

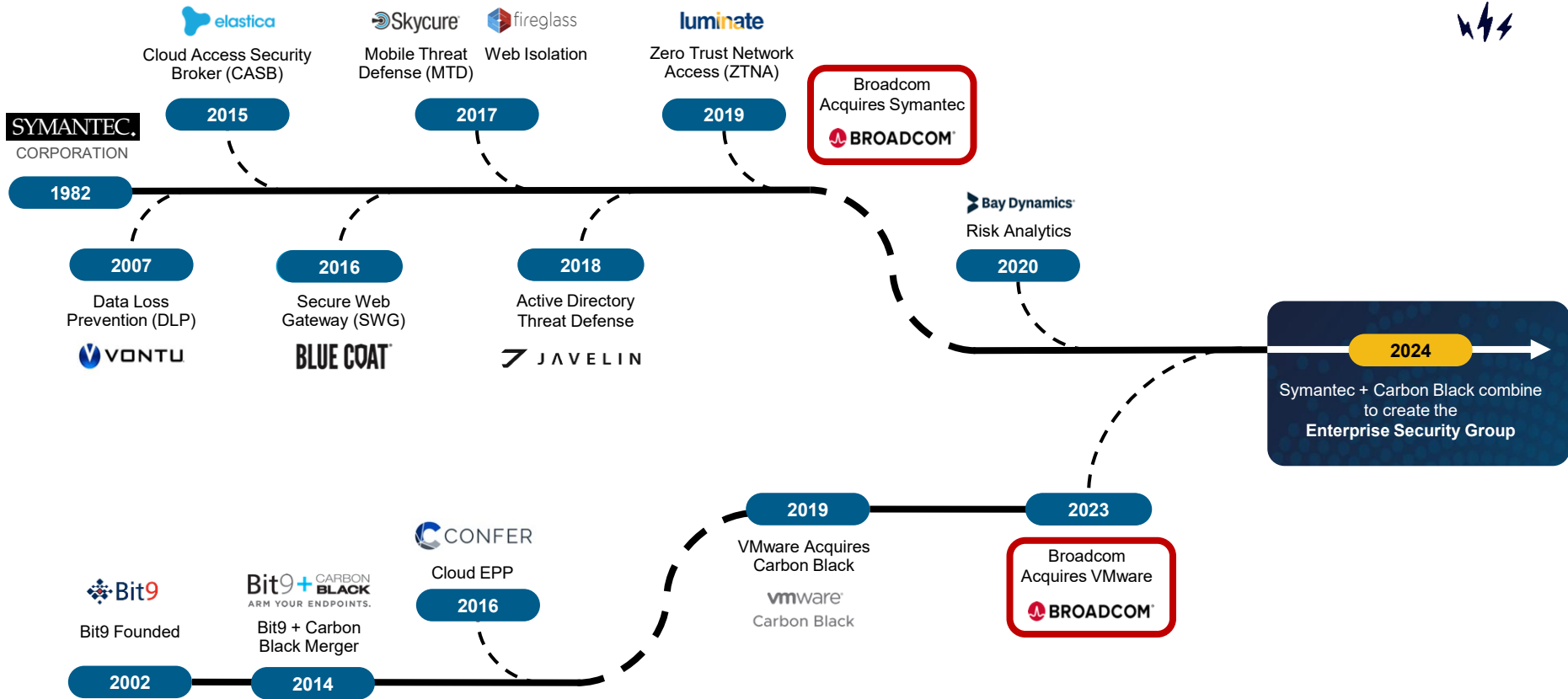


Symantec CBX Come Together

Miodrag Milenković, Senior Sales Engineer

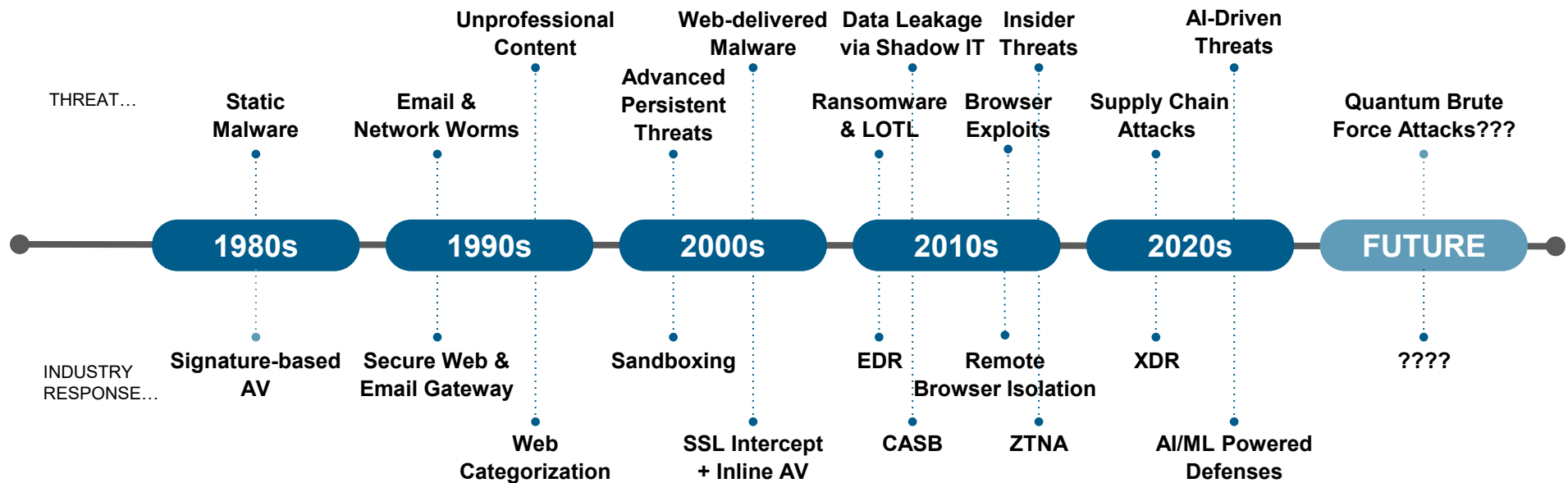


Legends Never Die



Cybersecurity Companies Cannot Rest

Cyber companies must constantly develop non-trivial innovations to keep up



GLOBAL INTELLIGENCE NETWORK





The Attack Landscape 'TAM' Has Expanded

Attackers have expanded their scope beyond governments, the military and large enterprises to **midmarket and commercial organizations**

Contributing Factors



Ransomware-as-a-Service



