



Smarter Endpoint Threat Hunting

FEBRUARY 19

Authored by:
Vincent Weafer
Chief Operating Officer, CTO
TriagingX, Inc



TriagingX

Smarter Endpoint Threat Hunting

What is Threat Hunting?

More and more companies are transitioning from a primary focus on threat prevention, to a better balance of threat prevention, detection (hunting) and response. The leading information security training institute, SANS, defines threat hunting as a focused and iterative approach to searching out, identifying and understanding adversaries internal to the defender's networks. The primary reason for doing this is the reality that sophisticated malware and targeted attacks are regularly being designed to evade traditional signature-based protections and some next-generation security technologies. Examples include attacks that use advanced malware, fileless techniques or the compromise of legitimate tools such as PowerShell and Windows Management Instrumentation (WMI) which are already deployed on the victim's system.

This transition has been aided by three factors:

- i. The common sense understanding that, even with the best protection tools and practices, data breaches occur far too frequently;
- ii. The introduction of better detection and analysis tools for endpoints and networks;
- iii. The introduction of standards and best practice guidance from programs such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

The NIST Cybersecurity Framework's core includes five high level functions: Identify, Protect, Detect, Respond and Recover. While Threat Hunting is directly applicable to the Detect and Respond functions, what we learn from Threat Hunting helps drive actions in the other cores as well.¹



Credit: N. Hanacek/NIST

The primary objective of Threat Hunting is to ascertain and find those threat vectors that can be a viable risk to your IT Infrastructure, before they can impact the lines of defense.

The SANS 2017 Threat Hunting Survey found that some of the benefits of Threat Hunting include:

- A 91% improvement in the response time to a cyberattack
- An 88% reduction in the Dwell Time (the actual time period from when the Malware executes its payload to when it is actually detected)
- An 84% reduction in the actual number of Security Breaches occurring, based on the total number of Breaches that have actually been detected
- A 74% reduction in the frequency and number of Malware infections

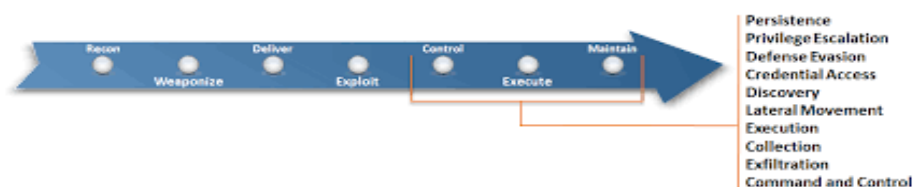
In the following sections, we examine threat hunting models, challenges associated with real-world threat hunting and how TXHunter can help by conducting highly focused endpoint or server incident investigations that go beyond traditional signature-based models. Rather than relying on detection of known IOCs, TXHunter is built on the principal that all threats will be dynamically analyzed in real-time in a contained and simulated environment in order to track actual behaviors.

FIRST-RESPONDER READY	<i>Fast, flexible hunting for cyber emergency response in minutes</i>
GOES BEYOND AV	<i>Fills in the detection gap on systems with only traditional AV protection</i>
FILLS THE EDR COVERAGE GAP	<i>No enterprise covers 100% of endpoints and servers with EDR deployments</i>
SERVER FRENDRY	<i>Deploys easily and safely on servers, where EDR agents can't be deployed due to performance or interoperability concerns</i>
COST EFFECTIVE	<i>Empowers Tier 1 Security & IT Ops Teams to run their own investigations</i>

The MITRE ATT&CK™ Framework

When a security practitioner first starts to think about how to defend critical data and computing assets from cyberattacks, it is useful to break down and classify those attacks in a consistent manner. This process should make the attacks easier to compare and contrast and provide guidance in determining how the attacker exploited the cloud, networks, servers or endpoints.

