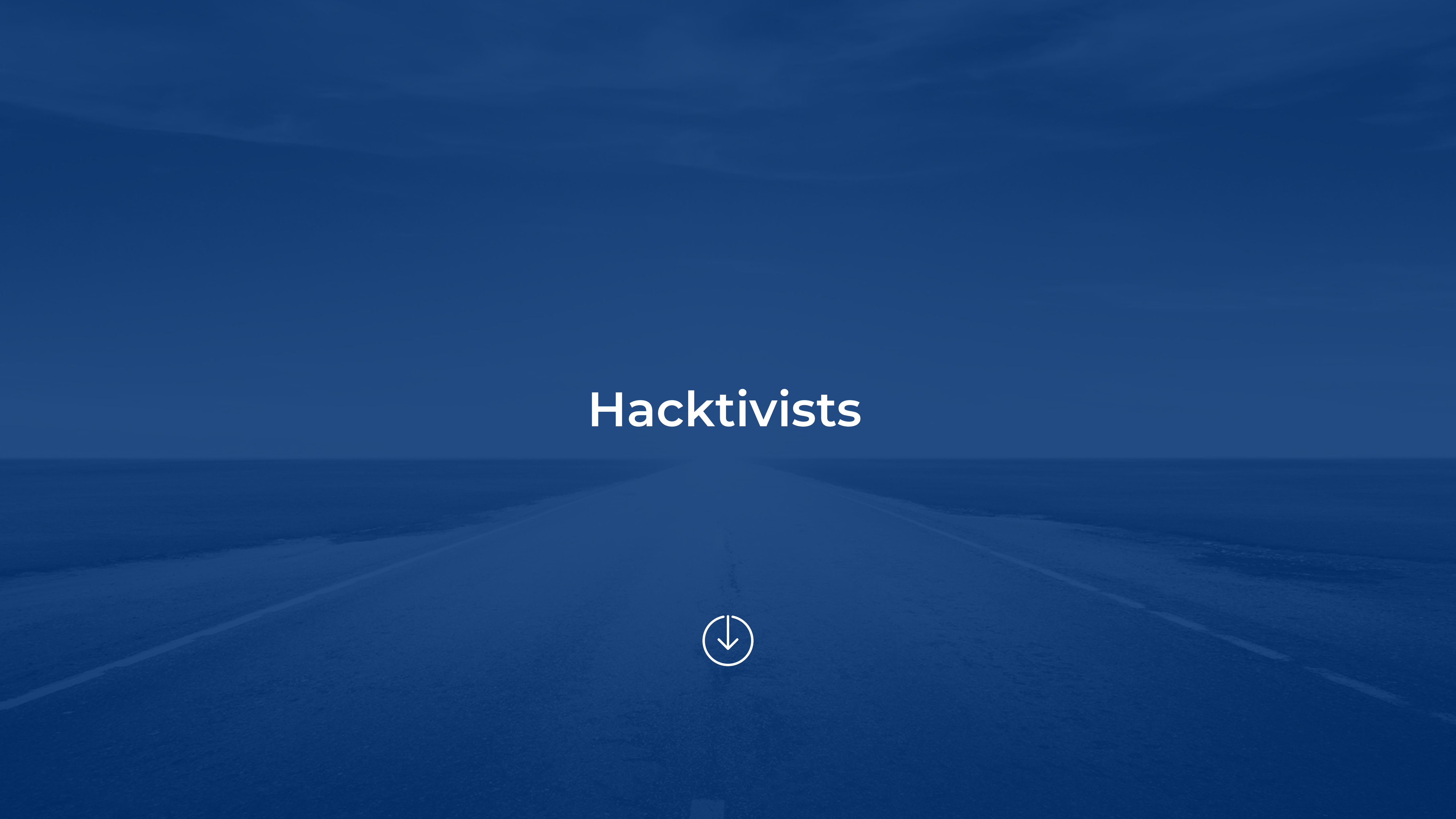


Firmware updates



Memory read and write operations

- None of the systems analyzed support logic signing and most (52%) compile their logic to native machine code
- 62% of those systems accept firmware downloads via Ethernet, while only 51% have authentication for this functionality.



Hacktivists

Hacktivist Groups are Targeting IoT/OT

General Trends

- **False Myths**: OT is only being exploited by state actor malware or cybercriminal gangs
- **The Social Plague**: Hacktivists **brag about** their attacks on social media platforms (likely to inspire next generations of threat actors to go even further in their attacks)

