



Rapidly Respond to Advanced Attacks in Motion with Carbon Black

Table Of Contents

Introduction	3
Typical Response Scenario	4
Evolving Enemies	5
Understanding the Kill Chain	5
Reconnaissance	6
Weaponization	6
Delivery	6
Exploitation	6
Installation	6
Command-and-Control (C2)	6
Action	6
Incident Response Lifecycle	7
Preparation	7
Detection & Analysis	7
Containment, Eradication & Recovery	8
Post-incident Activity	8
Security Lifecycle with Carbon Black	9
Prevention	10
Detection	10
Response	11
Incident Response with Carbon Black	
Enterprise Response	12
Original Infection Vector	14
Malware Actions	15
Attackers Objective	17
Response Summary	19
Where was Antivirus?	19
Conclusion	20

Introduction

Traditional incident response (IR) processes are being overwhelmed. The increased volume of attacks has caused the number of alerts from detection devices to balloon dramatically. Organizations try to apply traditional incident response processes and procedures for each alert, but discover those procedures are insufficient for continuous application at an enterprise scale.

Because of this, enterprises are now realizing it is no longer a matter of if they will get breached, but rather a matter of when. This increased awareness has driven the Endpoint Threat Detection and Response (ETDR) space as well as the market need for security solutions that can meet these requirements.

Incident response relies heavily on tools—especially during investigations. Ensuring that enterprises have the right tools, which enable them to uncover data about systems, user activity, relationships between files and systems, and more, can put them in a better position to rapidly contain a threat before it is too late.

During the response process, IR teams are likely to encounter major hurdles and roadblocks. One of the biggest hurdles is being able to collect and analyze the right data sets in a timely manner, while also having the right people and experts in place to analyze and understand the data to scope threats. Finding the right tools can be difficult. Hiring the right incident response experts can be even harder as well as expensive.

Without the right tools and staff, the time between an incident occurring and the organization being notified can be months or even years. This is why enterprises need to establish a security lifecycle within their business—one that can reduce the surface area to attack with leading prevention solutions, while also detecting advanced threats in real time, which can fuel rapid response.

This eBook will cover:

- Typical Response Scenario
- Evolving Enemies
- Understanding the Kill Chain
- Incident Response Lifecycle
- Security Lifecycle with Carbon Black
- Incident Response with Carbon Black Enterprise Response

Typical Response Scenario

It is late Friday afternoon, when Jack, an enterprise information security engineer, gets a call from the FBI. Two compromised systems on Jack's network are actively exfiltrating sensitive information to a monitored C2 server. Jack initiates the incident response procedures using the FBI-provided IP address.

Most IT teams are incapable of detecting this on their own, and to compound the problem, how do they scope their entire environment with thousands of endpoints and servers? Organizations need to understand what they are investigating, what the root cause is, and the timeframe for resolution.

To do this, they need the proper tools to perform log analysis, deep-dive forensics, identify command-and-control domains, and audit every endpoint and/or server. In addition, incident responders need to be able to answer four key questions:

- How did this start?
- What did it do?
- How many machines are infected?
- What do I do about it?

Answering these questions may require obtaining information from multiple sources as well as performing several different tasks—all of which take time. Threat intelligence also is critical for effective incident response. This means building profiles of threat actors based on behaviors and threat indicators to create threat profiles of who is targeting the enterprise, where the organization is at risk, and why it is a target for attackers.

To do this, businesses need incident response tools that meet essential endpoint detection and response criteria and give them visibility into each system as well as a real-time recorded history that continuously monitors—like a surveillance camera or DVR—to provide play-by-play of the activity across their entire organization. Enterprises cannot rely on point-in-time scanning or polling technologies that leave gaps in visibility across their environment and can take days, weeks or longer to identify and scope an attack.

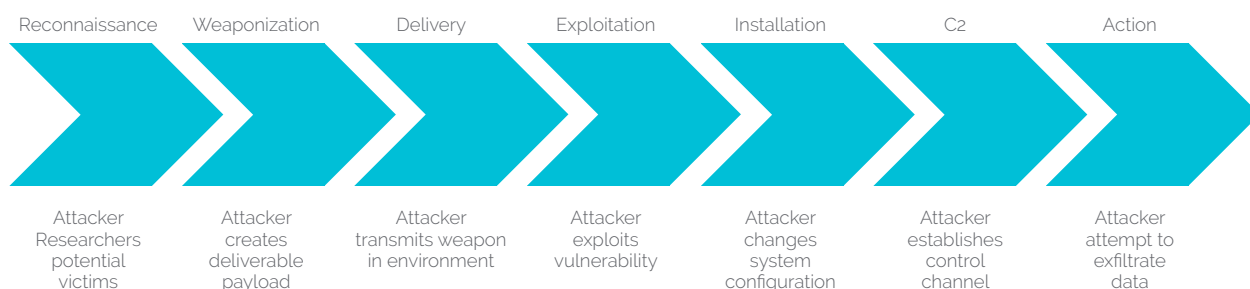
Evolving Enemies

Attacks have evolved over the past decade, but not all security solutions have evolved with them. In 2005, attacks were more about disruption than stealing data. By 2009, attacks developed into sophisticated cyber crime, spyware and bots. Today, organizations have to thwart not just common malware but also targeted attacks, zero-day exploits, dynamic Trojans, stealth bots, and advanced persistent threats (APTs). These can come from a variety of actors, including hacktivists, cyber criminals, and cyber spies.