Supply-chain Attacks



AI-driven Attacks



Nation-state Campaigns

34%

have no security protocol*

35%

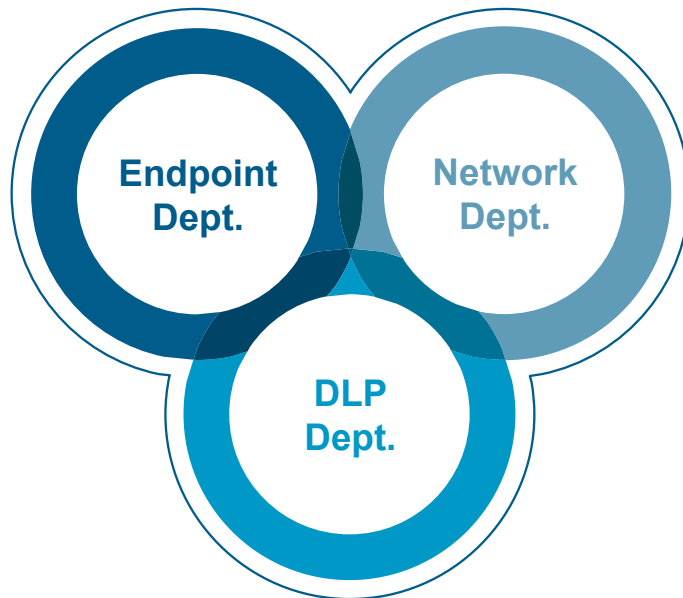
lack formal risk frameworks*

72%

have no formal security awareness training*

*Agrawal, Anurag. "2025 SMB & Midmarket Security Adoption Trends." Techaisle, LLC. June 2025

Modern Security Teams



Defining Attributes

Integrated structure

Fewer employees

Generalist operators

Agile

Prefer platform over
niche solutions

Outcome focused

Delivering enterprise-grade security for all.