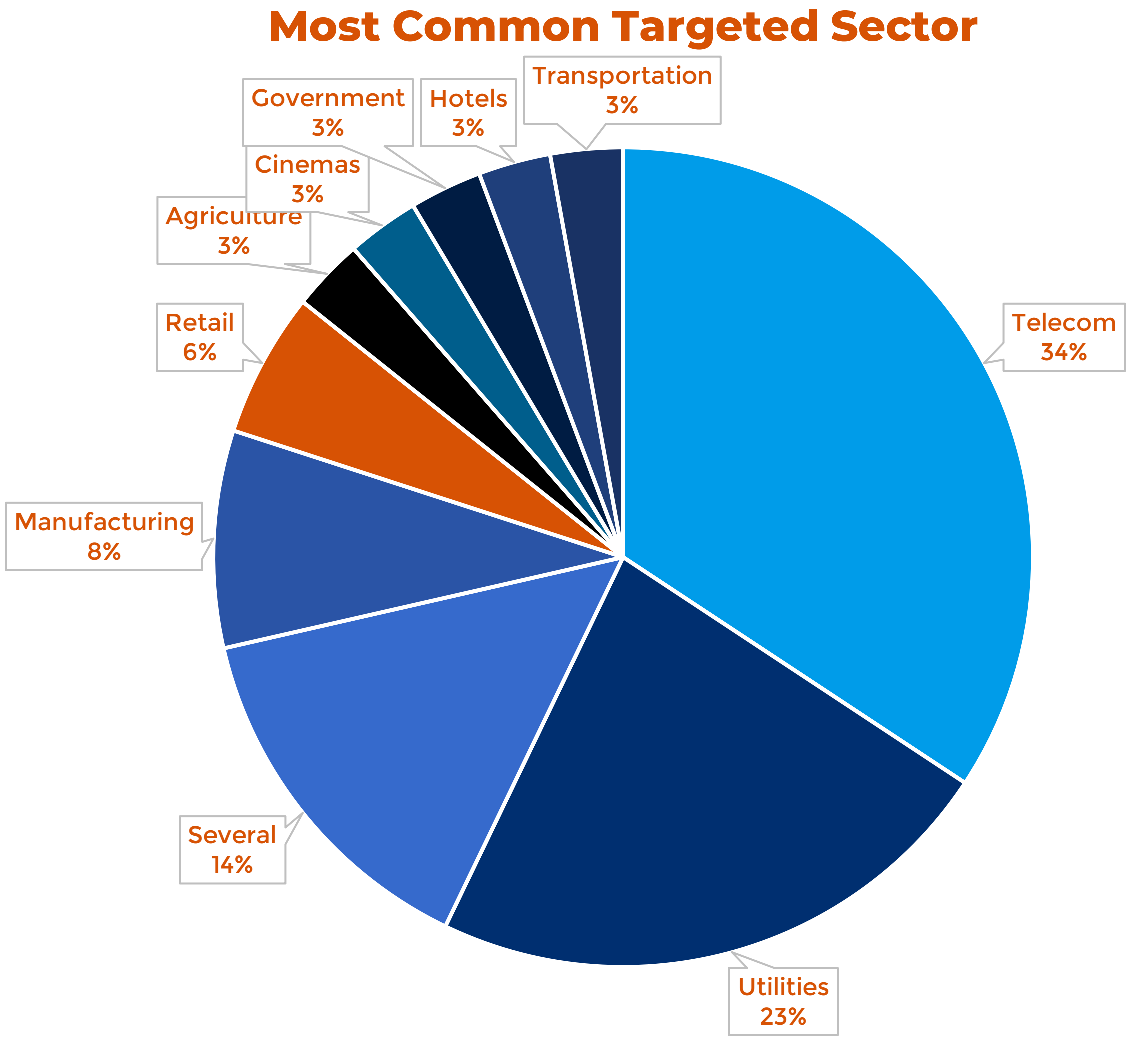
GhostSec

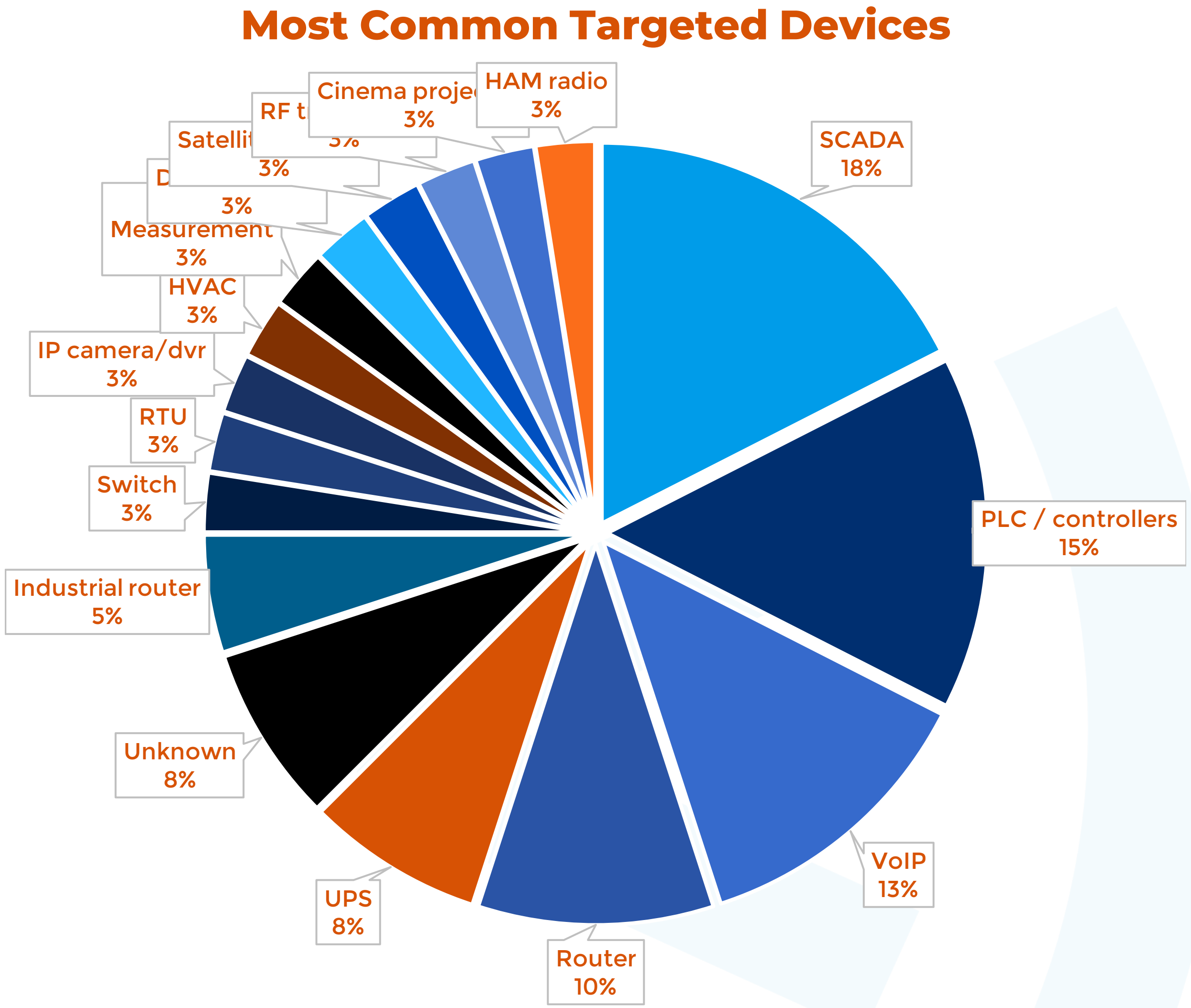
- Founded in 2015 with initiatives against ISIS
- ~16 members
- Highly organized activist group
- Heavy presence on Twitter and Telegram
- Has ties with Anonymous

OneFist

- Founded in March 2022 as a pro Ukrainian group
- Members are international
- All their targets are located in Russia
- Their main goal is to denying availability of services or causing physical destruction.