These newer attacks still leverage viruses, worms and malware, but the threat landscape is not as straightforward as it was 10 years ago. Enterprises no longer experience an infection, reimage the infected machines, and go on with their day—the process now requires an intensive investigation. Organizations are investigating what intellectual property was stolen, assessing damage to their brand, and calculating the cost of remediation. Attacks no longer ruin security professionals' day—they can destroy the organization. Resolving incidents with minimal damage requires a new kind of security solution.

Understanding the Kill Chain

The kill chain breaks down the stages of an attacker's process. It helps security professionals develop and deploy security controls and is essential to understanding the incident response lifecycle. The goal of the kill chain, for security professionals, is to disrupt or stop any link within the chain to thwart the attack.



Reconnaissance

The attacker researches the potential victim by identifying and selecting specific targets. The research uses public databases or scans of an organization's public Internet perimeter infrastructure. It is difficult to distinguish this activity from the typical Internet chatter. After selecting a target they can move into the next stage of the attack.

Weaponization

The attacker creates a deliverable payload to infiltrate an enterprise. Also, attackers do not like to use zero-day vulnerabilities to infiltrate organizations and will commonly use more known attack techniques in their place. This is because the value of a zero-day exploit is high. For an attacker, if they can accomplish their objective without sacrificing a valuable zero-day exploit, they will.

Delivery

After carefully selecting a target weapon, the attacker transmits it to the targeted environment. This can happen through spear-phishing, infected USB drives, storing an infected file on a known website, SQL-injection attack, sharing through a cloud-based file sharing mechanism among other techniques.

Exploitation

The attacker exploits a vulnerability or flaw in the organization's infrastructure or tricks an end user. At this point the attacker attempts to gain control of the enterprise. This could be through manipulating administrative privileges, configuring system settings or installing software.

Installation

The attacker installs backdoors or changes system configurations. This is where the attacker attempts to gain a foothold on the system. The goal is often to acquire long-term access to the system for monitoring purposes. To help with access, attackers install rootkits to maintain persistence.

Command-and-Control (C2)

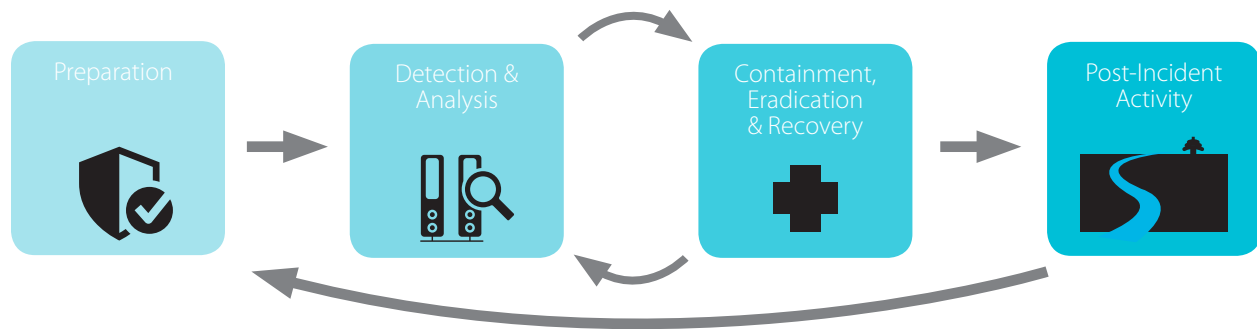
The attacker attempts to establish an outbound connection to a command-and-control server. This provides a way for the attacker to exfiltrate data stolen on the endpoint or server out of the company. Attackers usually establish an HTTPS connection to appear as a trusted connection in order to bypass intrusion detection systems.

Action

At this point the attacker has gained full control of the system and attempts to exfiltrate data. This is usually intellectual property, financial records, customer data and much more depending on the attacker's motives. It is in this final stage that the enterprise is fully breached and loses data.

Incident Response Lifecycle

Developed initially by the National Institute of Standards and Technology (NIST), the Incident Response Lifecycle is a four-step workflow any response team will have to go through to effectively respond to an incident.