CBX

CROSS PRODUCT ENRICHMENT AND CORRELATION

Endpoint Protection

EDR

Web Security

Data Security Enrichment

An enterprise-grade
solution with consumer-
grade simplicity

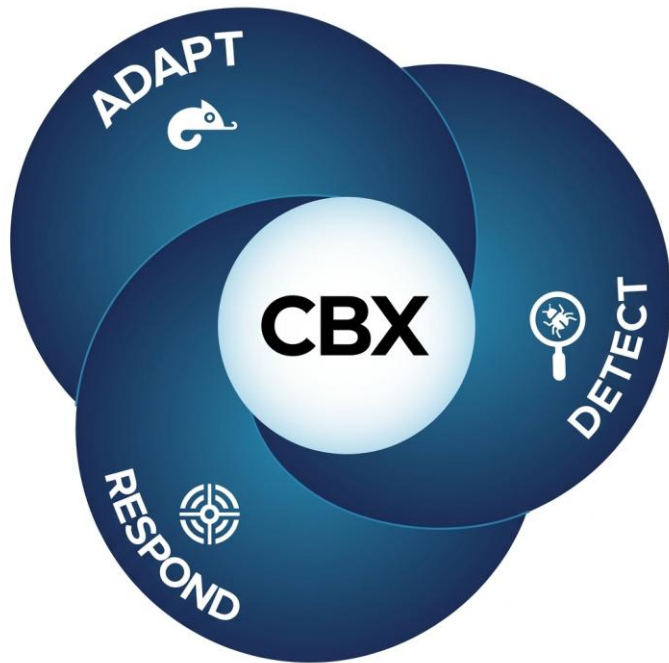


The broadest
natively correlated
security signals



Adaptive, automated prevention,
best-in-class detection, and
simplified response.

See More. Stop More. Respond Faster.



One endpoint product

One control plane

One agent

One source of truth



CBX:

KEY FEATURES



SINGLE ENDPOINT SECURITY AGENT

Endpoint, Cloud SWG, ZTNA, CASB, FWaaS, Web Isolation



UNIFIED ALERTING & VISIBILITY

Correlates metadata from DLP, Endpoint, and Web defense products for better outcomes



PREDICTIVE SECURITY

Advanced AI predicts attack paths allowing action earlier in the timeline



THREAT TRACER

A single pane of glass – no more context switching during investigations



ACCELERATED DETECTION & RESPONSE

Intelligent correlation and telemetry = Better data, better detections.

BUILT ON THE BEST TELEMETRY AND PURPOSE-BUILT AI MODELS

How CBX is different:

OTHER XDR PLATFORMS

Missing key context from **data and web security**

Re-create **SIEM problems**

Struggle to **curate data** in a consumable way

Cumbersome detection workflows for modern security teams



SYMANTEC CBX

Analyst workbench for entire **security lifecycle**

Lower cost and complexity of security platform

Curated telemetry enrichment using threat intel

Combined analyst experience, high-quality data, & prevention capabilities

CBX Investigation Summary

← 10 | Active Malicious Attack

Summary

Threat Tracer

Entities and Remediation

Alerts

Events

Active Malicious Attack

NAME

10

SEVERITY

99

ALERTS

8

DEVICES

Unassigned

ASSIGNED TO

May 13, 2026, 10:11:24 PM

UPDATED

Active Malicious Attack

COMMENTS

Open

STATUS

123

EVENTS

5

USERS

Analytics

CREATED BY

May 13, 2026, 9:23:59 PM

LAST SEEN

101145

INVESTIGATION ID

Analysis

Update

Summary

Attack Chain

Investigation Steps

Remediation

Last updated May 13, 2026, 8:08:28 PM

Executive Summary

A multi-stage, multi-host attack was observed across the environment, culminating in the deployment of ransomware. The actor demonstrated proficiency with hands-on-keyboard techniques, leveraging native Windows utilities like **powershell.exe** and **cmd.exe** for execution, discovery, and defense evasion. The attack chain involved downloading tools, executing obfuscated commands, performing network and system reconnaissance, attempting to harvest credentials from **lsass.exe** and the **SAM** registry hive, and attempting to delete Volume Shadow Copies. The final stage of the attack involved dropping a ransom note consistent with the Akira ransomware group on multiple endpoints, indicating a clear intent of financial extortion.