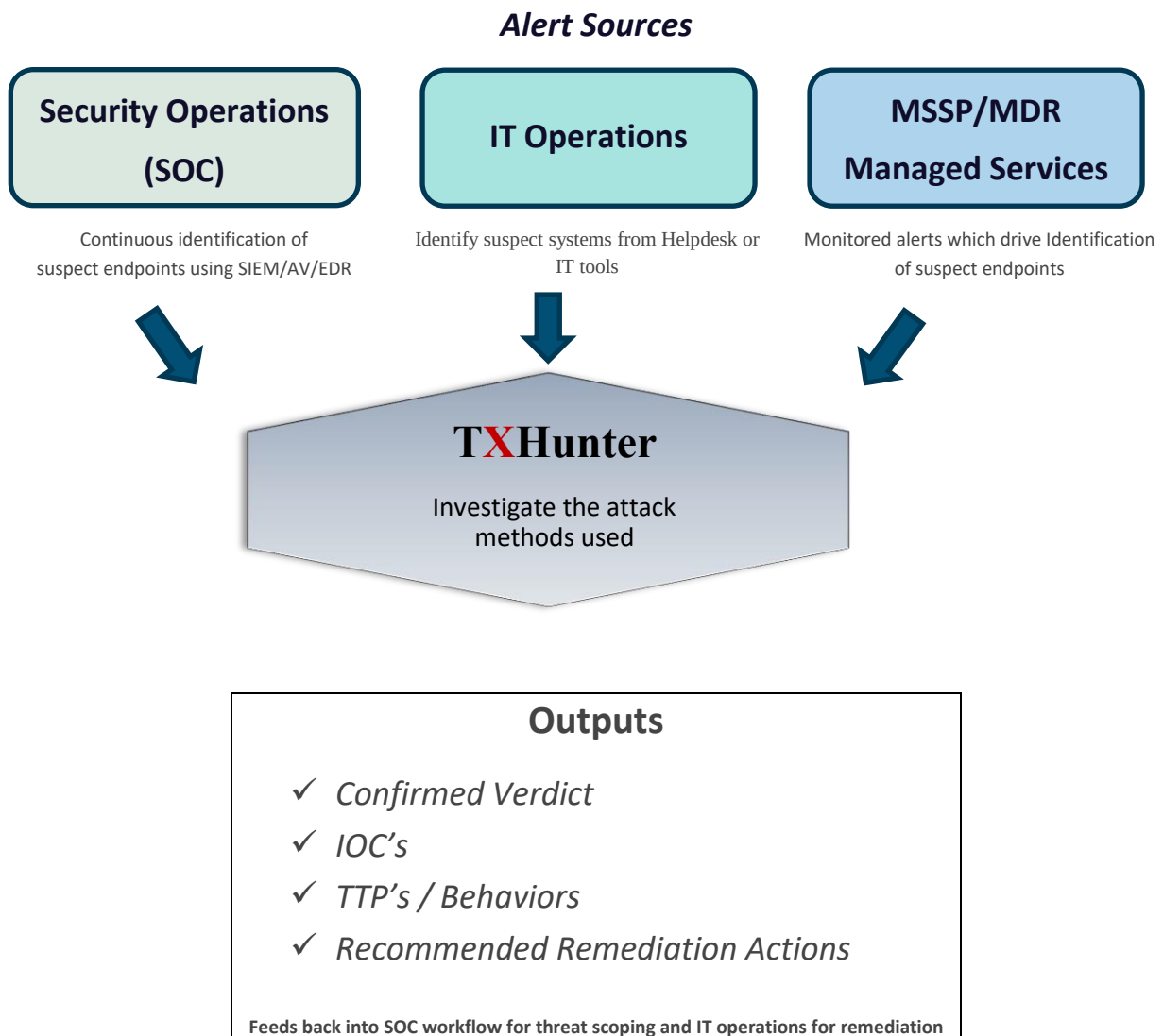
One of the most common and useful frameworks for this purpose is MITRE ATT&CK™ which is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK acronym stands for Adversarial Tactics Techniques and Common Knowledge. It is a curated knowledge base of 11 tactics and hundreds of techniques that attackers can leverage when compromising enterprises ⁽²⁾.



