



# **Intel 471's HUNTER Community: Your entry to the HUNTER threat hunt platform**

Explore a subset of HUNTER's intelligence-driven behavioral cyber threat hunt packages with the HUNTER Community

---

# Threat Hunting Made Easier with HUNTER Hunt Packages

Sometimes organizations want to get a more accurate sense of how behavioral threat hunting can reduce risk from unknown and undetected cyber threats in their IT environment. This is where Intel 471's HUNTER Community can help you get started.

The HUNTER Community allows you to execute HUNTER hunt packages in your environment before committing to the full HUNTER, the industry's leading threat hunting platform and its intelligence-driven behavioral hunt queries, which are written by threat hunting experts in the native query languages for most major security platforms.

## HUNTER versus HUNTER Community

With 30-day access to our HUNTER Community, you can:

- Access 60+ Emerging Threat hunt packages that identify adversary activity based on TTPs, not IOCs
- Research and execute up-to-date, pre-validated hunt query logic of your security tools and data sources
- Filter hunt packages by MITRE ATT&CK techniques and 20+ contextual tags
- Select access to Intel 471 threat actor profiles, adversary intelligence, and malware
- Access analyst notes, runbooks, mitigation recommendations, and hunt-specific documentation with transparent threat intelligence, remediation steps, and clear guidance
- View weaponized CVEs, MITRE technique IDs and names
- Download hunt emulation & validation packages
- View human-readable Query Logic Tables, breaking down the selections, fields, values and conditions



# Make HUNTER Community Your First Step Towards Full Threat Hunting

	HUNTER	HUNTER Community
Full access to almost 700 HUNTER behavioral hunt packages	YES	NO
Emerging Threats collection ~ 60 HUNTER packages	YES	YES*
Deploy hunt queries to your security tools**	YES	YES* (30-day access)
Emulation and validation files	YES	YES
Query logic	YES	YES
Hunt package collections by threat actor	75+	~10
Threat and Malware Profiles	100+	12
REST API for correlation and automated reporting	YES	YES
Use 'Open in Tool' to create deep link in your security tool using URI	YES	YES
Pre-built hunt reports	YES	YES
Team hunt space to plan, execute, report and manage HUNTER packages	YES	NO
Guided Threat Hunts	YES	NO
Build hunt templates to streamline recurring hunts, stage frequency, assign hunts	YES	NO
Workbench to customize hunts, document what works and does not	YES	NO
Direct access to the Intel 471 Threat Hunt team	YES	NO
Bring your own hunts (BYOH)	YES	NO
Track hunt KPIs and metrics	YES	NO
MITRE ATT&CK technique gap analysis	YES	NO

\*HUNTER Community users can contact sales to request access to additional HUNTER packages and/or an extension on the 30-day access.



\*\*Hunt query tool support include these platforms:

- CarbonBlack Cloud — Investigate
- CarbonBlack Response
- CrowdStrike EDR
- CrowdStrike LogScale
- Elastic EDR
- Elastic Signal
- Google SecOps
- Microsoft Defender
- Microsoft Sentinel
- Palo Alto Cortex XDR
- QRadar Query
- SentinelOne
- Splunk

## Intel 471's HUNTER Community — See How HUNTER Can Amplify Your Threat Hunt Program

Intel 471's HUNTER Community provides 30 days of free access to hunt packages within the HUNTER Emerging Threats collection — a subset of hunt packages from the full HUNTER platform, and limited access to hunt productivity features.

The HUNTER Community is intended for exploring HUNTER features and executing hunt packages in your environment. HUNTER Community users experience the intelligence-driven methodology through continually updated hunt packages informed by the up-to-date CTI from Intel 471, ensuring the latest behavioral intelligence is accurate and timely.

While HUNTER Community offers a subset of the available hunts on the HUNTER platform, users can still explore the coverage of hunts based on the MITRE ATT&CK framework, and additional contextual intelligence like actors and threats. For example, HUNTER Community users see, search, and filter all hunt packages available in HUNTER; however, they can also deploy or execute these packages on their security platforms. The key difference is that the full-featured HUNTER platform helps organizations drive efficient, consistent, and repeatable hunt practices using pre-validated hunts that cover most post-compromise MITRE ATT&CK techniques.

