HUNTERS

AXON IDENTITY THREAT PROTECTION

Stop Threat Actors Before They Exploit Your Employees' Credentials.
Gain exclusive visibility into compromised identities
and take action before attackers do.

Proactive Defense Against Identity Threats

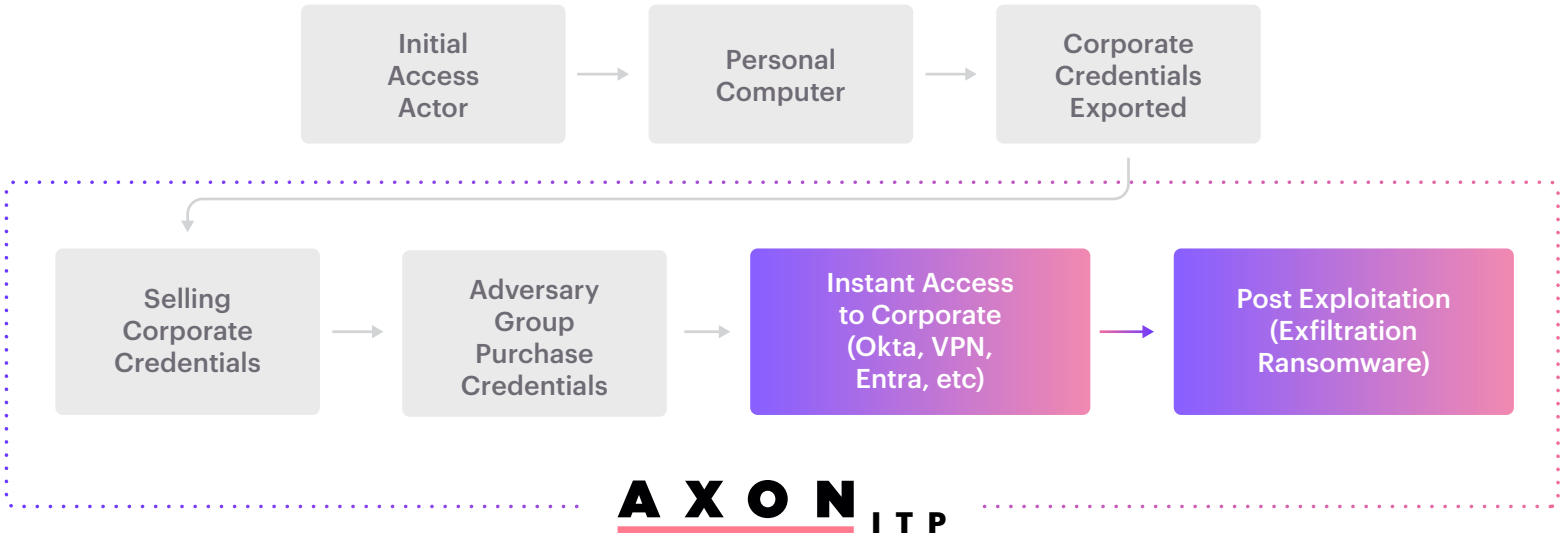
Challenges

Infostealers are a type of malware designed to steal sensitive information from victims' devices, including corporate and **personal machines.** Over the past few years, the number of incidents involving infostealers has risen by approximately 45%, highlighting their growing prevalence and danger. These attacks now account for a significant portion of credential-related security breaches.

Adversaries often leverage infostealers because they can easily target personal devices, bypassing robust corporate security measures such as EDRs, proxies, and firewalls - by exploiting weaker entry points, adversaries render these advanced security solutions ineffective. Infostealers also enable adversaries to obtain valuable information more quickly, efficiently, and cost-effectively than traditional methods.

A common use case is when threat actors **purchase credentials stolen from personal machines on underground marketplaces (also known as the dark web)** and use them as an entry point to corporate environments. By exploiting these credentials, attackers can establish initial access to an organization's network.

