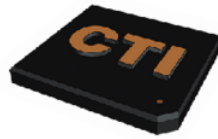


THREAT REPORT

2025-04-01 - 2025-04-30

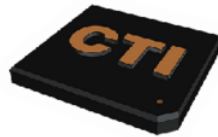


COMPUTER TEAM INC
www.computerteam.com
Providing solutions not just computers
since 1987!

COMPUTER TEAM INC

Powered By:





SUMMARY

During the time frame of this report, your cybersecurity platform **analyzed 9,750,523 events** from **42 entities** on your network.

Of those events, there were **303 signals detected** through automated and human analysis. Security analysts manually **investigated 23 signals** that were suspicious in nature. Those investigations led to **2 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



ANALYST NOTES

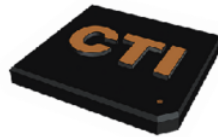


ROBERT KNAPP
MALWARE ANALYST

GLOBAL THREATS

- SOCIAL ENGINEERING

This month saw a spike in social engineering attacks - ranging from poisoned search results that led to attacker payloads, to cloud identity compromises using attacker-in-the-middle (AiTM) tools, or phishing attacks. The goal of these attacks is often data theft, account takeover, or privilege escalation. While the attack surface for these threats is vast and may feel daunting to defend, end-user education and empowering users to report anything they deem suspicious is a vital mitigation tactic.



PERSISTENT FOOTHOLDS

During this time frame, your cybersecurity platform **analyzed 36,664 autorun events** to discover persistent footholds that, if not remediated quickly, could become malicious threats to your business.

Of those events, there were **10 autorun signals detected** through automated and human analysis. None of the detected signals were suspicious in nature, thus no further investigation was warranted by your security team.

AUTORUN EVENT TRIAGE



36,664

Autorun Events Analyzed



10

Autorun Signals Detected



0

Autorun Signals Investigated



0

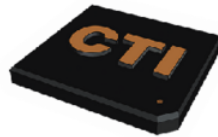
Foothold Incidents Reported

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.



RANSOMWARE CANARIES

During this time frame, your cybersecurity team monitored **1,094 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

211

Protected User Profiles

with **1,094** total canary files, deploying multiple canary files per user

0

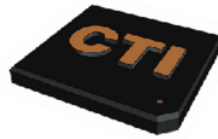
Ransomware Incidents Reported

across **42** 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 CI0p 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.

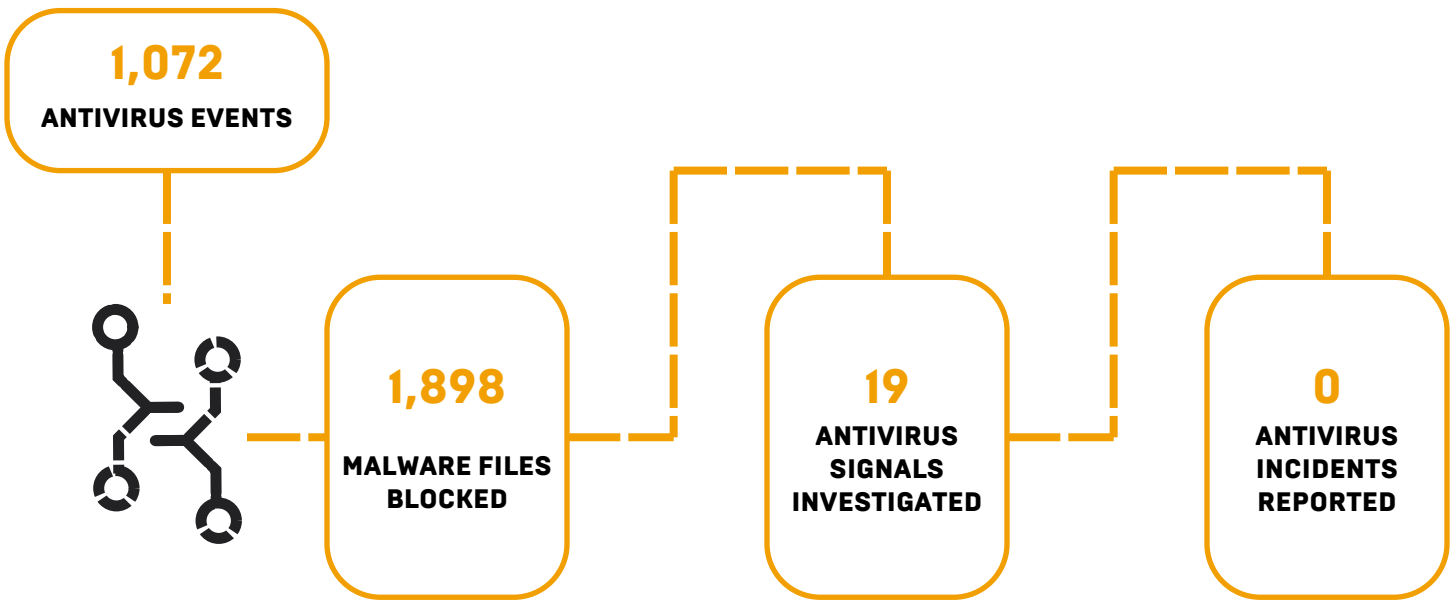


MANAGED AV

During this time frame, your cybersecurity platform **analyzed 1,072 antivirus events** and automatically **blocked 1,898 potential malware files** from executing on your Windows endpoints.

