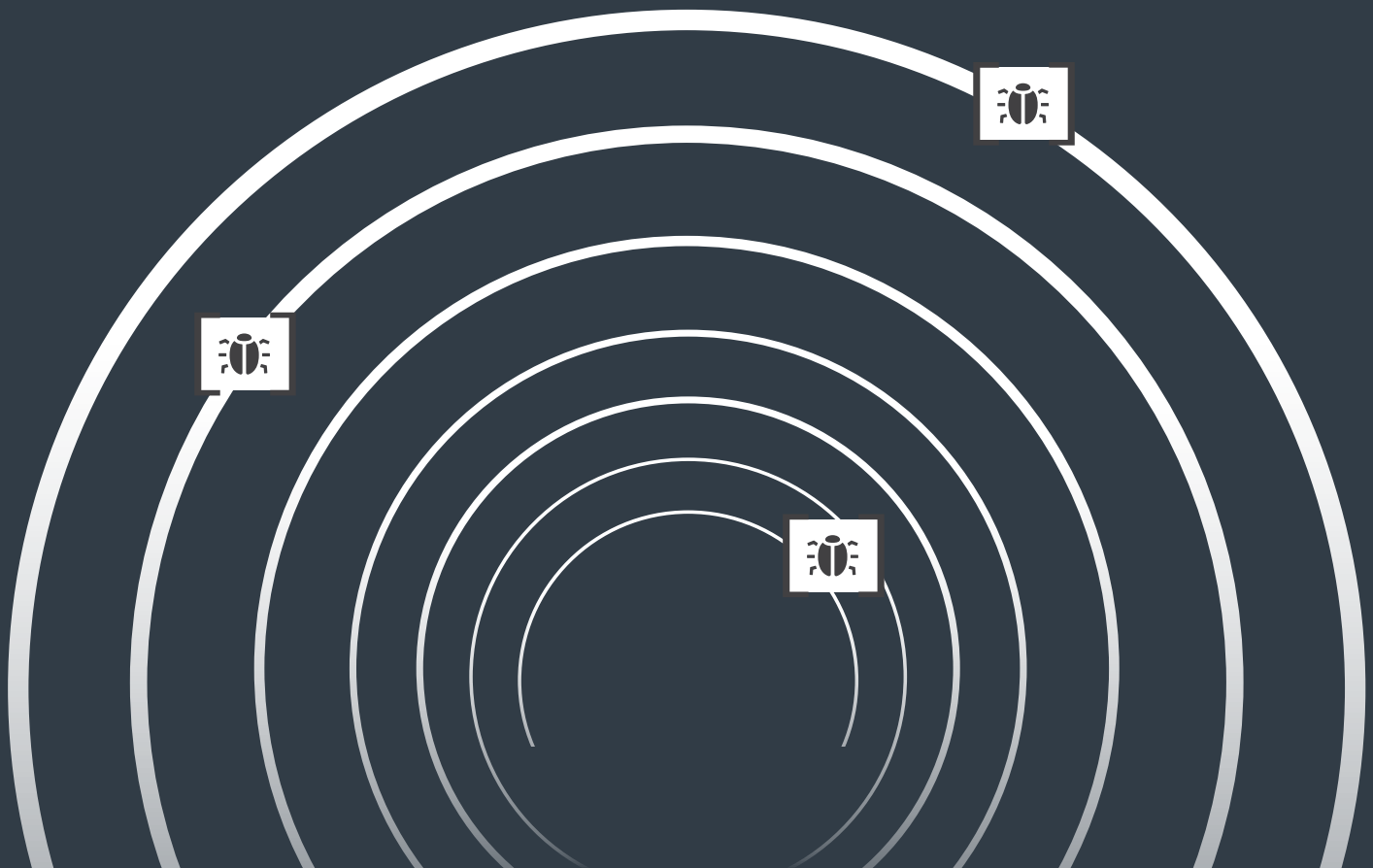
CARBON BLACK

ERADICATE CONCEALED THREATS:

ADVANCED THREAT HUNTING

WITH CARBON BLACK



OVERVIEW

In a SANS survey, **56% of incident responders claim they assume their enterprise is already compromised**[i]. By preparing for the inevitable breach, rather than believing it can be prevented, enterprises can deliver a better security posture and set the foundation to proactively hunt for threats.

With that said, many organizations still focus on—***and prioritize***—the wrong protection techniques across their environment.

Despite the fact that **65% of data breaches happened on company endpoints** (laptops, desktops, servers and POS systems)[ii], many enterprises still focus on securing their network; networks that are increasingly difficult to secure with more employees operating outside of them.

With only five percent of data breaches compromising networks[iii], it is clear attackers are ultimately targeting where the data is: the endpoint. However, even if an enterprise is focusing on its endpoints, it typically prioritizes detection capabilities over data collection. This makes it difficult to expand detection beyond the moment of compromise and accelerate the discovery of advanced threats.

Additionally, most attackers take minutes to compromise an enterprise. When they do, an advanced attacker can escalate their privileges within a given environment to establish persistence. If acquired, the attacker can essentially "live off the land" by using trusted tools to move in and out of an organization as well as exfiltrate data. This whitepaper will cover the capabilities necessary to proactively and efficiently hunt for threats across your enterprise.

