White Paper

Eliminate Blind Spots and Supercharge Your SOC with Symantec Threat Hunter Insights

At a Glance

The three ingredients to fast detection and incident response are:

- Data, both organization-wide and global.
- Artificial Intelligence to process the massive amounts of data.
- Human threat experts and researchers to identify reconnaissance attempts before the breach has manifested.

Threat Hunter is a new feature in SESC that brings together these three key ingredients to empower security teams to quickly respond to incidents and stop breaches.

Our .world-class threat analysts are the same cyber security experts who uncovered Suxtnet and Wastedlocker. They review the machine learning insights from global customer telemetry. They provide vital insights about potential breaches to organizations directly through the SESC product console to alert SOC teams about potential breach attempts on their organization.

Insights may include campaign details, tools, tactics, and procedures used by the attackers along with guidance on how to respond. SOC teams can leverage the human-reviewed incident information to then take suitable action using the rich SESC toolset, including quarantining devices, applying policies to allow or block applications, restricting undesirable behaviors of legitimate applications, and more.

Introduction

To combat today's sophisticated threats, organizations need more than just Endpoint Protection Platforms and Endpoint Detection and Response (EDR) solutions. They need new tools to protect them against their blind spots and for the tactics and techniques that attackers use inside an organization that traditional tools fail to see or stop. One such blind spot is the undiscovered signs of a breach. Even though a SOC team may have many of the tools in place to detect a threat, they often are overwhelmed with massive amounts of data. More important, they simply lack the resources to pursue every alert and to discover massive, global, and ongoing targeted attacks.

Symantec Endpoint Security Complete (SESC) provides the right context with its Threat Hunter feature.

Rethink Breach Detection with Symantec Threat Hunter

Traditional breach detection tools and techniques can easily miss the most dangerous threats to the organization. They typically only capture isolated scans from organization-wide termination points, such as endpoints, email, proxies, and so on. Because this approach doesn't provide global visibility or context into emerging threats, security teams must manually correlate these scans and integrate them with limited threat intelligence sourced from external feeds. Further, because most organizations lack the expertise to design artificial-intelligence algorithms and skilled threat researchers to investigate attack groups, they incur threat visibility gaps, less precise detections, and longer dwell times.

Threat Hunter empowers security teams to quickly respond to endpoint incidents and minimize the impact of attacks. Threat Hunter is a key feature of Symantec Endpoint Security Complete, which includes technologies to provide protection across the entire attack chain, including attack surface reduction, attack prevention, breach prevention, and detection and response. Threat Hunter combines rich telemetry, machine learning, and threat research from world-class threat researchers to provide SOC teams with tailored and prioritized incident notification and recommendations for response.

Threat Hunter differs from traditional managed detection and response in that the Symantec Enterprise Division team doesn't replace the SOC team, but empowers the SOC with intelligence and insights, rather than delivering tactical event monitoring. Symantec Threat Hunters are at the forefront of the industry's cutting-edge security research for years, identifying and tracking some of the most elusive, advanced persistent threat groups that have emerged. With their insights into the tools, tactics, and procedures used by attackers, they can find the smallest of clues and assemble them into a picture that details a current attack unfolding in your organization. They know how to respond, and they can guide you.

Symantec Threat Hunter Stops WastedLocker Ransomware in Its Tracks

Evil Corp is not just a fictional company in a TV show. It's a real-world sophisticated cybercrime gang that has continued undeterred by FBI indictments of its leaders. In June 2020, Evil Corp launched a targeted ransomware attack called WastedLocker against some of the largest U.S. companies. This attack could have easily knocked them all out.

The majority of the attack targets were major corporations, eight of which are Fortune 500 companies. All but one of the targeted organizations are U.S.-owned, with the exception being a U.S.-based subsidiary of an overseas multinational. The goal of the attacks was to cripple the victim's IT infrastructure by encrypting most of their computers and servers in order to demand a multimillion-dollar ransom.

