

Unlock the Power of Real-time Incident Response with Bit9

Ryan Nolette, Incident Response Consultant



CUSTOMER CONFIDENTIAL

©2012 Bit9. All Rights Reserved

Hello everyone. I hope you are having a pleasant day so far.

My name is Ryan Nolette and I am an Incident Response Consultant and Threat Researcher for Bit9.

Today I would like to show you a few new ways to do malware detection, remediation, and incident response. If we have time, we will go into forensic post mortem using Bit9 as well.

Without further ado, let's kick things off.

Today's Agenda

- ◆ What are a few things everyone knows we can do?
- ◆ A few things you might not know.
- ◆ Can I see an example of how this works?
 - CryptoLocker block rules leveraging Bit9
 - Zeus Incident Response leveraging Bit9
- ◆ Recap
- ◆ Questions

CUSTOMER CONFIDENTIAL



What are a few things everyone knows we can do?

- ◆ Whitelisting
- ◆ Baseline drift
- ◆ Different enforcement modes

CUSTOMER CONFIDENTIAL



Before we go into things that are new and shiny, I would like to quickly cover 3 areas everyone already knows about and that Bit9 does very well.

They are whitelisting, basline drift, and granular enforcement modes.

Whitelisting

- ◆ **What is traditional whitelisting?**

- Often called “application control” or “whitelisting.”
 - Archaic methods required you to specifically identify trusted software and a lot of constant maintenance.

- ◆ **How does Bit9 move customers beyond whitelisting?**

- “Default-Deny”
 - A proactive **prevention** approach ensures that only trusted software can execute on your machines—everything else is denied.
 - Policy-driven approach keeps your endpoints and servers safe from advanced threats and zero-days.
 - » Installs quickly
 - » Is easy to manage
 - » Delivers immediate results
 - Administrator define policies that determine the software you trust.
 - Trusted installers and Trusted installing sources
 - Trusted directories
 - Trusted publishers
 - Trusted updaters
 - Bit9 Software Reputation Service’s trust ratings
 - Ability to have user defined policies



CUSTOMER CONFIDENTIAL

Bit9

I can hear what a lot of you are thinking, “why is whitelisting a separate topic? Isn’t everything that Bit9 does just to support their whitelisting ability?”

No. no it isn’t.

White listing is just a portion of what Bit9 can do for you. Whitelisting is a dirty word. It isn’t a dirty word because it doesn’t work, on the contrary, it is a dirty word because it does the dirty work, and does it well.

Bit9’s approach to whitelisting is policy driven, just like your enterprise domain, just like your AV solutions, just like anything else in life that is well structured and built to scale with demand.

Above are a few things that separate us from traditional whitelisting the same way that fine wine is not a grape juice box.

Baseline drift

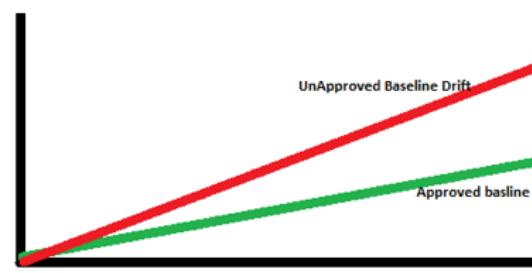
♦ What is baseline drift?

- The deviation of a host image from the baseline image (Golden Image)
- In Bit9, baseline drift, is the difference between a baseline of files and the current files on a target you specify.

♦ What can I do with baseline drift?

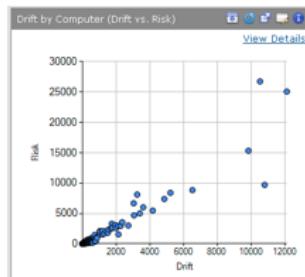
- This difference is available as a baseline drift report that you can view either in detail in dynamic tables or as graphic charts on a Bit9 dashboard.
- Reports provide simple numbers of file differences and also [risk analyses related to those changes](#).
- Once configured, a drift report runs every few hours, for up-to-date records of changes in your file inventory.
- You can create different baseline drift reports for different targets and baselines, and Bit9 provides some reports pre-configured for your use.