65% OF DATA BREACHES

HAPPENED ON COMPANY ENDPOINTS

(laptops, desktops, servers and POS systems)

THREAT HUNTING DEFINED

Threat hunting is a proactive process that looks for abnormal activity. Threat hunters search for anomalies on servers and endpoints to glean evidence of intrusion, such as a legitimate programs performing in unusual ways.

With non-malware attacks on the rise, the threat hunting process is becoming critical for organization's security. According to Verizon's 2016 Data Breach Report, 53% of breaches use no malware[iv]. Traditional antivirus and perimeter-defense solutions cannot address many of these new threats.

Most enterprises recoginize it is no longer a matter of if they will be breached, but rather when. As a result, many businesses are looking for detection and response solutions that can answer the ultimate question: "***Is my organization already compromised?***" To do so, they need tools that not only detect and respond to threats reactively, but can proactively hunt them as well. To hunt for threats, enterprises need tools that can accelerate threat discovery to quickly identify potential compromise.

> ***"Hunting down and understanding the source of threats allows us to protect against future threats that may come from the same sources."***
>
> – Cb Response customer and IT director of a CPA firm

NON-MALWARE ATTACKS ARE ON THE RISE.
53% OF BREACHES USE NO MALWARE.

VERIZON DATA BREACH REPORT, 2016

EXISTING CHALLENGES AND SOLUTIONS

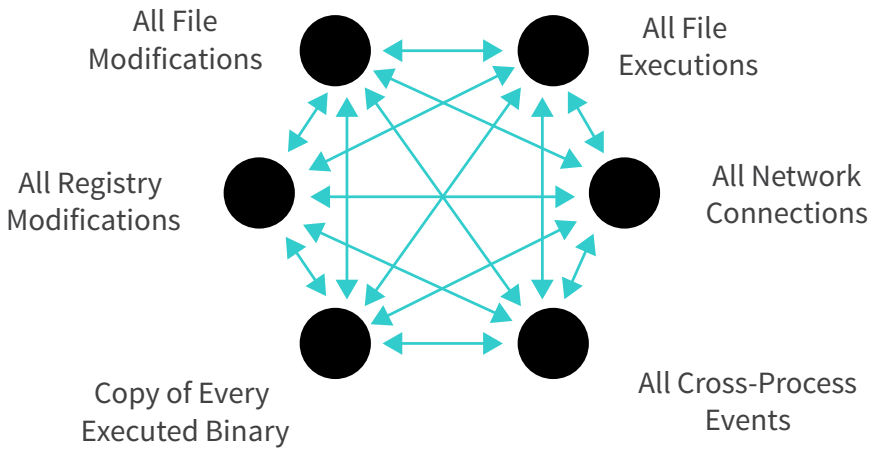
PRIORITIZE ENDPOINT DATA COLLECTION OVER DETECTION

Many enterprises overload on detection capabilities from network security and/or threat intelligence providers. Although this step is important, it shouldn't be the first one you take. A majority of incident responders (52%) say these platforms lack the necessary visibility into endpoint vulnerabilities—citing it as a chief obstacle to efficient IR.[v]

Unfortunately, the problem is getting worse. In a 2016 Ponemon Institute survey, 60% of respondents said that in the last 24 months it has become more difficult to manage endpoint risk.[vi] If you are only deploying scan-based technologies on the endpoint, you are leaving gaps in your data collection coverage as well as losing the context of an attack.

When preparing to hunt for threats, ensuring that your endpoint-security tools can continuously collect the critical data necessary to conduct immediate and conclusive threat discovery is essential. During an investigation, the data collection process can be tedious, time-consuming and expensive. By proactively collecting the critical data, enterprises can instantly leverage a historical record of their environment for threat hunting.

> ***"A majority of incident responders (52 percent) say they lack the necessary visibility into endpoint vulnerabilities."***
>
> – Sans