Discovery and Findings

The initial compromise involved the SocGholish framework, which was delivered to the victim in a zipped JavaScript file masquerading as a browser update through compromised legitimate websites. A second JavaScript file profiled the computer using commands such as whoami, net user, and net group. Next, it used PowerShell to download additional discovery-related PowerShell scripts. Once the attackers gained access to the victim's network, they used Cobalt Strike in tandem with a number of living-off-the-land tools to steal credentials, escalate privileges, and move across the network to deploy the WastedLocker ransomware on multiple computers.

The attacks were proactively detected on a number of customer networks by Symantec's targeted attack cloud analytics. The Threat Hunter team reviewed and verified the activity and quickly realized it corresponded closely to publicly documented activity seen in the early stages of WastedLocker attacks.

Threat Hunters Respond

The discovery enabled the Threat Hunter team to identify additional organizations that had been targeted by WastedLocker and identify additional tools, tactics, and procedures used by the attackers. This information enabled Symantec analysts to strengthen Symantec protections against all stages of the attack. Concurrently, the Threat Hunter team delivered early warnings to 68 customers. They explained that attackers had breached their networks and were in the process of laying the groundwork for staging ransomware attacks. By proactively reaching out by phone and email, the team successfully enabled the disruption of attacks. If the attacks been successful, could have led to millions in damages, downtime, and a possible domino effect on supply chains.

"What differentiates Threat Hunter from a managed service is that we are not trying to replace the customer's SOC or manage their entire environment. The whole point is to augment the customer's staff by providing as much information as possible and make it actionable so that the customer can respond quickly. It is really intended as a second set of eyes, finding critical attacks that may have been missed because the SOC staff is overwhelmed by other priorities."

"It's the sense of security that someone is watching over your shoulder in a good way. This safety net is valuable even for mature organizations that have their own threat hunting teams because we approach threat hunting from a different, global perspective. We're not looking at just that one customer's data. We're looking at data as a whole across all our customers. By detecting the same attack in other customer networks, we're able to deliver an early warning to customers that may be affected but have not yet seen the signs. For example, a SOC team might only see the first three steps of attacker activity. However, because of our global view, we know what the next three steps of attacker activity will be. Because Threat Hunter provides that global knowledge, the SOC team is able to search for and proactively prevent those next steps."

Challenges in the Security Operations Center

Early detection of an incident leads to easier remediation; however, security teams face multiple challenges when attempting to detect and fully expose the extent of an advanced attack. These challenges include alert fatigue, the need for more context, staffing issues, and the need for a safety net.

Alert Fatigue from False Positives

Security tools generate a lot of alerts, creating a quantity over quality situation, and security analysts can receive as many as 10,000 alerts per day. To resolve them, SOC analysts need to research each one to determine their validity. Because many are false positives, the work of the SOC analyst becomes even more burdensome. An ever-increasing number of alerts require sorting, tracking, and validation. The process is tiring, and security teams are stressed and overwhelmed. As a result, critical alerts can slip easily through the cracks as it may not be possible to address all alerts in one day.

Research conducted by the Enterprise Strategy Group on the relationship between security maturity and business enablement shows that as of March 2020, close to two-thirds of leading organizations ignore 25% of their security alerts and events because investing in every individual alert is too "impractical".[1] In addition, research conducted by the Ponemon Institute reveals that the mean time to identify a breach was 197 days, with the mean time to contain being 69 days.[2] Clearly, SOC teams need a way to help shorten detection and containment times and resolve unaddressed alerts.

