THREAT REPORT

2025-05-01 - 2025-05-31

COMPUTER TEAM INC
www.computerteam.com
Providing solutions not just computers since 1987!

COMPUTER TEAM INC

Powered By:
HUNTRESS

THREAT REPORT 2025-05-01 to 2025-05-31
COMPUTER TEAM INC

COMPUTER TEAM INC
www.computerteam.com
Providing solutions not just computers since 1987!

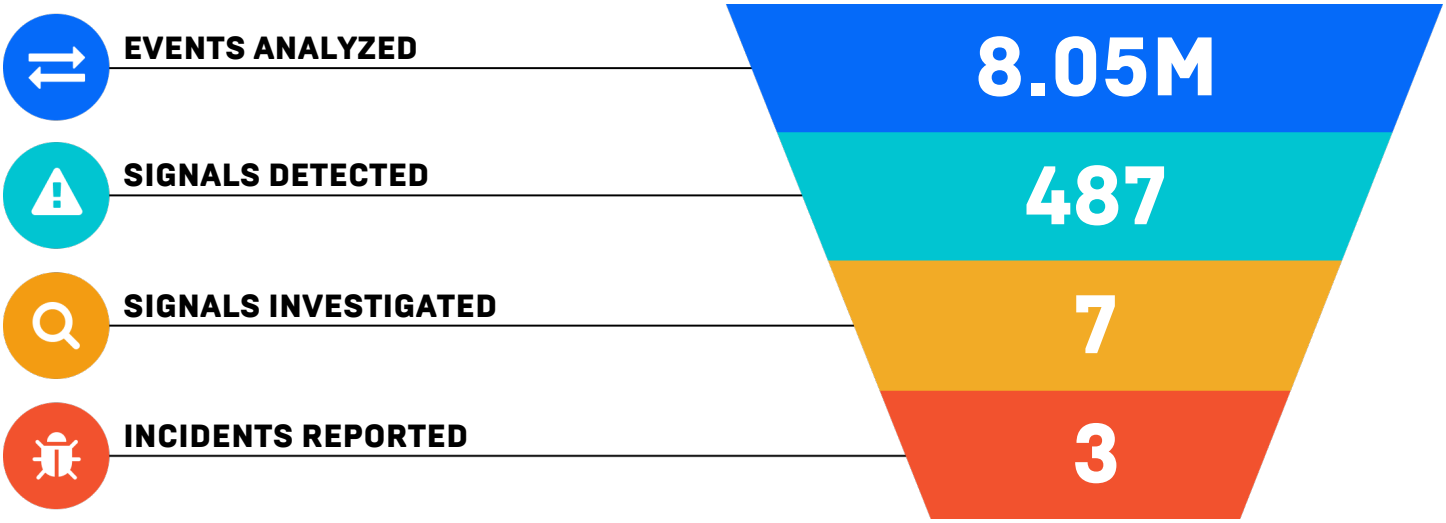
SUMMARY

During the time frame of this report, your cybersecurity platform **analyzed 8,052,581 events** from **23 entities** on your network.

Of those events, there were **487 signals detected** through automated and human analysis. Security analysts manually **investigated 7 signals** that were suspicious in nature. Those investigations led to **3 incident reports**, which required remediation of compromised entities by your security team. This defense strategy continues to reduce your risk, which maximizes your security and minimizes cyberattack damage to your business.

ENTITIES PROTECTED

23 16



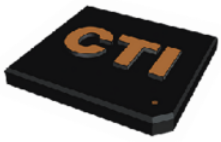
ANALYST NOTES

HERBIE ZIMMERMAN
MALWARE ANALYST

GLOBAL THREATS

- SOCIAL ENGINEEING
- AITM
- RMM TOOLS

This month, social engineering attacks remain the top threat, primarily involving remote management and monitoring (RMM) tools or cloud account takeovers (ATOs). Cloud ATOs persist because of proven tactics like Adversary-in-the-Middle (AiTM) and phishing attacks. For RMM attacks, attackers continue to use deceptive names like "client," "statement," "invoice," or "social security". Beyond technical solutions, a strong defense continues to be is training end-users to report suspicious activity.