FIVE PRINCIPALS OF THE THREAT BASED MODEL

1.	INCLUDE POST-COMPROMISE DETECTION <p>This is needed when the traditional perimeter lines of defense have allowed cyberattacks to penetrate through. Thus, the implementation of robust detection and investigation functionalities are required in order to discover any new threat vectors and adapt to those threats.</p>	<p><i>TXHunter conducts highly focused incident investigations in order to detect advanced threats, spyware, hidden processes and rootkits, unusual network connections and past abnormal activities, unknown Non-PE files and system misconfigurations.</i></p>
2.	FOCUS ON BEHAVIOR <p>Security Technology needs to have the ability to learn and model future threat vectors from the past behaviors of malware.</p>	<p><i>TXHunter sandbox provides a method for determining attack methods, the basis for other TriagingX solutions to automatically run 'fire-drill' tests on other connected systems in order to block those attack methods.</i></p>
3.	USE A THREAT-BASED MODEL <p>A sophisticated and detailed Threat Model must be created and implemented in order to scope out relevant and persistent threats from the cybersecurity landscape.</p>	<p><i>TXHunter sandbox provides powerful insights on executables, active document, script and malicious URL's and finds new threats that signature/IOC scanning fail to detect.</i></p>
4.	ITERATE BY DESIGN <p>The launch and execution modes of the cyber attacker change on a very quick and dynamic basis. Therefore, in order to keep up with this, a proactive mindset must be adopted in which the security tools and techniques of the organization must be constantly refined.</p>	<p><i>TXHunter sandbox features multiple classifiers for increased accuracy, lower false positives, as well as full-system emulation that defeats evasive malware crafted to bypass traditional sandboxes.</i></p>
5.	DEVELOP AND TEST IN A REALISTIC ENVIRONMENT <p>Any refinements that are made must be thoroughly examined and tested in an environment that emulates the real world, cyber threat landscape.</p>	<p><i>The TXHunter solution is built on the principal that all threats are dynamically analyzed in real-time in a contained and simulated environment in order to track actual behaviors, without relying on detection of known IOC's</i></p>

The Threat Investigation Processes



The hunting process starts with the collection and analysis of data from a multitude of core logs and sensor data, including but not limited to – DHCP, Proxy, Web and Application Server, Active Directory/LDAP, Domain Name Service (DNS), Application Firewall, Host/Network IDS/IPS, Antivirus and Network Infrastructure logs from VPN, Routers and Firewall.

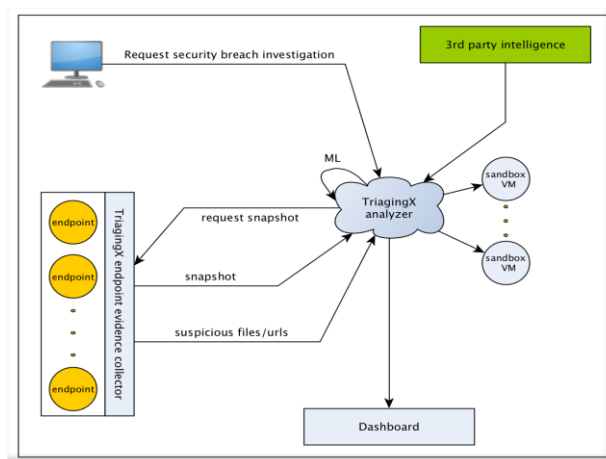
In addition, you'll need insights on endpoint/server events, including operating system events and endpoint detection events. **TXHunter** supports both On-Demand Investigation Mode (offline disconnected and connected systems) and Continuous Monitoring or Testing Mode. In this latter model the security operations team is continuously monitoring and/or or testing their security posture by conducting various penetration testing exercises in order to proactively identify and investigate any suspicious events.

How TXHunter “Hunts”

TXHunter provides an easy and convenient tool for conducting endpoint threat incident investigations remotely. Instead of sending your IT security staff to collect evidence remotely, or deploying endpoint agents across your entire network, TXHunter can perform a rapid and thorough investigation on its own.