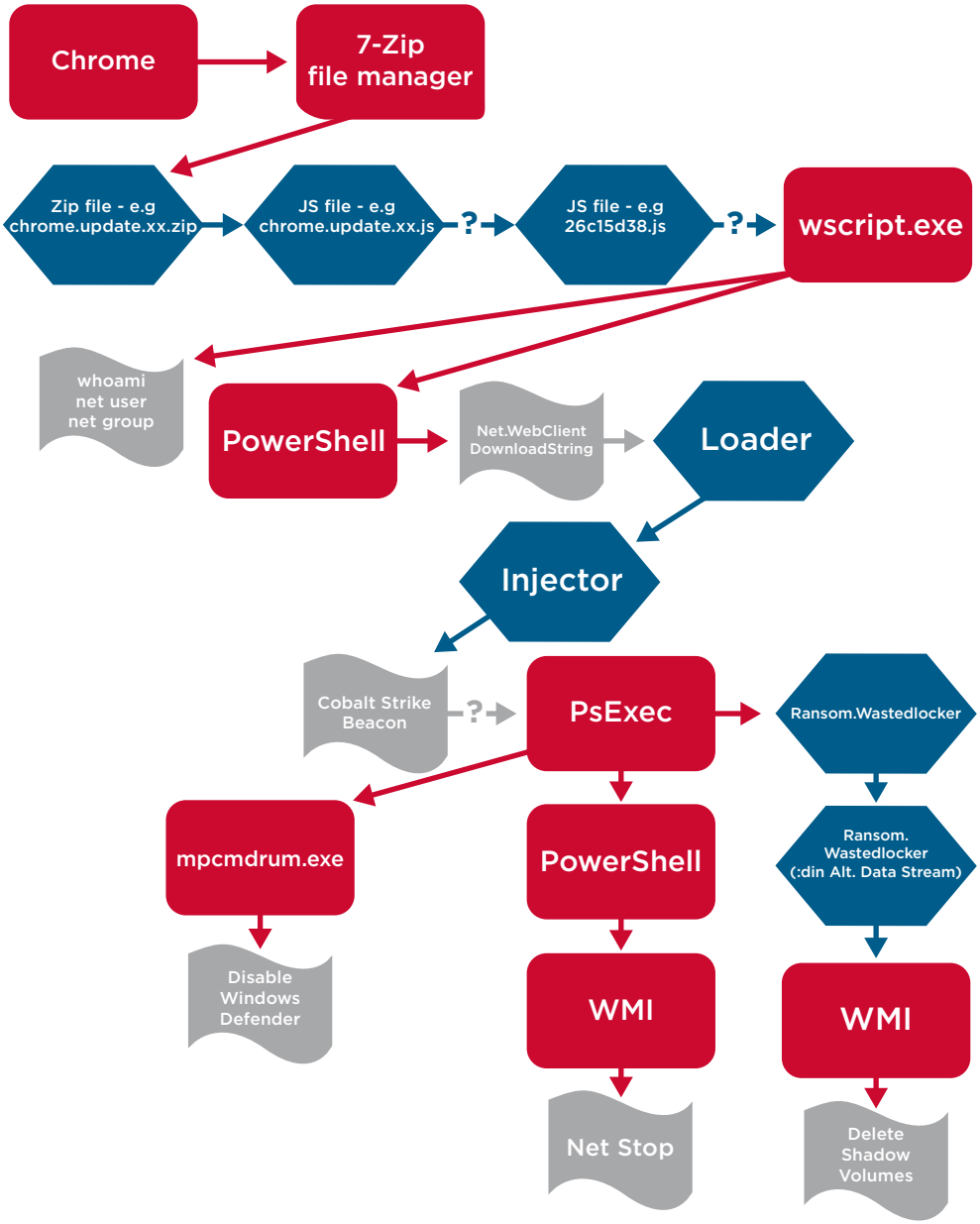
It's been a commonly held industry belief that correlating alerts will resolve the issue of alert overload. In reality, correlation and filtering is not easy either. What's needed is human expertise and algorithms created by experts.

Need for More Context

To resolve alerts, SOC analysts need all details about the attack and the attacker in order to focus on detection and remediation. Unfortunately, unless one has a deep understanding of attack Indicators of Compromise (IOCs) and signature names, it can be difficult to know which indicators might have been missed and to determine which discrete events are linked—and which are not.

Security teams need to know why an alert is serious and they need clues to help them determine how and where in their organizations they are being attacked. They also need to know everything about the attackers and their tactics, techniques, and procedures to best determine how to block the threat actors from accessing their networks and assets.

Figure 1: Threat Hunter can trace the intermediate steps between intrusion and the point of an attack. In the process, Threat Hunter targeted attack analytics and analysts can pick up malicious activity at any point along the way, vastly improving a customer's ability to find and eradicate the threat quickly.