Baseline Concept



CUSTOMER CONFIDENTIAL

Report Graph Example



Bit9

Another feature of Bit9 that is rarely spoken about in length our the baseline drift monitoring.

What is baseline drift? Baseline drift is the deviation of a host image from the golden image as specified by you.

What is a golden image? It is the custom os installation that most enterprises build to reimagine endpoints, create VDI's or VM's, or reimagine Servers.

Different enforcement modes

- ◆ **Low enforcement (Detect untrusted)**

- Using Bit9 for detection and visibility without requiring software approvals.

- ◆ **Medium enforcement (Prompt untrusted)**

- Allowing the user to approve their own software.

- ◆ **High enforcement (Block untrusted)**

- Preventing all but approved and trusted software.

CUSTOMER CONFIDENTIAL



And last but not least of this category is the ability to make multiple policies for every group, business unit, or endpoint type in your environment.

The combinations are really only limited by your imagination.

Though we at Bit9 always recommend you place your endpoints in High enforcement mode, we know that it is not always a possibility right away.

Because of these circumstances, we provide multiple enforcement levels, enforcement exception rules, and feature enhancements such as connectors and detection which we will be talking about shortly.

Here are a few things you might not know

◆ Bit9 Network Integration (Bit9 Connector)

- Enables second prevention method
 - “Detonate-and-Deny”
 - » Retrieve and send files from your endpoints and servers to a network security device for detonation and analysis. If a file is determined to be malicious, you can ban it for that individual user or globally ban it from executing across your entire organization.

◆ Detection

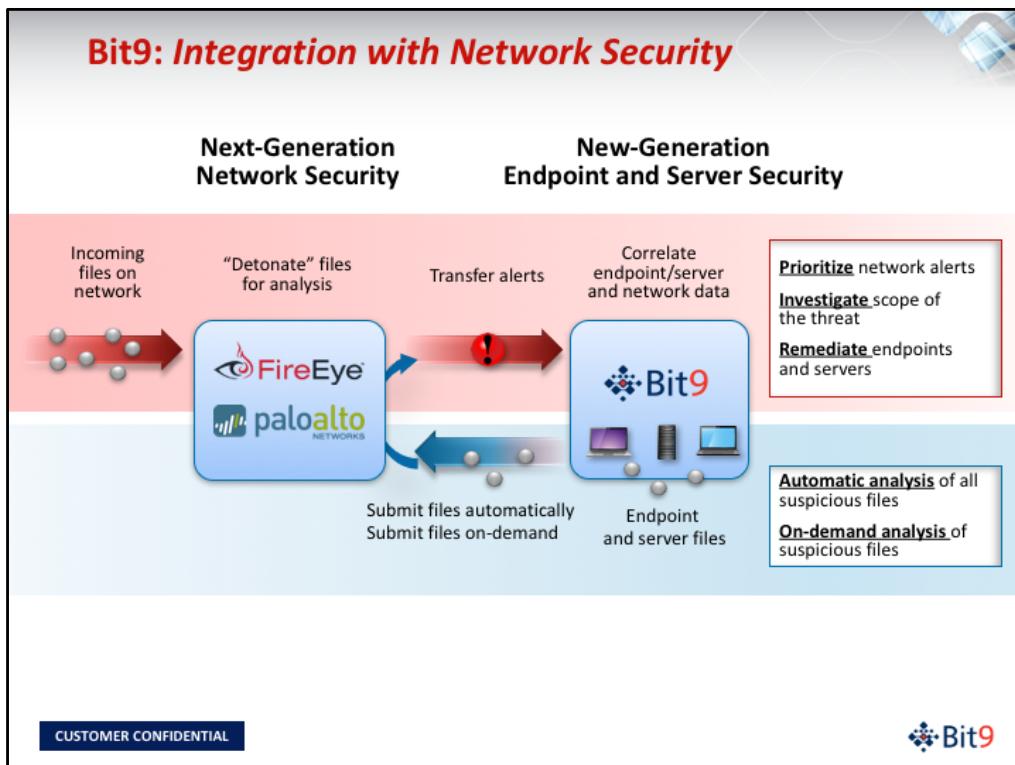
- ATIs
 - Signature-less detection of malicious behaviors and intent.

