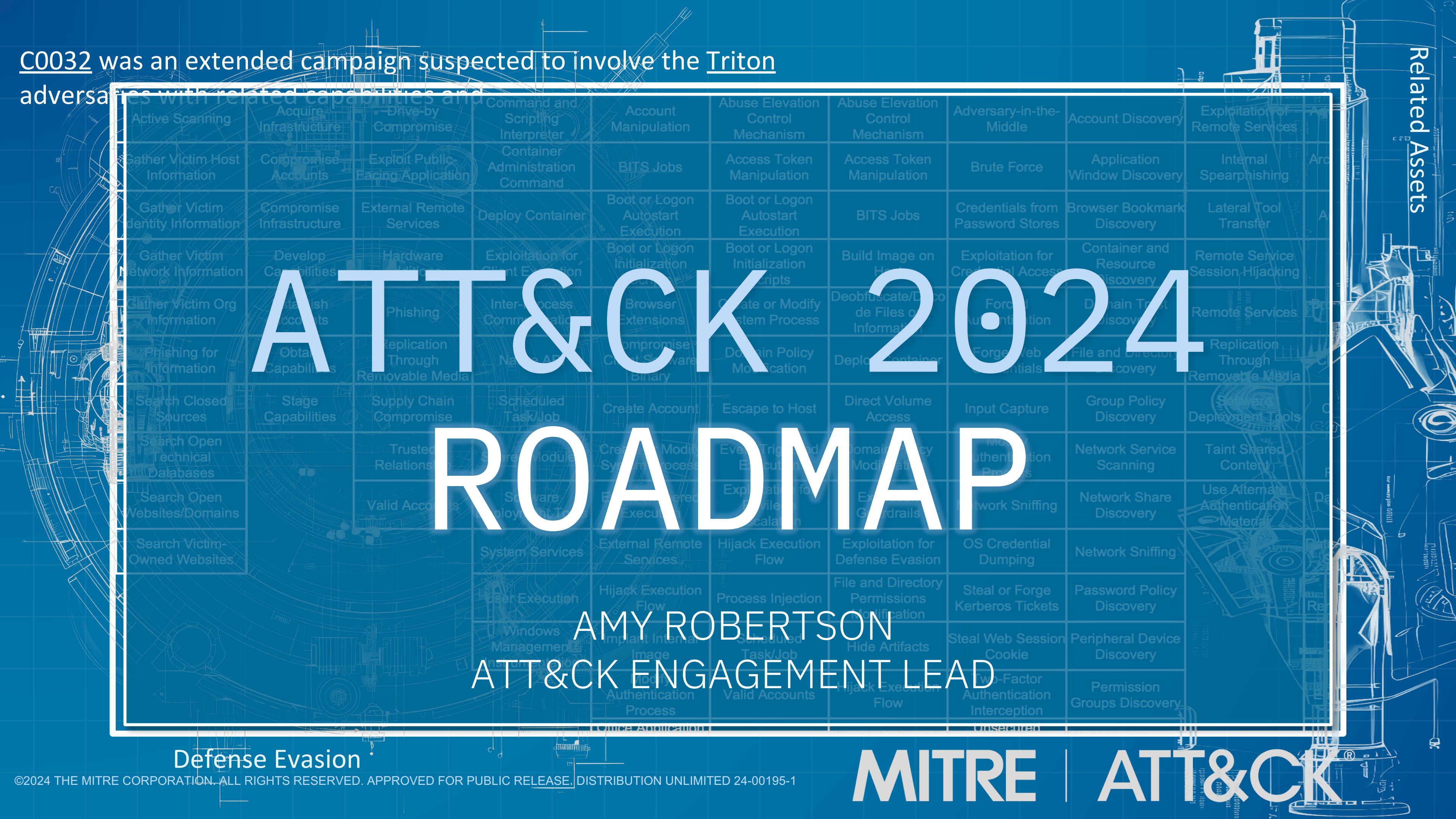


[C0032](#) was an extended campaign suspected to involve the [Triton](#) adversaries with related capabilities and

Related Assets

ATT&CK 2024 ROADMAP

AMY ROBERTSON
ATT&CK ENGAGEMENT LEAD

Defense Evasion

MITRE | ATT&CK®

ATT&CK Vision

ATT&CK was designed to empower defenders precisely where they need it most

&

Enable the broadest use across the widest spectrum of stakeholders

2024 Goals

Bolster Broader Usability

- ICS Sub-techniques
- TAXII 2.1
- Cloud Platform Rebalancing
- Related Assets
- ATT&CK Navigator, Workbench