Scope of Impact

- Attempted Credential Theft:** The actor attempted to dump credentials by saving the **SAM** registry hive using **reg.exe** and by dumping the memory of the **lsass.exe** process using **procdump64.exe**. The successful acquisition of these credentials would pose an immediate risk of widespread account compromise, privilege escalation, and lateral movement throughout the domain.
- Inhibition of System Recovery:** The execution of **vssadmin.exe** with the command **Delete Shadows /all /quiet** represents a direct attempt to destroy volume shadow copies. This action severely hampers system recovery efforts, posing the immediate risk of making data restoration impossible without external backups, thereby increasing the pressure to pay a ransom.
- Ransomware Deployment:** The attacker successfully executed a PowerShell script that creates a ransom note named **akira_readme.txt** on multiple hosts, including **sia-trigger** and **ss733223-zep-dev2**. This action signifies that the final impact stage of the ransomware attack has begun, posing an immediate risk of widespread, irreversible data encryption across affected systems.
- Execution of Arbitrary Code and Payloads:** The actor successfully downloaded and executed multiple tools and scripts, including a renamed **pythonw.exe** (**synaptics.exe**) and payloads via **AutoHotkey**. This demonstrates a loss of control over the affected endpoints, posing an ongoing risk of further malware deployment, data exfiltration, or other malicious actions.

Actor Intent

- The actor's primary intent is financial gain through a ransomware-for-extortion scheme. This is unequivocally demonstrated by the deployment of a PowerShell script that drops a detailed ransom note (**akira_readme.txt**) containing instructions for payment and negotiation via a Tor network address, which is characteristic of the Akira ransomware group.
- The actor intended to perform comprehensive discovery and credential harvesting prior to encryption. This is evident from the execution of commands like **systeminfo**, **net user /domain**, **net view**, and attempts to dump credentials from **lsass.exe** and the **SAM** hive, all aimed at maximizing the scope and impact of the final ransomware payload.
- The actor clearly intended to prevent system recovery and ensure the effectiveness of the ransomware attack. This is supported by the deliberate attempt to delete all volume shadow copies using **vssadmin.exe**, a common tactic to eliminate local backups and force the victim into a position where paying the ransom is the only perceived option for data recovery.