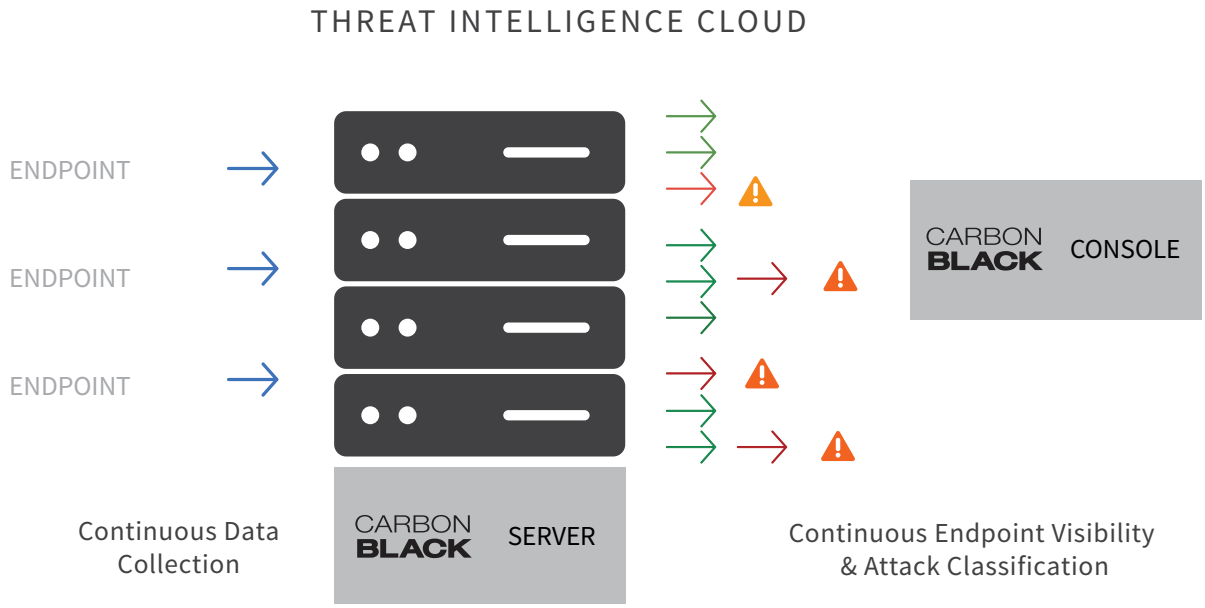


Carbon Black's Cb Response automates the data acquisition process by deploying endpoint sensors across the entire enterprise, and continuously recording all activity. The result is a solution that provides contextual and continuous endpoint visibility by maintaining the recorded relationships of every file execution, file modification, registry modification, network connection, and executed binary in your environment.

In conjunction with the Carbon Black Intelligence Cloud, organizations can efficiently classify threats to accelerate threat discovery.

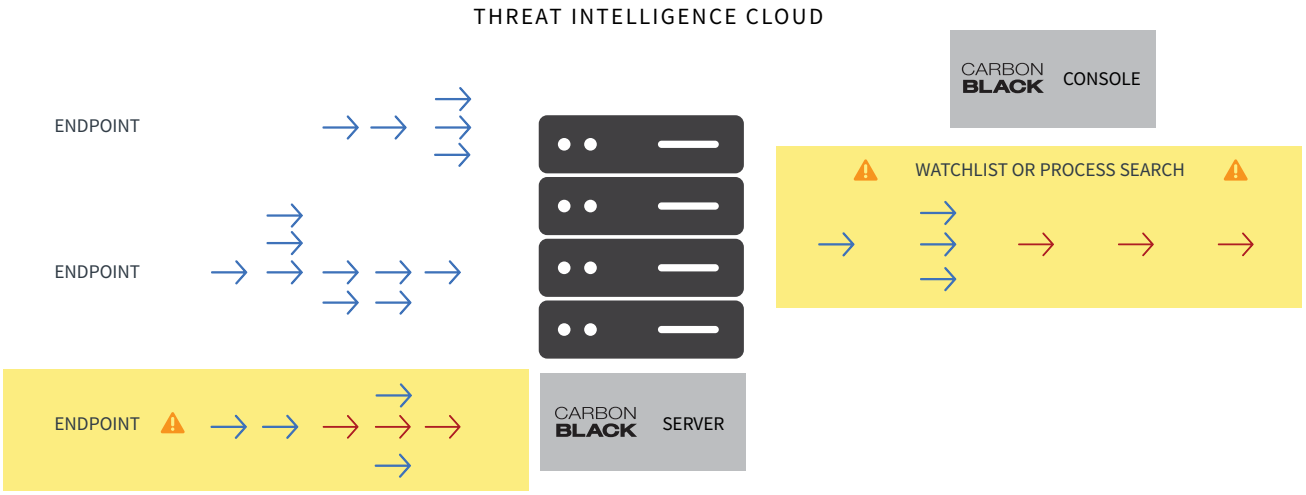
LEVERAGE COMPREHENSIVE THREAT INTELLIGENCE

Sixty-six percent of enterprises stated they suffered successive false alarms from their detection solutions[vii]. These false positives are due to organizations' inability to both collect the right data and classify it instantly. The result is an enterprise that cannot fully scope attacks impacting their business.



With Cb Response, enterprises get a holistic approach to threat hunting by layering a variety of threat intelligence feeds—from within the Carbon Black Intelligence Cloud—over its continuously recorded endpoint visibility. This enables businesses to classify threats based on software reputation, network circumvention attributes, open-source malware tracking, community-based threat intelligence, malicious domains, and custom feeds.

By combining its unique process search, Cb Response can hunt for threats based on its threat intelligence feeds, or by searching all attack processes captured by its continuous endpoint data collection. Also, by utilizing Cb Response's unique watchlist capabilities, any process search done in the Cb Response console can be saved as a watchlist to deliver real-time detection moving forward.