COMPUTER TEAM INC
www.computerteam.com
Providing solutions not just computers since 1987!

PERSISTENT FOOTHOLDS

During this time frame, your cybersecurity platform **analyzed 5,657 autorun events** to discover persistent footholds that, if not remediated quickly, could become malicious threats to your business.

Of those events, there were **0 autorun signals detected**.

AUTORUN EVENT TRIAGE

5,657
Autorun Events Analyzed

0
Autorun Signals Detected

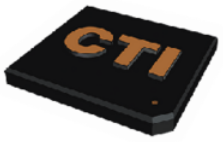
0
Autorun Signals Investigated

0
Foothold Incidents Reported

WHAT IS A PERSISTENT FOOTHOLD?

Persistent Footholds are mechanisms attackers use to gain long-term access to a network by exploiting common auto-starting applications (autoruns), such as Skype or Google Updater.

By abusing and masquerading as legitimate system components, attackers can slip by other security tools, remaining undetected while planning their next move.



COMPUTER TEAM INC
www.computerteam.com
Providing solutions not just computers since 1987!

RANSOMWARE CANARIES

During this time frame, your cybersecurity team monitored **379** **canary files deployed** on Windows endpoints, which acted as early warning signals for ransomware on your network.

Like the old canary in the coal mine, Ransomware Canaries enable faster and earlier detection of potential ransomware incidents. When deployed, small lightweight files are placed on all protected endpoints—and if those files are modified or changed in any way, an investigation is conducted.

CANARIES IN YOUR MINE

62

Protected User Profiles

with **379** total canary files, deploying multiple canary files per user

0

Ransomware Incidents Reported

across **23** endpoints

RANSOMWARE IN THE NEWS

In mid-March 2025, security researcher Yohanes Nugroho released a decryptor for the Linux/ESXi variant of Akira, leveraging GPU power to brute-force decryption keys. This file recovery tool takes seven days with a single GPU, while 16 GPUs reduce this to about 10 hours. This decryptor marks a significant victory for victims, offering a free recovery option for ransomware that's been around since 2023. So far in 2025, ransomware group Cl0p has roared back, compromising over 300 companies with zero day exploits in file transfer software. They averaged nearly 35 victims daily since February. Meanwhile, Medusa has adopted a new BYOVD driver dubbed ABYSSWORKER, signed with stolen certificates, to disable EDR tools, elevate privileges, and fuel a surge in double-extortion hits, encrypting data and selling stolen data on the dark web. Qilin has also returned, targeting cancer treatment hospitals and car dealerships, likely through RMM access obtained with infostealer malware.

COMPUTER TEAM INC
www.computerteam.com
Providing solutions not just computers since 1987!

MANAGED AV

During this time frame, your cybersecurity platform **analyzed 1,106 antivirus events** and automatically **blocked 2,123 potential malware files** from executing on your Windows endpoints.

Of those events, there were **0 antivirus signals investigated** because none were suspicious in nature.

ANTIVIRUS EVENT TRIAGE

WHAT IS MAV?

Managed antivirus helps your security team proactively scan and enforce policy settings on your organization's devices ensuring they are protected against the latest cyber threats.