Actionable Defensive Measures

- Upgraded Detections
- New Analytic Format
- Data Source Restructuring
- Mobile Structured Detections Expansion
- Cybercriminal/Underreported Activity

ENTERPRISE

Integrated Defense

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 Open Technical Databases

Search Open Websites/Domains

Search Victim-Owned Websites

Command and Scripting Interpreter: AutoHotKey & AutoIT

Compromise Infrastructure: Network Devices

Create or Modify System Process:

clusions

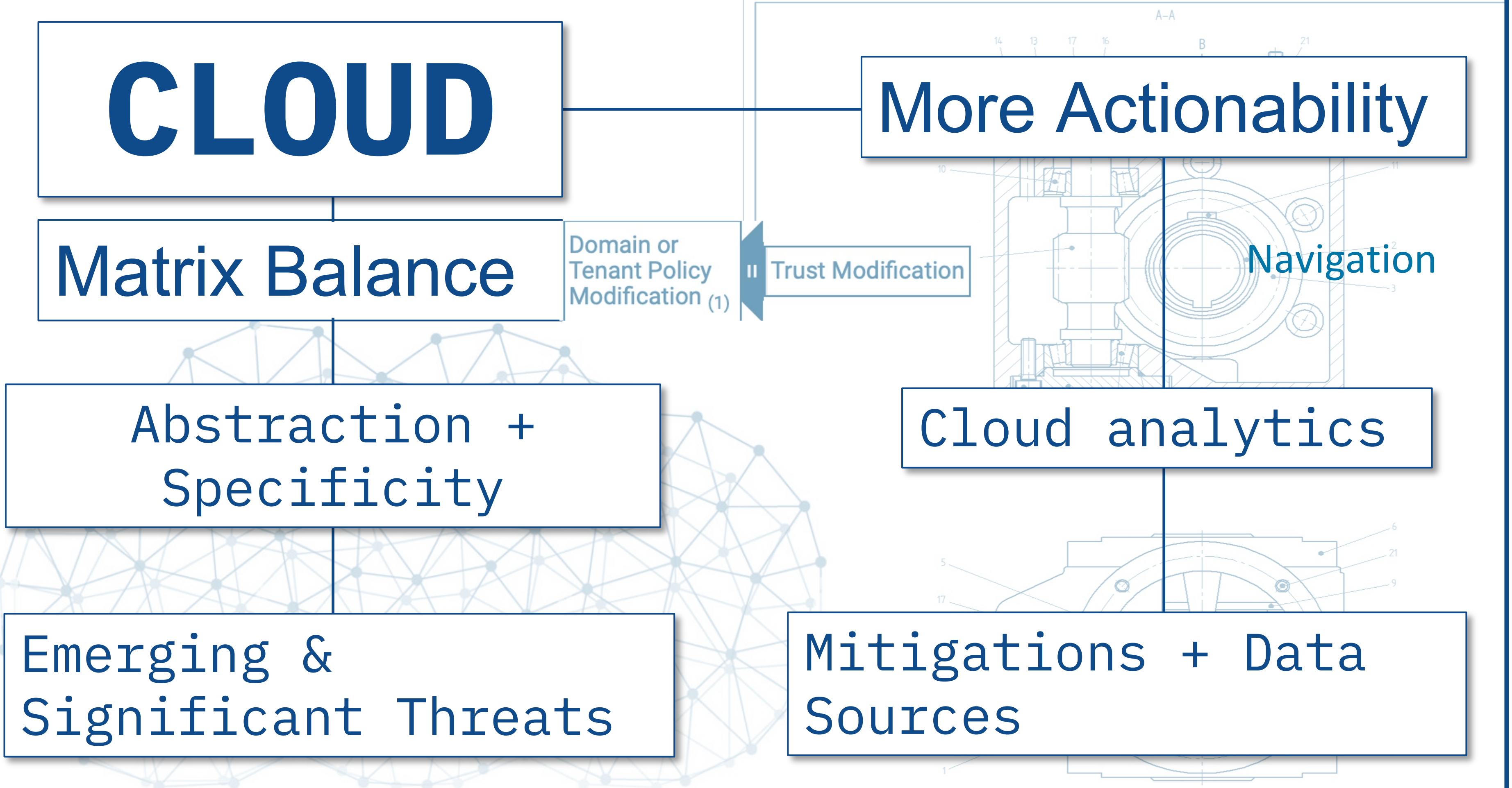
Hijack Execution Flow: AppDomainManager

Modify Authentication Process: Conditional Access Policies Obfuscated Files or Information: Encrypted/Encoded File Obtain Capabilities: Artificial Intelligence System Binary Proxy Execution: Electron Applications