Hacktivists – Main Targets





Hacktivists - Common TTPs

INTERNET

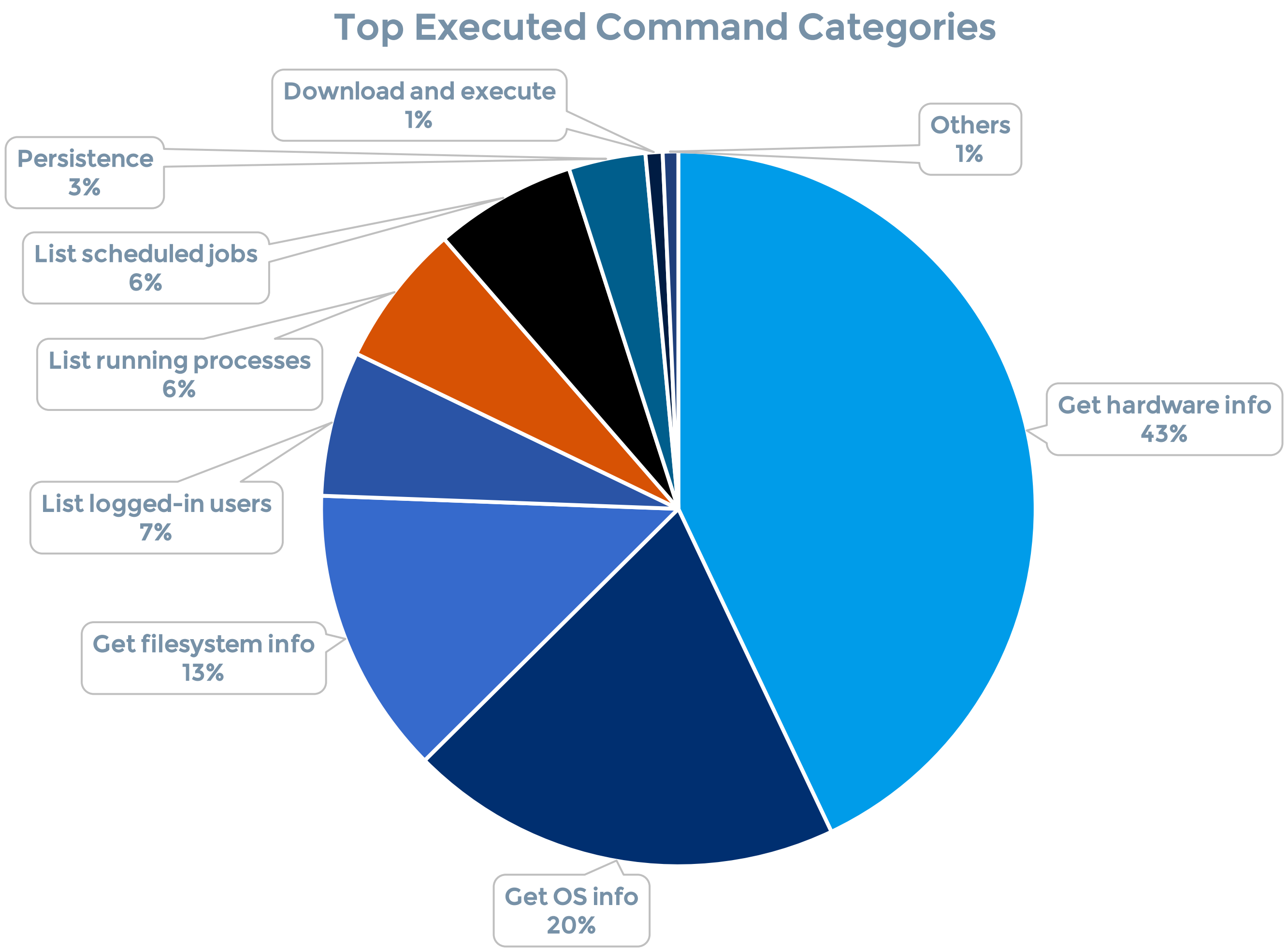
Shodan, Censys and Kamerka are used to discover **exposed devices** in the targeted countries

Routers and IP cameras are often compromised via either **default** or weak **credentials.**

Known vulnerabilities are being used to gain access to exposed routers.