CUSTOMER CONFIDENTIAL



In the past year, Bit9 has released these 2 new enhancements which you can help leverage in your environment for either proactive blocking and protection or reactive detection, remediation, and prevention.

As I am sure you all have heard of these, I will keep this short as well and then we can dive into the meat of this presentation, how to use these features for Incident Response and malware triage.



Connectors are awesome. Let's just get that out of the way right now. They are only getting better and more feature robust with every version and it is already one of our most popular features.

I'm a big fan of this because before I came to Bit9, I wrote something very similar to this manually for my Fireeye installation. Let's just say my coding attempts are better left uncommented to keep my peers from crying, but it worked.....ish

The connector method as shown above is, as I already said, pretty awesome. It allows you to send any file you want to fireeye or palo alto for detonation, and then to receive that detonation information back in the bit9 console to either be manually interpreted or to run against automated logic to auto ban files based on your specified criteria. It's all your preference.

It also allows direct input from those network appliances to auto ban files in your environment based on rules you can setup. it's like have a whole team of soc analysts and security administrators at your finger tips.

Within seconds of a client downloading a malicious file, it can be banned globally in your environment. This is how automated prevention and protection should be done. And that isn't my opinion as a Bit9 employee, but my opinion as a 10 year veteran of Incident response, SOC building, and Security architecting.

Use a setup like this, and you wont have much need to my IR presentation following.

Detection

- ◆ **Advanced Threat Indicators (ATI).**

- Bit9's threat research team constantly analyzes advanced threats to identify the common techniques and behaviors threat actors use to build Advanced Threat Indicators.

- ◆ **Detection of suspicious behavior.**

- Bit9 detects for memory violations, suspicious process behavior, registry changes, operating system tampering, and more. For example:
 - If Adobe spawns an executable on your host, it's probably malicious.
 - Binaries shouldn't have JPEG or PDF extensions.
 - Many more available

- ◆ **Detection of untrusted file execution.**

- Bit9's real-time endpoint sensor and recorder continuously monitor all new software that arrives and attempts to execute on a machine.

Real-time Detection of:

- Creation/execution of **untrusted software**
- Suspicious **registry changes**
- Unauthorized **USB devices**
- Unauthorized **process and memory access**
- File integrity** changes
- OS/application **tampering**
- User session changes

Threat Detection of:

- Advanced threats and zero-day attacks
- Malformed documents
- Phishing attacks
- Web-drive-by downloads
- Infected **USB devices**
- Remote system **vulnerability**

CUSTOMER CONFIDENTIAL



So what do you do if you don't want to spend millions on network security appliances to pair with Bit9 in your security stack? Grab our free detection enhancement and turn it on.

Now, no really, do it. pretty please? I mainly say that because I'm on the team that researches and develops the ATI's for the detection enhancement and I want you all to see how shiny it is.

Will the detection enhancement replace a full stack setup including connectors to network appliances? No. but it will give you actionable intelligence based on endpoint activity and help you find malicious and suspicious behavior in real time on your endpoints that AV and network appliances cannot do.

Can I see an example of how this works?

◆ **CryptoLocker**

- What is CryptoLocker?
- What does CryptoLocker look like to the user?
- How can I detect a CryptoLocker infection using Bit9?
- How do I stop a CryptoLocker infection using Bit9?

◆ **Zeus Is Often Paired with CryptoLocker**

- What can I do about a Zeus infection using Bit9?

CUSTOMER CONFIDENTIAL



Now that we have gone over a few of the features we will be using today, let's talk about a pretty hot topic. CryptoLocker. We are also going to discuss Zeus today. Why both? Because they are being paired together as a dual threat to your enterprise.

Read above questions

A Real Threat: CryptoLocker

◆ CryptoLocker

- Malware that surfaced in late 2013.
- It is a form of “ransomware” currently targeted at Microsoft Windows-based computers.
- It encrypts files stored on local hard drives and any mounted network drives it can access.
- When it has finished encrypting all the files, it presents a branded prompt stating your files will be decrypted if a fee is paid.
 - Threatens that if it is not paid by deadline, CryptoLocker will delete the private key for your data and that decryption is no longer possible.