Preparation

This is the time to prepare the battlefield to be able to detect and respond to incidents rapidly by formulating an IR plan and identifying the necessary security tools. It is critical for enterprises to have the proper endpoint threat detection and response tools in place before an attack happens. Enterprises should focus on tools that enable them to first reduce the attack surface in their environment while also detecting attacks in motion without the use of signatures. Alongside this, organizations should deploy security tools that deliver a full-recorded history of their entire environment from within a centralized database as well. This way, when an attack is detected, security professionals can reference their recorded history to understand the full scope of the threat and take proper action earlier in the kill chain and before data exfiltration.

Detection & Analysis

NIST calls for the ability to be able to detect from multiple attack vectors, quickly detect signs of an incident, understand sources of precursors and indicators, incident prioritization, incident notification, and be able to conduct incident analysis.

To accomplish this, enterprises should have security solutions already established within their organization that can both detect threats based off of threat intelligence feeds regarding known malware and, more importantly, also have the ability to detect advanced threats without the use of signatures. Organizations also need security solutions that can collect up-to-the second data on file modifications, system configuration changes, process behaviors and more to define the entire anatomy of the attack.

Containment, Eradication & Recovery

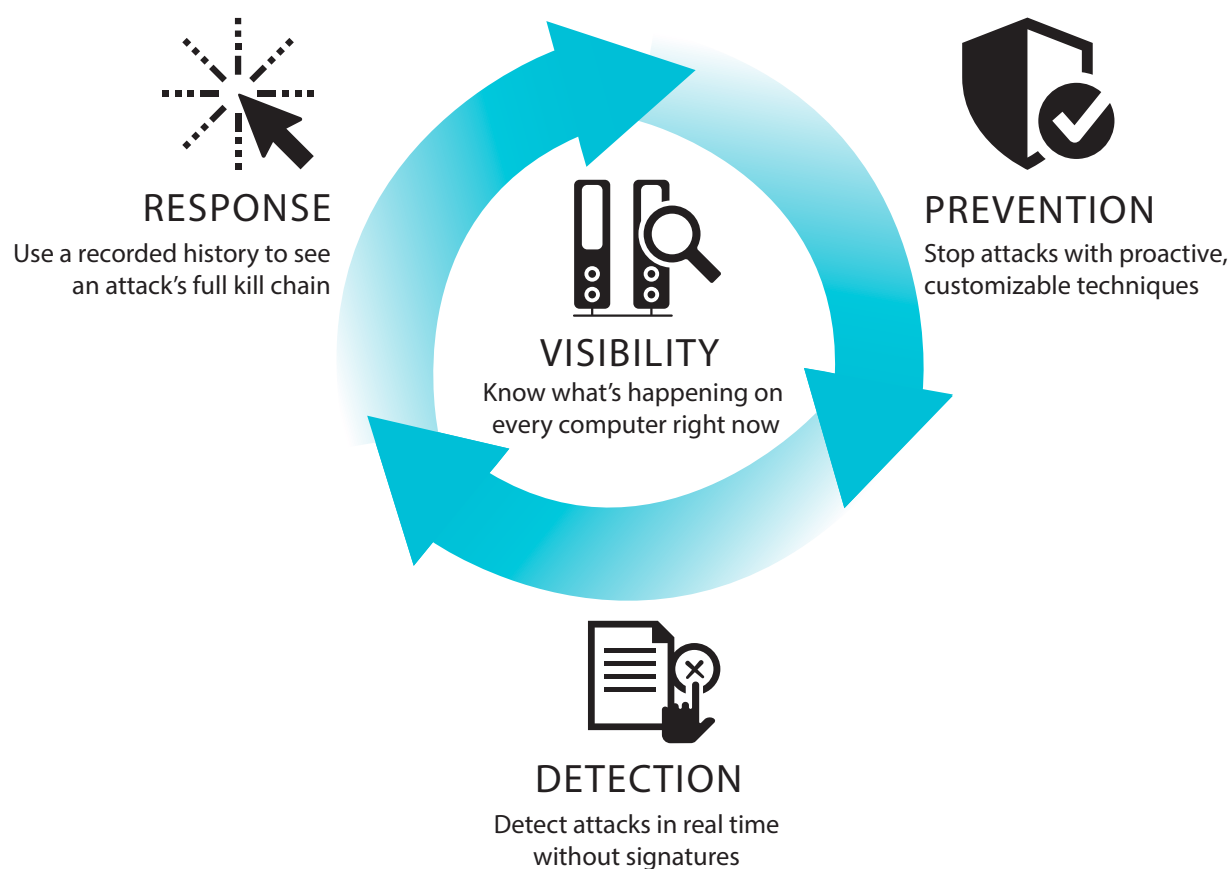
After an incident is detected, it is essential to contain, eradicate and recover from it. This starts by having a security solution that can fully scope the breadth of the attack. To do this properly, organizations need a full recorded history of their environment to not only understand where the threat currently is within the enterprise, but also where it was. Once fully scoped, businesses need to be able to prevent the execution of the malware based off of the initial response to block the attack and prevent the further spread of the attack. After all of the attacking hosts are identified and isolated, enterprises need to be able to eradicate and recover quickly—before data exfiltration occurs.