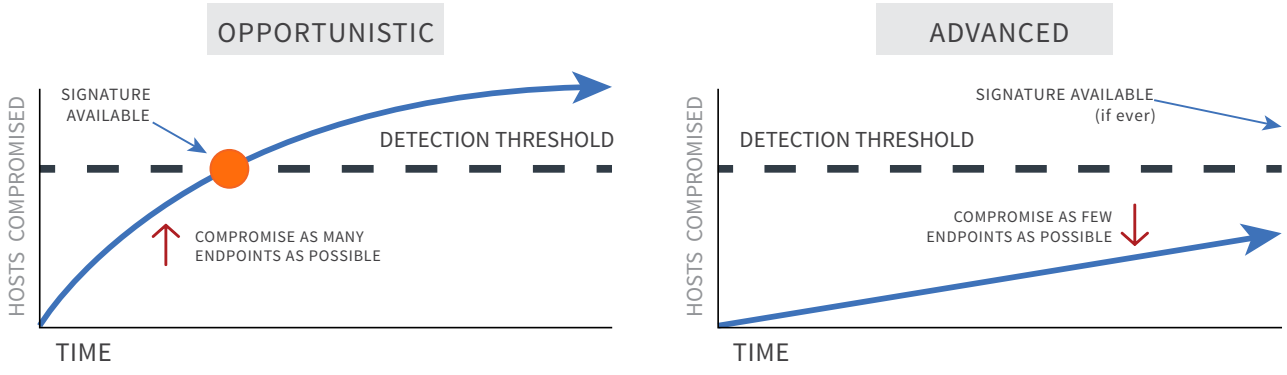
IN 93% OF BREACHES, ATTACKERS TAKE MINUTES OR LESS TO COMPROMISE SYSTEMS. [IX]

— 2016 VERIZON DATA BREACH INVESTIGATIONS REPORT

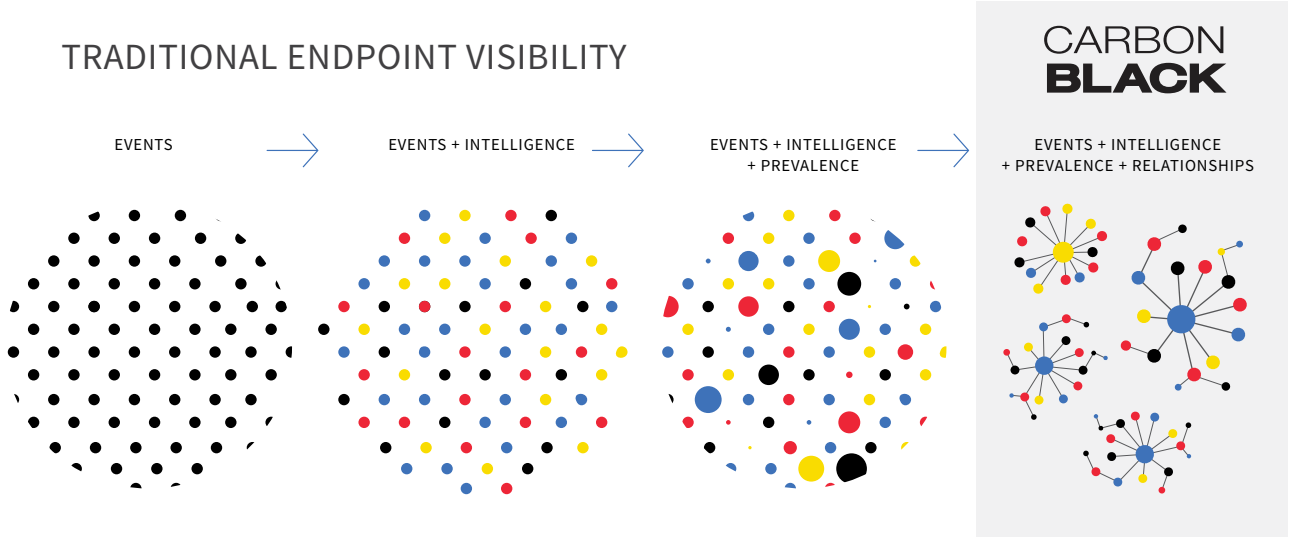
EXPAND DETECTION BEYOND THE MOMENT OF COMPROMISE

Approximately 93% of attacks take just minutes to compromise systems. Contrast that with the fact that it takes an average of 229 days to uncover a malicious attack, and then another 82 to contain it[viii], and it's clear organizations have a threat-discovery problem. This gap in time between initial breach and discovery leaves enterprises susceptible to prolonged data breaches.

Many enterprises have trouble discovering advanced threats because they rely exclusively on the limited detection capabilities of legacy antivirus solutions. The figure below demonstrates how signatures are only effective at discovering opportunistic attackers. Opportunistic attackers find value in scale. Their objective is to compromise as many endpoints as possible since it is likely that a signature will be developed shortly after the attack is first used. The advanced attacker, who only targets a finite number of assets needed to accomplish a specific mission, can remain below the detection threshold and can therefore spend a significant amount of time within a compromised network without registering a signature, if one registers at all.



Additionally, an advanced attacker will move laterally to more critical systems in an attempt to escalate their privileges within an environment. If the attacker succeeds, they can come and go as they please within a given enterprise and evade future detection by "living off the land," leveraging built-in tools to reduce the number of new executables and the amount of change they introduce into the environment. By proactively deploying continuous data collection to track an attacker's every move, and classifying threats by leveraging robust threat intelligence, enterprises can hunt across the attacker's entire kill chain.