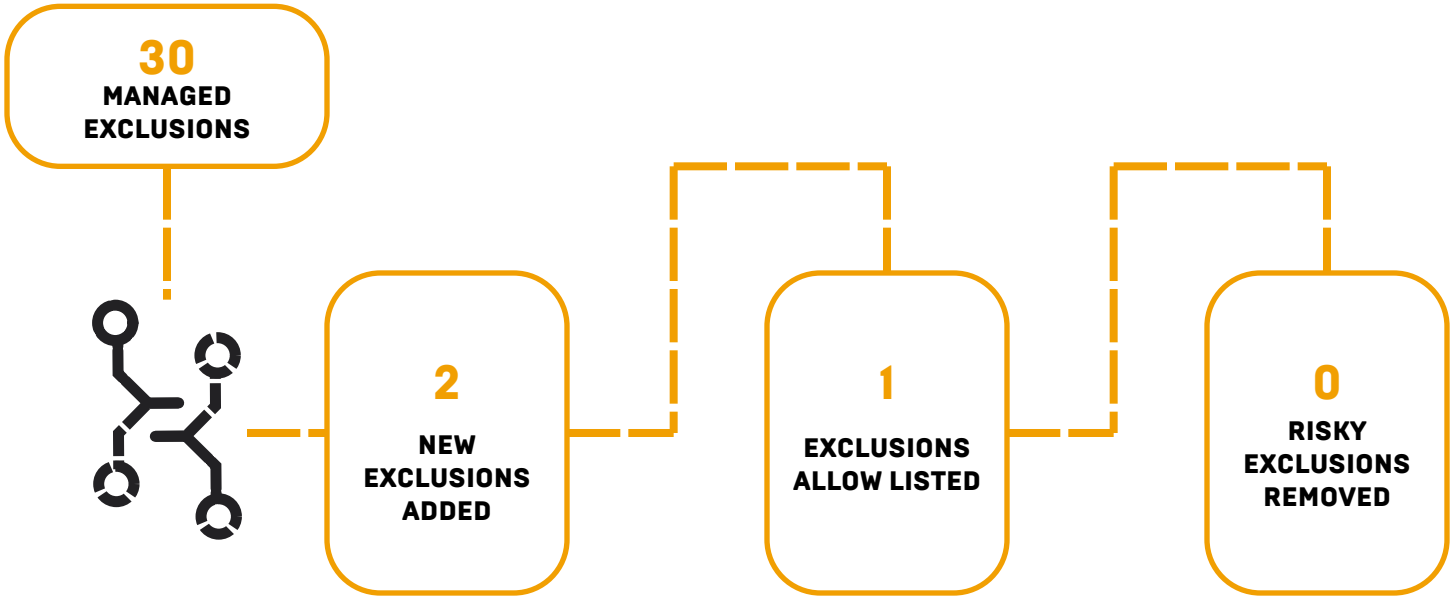
By aggregating antivirus findings into a single-pane of glass, your security team uses MAV to filter out noise and focus on the threats that are not mitigated by AV alone.

COMPUTER TEAM INC
www.computerteam.com
Providing solutions not just computers since 1987!

MANAGED AV EXCLUSIONS

During this time frame, your cybersecurity platform **analyzed 30 exclusions** and automatically **removed 0 risky exclusions** from decreasing the effective scan radius of Microsoft Defender.

EXCLUSIONS ANALYSIS



WHAT ARE RISKY EXCLUSIONS?

Risky Exclusions are settings that prevent Microsoft Defender from scanning specific file paths, file extensions, or process names. Defining these settings too broadly results in effectively lowering the surface radius of protection Defender can offer.

By aggregating exclusions into a single-pane of glass, you can choose whether to have your cybersecurity platform remove these risky exclusions automatically or you may review them manually. View all of your exclusions