Post-incident Activity

After responding to an incident, it is important for organizations to use their response activities to learn and improve. This means understanding how to evolve the security posture of the enterprise moving forward to prevent the same types of attacks from repeating themselves. It is important to remember that IT security is a constant cycle that never stops. Organizations that understand this and deploy security solutions to aid in this continuous cycle and process will be better prepared moving forward.

Security Lifecycle with Carbon Black

Traditional incident response is tedious, time-consuming and imperfect. To put themselves in the best possible security posture, enterprises need to start thinking about security as a lifecycle, and also understand which security solutions can meet or exceed these needs. For Carbon Black, the security lifecycle is built on three pillars: prevention, detection and response—with real-time visibility at the core of each. These pillars are not standalone entities and should be integrated fully for maximum effectiveness.



Prevention

Advanced threats use a variety of attack vectors. These can range from common or known vectors to zero-day exploits.

As traditional security solutions are being circumvented by advanced threats and zero-day attacks, the need for a powerful application control and whitelisting solutions becomes critical. For security professionals, there is a common misconception that application whitelisting is difficult to deploy due to cultural and organizational barriers. To avoid this, Carbon Black Enterprise Protection, from within the Carbon Black Security Platform, delivers multiple prevention options that enable organizations to dial-up and dial-down protection strategies to match line of business, user, and system policies and balance organizational culture and risk posture.

As an example, it is recommended that servers, fixed-function devices such as POS systems, and high-profile users such as the executive team be locked down in higher enforcement levels. This means only trusted software delivery systems or trusted publishers are allowed to execute on those endpoints or servers. However, enterprises can dial down prevention for different user groups, enabling Cb Enterprise Protection to prompt users of untrusted software before installation (medium enforcement) or simply enable security teams to view a catalog of what's running on the endpoint without user prompts (low enforcement).

However, because of today's rapidly advancing threat landscape organizations must assume that at one point or another they will experience a breach. This is why prevention is most effective when paired with real-time detection and response capabilities.

Detection

The most critical component of a detection solution is the ability to discover the sophisticated and hidden threats. Many solutions rely on knowing what's bad ahead of time, or use algorithms based on 'known bad' indicators of compromise. No single entity has a lock on the world's threat intelligence and once a file is known to be bad, it may already be too late. In many cases, the alerts are just symptoms of compromise, with no context to trace the detected threat back to the root cause of compromise.

Carbon Black Security Platform provides the most complete and adaptive detection engine. Leveraging the combination of continuous endpoint recording and centralized storage, a master system of record is created that is continuously enriched with multiple layers of threat intelligence - Carbon Black Threat Intel, third party information and customer-defined detection sources and rules. The centralized data and open API's make it easier for defenders to correlate processes and behavioral patterns across their entire enterprise and enrich the view of an attack with information from other security tools. A complete, contextual picture is presented to the security team, so whenever alerts are generated, defenders know how the threat landed on their corporate infrastructure and how the attack has spread, instantly.

The importance of having a reliable detection engine within an enterprise environment cannot be overstated. The ability to detect earlier in the kill chain means enterprises can respond earlier—before damage or data exfiltration.

Response

Rapid incident response should rely on an up-to-the-second recorded history of an enterprise's entire environment. This ensures the incident responder has all of the necessary data instantly at their fingertips. Post-event collection and antiquated forensic tools offer minimal visibility and don't provide clarity into lateral movement or the root cause of an advanced attack.

Only Carbon Black can dramatically change the economics of incident response, reducing the cost and effort by delivering a full recorded history available from a centralized location. By revealing a complete kill chain analysis, incident responders can drill down into an attack instantly to understand root cause and scope the reach of the attack immediately. If a file or process is determined to be malicious, enterprises can engage in live threat containment, banning and remediation activities to quickly stop the bleeding. Finally, detection and prevention policies can be instantly updated to disrupt any similar attacks from successfully repeating in the future.

Incident Response with Carbon Black Enterprise Response

This example will demonstrate how Carbon Black Enterprise Response can be used to detect and respond to an advanced attack. A user received a tip that a notepad.exe process with network connections was possibly malicious, since Metasploit uses notepad.exe as a default target for process injection. This organization was a medium multinational enterprise with approximately 1,000 hosts. Out of the 37 million processes recorded, the user found 10 instances of notepad.exe with at least one network connection. Nine were legitimate connections to a networked printer, but one was not.