System Script Proxy Execution: SyncAppvPublishingServer

Search Closed Sources

Active Scanning



CLOUD

Matrix Balance

Domain or Tenant Policy Modification (1)

Trust Modification

Abstraction + Specificity

Emerging & Significant Threats

More Actionability

Navigation

Cloud analytics

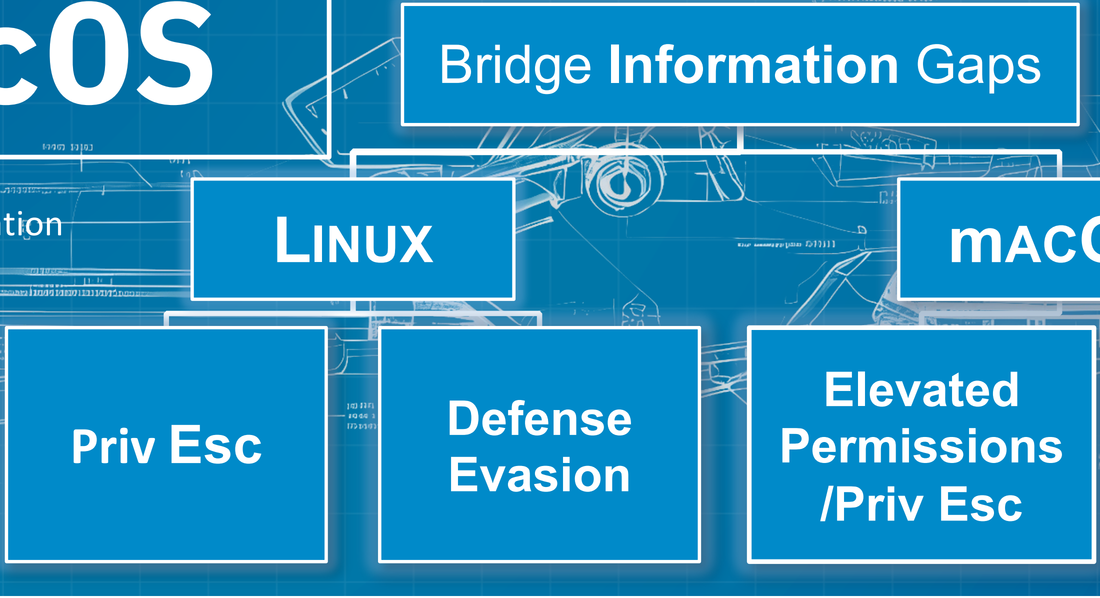
Mitigations + Data Sources

Create Account: Cloud Account

Conditional Access Policies

Linux/ macOS

Countermeasures: Priv Esc & Defense Evasion



Bridge **Information** Gaps

Linux

macOS

Priv Esc

Defense Evasion

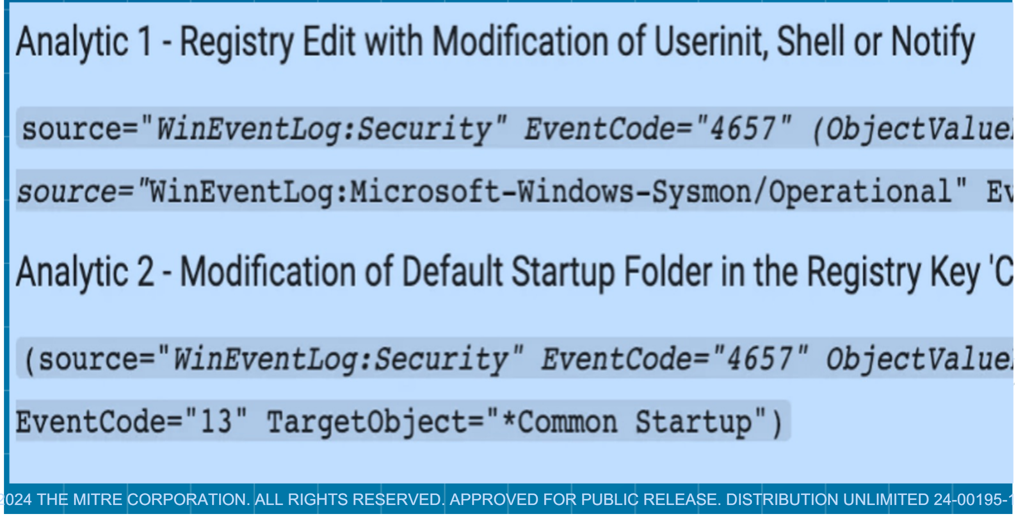
Elevated Permissions /Priv Esc

TCC Manipulation

Exaramel:Linux

Defensive Coverage

Upgrading, Converting & Restructuring



Analytic 1 - Registry Edit with Modification of Userinit, Shell or Notify

```
source="WinEventLog:Security" EventCode="4657" (ObjectValue
source="WinEventLog:Microsoft-Windows-Sysmon/Operational" Ev
```

Analytic 2 - Modification of Default Startup Folder in the Registry Key 'C

```
(source="WinEventLog:Security" EventCode="4657" ObjectValue
EventCode="13" TargetObject="*Common Startup")
```

- Cloud Analytics
- Detection Logic/New Analytic Format