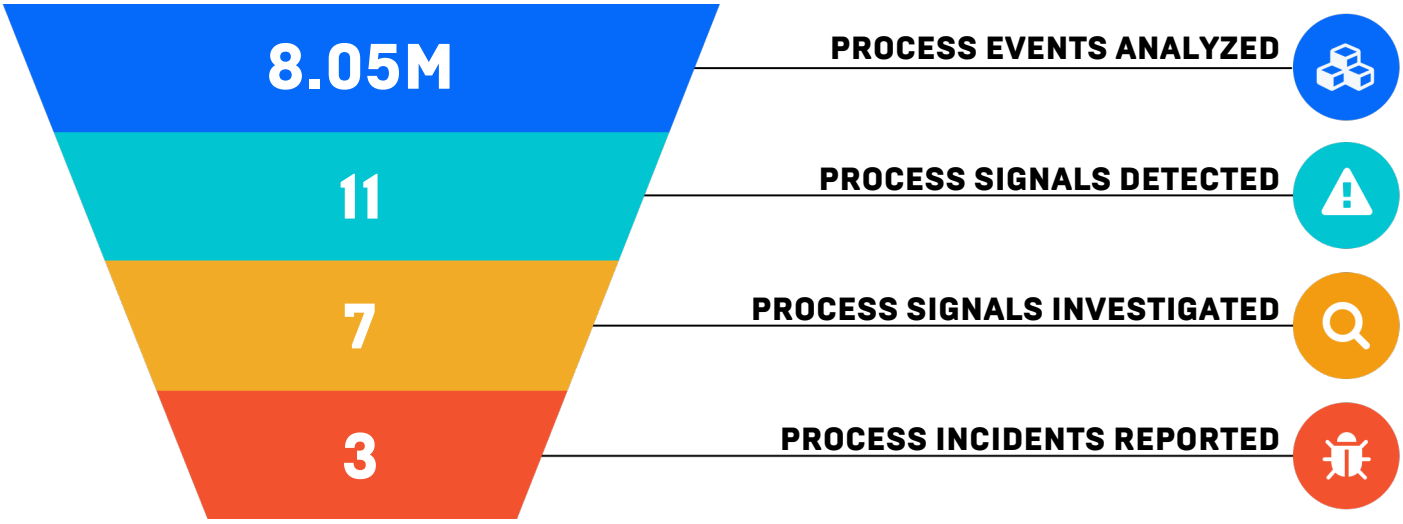
COMPUTER TEAM INC
www.computerteam.com
Providing solutions not just computers since 1987!

PROCESS INSIGHTS

During this time frame, your cybersecurity platform **analyzed 8,045,393 process events** to identify suspicious processes that could lead to malware execution.

Of those events, there were **11 process signals detected** through automated and human analysis. Security analysts manually **investigated 7 signals** that were suspicious in nature. Those investigations led to **3 process incident reports**, which required remediation of compromised endpoints by your security team.

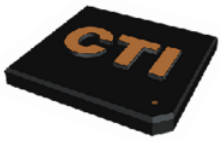
PROCESS INSIGHTS EVENT TRIAGE



WHAT IS PROCESS INSIGHTS?

Before causing disruption, malicious actors use covert processes to stalk the systems they plan to exploit. Process Insights enables your security team to detect these precursor actions.

Once identified your cybersecurity platform is able to stop the maliciously running processes in their tracks, preventing further cyber attack spread.



COMPUTER TEAM INC
www.computerteam.com
Providing solutions not just computers since 1987!

INCIDENT SUMMARY

During this time frame, your security team responded to a total of **3 incident reports**. This page provides summary metrics, broken down by incident severity, product, most common antivirus signals reported, and most targeted entities."

INCIDENT SEVERITY & SOURCE

3
Total

- **1** Critical
- **0** High
- **2** Low

- **3** EDR
- **0** ITDR

MOST REPORTED AV SIGNALS

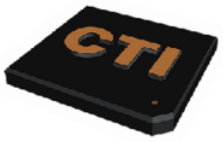
No AV Signals Reported!

MOST TARGETED DEVICES

- CTIEMS3
- CTIDRS-LEN
- CTI-Dustin

INCIDENT SAVINGS

Save your organization thousands, if not millions, of dollars by identifying and remediating cyber incidents in a timely manner. The costs increase dramatically depending on the size of your organization and the value of your data. Use our downtime calculator to see what an incident could potentially cost your organization.



COMPUTER TEAM INC
www.computerteam.com
Providing solutions not just computers since 1987!

INCIDENT LOG

During this time frame, your security team resolved 3 out of the 3 incidents reported. This log highlights the critical and high severity incidents.

2025-05-15 Critical

Closed - Incident on CTIEMS3

*** Active remediations are in process to address this threat, review any remaining remediations (such as reboots) before marking this incident as resolved in the Huntress Platform. ****** The Huntress Agent has been tasked to block these IP addresses for the entire organizat... [see more]

Computer Team Inc