+ Add Criteria ▾

Process name: notepad.exe ✖ ▾

Count of network connections is gt 1 ✖ ▾

Showing results for: `process_name:notepad.exe, netconn_count:[1 TO *]`

The organization's Carbon Black Enterprise Response server had recorded execution of 37 million processes over the last 83 days. In that timeframe, there were 10 instances of notepad.exe with more than one Internet connection:

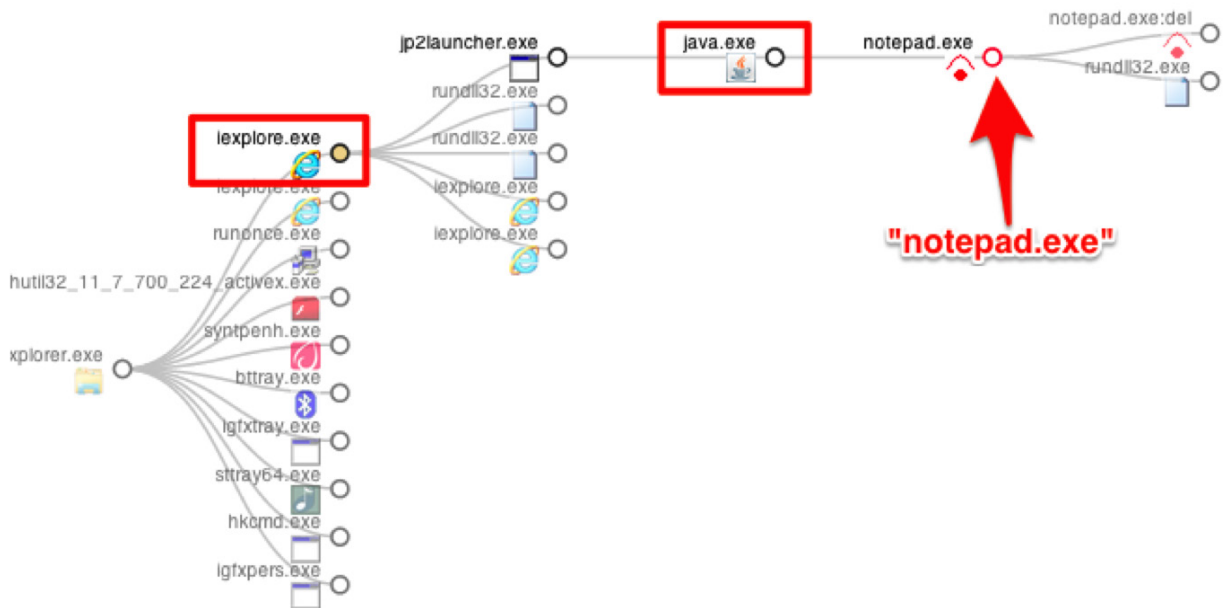
Showing 1 - 10 of 10 matching processes						Sort by Process start time ▾	
	notepad.exe	about 1 days ago on 	regmods 12	filemods 1	modloads 110	netconns 1	  >
c:\windows\system32\notepad.exe							
	notepad.exe	about 6 days ago on 	regmods 6	filemods 1	modloads 105	netconns 1	  >
c:\windows\system32\notepad.exe							

Nine of those were legitimate, but one stood out:

Showing 1 - 10 of 10 matching processes						Sort by Process start time ▾	
	notepad.exe	about 2 days ago on 	regmods 12	filemods 1	modloads 110	netconns 1	  >
c:\windows\system32\notepad.exe							
	notepad.exe	about 7 days ago on 	regmods 6	filemods 1	modloads 105	netconns 1	  >
c:\windows\system32\notepad.exe							
	notepad.exe	about 13 days ago on 	regmods 10	filemods 9	modloads 63	netconns 2	  >
c:\users\...appdata\local\temp\notepad.exe							

This process calls itself notepad.exe so a quick review of the process list in Task Manager won't show anything unusual, but the icon is unusual and the full path is outside of the user's %TEMP% folder. After the initial assessment, this process, which calls itself notepad.exe, is clearly worth investigating.

The process tree makes the process look even more suspicious. In fact, it nearly confirms the process is malware:



The notepad.exe process instance is a child process of java.exe, which itself is a child process of iexplorer.exe, via the intermediary jp2launcher.exe. This is the time when the Tier 1 helpdesk or monitoring staff can call this an incident and pass to Tier 2 IR staff for review and action.

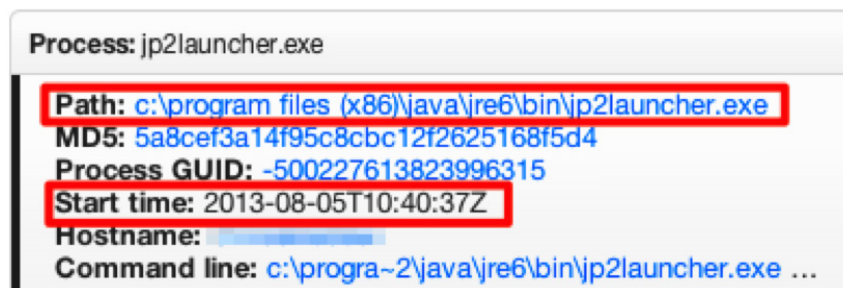
A Tier 2 responder wants to answer three critical questions:

- What was the original infection vector?
- How do I remove the malware? Where is the "real" malware binary? How does the malware gain execution at reboot?
- What is the attacker's objective? Is the malware targeted or opportunistic?