◆ How can I use Bit9 and its products to defend against CryptoLocker?

- Leverage the Bit9 Security Platform
 - Detection (ATIs)
 - Bit9 Network Integration (Bit9 Connectors)
 - Bit9 Prevention approaches and Enforcement Levels

CUSTOMER CONFIDENTIAL



talk about cryptolocker a bit

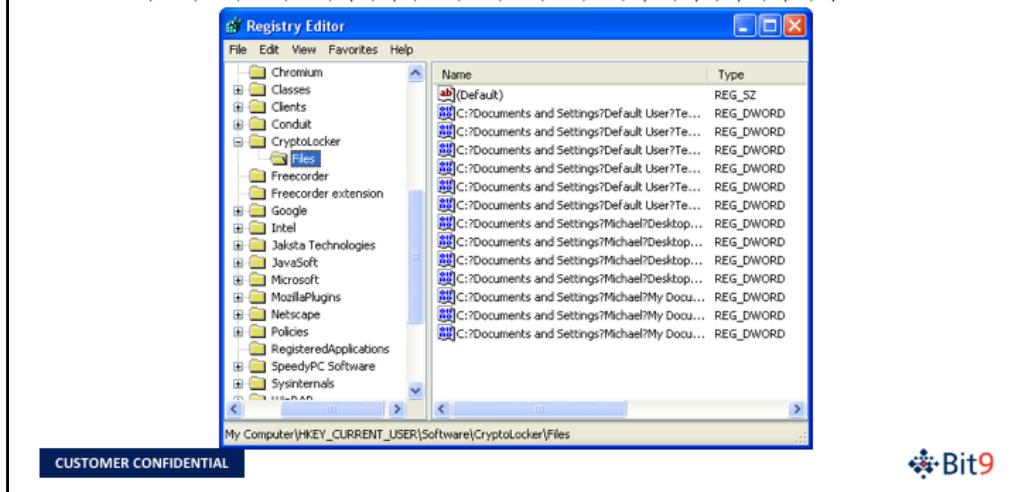
What does CryptoLocker look like to the user?



This is all the user see's when they get infected with CryptoLocker. The problem is, by the time they have seen this it is already too late.

What does CryptoLocker do?

- For each file that is encrypted, a resulting registry value will be created under this key: HKCU\Software\CryptoLocker\Files
 - Once the infection is active on your computer it will scan your drives (local & network) and encrypt the following types of files with a mix of RSA & AES encryption:
 - .odt, .ods, .odp, .odm, .odc, .odb, .doc, .docx, .docm, .wps, .xls, .xlsx, .xlsm, .xlbs, .xlk, .ppt, .pptx, .pptrn, .mdb, .accdb, .pst, .dwg, .dxf, .dkg, .wpd, .rtf, .wb2, .mdf, .dbf, .psd, .pdd, .eps, .ai, .indd, .cdr, ????????.jpg, ????????.jpeg, .img, .png, .3fr, .arw, .srif, .sr2, .bay, .crw, .cr2, .der, .kdc, .erf, .mef, .mrw, .nef, .nrw, .orf, .rat, .raw, .rw1, .rw2, .r3d, .ptx, .pef, .x3f, .der, .cer, .cert, .pem, .pkix, .p12, .p7b, .p7cThe



Why is it already too late? Because once Cryptlocker starts running, it encrypts everything with the file extensions you see above, more too probably but in the samples I analyzed, there were only these extensions being encrypted.

How do I stop CryptoLocker?

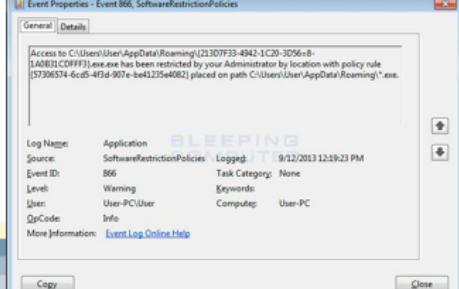
- ◆ Lock Down!
- ◆ No really. Blocking executables in group policy is the only known method of preventing CryptoLocker, besides a Bit9 solution, currently.

