HuntersAI

Find the Needle in the Tech Stack

Hunters.AI is an open XDR that automates expert threat hunting techniques to scale threat detection & response. It searches potential attack signals and automatically analyzes, scores, and correlates them across environments. Connect Hunters.AI to your existing stack - uncover attacks while eliminating triage time and expediting response.

Attackers are using the surge in data volumes to blend in environments and stay under the radar. They don't attempt to cover their tracks, but rather act as a legitimate part of your organization. This is why many security leaders believe to be exposed even with a significant security stack deployed. As if that's not enough, attack surfaces expand: Cloud, SaaS, Endpoints, Network, iOT, and more.

Detecting at an Attacker's Pace

Hunters.AI was built to detect stealth attack campaigns where threat actors blend in in a way that existing security solutions fail to detect. The following examples describe some real world attack scenarios detected by Hunters.AI where all other security tools remain mute.

1. Malicious activity with AWS Credentials Theft

Malicious activity using stolen instance credentials is a common TTP used in AWS, but is difficult to detect. Hunters.AI identifies the concurrent use of AWS instance credentials from more than one IP Addresses, which is also quite common, but is able to discern which of these is not a legitimate use of multiple IPs.

2. Data Breach Through Unauthorized Cloud Access

Many attacks are leveraging unsecured user logins into on-premise servers and cloud services. Hunters.AI determines whether an access attempt is unauthorised and unsecured by identifying if the endpoint protection is working properly on the user device. It investigates if managed endpoints were ever seen using that same source IP address, and if there is a match between the user's device OS and the login attempt device OS, and if the login was successful.

Know What to Look For

Hunters.AI covers a variety of Tactics, Techniques, and Procedures (TTPs) across different IT environments, to surface all potential attack signals

- Multiple TTPs across attack surfaces: cloud, endpoints, network, SaaS, and more.
- MITRE ATT&CK coverage analysis
- Hunters' proprietary TTPs include extended coverage such as: User, Identity, Email, HR, and more

3. Asset Compromise Using Former Employee Credentials

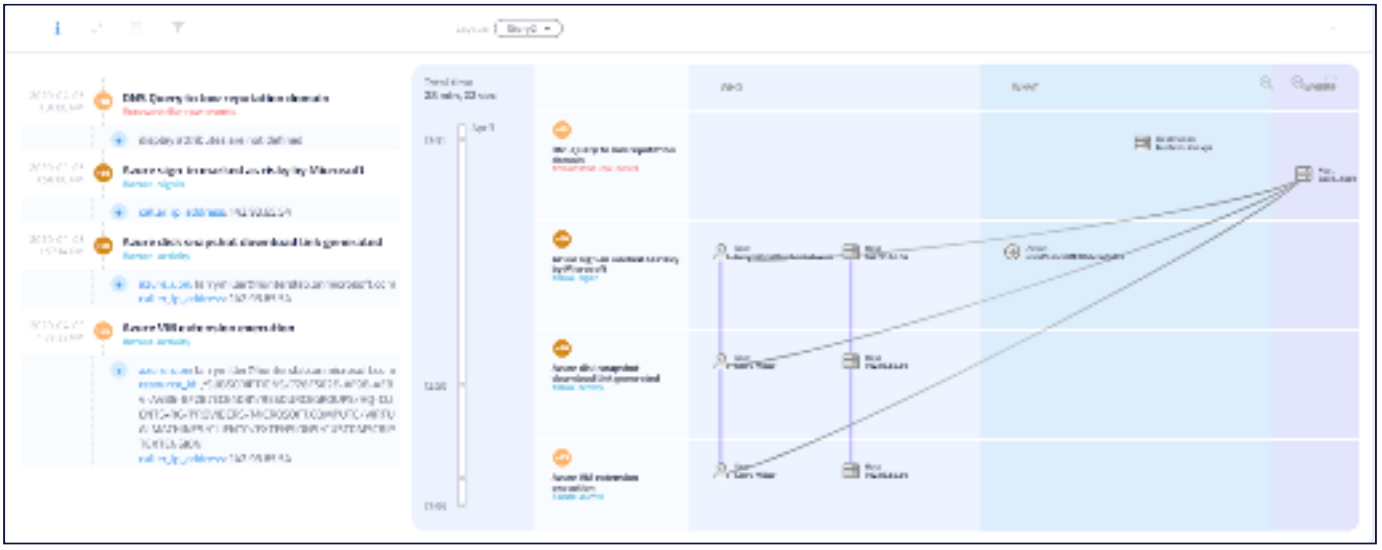
A common attack practice is to use existing employee credentials, including credentials of an employee that was laid off and was not properly revoked. THe credentials can then be used to connect to a database server and exfiltrate data to an external server. Hunters.AI identifies the connection attempt as malicious by correlating user credentials with HR data. It also detects the attempt to transfer data to an unknown destination.

4. AWS Compromise using TOR-Based WAF Access

In an attack scenario similar to the Capital One breach (August 2019), malicious actors use TOR to access a public web service like WAF; exploit a vulnerability to configure access rules to allow access to EC2, and then use SSM to exfilirate data. Hunters.AI identifies the TOR to the WAF server, and detects the denied access to AWS services, and detects the EBS snapshot.

5. Data Exfiltration from Azure Server Following Spear Phishing

Malicious actors obtain Azure credentials using a spear phishing attack campaign. They access Azure, exfiltrate a disk snapshot, and create a VM extension for persistency. Hunters.AI identifies the early stage of the malicious operation starting with the detection of the initial DNS resolution of a new domain resulting with the phished link. Then, detection of the risky Azure sign-in attempt of the resolved IP address. And lastly, detection of an attempt to exfiltrate a disk snapshot, followed by execution of a VM extension.



Hunters.AI Incident Story Overview: Data Exfiltration from Azure Server Following Spear Phishing