Of those events, there were **19 antivirus signals investigated** by security analysts because the executing file was not successfully blocked by antivirus. Those investigations led to **0 antivirus incident reports**.

ANTIVIRUS EVENT TRIAGE

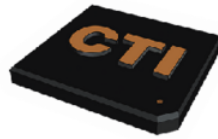


WHAT IS MAV?



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.

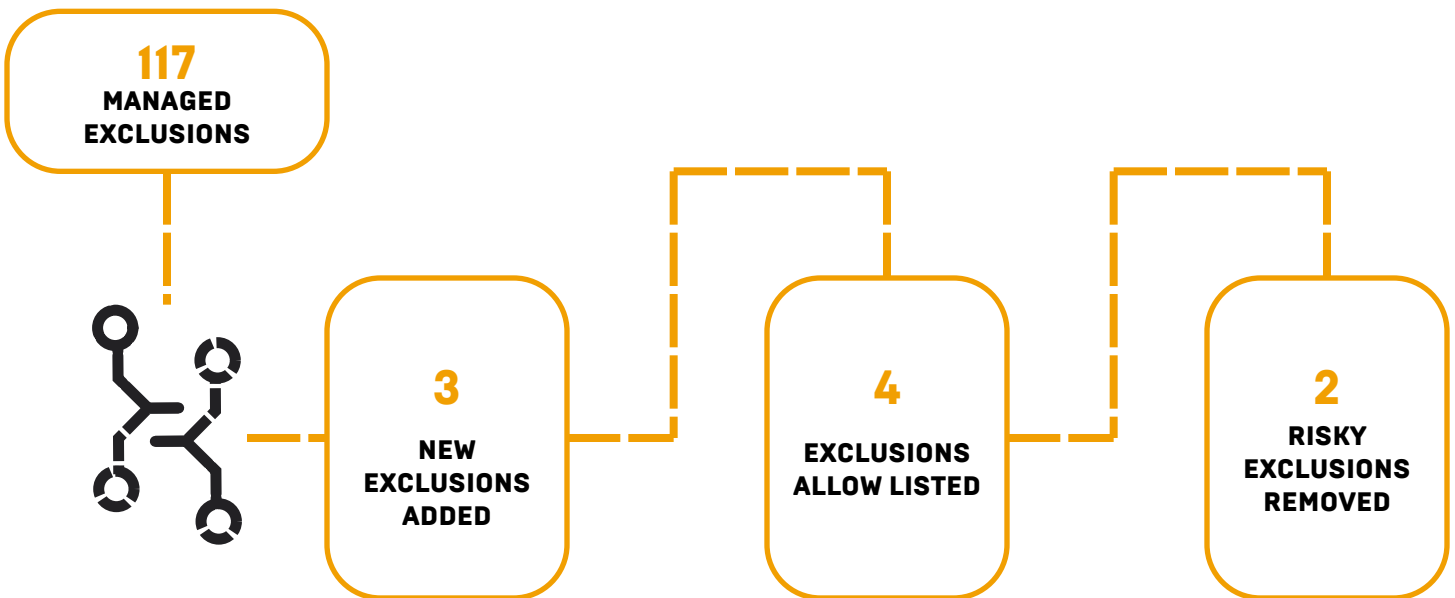
By aggregating antivirus findings into a single-pane of glass, your security team uses MAV to filter out noise and focus on the threats that are not mitigated by AV alone.



MANAGED AV EXCLUSIONS

During this time frame, your cybersecurity platform **analyzed 117 exclusions** and automatically **removed 2 risky exclusions** from decreasing the effective scan radius of Microsoft Defender.

EXCLUSIONS ANALYSIS

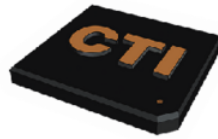


WHAT ARE RISKY EXCLUSIONS?