There is no need to create a hypothesis to start the Threat Hunting process. You only need to “tell” TXHunter which endpoint(s) you want to investigate, download the disposable run-time agent to gather the information and data, and then just wait for the analysis complete.

- 1 *Install TXHunter server either On-Premise/Private Cloud, or use as Cloud Service*
- 2 *Deploy tiny agent to target system under investigation*
- 3 *Collect Data from system*
- 4 *Run analysis on collected data, and request additional suspect objects (files) from target system*
- 5 *Generate a report. Send data back into SOC workflow / SIEM*



The following are the principal features and benefits of TXHunter:

1) Includes Built in Intelligence and Automated Analysis Mechanism:

TXHunter provides a straight and clear answer as to whether an endpoint has been infected or hacked into, the severity level of that attack; and all supporting data that was used to reach these decision thresholds. TXHunter’s intelligent engine learns from every new discovery found during a Threat Hunting investigation.

2) Focus on Behaviors, Not Just the IOC's Themselves:

The cyber attacker of today is getting much more sophisticated at avoiding detection via known Indicators of Compromise (IOCs). Thus, many of the IOC's that are commonly collected today are historic and brittle. The threat hunting tools should focus instead on attacker techniques and anomalies. TXHunter focuses on collecting and analyzing the system behaviors as well as the tactics, techniques, and procedures (TTPs) of the cyber attacker.

3) Collection of comprehensive datasets:

Following are the types of data collected by TXHunter:

- File system Meta-data
- Windows prefetch data
- Event logs
- Scheduled task data
- Registry data
- Artifacts of interactive sessions such as Web History
- Memory data
- Alternative persistence mechanisms
- Network Connections
- Windows Firewall Rules
- Kernel related data such as: GDT, IDT, SSDT, Shadow SSDT, Hidden Process, Exports

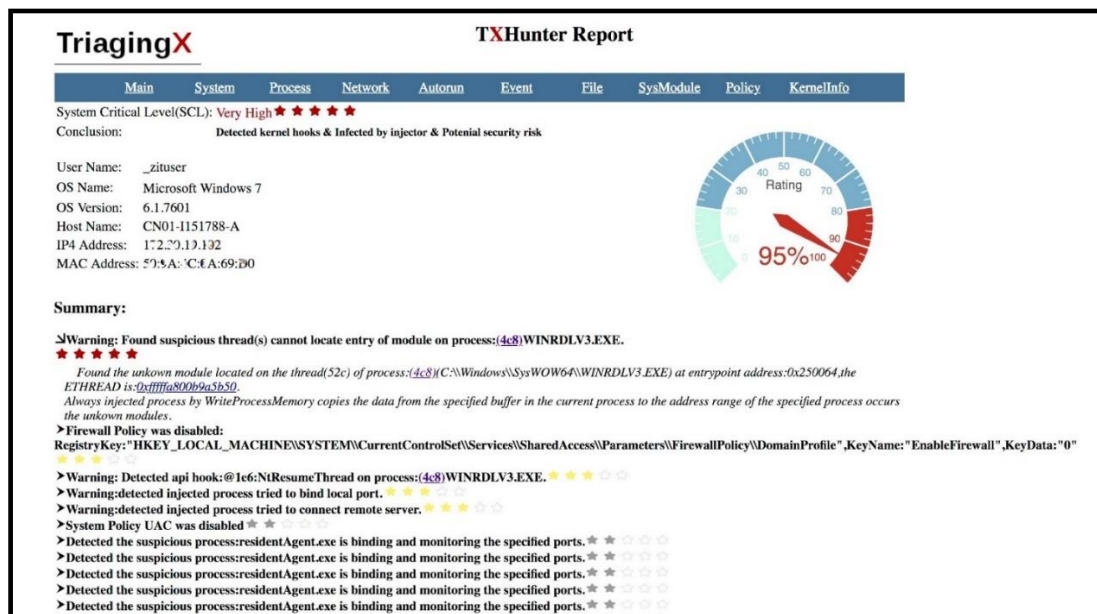
4) Empowering Tier 1 / Tier 2 Security Engineers:

Effective Threat Hunting requires core technical skills, knowledge of the key areas and professional expertise of highly-trained threat hunting specialists coupled with a quality methodology. According to the SANS Threat Hunting Survey, threat hunting tools driven by trained analysts can help increase the scalability and accuracy of Threat Hunting operations.