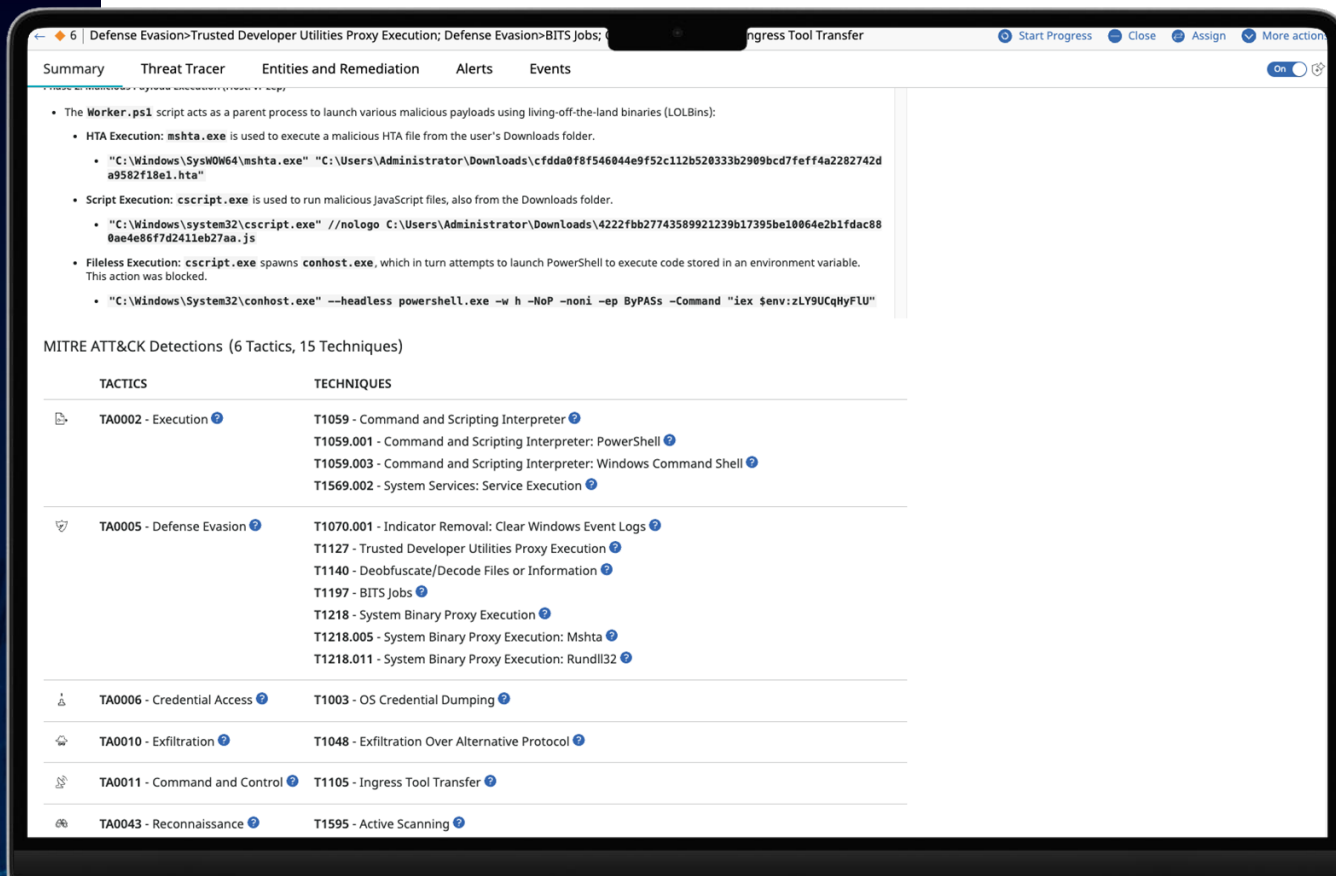
Urgent Threat: Deny Predicted Behaviors

Cloud analytics have predicted the following behaviors to occur in the attack progression:

Predicted Behavior	Probability
Windows Scripting Host (WScript) modifying services registry entries	100%
Microsoft Outlook executing cmd.exe	100%
Windows Management Instrumentation (WMI) launching Schtasks	100%
PowerShell accessing memory of Local Security Authentication Server (Lsass)	100%
Regedit dumping credentials in SAM registry key	100%
CMSTP launching	100%
Schtasks creating a job on HTA application execution	100%
Windows Scripting Host (WScript) creating PE executable	100%
PowerShell launching under a different process name	100%

Broadcom Proprietary and Confidential. Copyright @ 2026 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Investigation Summary



The screenshot displays a security analysis tool interface. The top navigation bar includes tabs for Summary, Threat Tracer, Entities and Remediation, Alerts, and Events. The main content area shows a detailed summary of a defense evasion attack, listing several tactics and techniques used by the attacker. Below this, a table titled "MITRE ATT&CK Detections (6 Tactics, 15 Techniques)" provides a structured overview of the detected activities.