"The big thing that sets Threat Hunter apart from an internal hunting team is access to all of the Symantec telemetry. That includes endpoint as well as email, network, cloud, and other data sources. We can use this information to trace a threat back to a specific vector, verify if an attack is real, and get additional context. For example, we can trace malware back to a malicious file that was delivered in a specific email because we have email data."

Staffing Issues and the Need for a Safety Net

Because of the threat overload and the pace at which analysts work to protect their organizations, the risk of missing an alert due to a staffing issue is real—and there are real business implications. According to an April 2019 research report completed by the Ponemon Institute, the average cost of a data breach is $3.92 million.[3] Internal SOC teams need to know that if something is missed, there is another team of skilled analysts with robust tools to catch what might have been overlooked.

Threat Hunter Analytics

Threat Hunter combines local and global telemetry, machine learning analytics, and manually reviewed and validated analysis from Symantec's expert threat hunters to expose attacks that otherwise would evade detection.

Expansive Dataset of Local and Global Telemetry

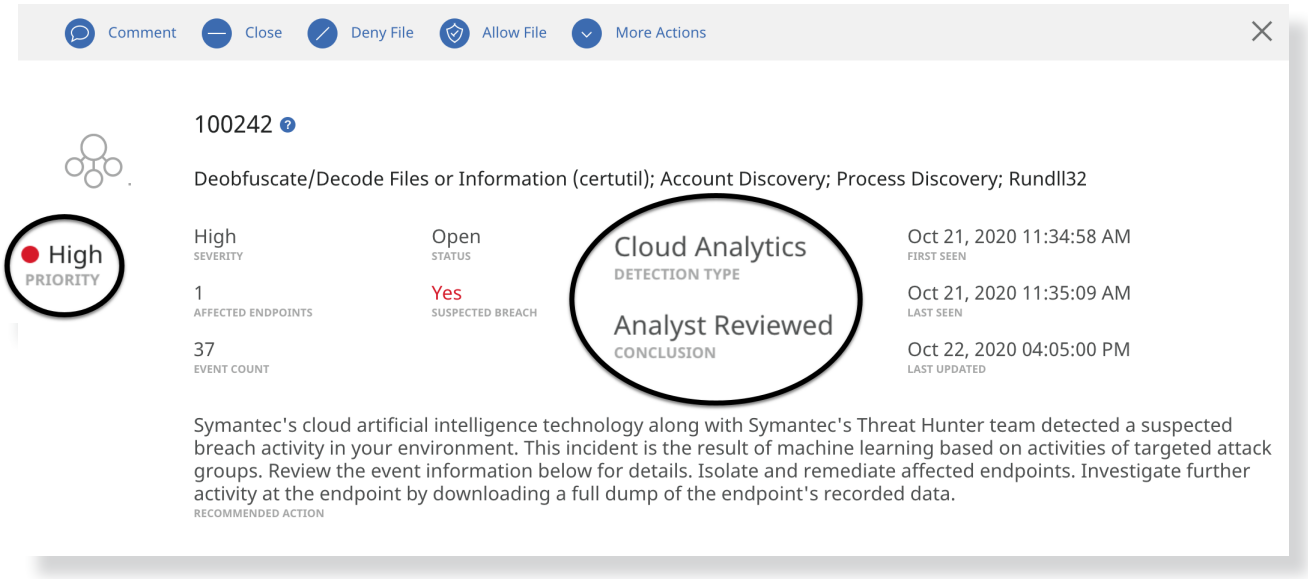
Threat Hunter relies on a huge, global dataset to perform its analytics. Our authoritative data lake collects event data from all products in the Symantec Enterprise Division portfolio, including endpoint, network, email, and cloud apps. Threat Hunter also gathers details about threats other customers may have experienced to expand the global view. The massive dataset allows Threat Hunter to build better analytics and to keep improving upon them as new data is received.

Targeted Attack Analytics

Threat Hunter analytics are based on targeted attack analytics, which includes analytic applications for detecting breach, PowerShell, lateral movement, and command-and-control beaconing activity. Targeted attack analytics uses advanced machine learning and cloud-based artificial intelligence to sift through the data lake to identify incidents and deliver evolving analytics. Data scientists rely on deep expertise to continually develop new, superior artificial intelligence algorithms that run on this data lake. In addition, security analysts evaluate the insights and provide feedback. This human retraining of algorithms further refines the analytics engine to limit false positives and reinforce correct alerts.