Threat Actors develop **custom tools** for data collection and attack execution

After initial access, attackers explore the system



Data Points

After initial access, attackers spend time getting information on the target system

The most common tactics include Discovery (95%), Persistence (3%) and Execution (1%)

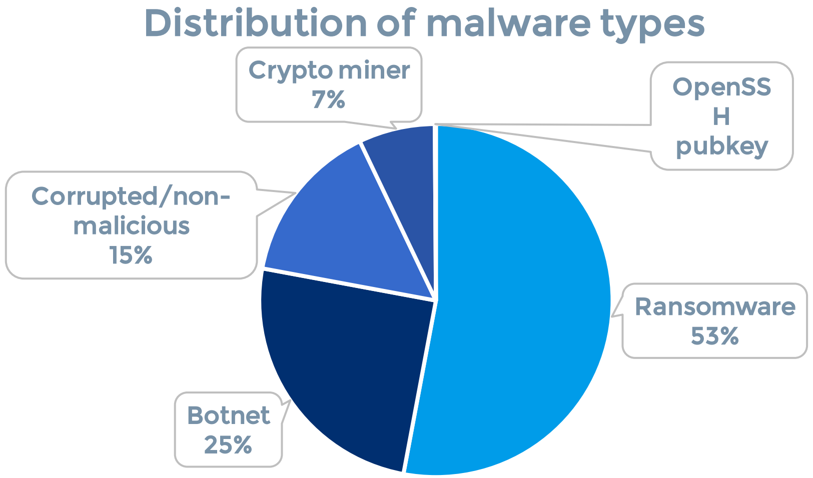
Tips for Defenders

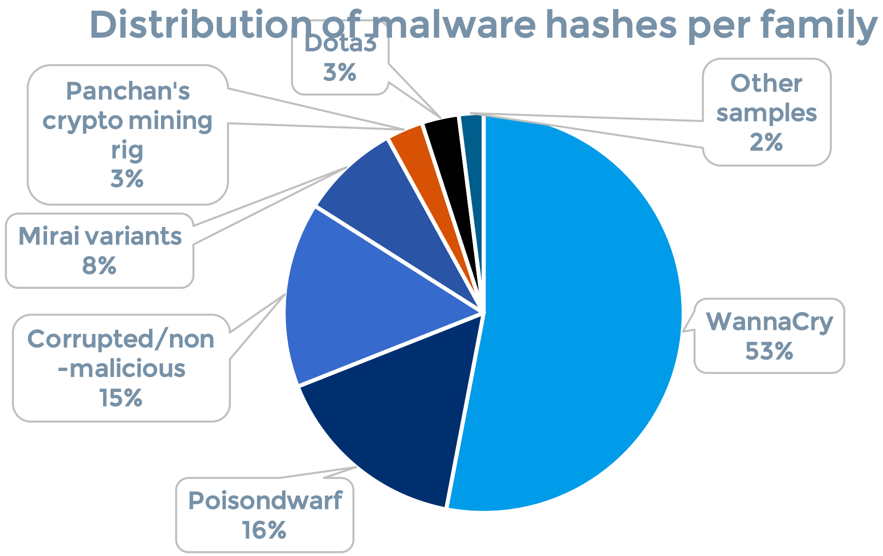
While attackers explore the systems, defenders get some buffer time to identify and mitigate malicious activities

Endpoint security capabilities needs to be enabled.

TA0007 – Discovery (95%) / TA0003 – Persistence (3%) / TA0002 – Execution (1%)

And then drop malware





Data Points

There are endemic threats such as the WannaCry ransomware and variants of the Mirai botnet that will probably never go away

Large hosting providers such as Google Cloud, OVH SAS are used by attackers to host malware

Tips for Defenders

Malware hashes are insufficient as IoCs because some malware changes its hash for each new victim.

Better to detect/hunt for TTPs and anomalous behavior than to rely solely on IoCs

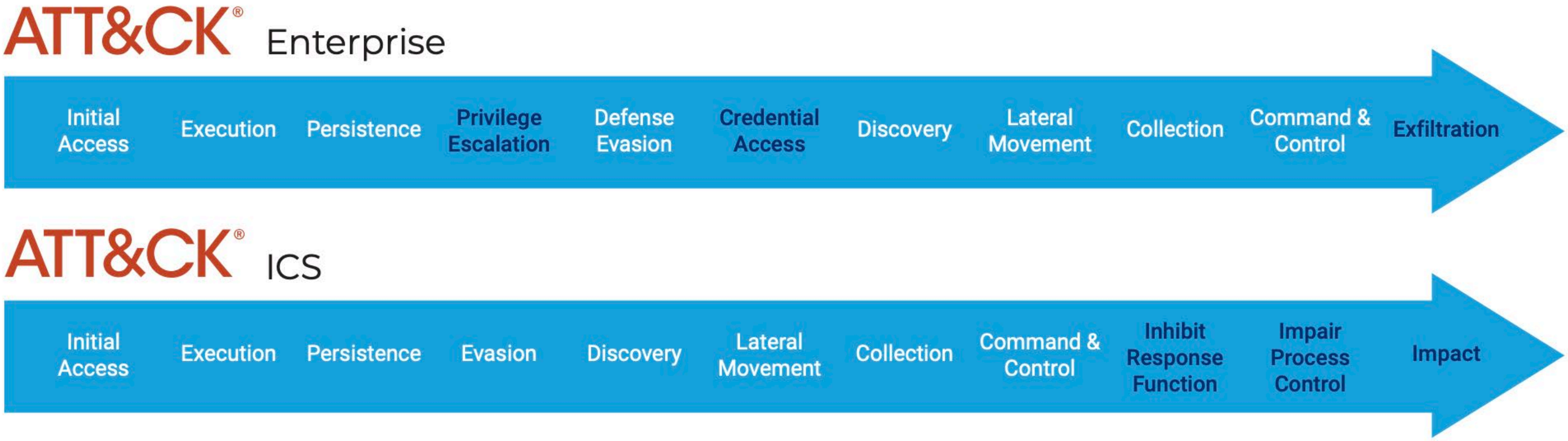
MITRE ATT&CK

Why Use MITRE ATT&CK

- ATT&CK stands for Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). MITRE Ingenuity ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
- main challenges in cybersecurity is the semantic gap between attackers and defenders
- While attackers think strategically and employ different TTPs to achieve their goals, defenders must process low-level events that are generated by IDS that only provide information about small steps within larger attacks.
- **Tactics** refer to the objectives that attackers want to achieve, such as gaining initial access into a network.
- **Techniques** are the actions that attackers take to achieve a tactical objective, such as exploit public facing applications.
- **Procedures** are specific implementation examples of Techniques used by adversaries, such as using sqlmap for SQL injection

Microsoft Distinguished Engineer John Lambert: “Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.”