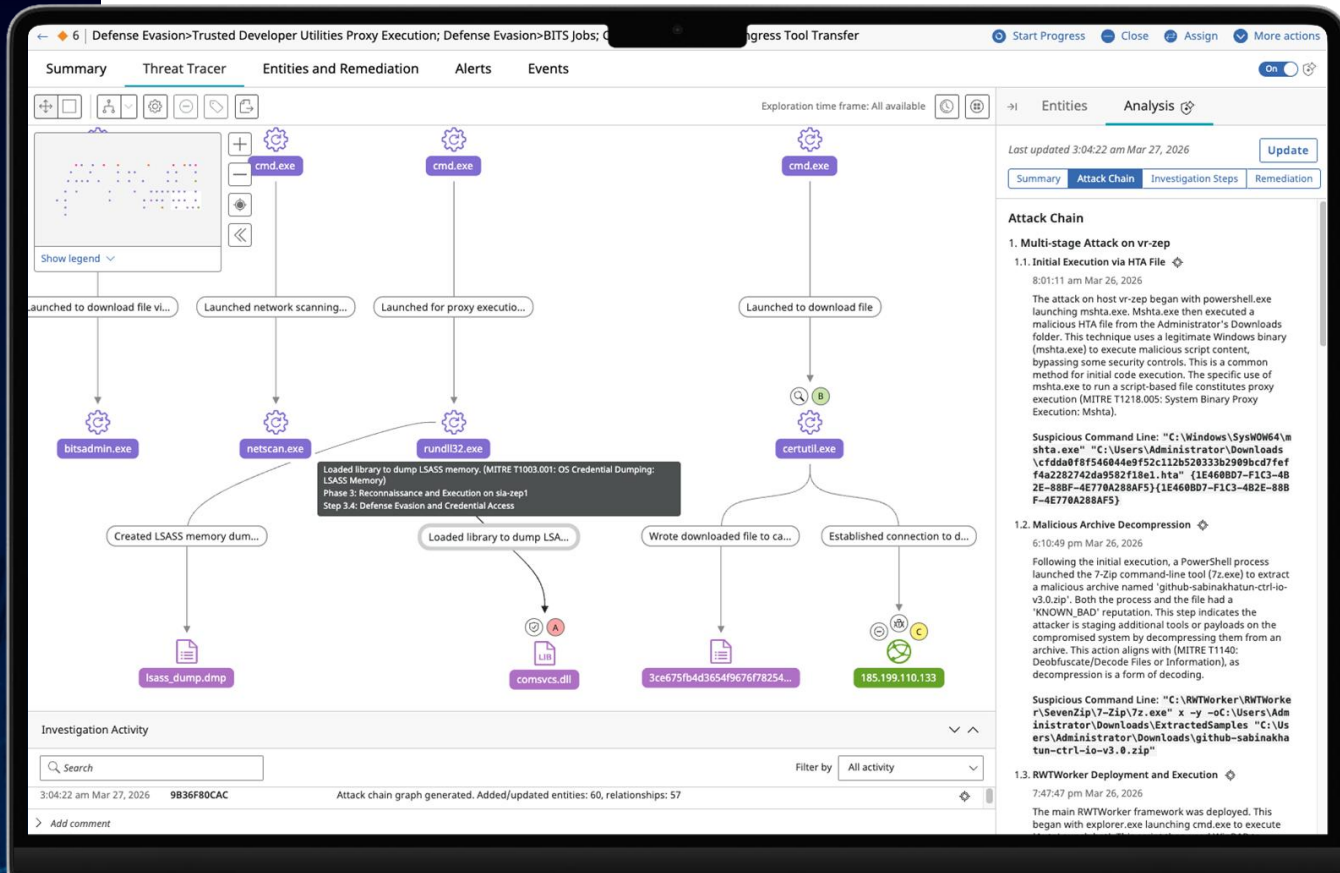
Summary of Defense Evasion Tactics and Techniques:

- The **Worker.ps1** script acts as a parent process to launch various malicious payloads using living-off-the-land binaries (LOLBins):
 - HTA Execution:** **mshta.exe** is used to execute a malicious HTA file from the user's Downloads folder.
 - Command: `"C:\Windows\System32\cmd.exe" /c "C:\Users\Administrator\Downloads\cfdda0f8f546044e9f52c112b520333b2909bcd7feff4a2282742da9582f18e1.hta"`
 - Script Execution:** **cscript.exe** is used to run malicious JavaScript files, also from the Downloads folder.
 - Command: `"C:\Windows\System32\cmd.exe" /c "C:\Users\Administrator\Downloads\4222fbb27743589921239b17395be10064e2b1fdac880ae4e86f7d2411eb27aa.js"`
 - Fileless Execution:** **cscript.exe** spawns **conhost.exe**, which in turn attempts to launch PowerShell to execute code stored in an environment variable. This action was blocked.
 - Command: `"C:\Windows\System32\conhost.exe" --headless powershell.exe -w h -NoP -noni -ep ByPASS -Command "iex $env:zLY9UCqHyFLU"`

MITRE ATT&CK Detections (6 Tactics, 15 Techniques)

TACTICS	TECHNIQUES
TA0002 - Execution	T1059 - Command and Scripting Interpreter T1059.001 - Command and Scripting Interpreter: PowerShell T1059.003 - Command and Scripting Interpreter: Windows Command Shell T1569.002 - System Services: Service Execution
TA0005 - Defense Evasion	T1070.001 - Indicator Removal: Clear Windows Event Logs T1127 - Trusted Developer Utilities Proxy Execution T1140 - Deobfuscate/Decode Files or Information T1197 - BITS Jobs T1218 - System Binary Proxy Execution T1218.005 - System Binary Proxy Execution: Mshta T1218.011 - System Binary Proxy Execution: Rundll32
TA0006 - Credential Access	T1003 - OS Credential Dumping
TA0010 - Exfiltration	T1048 - Exfiltration Over Alternative Protocol
TA0011 - Command and Control	T1105 - Ingress Tool Transfer
TA0043 - Reconnaissance	T1595 - Active Scanning

Threat Tracer Visualization



Remediation

The screenshot displays a security tool interface with a top navigation bar containing tabs: Summary, Threat Tracer, Entities and Remediation (active), Alerts, and Events. Below the tabs is a search bar and a section titled "Showing list of Entities (Showing 1 to 50 of 60)".