Responders also want to know unique techniques they can use to recognize this malware in the future.

Original Infection Vector

jp2launcher.exe was launched at 2013-08-05 10:40:37 GMT:



The user launched java.exe with md5 d2ae56ceafd824ca022164a79fcb2f5c, which is Java version 6.0.31, released on 14 Feb 2012. There are more than a hundred critical security fixes since then.

Immediately preceding the launch of the JRE, Internet Explorer made a network connection to an ad network:

Mon, 05 Aug 2013 10:40:31 GMT	netconn	Connection to 54.1[redacted] on tcp/80 ([redacted].us-east-1.elb.amazonaws.com)
----------------------------------	---------	---

Walking back to the first top-level network connection in Internet Explorer, the responder should discover a link to the user's local news station. This occurred shortly after launching the browser:

Mon, 05 Aug 2013 10:40:05 GMT	netconn	Connection to 174.3[redacted] on tcp/80 ([redacted].com.cdngc.net)
----------------------------------	---------	--

This implies the following chain of events:

- 10:40:01 GMT – user opens IE
- 10:40:05 GMT – user surfs to his local news station's website
- 10:40:31 GMT – an malicious ad is loaded from a third-party provider
- 10:40:31 GMT – the malicious ad exploits the user's unpatched Java

Malware actions

Shortly after startup, java.exe connected to 72.51.47.69, created a file named notepad.exe in the user's temporary directory, then launched it as a child process:

Mon, 05 Aug 2013 10:40:40 GMT	netconn	Connection to 72.51.47.69 on tcp/80
Mon, 05 Aug 2013 10:40:46 GMT	filemod	Created c:\users\...\appdata\local\temp\notepad.exe
Mon, 05 Aug 2013 10:40:46 GMT	filemod	First wrote to c:\users\...\appdata\local\temp\notepad.exe
Mon, 05 Aug 2013 10:40:47 GMT	modload	Loaded c:\users\...\appdata\local\temp\notepad.exe (47c42a207aa401cbb47cb4050f957084)

The malicious notepad.exe then created another binary, wow.dll, in the user's temporary directory. It also created wow.ini alongside the binary:

Mon, 05 Aug 2013 10:42:15 GMT	filemod	Created c:\users\...\appdata\local\temp\snaipmu\sxbncta\wow.dll
Mon, 05 Aug 2013 10:42:15 GMT	filemod	First wrote to c:\users\...\appdata\local\temp\snaipmu\sxbncta\wow.dll
Mon, 05 Aug 2013 10:42:15 GMT	filemod	Last wrote to c:\users\...\appdata\local\temp\snaipmu\sxbncta\wow.dll (d7042fdeb6beb23bdddef9dc74674e5)
Mon, 05 Aug 2013 10:42:15 GMT	filemod	Created c:\users\...\appdata\local\temp\snaipmu\sxbncta\wow.ini
Mon, 05 Aug 2013 10:42:15 GMT	filemod	First wrote to c:\users\...\appdata\local\temp\snaipmu\sxbncta\wow.ini

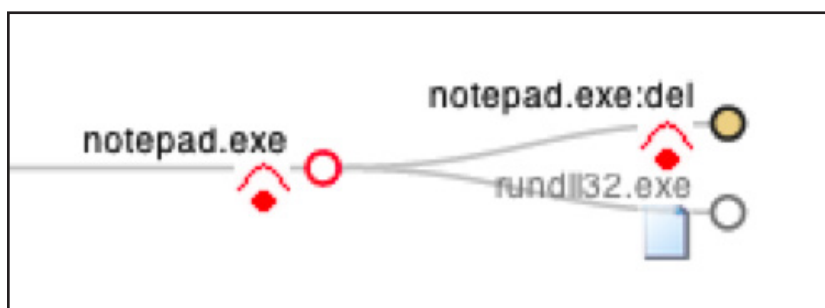
The malware then wrote to an InprocServer32 registry key:

Mon, 05 Aug 2013 10:42:15 GMT	regmod	Created \registry\user\s-1-5-21-...-5267_classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}
Mon, 05 Aug 2013 10:42:15 GMT	regmod	Created \registry\user\s-1-5-21-...-5267_classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\Inprocserver32
Mon, 05 Aug 2013 10:42:15 GMT	regmod	First wrote to \registry\user\s-1-5-21-...-5267_classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\Inprocserver32

This is one way malware can gain execution at reboot: by overwriting the COM server registration DLL for a Class ID (CLSID) of a system COM object. The CLSID {fbeb8a05-beee-4442-804e-409d6c4515e9} is associated with Explorer.exe's ability to burn

to optical media, and is itself not malicious. Adding an entry for this CLSID in HKCU means the new, malicious entry takes precedence over the valid machine-wide setting for this user. Each time explorer starts, it will load the COM object for burning CDs, which will, in turn, load the DLL responsible. Since the malware has changed the responsible DLL, the attacker's new wow.dll will get loaded instead of the expected shell32.dll.