When the algorithms detect suspicious activity, the Threat Hunter research team reviews the activity and annotates the alert with detailed information of attackers' tactics, techniques, and procedures to provide context around the attack and enable SOC analysts to quickly identify the threat. See the following figure.

Figure 2: Threat Hunter analysts review and apply their insights to alerts with suspicious activity. Their commentary is placed directly in the EDR console so SOC teams have complete visibility into the IOC, as well as the individuals and machines affected in the organization.



"The context that Threat Hunter provides is important—especially in situations where parts of the network are not visible to Symantec. When we provide context around a Trojan that we detected on a computer, those SOC analysts are able to combine that information with a bigger list of IOCs and apply it to the parts of their network where we lack visibility. That is a huge value-add as compared to an endpoint customer who might not have paid attention to a Trojan detection and is not conversing with Symantec on any level."

Symantec Threat Hunter Team

The Threat Hunter team is uniquely positioned to address blind spots. Symantec analysts provide a well-trained eye on critical incidents and set up notifications within the Symantec Endpoint Security Complete product when an attacker is looming—or strikes. By doing so, Symantec Threat Hunter analysts bring attention to the areas where SOC teams need to direct their focus.

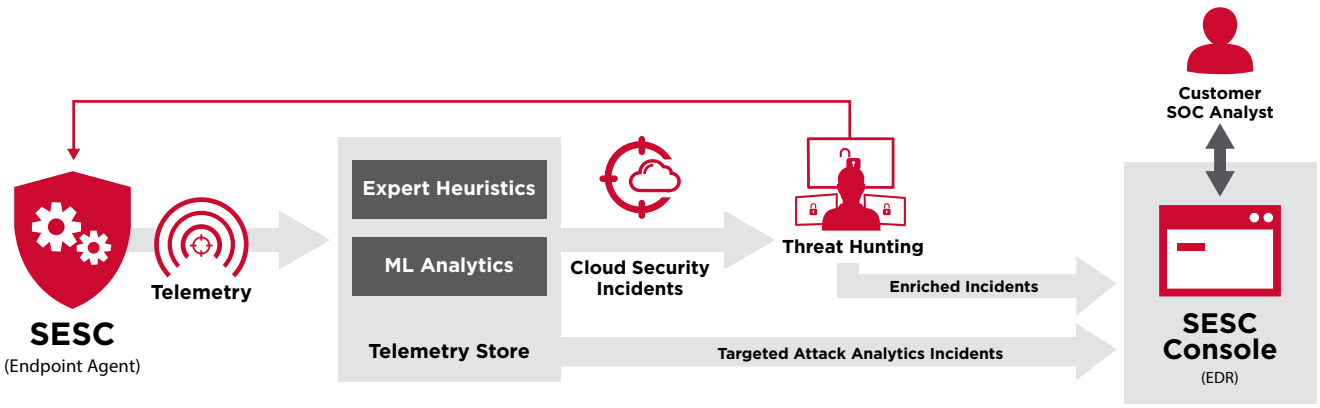
In addition to being at the forefront of the industry's cutting-edge security research for years, Symantec Threat Hunter analysts have decades of experience with the global Symantec data. This experience is further strengthened by their industry expertise and technical skills in building tools to better understand the threat landscape. With their collective talents, they bring a global view to the evolution of threats, tactics, and techniques happening outside the SOC environment.

Collaboration for Fast, Effective Response

The individual inputs from the Threat Hunter team are fortified by the collective might of the Symantec portfolio. When an attack is uncovered, the Threat Hunter analysts collaborate with the Symantec Security Response team to analyze attacks, ensure protections are in place, and pinpoint the nature of the attack. Symantec Security Response will work to improve upon existing protection measures and create any additional controls needed. Those new and updated protections are distributed inside the organization to stop the attack. Other customers benefit as well. They may be affected by the same threat—but have not yet seen the signs. The new protection is published globally to all Symantec customers so the new controls can be implemented throughout the entire Symantec customer community.