The example above also illustrates the shortcomings of endpoint visibility provided by most security solutions. With no reputation or threat intelligence data to draw on, how do enterprises pick the needles out their data-collection haystack? Without understanding the prevalence of endpoint activity, how can organizations effectively prioritize detection events to accelerate the discovery of targeted attacks? And without continuously maintaining the relationships of the data they collect, how do they fully scope their entire enterprise.

THREAT HUNTING WITHIN CB RESPONSE

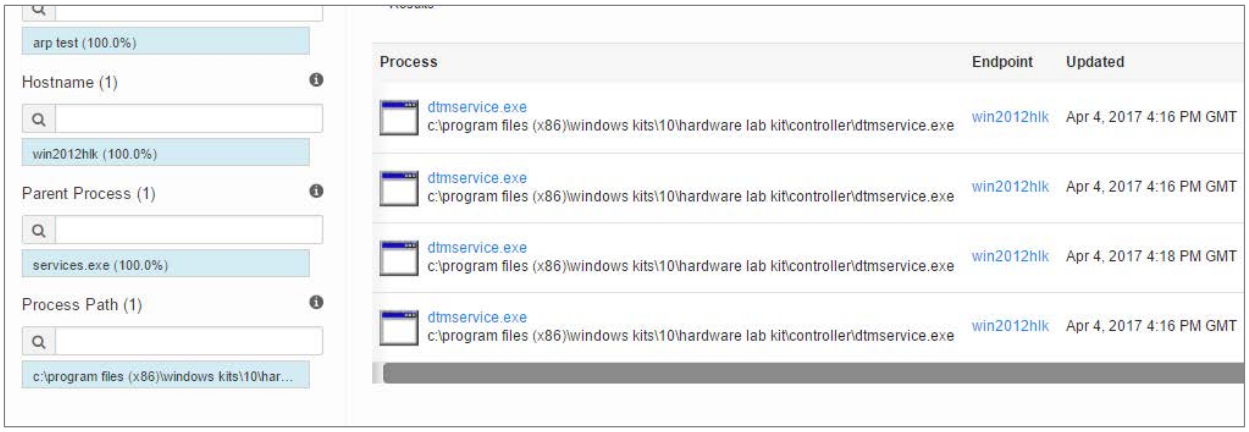
GENERAL THREAT HUNTING

In a 2016 survey, more than 50% of respondents found threat hunting to be the most accurate way to determine the scope of events surrounding a discovered threat[x]. Carbon Black's Cb Response is the most powerful and comprehensive endpoint threat hunting solution. This powerful solution enables the Security and Operations Center (SOC) and Incident Response (IR) teams to quickly and accurately hunt anomalies.

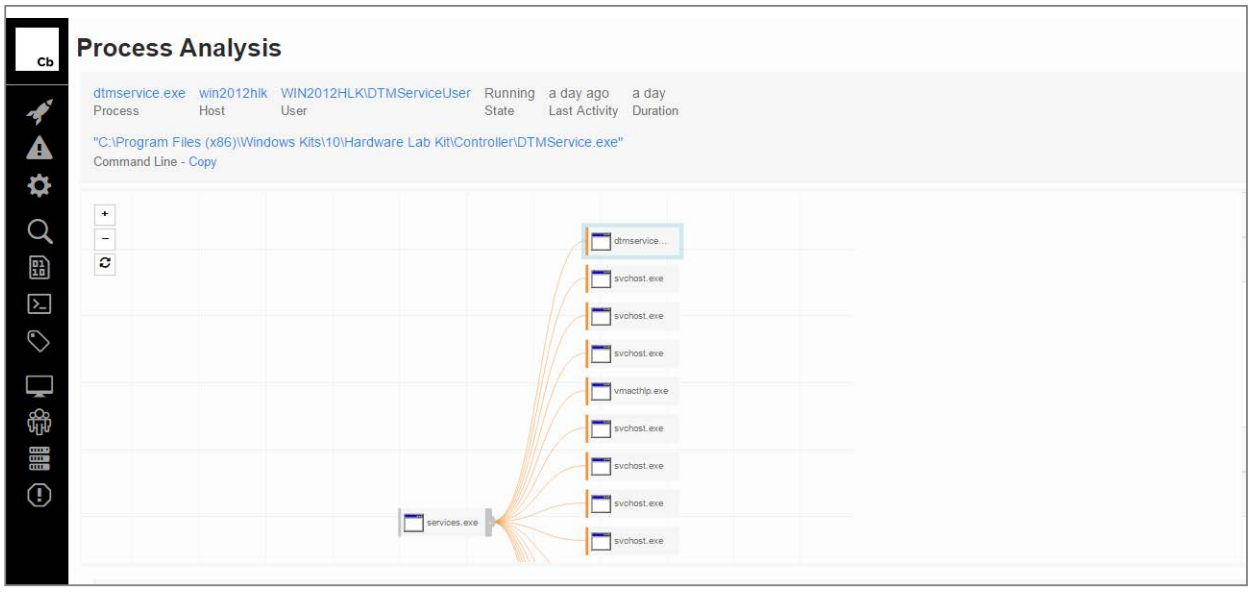
Cb Response continuously records and captures all threat activity, so you can hunt threats in real-time, visualize the complete attack kill chain, and then quickly respond and remediate attacks.