CryptoLocker SRP
Data collected on: 9/17/2013 10:58:16 AM
Computer Configuration (Enabled)

Policies
Windows Settings
Security Settings
Public Key Policies/ Trusted Root Certification Authorities
Software Restriction Policies
Software Restriction Policies/ Security Levels
Software Restriction Policies/ Additional Rules
Path Rules

%AppData%*.*.exe	Security Level	Disallowed	Cryptolocker AppData test. 9/17/2013 10:42:30 AM
%AppData%**.*.exe	Security Level	Disallowed	Cryptolocker nested test. 9/17/2013 10:57:29 AM

CUSTOMER CONFIDENTIAL




There are only 3 things you can do about cryptolocker. You can have a preventive approach like Bit9 or another method block executables in specific locations (which can cause legitimate applications to stop working), restore from backups after the fact and deal with the data loss, or you can do nothing and cry.

How can I detect a CryptoLocker V1.0 infection using Bit9?

• Registry evidence

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "CryptoLocker"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce **CryptoLocker"
- HKCU\Software\CryptoLocker\Files*

• File Evidence

- %AppData%*.exe
 - C:\Users\User\AppData\Roaming\{213D7F33-4942-1C20-3D56=8-1A0B31CDFFF3}.exe (Vista/7/8)
 - C:\Documents and Settings\User\Application Data\{213D7F33-4942-1C20-3D56=8-1A0B31CDFFF3}.exe (XP)
- %AppData%**.exe

• Known issues with traditional defenses

- Blocking all “*.exe” files in AppData via GPO can block legitimate applications from running.
- Blocking only dropped executables by name will not stop the infections, the filenames change each instance.
- Removing the executable after it has run will stop you from decrypting your data if you decide to pay.

CUSTOMER CONFIDENTIAL



What do we know about how cryptolocker works along all installations? These persistent behaviors and endpoint artifacts.

Why does this matter? If a piece of malware is dependent on constant to succeed, we have something we can take away from it to make it fail. Similar to pulling away the lowest blocks in the jenga tower, the application will fail. This is also similar to installation an application without it's dependencies. The installation will fail and the application will not run.

CryptoBlocker v1.0 in console

The screenshot shows the Bit9 software interface with the title "CryptoBlocker v1.0 in console". The main window displays the "Edit Registry Rule" dialog. The rule is named "CryptoLocker" and has the following details:

- Description:** This rule detects the installation of CryptoLocker.
- Status:** Enabled (radio button selected).
- Platform:** Windows.
- Write Action:** Block (selected) and Use Policy Specific Behavior (unchecked).
- Registry Path:** HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce.
- Process:** Any Process.
- User Or Group:** Any User.
- Rule Applies To:** All policies (radio button selected).

The left sidebar lists various policy categories: Policies, Policies Tab, Mappings, Natives, Software Rules, Updaters, Publishers, Users, Directories, Files, Custom, Memory, Registry, Scripts, Reputation, and Event Rules.

CUSTOMER CONFIDENTIAL

Bit9

This is what our blocking rule looks like in the console.

How can I detect a CryptoLocker V2.0 infection using Bit9?

- ◆ **Old reg:**

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "CryptoLocker"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "*CryptoLocker"

- ◆ **New reg:**

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "CryptoLocker_<version_number>"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "*CryptoLocker_<version_number>"

- ◆ **Example of new key name**

- CryptoLocker_0388

- ◆ **Old rule**

- Pattern example
 - HKCU-SoftwareX86\Software\Microsoft\Windows\CurrentVersion\Run\CryptoLocker

- ◆ **New proposed rule**

- Pattern example
 - HKCU-SoftwareX86\Software\Microsoft\Windows\CurrentVersion\Run\CryptoLocker*

CUSTOMER CONFIDENTIAL



Just adding a wildcard to the end of the registry value allows for us to block both versions of CryptoLocker from completing installation and running.