- Tier 1 Security Operations focus on reviewing alerts, running vulnerability scans and assessments and managing security tools
- Tier 2 Security Operations focus on review tickets, identifying scope of attack and ultimately driving contain & recovery
- Tier 3 Security Operations focus on identifying advanced threats such as APT and Stealth threats, Penetration Testing and optimizing defenses.

One of the goals for TXHunter is to enable engineers with skills in Tiers 1 and 2 to be able to run advanced endpoint hunting and to provide prompt and efficient access to key data for Tier 3 Operations.

Example of Output from TXHunter



- **Conclusion:** Investigation results are written in plain English, accompanied by a Severity gauge for visual representation
- **Summary:** Top items discovered during the investigation that lead to the conclusion are shown in priority order
- **Details:** Detailed information on system, process, network connections, events, policies
- **Report Format:** Report Available in PDF format, Web HTML Format along with exportable log and IOC data
- **Drill Down:** Security Teams can drill down in the web report to uncover key investigation details using the web based report; for example, by clicking on an MD5 hash or filename to immediately access sandbox dynamic analysis results

Comparison to EDR Solutions

One of the most common questions we receive are questions related to how TXHunter compares to Endpoint Threat Detection and Response (EDR) solutions.

FEATURE	TXHUNTER	TRADITIONAL EDR
FIRST RESPONDER READY	Fast, flexible hunting for emergency response in minutes. No permanent agent required. Supports 'Just in Time' investigation mode as well as pre-deployment and offline modes.	Requires pre-deployment of agents across the customer environment and may require additional supportive infrastructure components such as reputation servers, sandboxes. *
UNLIMITED SYSTEM INVESTIGATIONS	Investigations can be run on any connected IP system in online, offline or continuous monitoring modes. Fills gap in coverage as no enterprise covers 100% of their endpoints/servers with EDR system deployments due to performance or interoperability concerns.	Capacity typically tied to number of purchased agents.
FIND HIDDEN THREATS	Threats like to live in your computer's memory where it is expensive to scan, and may persist in alternative locations such as registry hives or Windows Management (WM) Store. Unlike EDR, TXHunter takes the time to do a deep scan on the endpoint to find advanced threats and detonates them in virtual environments in near real time.	Runs a series of rules to alert on known patterns of attack behaviors.
LOW IMPACT ON CLIENTS	Tiny agent that collects data for analysis on the server with very low impact on system performance or operations. Completely safe to use on servers.	Continuously runs active rules on client with risk of false alerts and performance impacts.
DATA PROTECTION	Customer data stays within their environment. Suitable for sensitive or air-gapped network investigations.	Frequently will send data to vendor cloud services for additional analysis.
EASY TO USE	Empowers Tier 1 Security & IT Ops teams to run their own investigations with easy to understand yet comprehensive reporting to meet the needs of even the most senior analyst.	Data collected and displayed on vendor console for analyst to interpret and investigate. Requires continuous monitoring.

*Some EDR solutions support a just in time agent deployment

A Case Study

In 2018, a major US based Private Wealth Management company suspected a cyber breach had occurred in their environment and called in one of the industry's leading digital forensics and incident response companies (DFIR) to investigate. The team deployed an industry endpoint detection and response (EDR) solution across the network to identify and stop the potential breach. However, as they battled to properly identify the scope and severity of the attack, they suspected that they were missing key pockets of the attack and were still suffering data leakage. By leveraging the TXHunter solution, the team was able to quickly deploy the disposable client to those suspect systems and promptly identified the presence of the Win32/Emotet banking Trojan on a critical production windows server, even though the EDR solution had previously been deployed to that server. This helped set the extent and severity of the incident for risk analysis and remediation.