The following graphics illustrate a threat hunting scenario. For example, you read an article, or have previously seen a malicious actor perform an action, such as an unsigned binary with at least one network connection that is running out of a temp folder. To hunt for these characteristics, you query within Cb Response's process search.

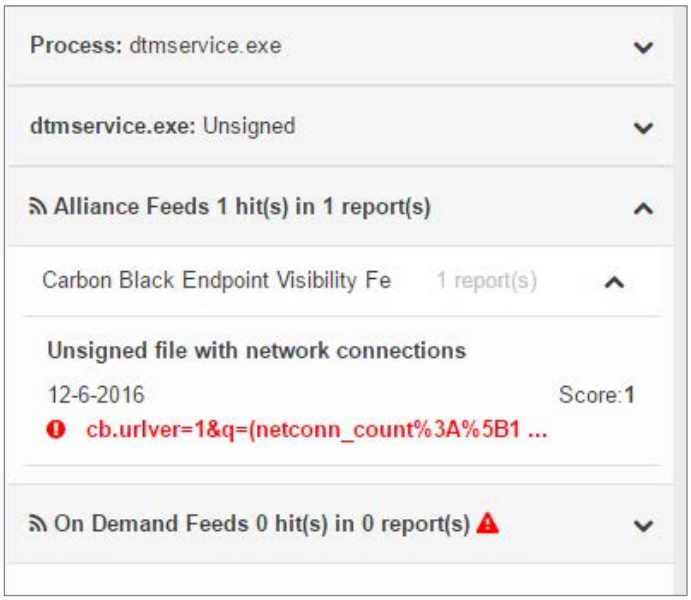
> **POWERSHELL MALWARE COMMONLY ESCAPES OTHER ANTI-MALWARE UTILITIES. BEING ABLE TO SEARCH FOR AND VETT MALICIOUS-LOOKING ACTIVITY IS ONE OF THE BIGGEST STRENGTHS Cb RESPONSE OFFERS**
>
> – CB RESPONSE CUSTOMER AND SR. IT SECURITY ANALYST AT A LARGE COMMERCIAL IMAGING COMPANY



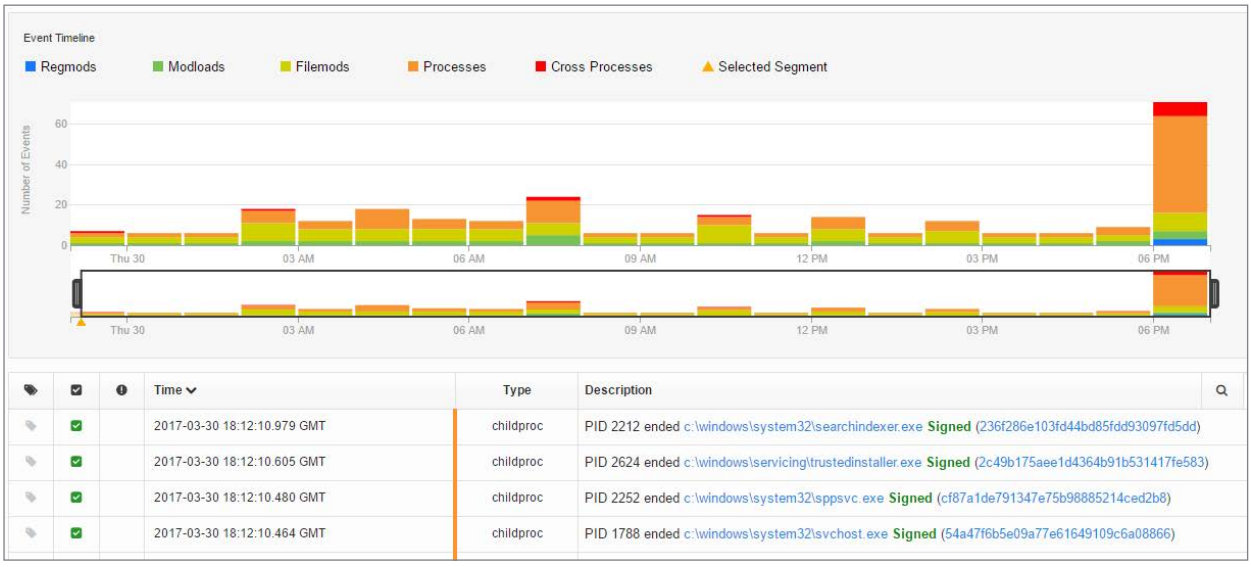
Once searched, you receive 76 hits. One at the bottom that jumps out at you. To dive further, you click on this particular binary to open up Cb Response's process analysis view.