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](#)

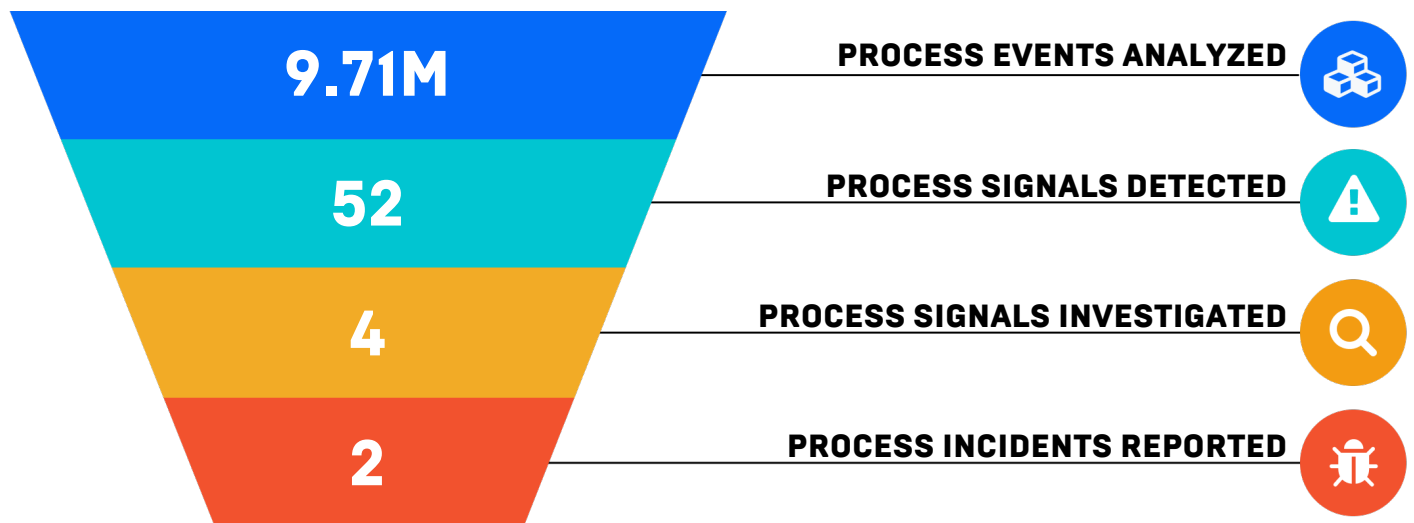


PROCESS INSIGHTS

During this time frame, your cybersecurity platform **analyzed 9,711,609 process events** to identify suspicious processes that could lead to malware execution.

Of those events, there were **52 process signals detected** through automated and human analysis. Security analysts manually **investigated 4 signals** that were suspicious in nature. Those investigations led to **2 process incident reports**, which required remediation of compromised endpoints by your security team.

PROCESS INSIGHTS EVENT TRIAGE

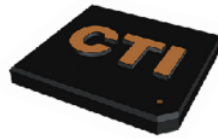


WHAT IS PROCESS INSIGHTS?



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.

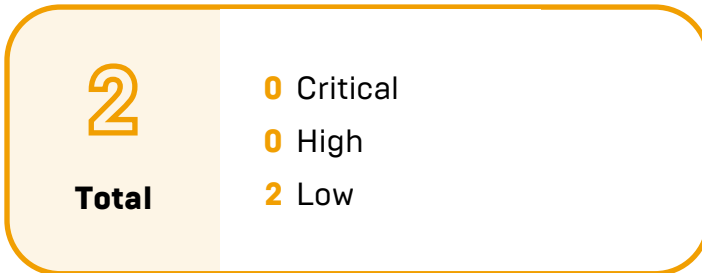
Once identified your cybersecurity platform is able to stop the maliciously running processes in their tracks, preventing further cyber attack spread.



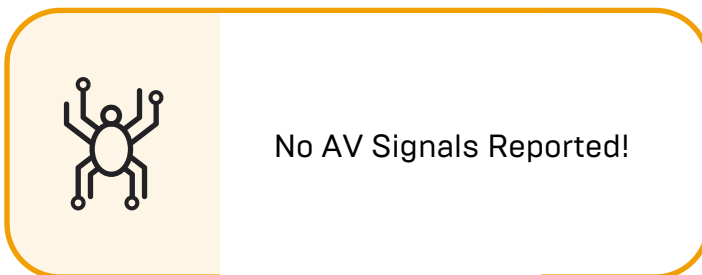
INCIDENT SUMMARY

During this time frame, your security team responded to a total of **2 incident reports**. This page provides summary metrics, broken down by incident severity, product, most common antivirus signals reported, and most targeted entities."

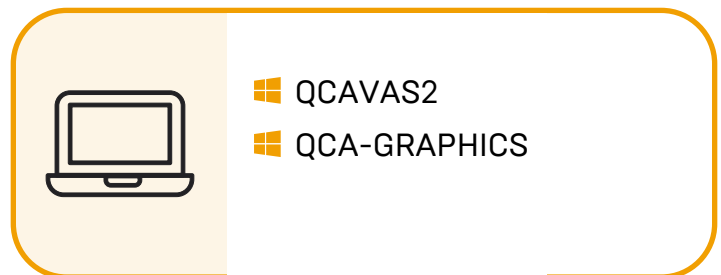
INCIDENT SEVERITY & SOURCE



MOST REPORTED AV SIGNALS



MOST TARGETED DEVICES



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.