The malicious notepad.exe then launched two child processes:



The first child process was rundll32.exe, with the following command line:
rundll32 c:\users\xxx\AppData\Local\Temp\snafpmu\sxbncta\wow.dll,0

This immediately executes the new wow.dll, so the attacker does not have to wait until Internet Explorer restarts.

The second child process, an alternate data stream on itself, was called del. After startup, it completed only one action: to delete the original notepad.exe:

	Mon, 05 Aug 2013 10:42:17 GMT	filemod	Deleted c:\users\ [redacted] \AppData\Local\Temp\notepad.exe
--	----------------------------------	---------	--

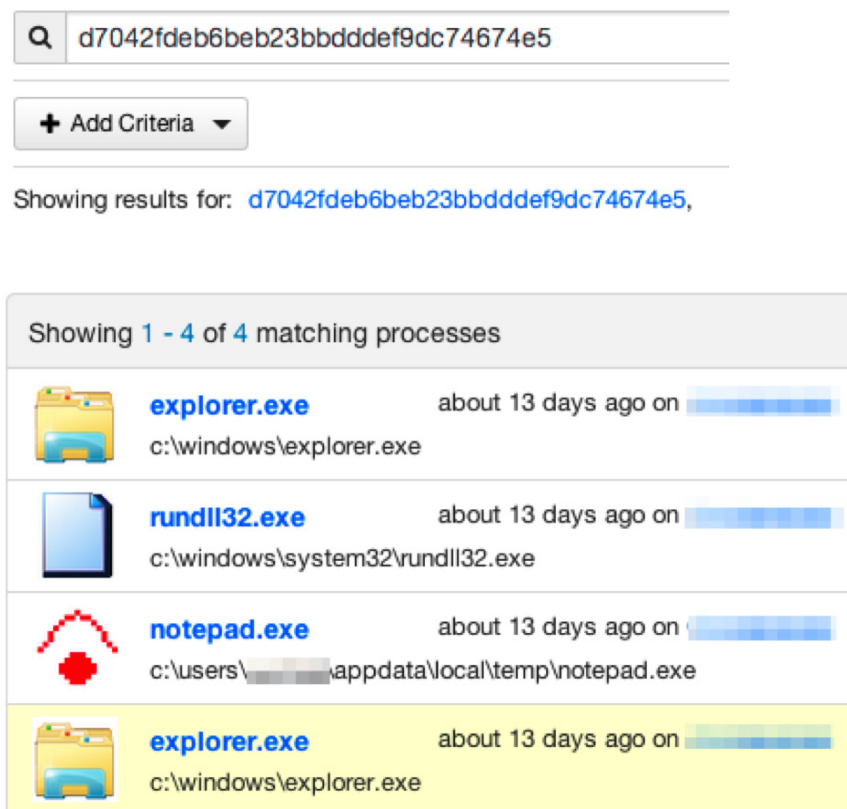
This is a clever and unique self-delete technique. Malware authors frequently remove binaries to thwart forensics analysis, but Windows does not allow the deletion of any file loaded for execution, so malware must jump through some hoops to do so. There are a number of techniques out there, but none mention the use of alternate data streams.

In summary, the malicious notepad.exe performed the following major actions:





- Created wow.dll and wow.ini
- Wrote to the InprocServer32 registry key to gain execution at reboot
- Launched wow.dll via rundll32
- Self-deleted using a relatively obscure technique with alternate datastreams

Attacker's objective

By searching for the md5 of wow.dll, responders can find all processes that loaded the malicious binary:

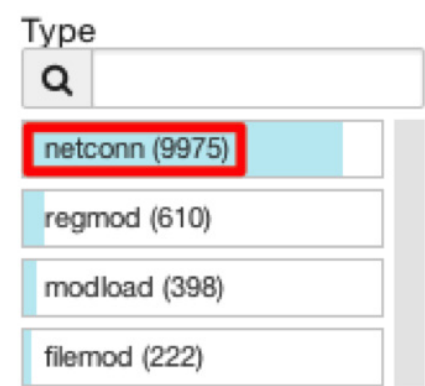


The screenshot shows a search interface with a search bar containing the MD5 hash `d7042fdeb6beb23bbdddef9dc74674e5`. Below the search bar is a button labeled "+ Add Criteria". The results section is titled "Showing results for: d7042fdeb6beb23bbdddef9dc74674e5," and displays a list of processes. The list is titled "Showing 1 - 4 of 4 matching processes". The processes are listed in a table-like format with icons, process names, start times, and file paths. The first three processes are `explorer.exe`, `rundll32.exe`, and `notepad.exe`. The fourth process is another instance of `explorer.exe`, which is highlighted in yellow.