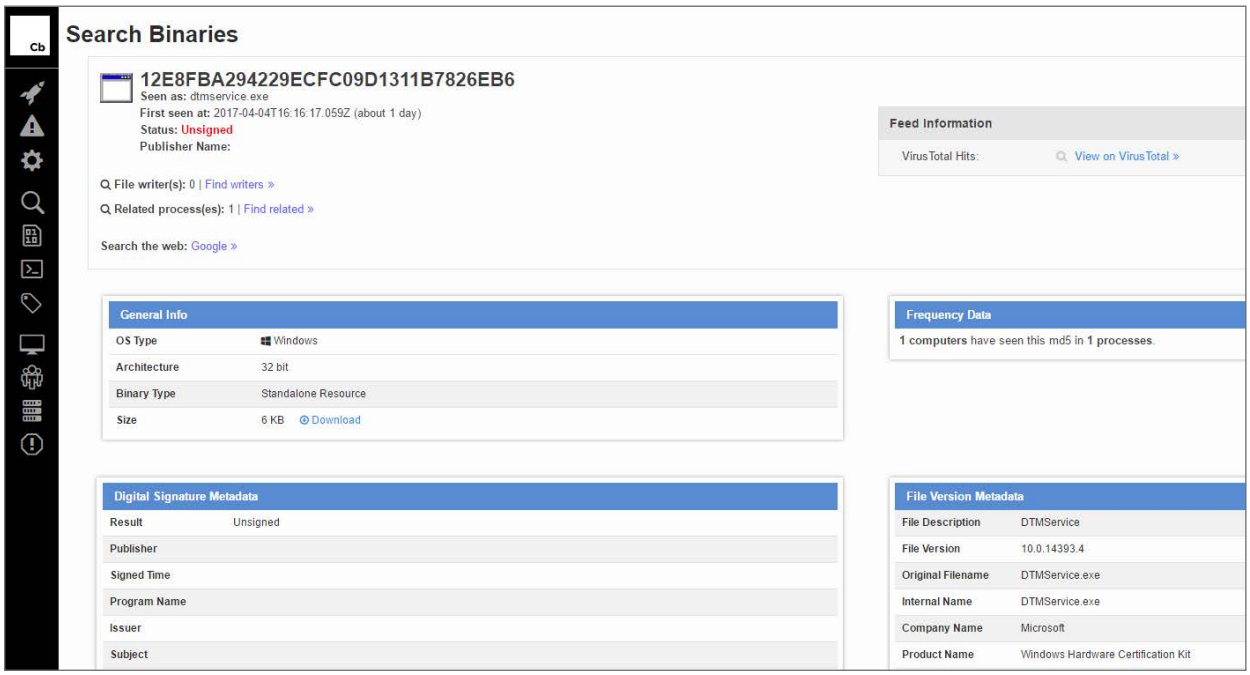
When analyzing this binary on the process analysis page, Cb Response puts a variety of information at your fingertips. You immediately see that the process is unsigned and has spawned a rundll32.exe process. To get further context, you click on the Alliance Feed drop-down to further classify the potential attack.



In the Alliance Feed section, you notice some very troubling scores associated with this given process.



When you scroll down to look at what this given process did to the file system you notice that it wrote multiple binaries.



When diving in deeper and looking at the details of a specific binary, you notice that it has very little metadata, it is unsigned and it has a large threat score. At a glance, you can also see that three hosts (endpoints) have observed this particular binary.

Additionally, you can see that it has made a network connection. Moving forward, you can use this IP and domain as an indicator of compromise for future detection alongside the filename, hash value and other exhibit behaviors.