Threat investigations enabled by Threat Hunter become part of a powerful detect to prevent process where past detections lead to a stronger prevention policy. By linking back to the alerts triggered by the malicious behavior and adapting their behavior isolation policies, SOC analysts can use every investigation to actually improve their endpoint security posture over time. Our fully integrated prevention and Endpoint Detection and Response solution, uniquely empowers SOC analysts to be more efficient and effective. See the following figure.

Figure 3: Threat Hunter takes telemetry from the SESC agent and feeds it into the machine learning engine where incidents are identified and made available for further analyst analysis and review. Threat Hunter analysts apply their experience, tools and knowledge to flagged incidents and can generate additional insights to help a customer identify and control a possible attack in the organization. As incidents uncovered by Threat Hunter analysts are defined and confirmed, they are fed back into the Threat Hunter machine learning engines so future incidents of a similar nature are immediately found.



Threat Hunter Response Brings a Halt to Cicada

Cicada (also known as APT10) is an APT group whose interest in the Managed Services Provider (MSP) and Managed Security Services Provider (MSSP) market space is publicly well documented. If successful, breaches of MSPs usually result in breaches across multiple Fortune X companies. In April 2020, Symantec analysts observed threat activity involving the Cicada group. The target of the attack was one of the world's largest MSP and MSSP providers. More recently Cicada has been targeting Japanese conglomerates, this activity again being discovered by the Threat Hunter team.

Suspicious PowerShell Activity

Targeted attack analytics triggered on suspicious PowerShell activity within an organization. The PowerShell connected to a remote server to download content and saved additional malicious files on the computer. Each downloaded file was unique, and the PowerShell in each case was partially unique. The attacker used each remote server for one or two targeted computers only, rendering network object IOCs useless from a global protection perspective.

The Threat Hunter team pivoted off the partial common PowerShell to locate more activity across the globe and found a dozen remote servers pushing content onto different targets. Once on the victim's box, the attacker executed a number of discovery-related scripts to find vulnerable machines, map out the network, check privileges, and probe the domain controller. All these tools leveraged native applications on the target computers. The actors spent a considerable effort trying to evade the Symantec security application by clearing system logs related to events and PowerShell.

Sharing Attack Details Enables Isolation

The Symantec Threat Hunter team prevented a massive breach by reaching out and notifying the customer about specific activities occurring in their network. By sharing the attack details, the Threat Hunter team enabled the customer to immediately isolate the affected machines, use any unique IOCs that were specific to the organization to locate computers not running Symantec Endpoint Protection in their network, and investigate the attack activity. By proactively engaging the customer, the team helped discover and stop the attack before other organizations transacting business with the customer were affected.

"With Symantec Threat Hunter analysts, our customers receive the highest level of security research talent in the industry."

"Because of their experience, [Symantec Threat Hunters] bring a global view to the evolution of threats, tactics and techniques happening outside the SOC environment."

Summary

The most dangerous and damaging threat is the one you don't see coming. As targeted attacks increase in sophistication and volume, enterprises need to reduce the overall number of incidents analysts have to investigate and ensure that responders are focused on the highest priority incidents. To accomplish this, security teams need help in detecting true attacks. They need context, including everything that is known about the attack and attacker. Because of the pace at which they work to protect the organization, they need a backup in case something critical is missed.

Symantec Threat Hunter, a key feature of Symantec Endpoint Security Complete, solves these needs. Threat Hunter combines the power of precise detections from time-tested Symantec Targeted Attack Analytics, Symantec global and local telemetry, and attack analysis from world-class threat researchers.

With Threat Hunter, we provide you with a detailed analysis of the attacker, techniques, impacted machines, and remediation guidance. We empower the SOC team to quickly close out endpoint incidents and minimize attack impacts.

References:

1 Enterprise Strategy Group, The Relationship Between Security Maturity and Business Enablement (May 5, 2020).

2 Ponemon Institute, 2018 Cost of a Data Breach Study: Global Overview, (July 2018).

3 Ponemon Institute, Cost of a Data Breach Report 2019 (April 2019)

Symantec
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-Threat-Hunter-WP100 November 17, 2020