- Upgraded Detections
- Restructured Data Sources

MITRE | ATT&CK®

C0032

ICS

Subs, Asset Expansion, & Cross-Domain Integration

Triton

- ○ Related Assets
- ○ Sub-techniques
- ○ Cross-mapped Campaigns

UNITRONICS

T0895: Autorun Image

UKRAINE 2022

MITRE | ATT&CK®

Building Out Structured Detections

Expanding Mitigations

EXPLORING LEFT-OF-EXPLOIT ACTIVITY

MOBILE

PROMETHIUM
G0056

Encrypted Channel: SSL Pinning

Encrypted Channel: SSL Pinning

M1059 Do Not Mitigate

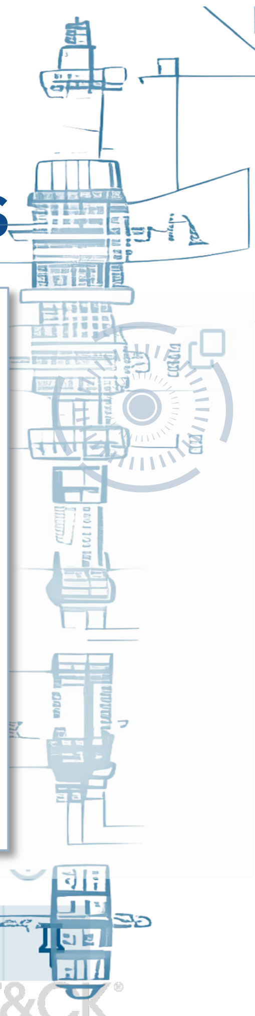
MITRE | ATT&CK®

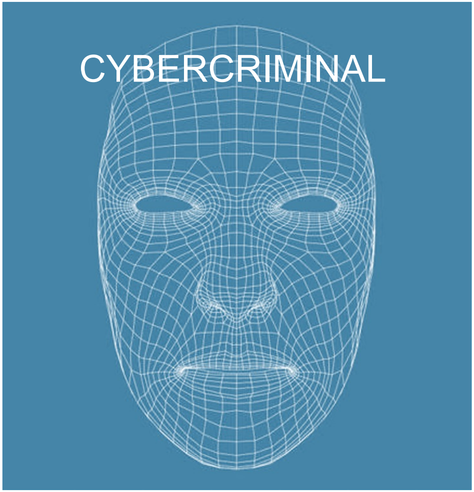
Software Development

Enhanced Usability & Streamlined Workflows

- Enhancing ATT&CK Navigator User Experience
- Optimizing ATT&CK Workbench Workflows for Swifter Updates
- Upgrading TAXII Server (v2.1)

```
.
├─ enterpr
│   ├─ ent
│   ├─ ent
│   └─ [ot
├─ mobile-
│   └─ [Mo
├─ ics-att
│   └─ [AT
├─ index.j
└─ index.m
```





CYBERCRIMINAL

Malteiro

ToddyCat

Mustard Tempest

AKIRA

UNDERREPORTED

BITTER (G1002)

Cyber Threat Intelligence

CYBERCRIMINAL, UNDERREPRESENTED GROUPS

Community Engagement

QUESTIONS?

@MITREATTACK

LINKEDIN/MITRE-ATT&CK

Attack@mitre.org