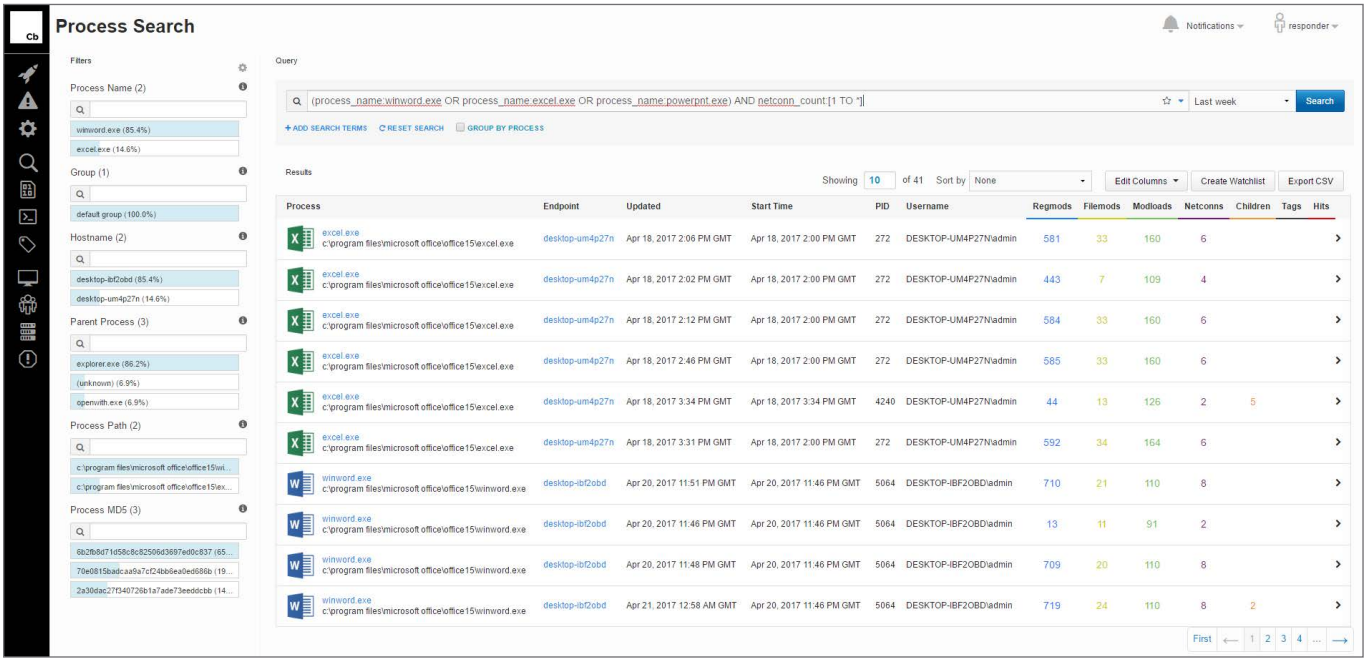
HUNTING A SPECIFIC THREAT

A new CVE comes out relating to a zero-day found in Microsoft Office. You've read a few technical blog posts detailing the Office exploit and you know it uses a new technique that executes embedded powershell, spawning an in-memory Remote Access Tool (RAT). With this information in-hand you use Cb Response to search on three known sets of criteria:

- Targets Word, Excel, Powerpoint
- Spawns a powershell process
- Will create a network connection

Using Cb Response you can instantly identify this criteria:

(process_name:winword.exe OR process_name:excel.exe OR process_name:powerpnt.exe) AND netconn_count:[1 TO *]



Once searched, you will see 41 matching processes. You then take the next step into looking for instances where these processes spawned powershell as a child process:

(process_name:winword.exe OR process_name:excel.exe OR process_name:powerpnt.exe) AND netconn_count:[1 TO *] AND childproc_name:powershell.exe

You then dive further into a specific instance of Excel and immediately see it has spawned a number of powershell processes with obfuscated and encoded command-line parameters. Digging further into the powershell processes you see that it dropped a batch script which executed a number of “living off the land” network and user reconnaissance commands that leveraged net.exe, sc.exe, tasklist.exe, arp.exe, and netstat.exe.

This behavior is clearly malicious, so you isolate the host from your network and begin your remediation process directly from the Cb Response console.

CUSTOMER SPOTLIGHT

Manufacturing Company with 71,000 employees

CHALLENGE

Current AV was not providing adequate protection and the company experienced more than 600 compromises. Malware was generally not detected by their AV software and when it was, it was 24 hours to three days before AV alerted them to the issue. The company needed faster & more reliable network security protection.

SOLUTION

The customer chose Cb Response to close the security gap. With Cb Response they were able to:

- Handle 90% of detection through five Cb Response watchlists
- Detect events in real-time, significantly reducing detection delays
- Accelerate root cause identification by 75%

SUMMARY

Cb Response helped the company improve security with faster & more reliable threat response.

SUMMARY

With the number of advanced attacks increasing every day, and most going undiscovered by traditional detection and response tools, hunting for threats within your environment can be a laborious task. To combat this, enterprises must focus on:

Prioritizing Endpoint Data Collection Over Detection

Businesses need to continuously record all critical data necessary while also maintaining the relationships of within those data sets to fully scope an attack.

Leveraging Comprehensive Threat Intelligence

Alongside continuous data collection, enterprises must possess the capability to layer threat intelligence and reputation over the data they collect to instantly classify and prioritize threats,accelerating threat discovery in the process.

Expanding Detection Beyond the Moment of Compromise

Businesses should deploy solutions that can hunt both past and present threats based off of a continuously recorded history, not just from individual events.

Organizations need to continue to make the endpoint a priority when it comes to information security. When hunting for threats, enterprises need a solution that can “roll back the tape” to understand an attack’s root cause. Carbon Black’s Cb Response delivers the best solution to hunt for threats, accelerate threat discovery, respond in seconds, and proactively prepare businesses for a breach.

i The Case for Visibility: SANS 2nd Annual Survey on the State of Endpoint Risk and Security
ii 2014 Verizon Data Breach Investigations Report
iii 2014 Verizon Data Breach Investigations Report
iv 2016 Verizon Data Breach Investigations Report
v A SANS Survey, Incident Response: How to Fight Back, Alissa Torres, August 2014
vi Ponemon Institute 2016 State of the Endpoint Report
vii A SANS Survey, Incident Response: How to Fight Back, Alissa Torres, August 2014
viii Ponemon Institute 2016 Data Breach Study
ix 2016 Verizon Data Breach Investigations Report
x Exploits at the Endpoint: SANS 2016 Threat Landscape Survey

CARBON BLACK

1100 Winter Street, Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499

www.carbonblack.com

ABOUT CARBON BLACK

Carbon Black is the leading provider of a next-generation endpoint-security platform designed to enable organizations to stop the most attacks, see every threat, close security gaps, and evolve their defenses. The Cb Endpoint Security Platform helps organizations of all sizes replace legacy antivirus technology, lock down systems, and arm incident response teams with advanced tools to proactively hunt down threats. Today, Carbon Black has approximately 2,000 worldwide customers, including 25 of the Fortune 100 and more than 650 employees. Carbon Black was voted Best Endpoint Protection by security professionals in the SANS Institute's Best of 2015 Awards.