MITRE ATT&CK Mapping - Tactics



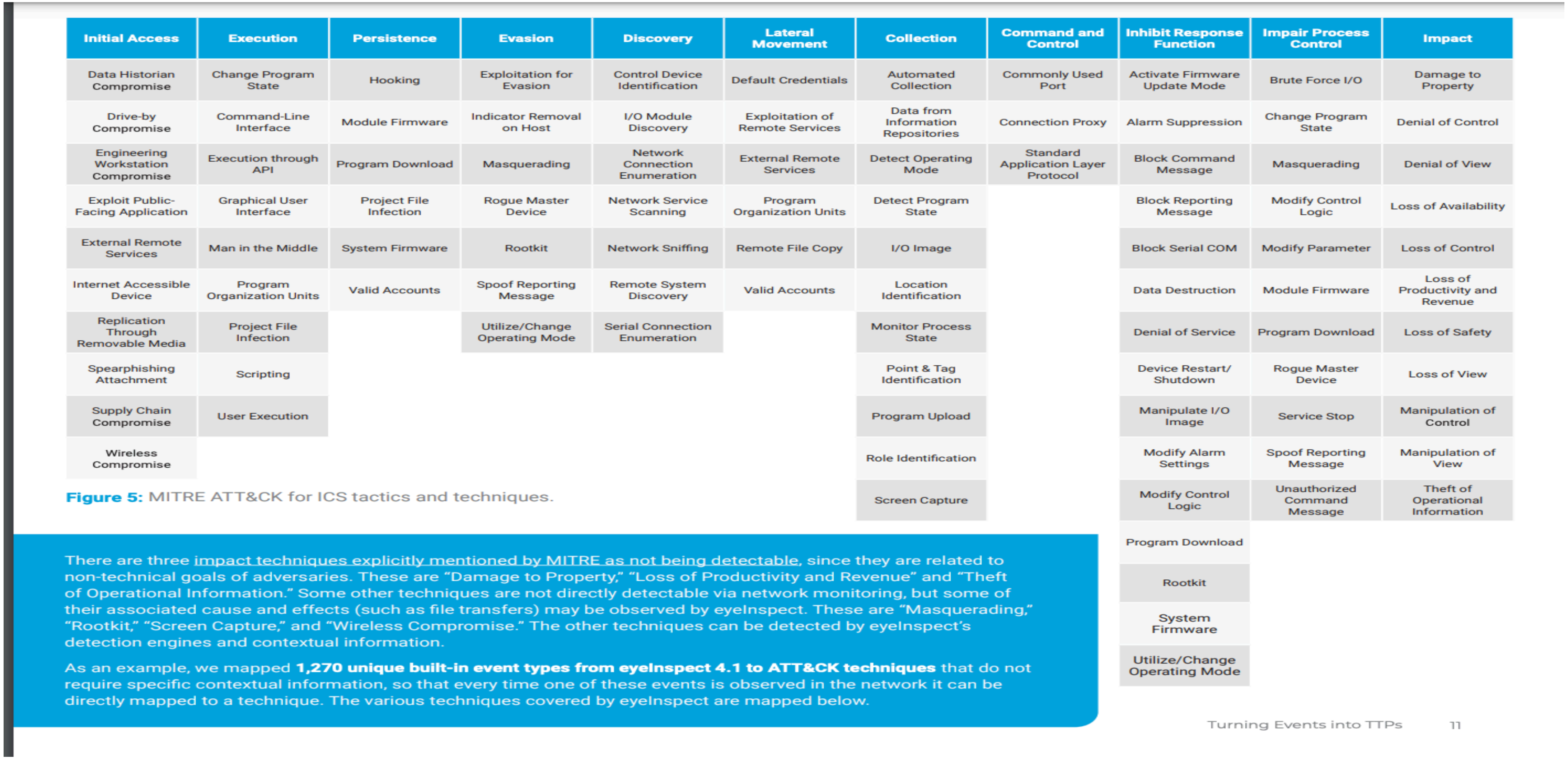
ATT&CK® Enterprise

Initial Access → Execution → Persistence → Privilege Escalation → Defense Evasion → Credential Access → Discovery → Lateral Movement → Collection → Command & Control → Exfiltration

ATT&CK® ICS

Initial Access → Execution → Persistence → Evasion → Discovery → Lateral Movement → Collection → Command & Control → Inhibit Response Function → Impair Process Control → Impact

Turning Low Level Events to TTPs



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		

Figure 5: MITRE ATT&CK for ICS tactics and techniques.

There are three impact techniques explicitly mentioned by MITRE as not being detectable, since they are related to non-technical goals of adversaries. These are "Damage to Property," "Loss of Productivity and Revenue" and "Theft of Operational Information." Some other techniques are not directly detectable via network monitoring, but some of their associated cause and effects (such as file transfers) may be observed by eyeInspect. These are "Masquerading," "Rootkit," "Screen Capture," and "Wireless Compromise." The other techniques can be detected by eyeInspect's detection engines and contextual information.

As an example, we mapped **1,270 unique built-in event types from eyeInspect 4.1 to ATT&CK techniques** that do not require specific contextual information, so that every time one of these events is observed in the network it can be directly mapped to a technique. The various techniques covered by eyeInspect are mapped below.