Recent high-profile breaches, including those at Orange Spain, Uber, and CircleCI, demonstrate the severity and far-reaching consequences of infostealer-based attacks. **As organizations increasingly adopt remote and hybrid work models, the visibility gap into employees' personal devices poses a growing challenge for security teams, making it harder to effectively detect and mitigate these threats.**

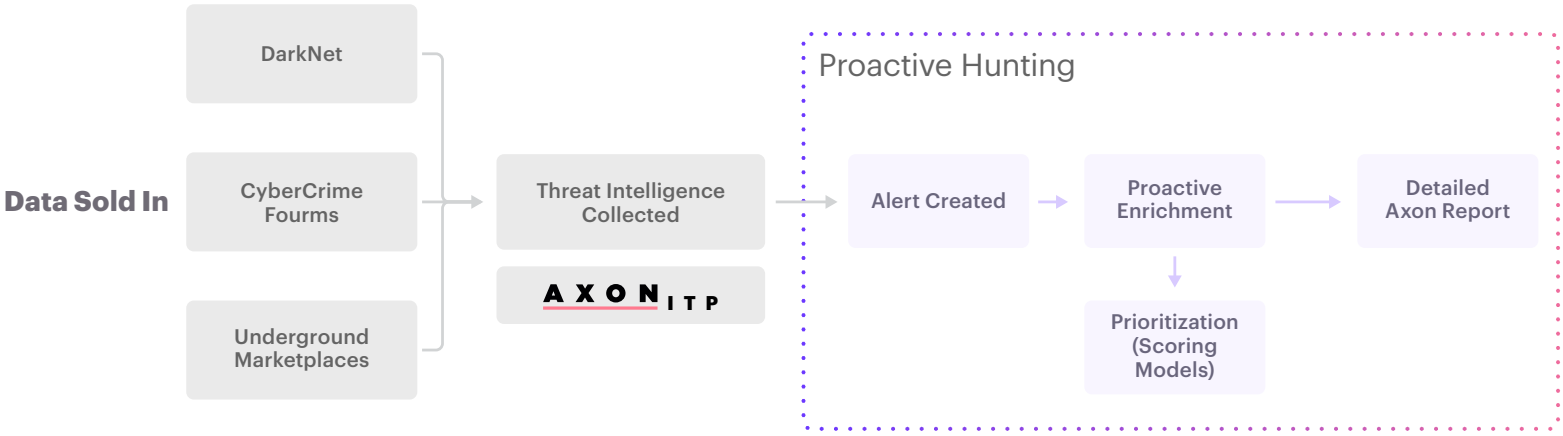


Solution

Axon Identity Threat Protection delivers premium threat intelligence by leveraging a fresh and exhaustive dataset based on infostealers compromised data. This highly detailed and up-to-date intelligence provides unmatched visibility into compromised employees and identities. Our comprehensive monitoring covers cybercrime forums, darknet markets, adversary phishing kits, and more, ensuring robust coverage.

By leveraging data ingested into Hunters, Axon Identity Threat Protection provides continuous monitoring and threat hunting to identify active employee accounts linked to compromised credentials. Suspicious post-infection activities are promptly detected, allowing security teams to respond in real-time. When necessary, tactical investigations offer detailed remediation steps to mitigate risks effectively and strengthen organizational defenses.

Axon Identity Threat Protection not only helps to detect and analyze compromised credentials but also enhances security operations with automated workflows and integration capabilities. By correlating identity intelligence with enterprise security telemetry, organizations can prioritize and respond to the most pressing threats efficiently. This proactive approach minimizes alert fatigue and ensures security teams focus on the most critical risks.



Key Capabilities

✓ Continuous Credential Monitoring & Threat Intelligence:

Axon actively tracks cybercriminal marketplaces, forums, and infostealer logs to detect stolen credentials linked to your employees, providing early warnings and enabling swift remediation before attackers exploit the data. The team has unique access to closed channels and marketplaces, which gives us exclusive results. The data is highly comprehensive and includes origin details of the compromise, plain text passwords, and intelligence on the infostealer family that stole the data.

✓ Automated Threat Detection & Real-Time Hunting:

By correlating compromised credentials with enterprise security telemetry from Okta, Azure AD, On-premises, and any other data ingested to Hunters, Axon can identify active threats and proactively hunts for unauthorized access attempts before they escalate. By leveraging the data ingested into Hunters, Axon prioritizes alerts by analyzing suspicious activity and key metadata, such as determining whether the compromised user account is still active and its associated permissions, to enhance response efficiency.

✓ Incident Investigation & Remediation:

Axon provides an in-depth analysis of compromised credentials, evaluating their usage to determine the breach impact and offering clear mitigation steps, including forced password resets, account restrictions, and increased monitoring.

HUNTERS