NAME	TYPE	CREATED	UPDATED
12a4fd996a70ad7bebe662c60f44e51b716e6f10fbeb58214ee6...	Script	3:04:22 am Mar 27, 2026	12:32:21 pm Apr 8, 2026
185.199.110.133	IP Address	3:04:22 am Mar 27, 2026	12:33:52 pm Apr 8, 2026
1desktop-mt-sea	Device	3:04:22 am Mar 27, 2026	12:32:21 pm Apr 8, 2026
3ce675fb4d3654f9676f78254fd4f2e	Script	3:04:22 am Mar 27, 2026	12:32:21 pm Apr 8, 2026
4222fbb27743589921239b17395be10064e2b1fdac880ae4e86f7d24...	Script	3:04:22 am Mar 27, 2026	12:32:21 pm Apr 8, 2026
7z.exe	Process	3:04:22 am Mar 27, 2026	12:32:21 pm Apr 8, 2026
autolaunch.bat	Script	3:04:22 am Mar 27, 2026	12:32:21 pm Apr 8, 2026
bitsadmin.exe	Process	3:04:22 am Mar 27, 2026	12:32:21 pm Apr 8, 2026
certutil.exe	Process	3:04:22 am Mar 27, 2026	12:34:29 pm Apr 8, 2026
cfdda0f8f546044e9f52c112b520333b2909bcd7feff4a2282742da958...	Script	3:04:22 am Mar 27, 2026	12:32:21 pm Apr 8, 2026
chrome_clicker.py	Script	3:04:22 am Mar 27, 2026	12:32:21 pm Apr 8, 2026
chrome.exe	Process	3:04:22 am Mar 27, 2026	12:32:21 pm Apr 8, 2026
cmd.exe	Process	3:04:22 am Mar 27, 2026	12:32:21 pm Apr 8, 2026
cmd.exe	Process	3:04:22 am Mar 27, 2026	12:33:31 pm Apr 8, 2026
cmd.exe	Process	3:04:22 am Mar 27, 2026	12:32:21 pm Apr 8, 2026
cmd.exe	Process	3:04:22 am Mar 27, 2026	12:34:49 pm Apr 8, 2026

Below the table is an "Investigation Activity" section with a search bar and a filter dropdown set to "All activity". A log entry shows: "3:04:22 am Mar 27, 2026 9B36F80CAC Attack chain graph generated. Added/updated entities: 60, relationships: 57".

The right sidebar shows details for "certutil.exe". It includes a "PROCESS" section with buttons for "Allow Hash", "Deny Hash", and "More actions". Below this is a search bar and a "Set B" button. The main text describes the process: "Certutil.exe used to download a file from a remote URL. Phase 3: Reconnaissance and Execution on sia-zep1 Step 3.3: Ingress Tool Transfer".

The "CMD" section shows the command: "certutil -urlcache -split -f https://raw.githubusercontent.com/SigmaHQ/sigma/master/README.md C:\PerfLogs\dual_use_testdata\certutil_downl...".

The "Process Access Control" section shows "Integrity Level Medium".

The "File Details" section shows "Current Reputation Good", "Historical Reputation Good", and "Prevalence Many Users". It also shows the "Path" and "SHA-256" hash.

The "Effective Signature" section shows "Issuer Microsoft Windows Production PCA 2011", "Publisher Microsoft Windows", and "State Catalog Signed, OS, Signed, Trusted, Verified".

The "Sandbox Analysis" section shows "Verdict --" and "Analyzed --".

Remediation

The screenshot displays a security tool interface with a top navigation bar containing tabs: Summary, Threat Tracer, Entities and Remediation (active), Alerts, and Events. Below the navigation bar is a search input field labeled "Search".

The main content area is titled "Showing list of Entities (Showing 1 to 50 of 60)". It contains a table with the following columns: NAME, TYPE, CREATED, and UPDATED. The table lists various entities, including scripts, IP addresses, devices, and processes. The entity "certutil.exe" is highlighted in blue.

Below the table is an "Investigation Activity" section with a search input field and a "Filter by" dropdown menu set to "All activity". Below this, a timeline entry shows "3:04:22 am Mar 27, 2026" with the ID "9B36F80CAC" and the description "Attack chain graph generated. Added/updated entities: 60, relationships: 57".