ATT&CK MITRE – Example Remote Access

1. Techniques
2. ICS
3. **Remote Services**

- Remote Services
- Adversaries may leverage remote services to move between assets and network segments. These services are often used to allow operators to interact with systems remotely within the network, some **examples are RDP, SMB, SSH, and other similar mechanisms.** [1] [2] [3]
- Remote services could be used to support remote access, data transmission, authentication, name resolution, and other remote functions. Further, remote services may be necessary to allow operators and administrators to configure systems within the network from their engineering or management workstations. An adversary may use this technique to access devices which may be dual-homed [1] to multiple network segments, and can be used for Program Download or to execute attacks on control devices directly through Valid Accounts.
- Specific remote services (RDP & VNC) may be a precursor to enable Graphical User Interface execution on devices such as HMIs or engineering workstation software.
- Based on incident data, CISA and FBI assessed that Chinese state-sponsored actors also compromised various authorized remote access channels, including systems designed to transfer data and/or allow access between corporate and ICS networks. [4]
- ID: T0886
- Sub-techniques: No sub-techniques

▶ ⓘ

- Tactics: Initial Access, Lateral Movement

ID	Name	Description
S1045	INCONTROLLER	INCONTROLLER can use the CODESYS protocol to remotely connect to Schneider PLCs and perform maintenance functions on the device.[5] INCONTROLLER can use Telnet to upload payloads and execute commands on Omron PLCs.[6][7] The malware can also use HTTP-based CGI scripts (e.g., cpu.fcgi, ecat.fcgi) to gain administrative access to the device.[5]
C0009	Oldsmar Treatment Plant Intrusion	During the Oldsmar Treatment Plant Intrusion, the threat actors gained access to the system through remote access software, allowing for the use of the standard operator HMI interface.[8]
S0496	REvil	REvil uses the SMB protocol to encrypt files located on remotely connected file shares.[9]
G0034	Sandworm Team	Sandworm Team appears to use MS-SQL access to a pivot machine, allowing code execution throughout the ICS network.[10]
S0603	Stuxnet	Stuxnet executes malicious SQL commands in the WinCC database server to propagate to remote systems. The malicious SQL commands include xp_cmdshell, sp_dumpdbilog, and sp_addextendedproc.[11]
G0088	TEMP.Veles	TEMP.Veles utilized remote desktop protocol (RDP) jump boxes to move into the ICS environment.[2]

Connecting Risk and threats

Mapping Defense Lines

Today's SOC Reality

450

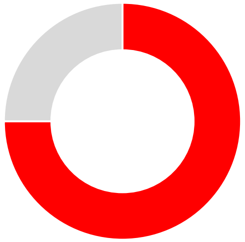
alerts per hour [1]

28%

of alerts are simply never addressed [1]

45%

of alerts are false positives [2]



75%

of enterprises spends an equal amount, or more time, on false positives than on legitimate attacks. [3]

[1] "The State of Security Operations", Forrester 2020

[2] "The Voice of the Analysts: Improving Security Operations Center Processes Through Adapted Technologies" IDC InfoBrief

[3] "Reaching the Tipping Point of Web Application and API Security", 2021, ESG

Planning Defense Lines via MITRE ATT&CK mapping

Plan

Emulate

Identify Gaps

Integrate Threat Intel

Plan : Use ATT&CK to plan your cyber security strategy.
Build your defenses to counter the techniques known to be used
against your type of organization and equip yourself with security monitoring to detect evidence of
ATT&CK techniques in your network

Run Adversary Emulation Plans

Use ATT&CK for Adversary Emulation Plans to improve Red team performance. Red teams can develop and deploy a consistent and highly organized approach to defining the tactics and techniques of specific threats, then logically assess their environment to see if the defenses work as expected.

Identify Gaps in Defenses

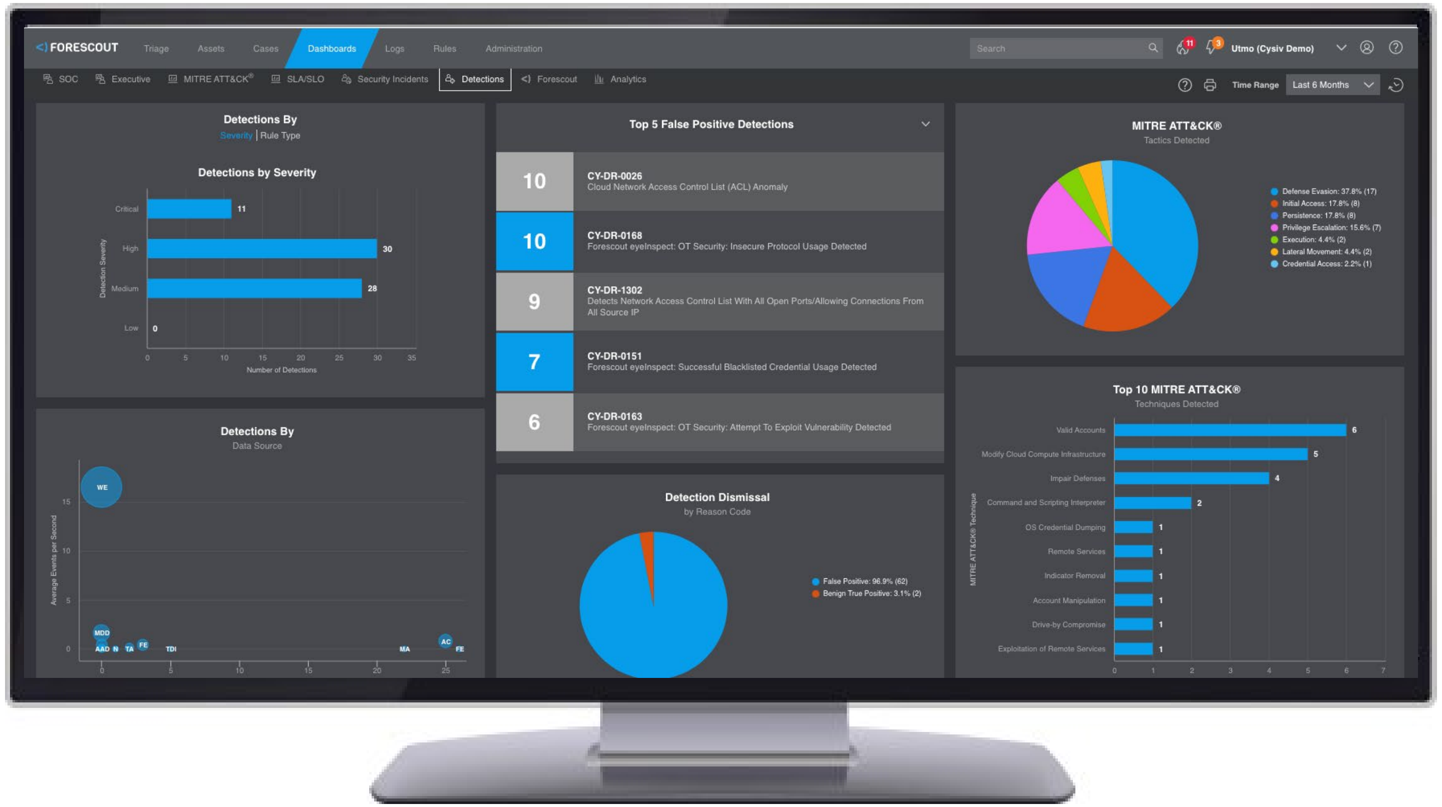
ATT&CK matrices can help Blue teams better understand the components of a potential or ongoing cyber attack to identify gaps in defenses and implement solutions for those gaps. ATT&CK documents suggested remediations and compensating controls for the techniques to which you are more prone.