Read more about business value of threat hunting:

[DOWNLOAD](#)





Search mitre, actors, tags etc...

Emerging Threats

Recently Updated

My Environment

MITRE

Collection
**VANHELISING RANSOMWARE**

Created March 25, 2025
Updated April 1, 2025

In March 2025, a new ransomware-as-a-service (RaaS) program named VanHelsing was launched, quickly gaining traction within the cybercriminal community. The program has targeted and infected three victims within two weeks, demanding ransoms of \$500,000 in Bitcoin for decryption and data deletion. The program allows affiliates to participate by paying a \$5,000 deposit, with these affiliates retaining 80% of ransom payments while the core operators receive 20%. VanHelsing ransomware is cross-platform, capable of infecting Windows, Linux, BSD, ARM, and ESXi systems, and offers an intuitive control panel for managing attacks - notably prohibiting the targeting of entities within the Commonwealth of Independent States (CIS). Researchers have also observed this new variant already evolving in sophistication, meaning its active development and thus the need for up-to-date security measures to defend against this emerging variant.

**Intel 471 TITAN References**  
TITAN Info Report: Actor VanHelsingRAAS recruits affiliates to join new Vanhelsing Locker ransomware-as-a-service affiliate program

HUNT PACKAGES
Details
THREAT PROFILES

MODIFICATION TO VOLSnap VOLUME DELETEPROCESS REGISTRY KEY

High

Created April 11, 2025
Updated April 11, 2025

Dependencies
Endpoint - Sysmon, Endpoint - WinEventLog, Endpoint Detection & Response (EDR), XDR

This content is designed to capture modifications to the VolSnap per-volume DeleteProcess value, which may indicate tampering with Volume Shadow Copy records or process deletion tracking.

COPYING A FILE TO A HIDDEN SHARE DIRECTORY

High


Created May 3, 2022
Updated March 26, 2025

Dependencies
Endpoint - Sysmon, Endpoint - WinEventLog, Endpoint Detection & Response (EDR), XDR

This package is designed to capture activity when a command is issued to copy a file to a hidden share to include the C\$ file share. This can be indicative of access to a restricted share on another system or an indication of lateral movement attempts.

## HUNTER Threat Hunting Platform

Intel 471's HUNTER platform is a powerful, cloud-based application used for enhancing and amplifying cyber threat hunt team capabilities at all hunt maturity levels. With a library of nearly 700 continually updated behavioral hunt packages, HUNTER helps threat hunters proactively identify unknown and undetected threats before they manifest into a more serious event. HUNTER's centralized hunt management tools help teams measure hunt success, identify technique gaps, document findings, and enhance productivity with pre-filled hunt reports and the ability to launch hunts directly into major EDR/XDR, NDR, SIEM, and data platforms.



© Intel 471 Inc. All rights reserved.

# Experience *Real* Threat Hunting with HUNTER Community

Discover how HUNTER can take your threat hunting team to the next level. Sign up for the HUNTER Community to gain free access for one month to dozens of pre-validated hunt packages written for your security and data platforms. The HUNTER Community is a straightforward SaaS application, with no deployment or downloads required.

You can join the HUNTER Community on our web site at [intel471.com](https://intel471.com). Test our intelligence-driven threat hunting capabilities! Get your [HUNTER Community account](#).

## About Intel 471

Intel 471 equips enterprises and government agencies with intelligence-driven security offerings powered by real-time insights into cyber adversaries, threat patterns, and potential attacks relevant to their operations. By integrating human-sourced intelligence with advanced automation and curation, the company's platform enhances security measures and enables teams to bolster their security posture by prioritizing controls and detections based on real-time cyber threats. Organizations are empowered to neutralize and mitigate digital risks across dozens of use cases across our solution portfolios: Cyber Threat Exposure, Cyber Threat Intelligence, and Cyber Threat Hunting. Learn more at [intel471.com](https://intel471.com).

**Our customers' eyes and ears outside the wire.**