On the right side of the interface, there is a "Details" panel with a sub-tab "Analysis". It shows the "Last updated" time as "3:04:22 am Mar 27, 2026" and a button labeled "Update". Below this, there are tabs for "Summary", "Attack Chain", "Investigation Steps", and "Remediation" (active). The "Remediation Actions" section is titled "Containment" and lists several actions:

- Isolate Endpoints: Immediately isolate the following endpoints from the network to prevent further spread and C2 communication:
 - vr-zep (Device ID: vEa9ERlqSRamH4KcwJOBA) - Use Quarantine.
 - sia-zep1 (Device ID: ssFouDT9055jctephTYPg) - Use Quarantine.
 - ldesktop-mt-sea (Device ID: 1gBxxIrAR8WbqvdoUNZg) - Use Quarantine.
 - desktop-n4d6u2q (Device ID: CjDFG-46QU0zXV AepFU60A) - Use Quarantine.
 - The internal staging server at 10.225.128.74 must be identified and isolated via network controls.
- Block Malicious Network Indicators:
 - Block outbound connections to the domain raw.githubusercontent.com and IP address 185.19.9.110.133 at the network perimeter. Use Block Domain.
- Block Malicious File Hashes:
 - Add the following SHA256 hashes to a deny list policy to prevent execution across all managed endpoints. Use Deny Hash for each hash:
 - 344f076bb1211cb02eca9e5ed2c8ce59bcf74ccbc749ec611538fa14ecb9aad2 (c:\rwtworker\rwtworker\sevenzzip\7-zip\7z.exe)
 - 2fcd212f59f4a7a004ea315f61fc36e78b15ad19d2c4b689826c019070e89020 (c:\dual-use-tools\netscan.exe)
 - 4fb049eeddd221e5470cd33177299dd13f85eba25beef7aced7a0890ad85181f (python.exe)
 - Any hashes associated with the .hta and .js files once retrieved.



Reassess



Win11-003

NAME

Microsoft Windows 11 Pro

OS NAME

10.0.26200

OS VERSION

Sep 30, 2026, 1:43:01 PM

LAST ASSESSMENT

Vulnerabilities

Filters | 3 Selected

RISK Critical OR RISK Important OR RISK Moderate

Vulnerabilities

	CVE ID	RISK	TYPE ↑	ISSUED	FIX VERSION
>	CVE-2026-74936	♦ Moderate (5.5)	APP	Aug 18, 2026, 3:17:29 PM	153.1
>	CVE-2026-74939	♦ Moderate (5.4)	APP	Aug 18, 2026, 3:17:30 PM	153.1
>	CVE-2026-84118	♦ Moderate (5)	APP	Sep 1, 2026, 3:20:05 PM	153.2

Vulnerabilities

Devices

CVEs

Filters

▼ Highest Risk

Critical 0

Important 0

Moderate 1

Low 1

▼ OS

Windows 2

macOS 0

Linux 0

Select

Vulnerabilities

Win11-003

Win11-003

Symantec AI



CBX Complet...ne Demo Lab ▾

Miodrag Milenkovic ▾

 SymantecAI



koje su najveće pretnje koje trenutno imamo u organizaciji?

Evo pregleda najvećih pretnji i najkritičnijih upozorenja u vašoj organizaciji u poslednjih 30 dana:

Top Threat Names (by Observation Count)

Here are the top 10 most observed threat signatures over the past 30 days:

1. ACM.Ps-Net!g1
 - Observation Count: 67
2. ISB.Downloader!sr180
 - Observation Count: 67
3. ACM.Ps-CPE!g2
 - Observation Count: 22
4. ACM.Rdp-Lnch!g1
 - Observation Count: 22
5. ACM.Ps-Arp!g1
 - Observation Count: 17
6. ACM.Btsad-Lnch!g1
 - Observation Count: 16
7. ACM.Crtutl-Http!g1
 - Observation Count: 16
8. ACM.Ps-Enc!g1
 - Observation Count: 16
9. ACM.Ps-Sc!a1

Ask SymantecAI...

Responses might contain mistakes or unexpected content.



Proven. Trusted. Recognized.





Symantec CBX & Defender work together



- Symantec CBX and Defender endpoints can work together without interfering with each other's ability to protect
- Symantec CBX can provide a greater level of threat prevention even with Defender enabled



Carbon Black.
by Broadcom

Thank You

⚡⚡
Legends Never Die