Integrate Threat Intelligence

ATT&CK can effectively integrate your threat intelligence into cyber defense operations. Threats can be mapped to the specific attacker techniques to understand if gaps exist, determine risk, and develop an implementation plan to address them.

XDR

Better Detection and Response of True Threats, from a Single Pane of Glass



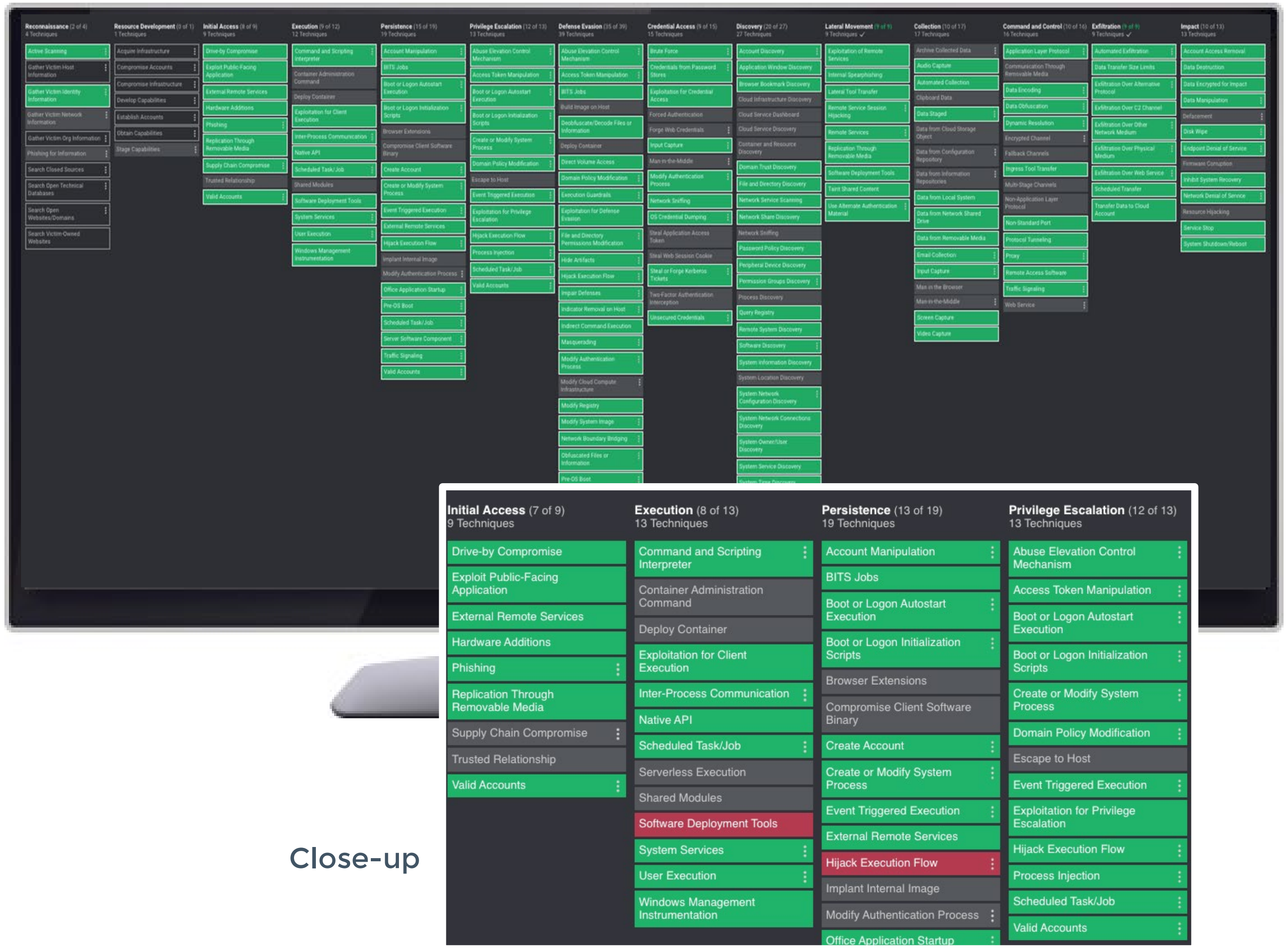
Top 5 False Positive Detections

10	CY-DR-0026 Cloud Network Access Control List (ACL) Anomaly
10	CY-DR-0168 Forescout eyeInspect: OT Security: Insecure Protocol Usage Detected
9	CY-DR-1302 Detects Network Access Control List With All Open Ports/Allowing Connections From All Source IP
7	CY-DR-0151 Forescout eyeInspect: Successful Blacklisted Credential Usage Detected
6	CY-DR-0163 Forescout eyeInspect: OT Security: Attempt To Exploit Vulnerability Detected