The Win32/Emotet banking Trojan typically spreads via fake invoice emails with Microsoft Word attachments. Executing that document leads to the download of payloads from the attacker's command and control servers. When one machine is infected the malware moves laterally through a network by using the default \$admin SMB file share across Windows machines. Depending on the infected user's permission level, persistence can be gained through registry run keys or a service. It evades detection by using randomly generated file names by victim asset and altering its file composition on disk at regular intervals to evade detection based on file hash. The level of code obfuscation and encryption used to hide the code is quite complex, well-executed and actively maintained by the attackers.


INVESTIGATIVE PROCESS USING MANUAL STEPS

This requires multiple actions and deep knowledge of the Operating System and System Tools.

- 1) The first step for an investigator would be to build a query on the suspect endpoint to retrieve events generated by PowerShell from the Microsoft-Windows-PowerShell events table.
- 2) Once they discover the encoded PowerShell command, they would then look in the logs for the script text code generated after decoding the command.
- 3) As PowerShell downloads the payload, the log socket connections opened by any process are logged. To find this, the investigator would compare the data in the process open socket table and process table to see which processes are making network connections.
- 4) If the investigator wants to see which files have been written on disk during the payload download, they would query the file table for files created in particular folders or files created in the past x minutes.
- 5) The downloaded file from PowerShell is an Emotet dropper that extracts the final payload and executes it (typically squarectx.exe). They now need to query the system running processes to find it.
- 6) If they find the data in the running processes, they know that Emotet malware is running in the target environment and likely reaching out to a command and control server.

- 7) To find that connection they now search the network connections from system processes and look for the remote IP address and remote Port associated with this process. Using this information, they can detect the communications to the Command and Control server.

By contrast TXHunter takes just 3 quick steps to download the investigative agent, run the analysis and view the report.

INVESTIGATIVE PROCESS USING TXHUNTER	
<ol style="list-style-type: none">1) Deploy tiny agent to target system under investigation.2) TXHunter agent collects snapshot data from the target system, runs an analysis on collected data and requests additional suspect objects (files) from the target system.3) A report is generated with clear conclusion, enabling security engineers to drill down into the details. Data is sent back into SOC workflow / SIEM.	 <ul style="list-style-type: none">➤ <i>Detected suspicious process that tried to connect to outside IP Address</i>➤ <i>Detected and analyzed suspicious files which were collected from the system</i>

Conclusion

As surely as death and taxes, advanced threats will continue to evolve and be successful at gaining access into enterprise networks. Companies are increasingly taking a more proactive approach to Threat Hunting and by doing so taking security into their own hands instead of waiting for the breach notice to occur. Threat Hunting takes skill and expertise and can only be partially automated; security teams should take advantage of automation and analysis when available to augment those skills and speed up the process. TXHunter is a powerful tool for use by network defenders for creating and maintaining a capability to detect these threats on the endpoints. Detection using its methods does not rely on typical known-bad IOCs or external notification of a network breach and so can lead to the rapid discovery of a network compromise by detecting an adversary's use of techniques as described in the Mitre ATT&CK™ model.

References

- 1) NIST CyberSecurity Framework - <https://www.nist.gov/cyberframework/>
- 2) "Finding Cyber Threats with ATT&CK™ Based Analytics", by the MTIRE Corporation - <https://attack.mitre.org/>

TriagingX

Smarter Solutions for Cyber First Responders



+1-408-568-7372



support_triagingx@triagingx.com



***6050 Hellyer Avenue, Suite 150-6,
San Jose, CA 95138***



www.triagingx.com

Headquartered in Silicon Valley, TriagingX is led by a team that successfully created the first-generation malware sandbox that is being used by many Fortune 500 companies for daily malware analysis. Our goal is to augment cyber responders with powerful tools and insights that are highly accurate, simple to understand, easy to deploy and deal with the newest threats, unknown to the traditional security scanners.

Copyright © 2019 TriagingX, Inc.