Icon	Process Name	Start Time	File Path
	explorer.exe	about 13 days ago on	c:\windows\explorer.exe
	rundll32.exe	about 13 days ago on	c:\windows\system32\rundll32.exe
	notepad.exe	about 13 days ago on	c:\users\[redacted]\appdata\local\temp\notepad.exe
	explorer.exe	about 13 days ago on	c:\windows\explorer.exe

These are sorted by process start time. In addition to the already-known notepad.exe and rundll32.exe, wow.dll was only loaded in two other explorer.exe processes: the first was the explorer.exe that was running at the time of infection, the second was started about an hour later after the user rebooted his system.

Reviewing the activity of each explorer.exe instance, it demonstrates an unusually high number of network connections:



Reviewing a sampling of that network traffic reveals the intent of the attacker:

	Tue, 06 Aug 2013 12:38:14 GMT	netconn	Connection to 216.23.166.110 on tcp/80 (uswest-clients.bluecava.com)
	Tue, 06 Aug 2013 12:37:51 GMT	netconn	Connection to 64.208.138.174 on tcp/80 (ib.adnxs.com)
	Tue, 06 Aug 2013 12:37:41 GMT	netconn	Connection to 173.192.82.194 on tcp/80 (realtime.services.disqus.com)
	Tue, 06 Aug 2013 12:37:39 GMT	netconn	Connection to 67.228.244.117 on tcp/80 (referrer.disqus.com)

In the space of an hour, the malware made thousands of HTTP connections to various ad-related websites, strongly implying click-fraud.

Response Summary

On 5 Aug 13 at 10:40 GMT, the user surfed to his local news station's website. The user was running JRE6 update 31, released 18 months ago. A compromised ad provider served a malicious java applet, exploiting the user's vulnerable software. The malicious applet created a file called notepad.exe in the user's temp folder then launched it. "notepad.exe" created wow.dll in the temp folder, added it to the InprocServer32 registry key and then deleted itself. wow.dll was loaded by explorer.exe and was used as part of an what appears to be a click-fraud operation.

Where was Antivirus?

The infected host runs Trend Micro. At the time of this writing, the malicious notepad.exe is only identified by six of the 45 antivirus products referenced. The malicious wow.dll is only identified by nine. TrendMicro is not alerting on either, and neither is Symantec. Kaspersky and McAfee alert on one but not the other. Most do not alert on either.

Endpoint antivirus limits the effectiveness of an organization's protections to the opinion of one antivirus provider, but Carbon Black gives enterprises a consensus opinion. With its out-of-the-box watchlists, Carbon Black Enterprise Response will notify an enterprise as soon as 4 or more vendors identify a binary as malicious.

Additionally, it does not matter which malicious binary exceeds the threshold. In fact, since Carbon Black Enterprise Response stores the relationships between processes and records their actions, any alert on any indicator—even an IP address from an enterprise's network firewall—will enable them to detect the activity and make an intelligent response.

Conclusion

Enterprises need to realize they are in a continuous state of compromise. Because of this, they need a security solution with all three critical elements of the security lifecycle: prevention, detection and response—preferably from a single solution. This should better prepare organizations throughout the incident response lifecycle, enabling them to respond earlier in the kill chain and before data exfiltration.

Most solutions, however, lack an up-to-the-second recorded history of their entire environment, which would allow them to fully identify, scope, contain and remediate a threat once it is detected. Without a full recorded history, understanding the breadth of an incident can take days or months as opposed to hours or minutes with Carbon Black Enterprise Response. Moving forward, it will be the security solutions that integrate and collaborate with other solutions as well as ones that provide rich actionable intelligence of an entire environment that succeed in responding and defending against tomorrow's advanced attacks.

About Carbon Black

Carbon Black leads a new era of endpoint security by enabling organizations to disrupt advanced attacks, deploy the best prevention strategies for their business, and leverage the expertise of 10,000 professionals to shift the balance of power back to security teams. Only Carbon Black continuously records and centrally retains all endpoint activity, making it easy to track an attacker's every action, instantly scope every incident, unravel entire attacks and determine root causes. Carbon Black also offers a range of prevention options so organizations can match their endpoint defense to their business needs. Carbon Black has been named #1 in endpoint protection, incident response, and market share. Forward-thinking companies choose Carbon Black to arm their endpoints, enabling security teams to: Disrupt. Defend. Unite.



1100 Winter Street
Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499
www.carbonblack.com