- Automates and accelerates the process of **detecting, investigating, hunting for, and responding to** advanced threats across the entire enterprise:
  - Campus
  - Remote
  - Datacenter
  - Cloud
  - IT / OT / IoMT
- Combines essential SOC technologies and functions into single,   TIP , SOAR , UEBA

MITRE ATT&CK® for Detection Coverage

XDR let's you see which TTPs you will be able to detect based on specified data sources



Reconnaissance (2 of 4)
4 Techniques
Active Scanning
Gather Victim Host Information
Gather Victim Identity Information
Gather Victim Network Information
Gather Victim Org Information
Phishing for Information
Search Closed Sources
Search Open Technical Databases
Search Open Websites/Domains
Search Victim-Owned Websites

Resource Development (0 of 1)
1 Techniques
Acquire Infrastructure
Compromise Accounts
Compromise Infrastructure
Develop Capabilities
Establish Accounts
Obtain Capabilities
Stage Capabilities

Initial Access (8 of 9)
9 Techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts

Execution (9 of 12)
12 Techniques
Command and Scripting Interpreter
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication
Native API
Scheduled Task/Job
Shared Modules
Software Deployment Tools
System Services
User Execution
Windows Management Instrumentation

Persistence (15 of 19)
19 Techniques
Account Manipulation
BITS Jobs
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Browser Extensions
Compromise Client Software Binary
Create Account
Create or Modify System Process
Event Triggered Execution
External Remote Services
Hijack Execution Flow
Implant Internal Image
Modify Authentication Process
Office Application Startup
Pre-OS Boot
Scheduled Task/Job
Server Software Component
Traffic Signaling
Valid Accounts

Privilege Escalation (12 of 13)
13 Techniques
Abuse Elevation Control Mechanism
Access Token Manipulation
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Create or Modify System Process
Domain Policy Modification
Escape to Host
Event Triggered Execution
Exploitation for Privilege Escalation
Hijack Execution Flow
Process Injection
Scheduled Task/Job
Valid Accounts

Defense Evasion (35 of 39)
39 Techniques
Abuse Elevation Control Mechanism
Access Token Manipulation
BITS Jobs
Build Image on Host
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification
Execution Guardrails
Exploitation for Defense Evasion
File and Directory Permissions Modification
Hide Artifacts
Hijack Execution Flow
Impair Defenses
Indicator Removal on Host
Indirect Command Execution
Masquerading
Modify Authentication Process
Modify Cloud Compute Infrastructure
Modify Registry
Modify System Image
Network Boundary Bridging
Obfuscated Files or Information
Pre-OS Boot

Credential Access (9 of 15)
15 Techniques
Brute Force
Credentials from Password Stores
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials
Input Capture
Man-in-the-Middle
Modify Authentication Process
Network Sniffing
OS Credential Dumping
Steal Application Access Token
Steal Web Session Cookie
Steal or Forge Kerberos Tickets
Two-Factor Authentication Interception
Unsecured Credentials

Discovery (20 of 27)
27 Techniques
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Container and Resource Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Software Discovery
System Information Discovery
System Location Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery

Lateral Movement (9 of 9)
9 Techniques ✓
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking
Remote Services
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material

Collection (10 of 17)
17 Techniques
Archive Collected Data
Audio Capture
Automated Collection
Clipboard Data
Data Staged
Data from Cloud Storage Object
Data from Configuration Repository
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Email Collection
Input Capture
Man in the Browser
Man-in-the-Middle
Screen Capture
Video Capture

Command and Control (10 of 16)
16 Techniques
Application Layer Protocol
Communication Through Removable Media
Data Encoding
Data Obfuscation
Dynamic Resolution
Encrypted Channel
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy
Remote Access Software
Traffic Signaling
Web Service

Exfiltration (9 of 9)
9 Techniques ✓
Automated Exfiltration
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Exfiltration Over Web Service
Scheduled Transfer
Transfer Data to Cloud Account

Impact (10 of 13)
13 Techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation
Defacement
Disk Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Service Stop
System Shutdown/Reboot

Initial Access (7 of 9)
9 Techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts

Execution (8 of 13)
13 Techniques
Command and Scripting Interpreter
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication
Native API
Scheduled Task/Job
Serverless Execution
Shared Modules
Software Deployment Tools
System Services
User Execution
Windows Management Instrumentation

Persistence (13 of 19)
19 Techniques
Account Manipulation
BITS Jobs
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Browser Extensions
Compromise Client Software Binary
Create Account
Create or Modify System Process
Event Triggered Execution
External Remote Services
Hijack Execution Flow
Implant Internal Image
Modify Authentication Process
Office Application Startup

Privilege Escalation (12 of 13)
13 Techniques
Abuse Elevation Control Mechanism
Access Token Manipulation
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Create or Modify System Process
Domain Policy Modification
Escape to Host
Event Triggered Execution
Exploitation for Privilege Escalation
Hijack Execution Flow
Process Injection
Scheduled Task/Job
Valid Accounts

Close-up

The Value:

- **Onboarding Prioritization**: What data sources should be ingested for broad, or specific, technique coverage?
- **Gap Analysis**: Where are potential blinds spots that adversaries can exploit to gain access?
- **Coverage Planning**: What happens to MITRE ATT&CK coverage if other data sources are added**?**

← Dashboard indicates (in green) all of the TTPs that can be detected with these data sources, for example:

- Firewall
- EDR
- Windows Sysmon
- Windows Events

Q&A