I also suggest removing all files that these rules show as they are the executables for CryptoLocker.

CryptoBlocker v2.0 in console

Edit Registry Rule

General

Name: CryptoLocker
Description: This rule detects the installation of CryptoLocker
Status: Enabled Disabled
Platform: Windows

Definition

Select the action you would like to take...
Write Action: Block Use Policy Specific Notifier

When the registry create, modify or delete path matches...

Registry Path: Add Remove
HKCU\Software\X86\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\X86\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\Software\CryptoLocker\Files*
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

And when the running process matches...

Process: Any Process
User Or Group: Any User

Rule Applies To: All policies Selected policies

CUSTOMER CONFIDENTIAL

Bit9

Version 2.0 looks an awful lot like version 1.0 doesn't it? This is because the authors did not change the malware's logic, and because of this, we can use the same technique as before to disable it.

How do I stop a CryptoLocker infection using Bit9?

- What is Bit9 doing about it? We built a rule to block the installation steps of the current known version of CryptoLocker.

- ◆ What is this actually doing?

- This is a registry rule
 - It is looking for any process to create or modify the registry entries
 - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "Cryptolocker"
 - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "Cryptolocker"
 - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce Wow64Extensis

- ## ◆ Does it work?

CUSTOMER CONFIDENTIAL

Bit9

The previous few slides detailed the method that we use to prevent CryptoLocker from running. Above is a raw XML output of the CryptoBlocker rule directly from the console.

Does it work? Yes it does. As you can see here, we are successfully blocking CryptoLocker from installing over and over again. Want to see more?

CryptoLocker Infection Timeline			
Timestamp	Priority	Type	Subtype
Oct 30 2013 09:25:10AM	Notice	Discovery	New unapproved file to computer
Oct 30 2013 09:25:10AM	Info	Discovery	New file on network
Oct 30 2013 07:55:14AM	Notice	Policy Enforcement	Write block (registry rule)
Oct 30 2013 07:55:11AM	Info	Discovery	First execution on network
Oct 30 2013 07:55:11AM	Notice	Discovery	New unapproved file to computer
Oct 30 2013 07:55:08AM	Info	Discovery	File group created
Oct 30 2013 07:55:08AM	Notice	Discovery	New unapproved file to computer
Oct 30 2013 06:48:03AM	Warning	Computer Management	Agent health check
Timestamp	Process	File Path	
Oct 30 2013 09:25:10AM	<PATH>\uqaqoz\vuik.exe	c:\users\<USERNAME>\appdata\local\temp\qxs1b16	
Oct 30 2013 09:25:10AM	<PATH>\uqaqoz\vuik.exe	c:\users\<USERNAME>\appdata\local\temp\qxs1b16	
Oct 30 2013 07:55:14AM	<PATH>\izosmjnypvgrjxx.exe	\registry\user\<SID>\software\microsoft\windows\currentversion\run	
Oct 30 2013 07:55:11AM	<PATH>\uqaqoz\vuik.exe	c:\users\<USERNAME>\appdata\local\temp\uj\21e4	
Oct 30 2013 07:55:11AM	<PATH>\uqaqoz\vuik.exe	c:\users\<USERNAME>\appdata\local\temp\uj\21e4	
Oct 30 2013 07:55:08AM	<PATH>\uqaqoz\vuik.exe	<PATH>\uqaqoz	
Oct 30 2013 07:55:08AM	<PATH>\uqaqoz\vuik.exe	c:\users\<USERNAME>\appdata\local\temp\kgb6461	
Oct 30 2013 06:48:03AM	N/A – agent health check event	N/A – agent health check event	

CUSTOMER CONFIDENTIAL

 Bit9

The next few slides are sanitized customer data. Since the columns are so long in the console, I have taken that data and directly placed it into these tables. The data has not been changed, only sanitized.

To keep a constant across all tables, I have the same timestamp column represented across each table.

What you can see from these columns is an unrelated health check on the host, then an hour later, Zeus gets dropped on the host, brings down cryptolocker and tries to run and install cryptolocker. You can see the attempt being blocked.

CryptoLocker Infection Timeline

Timestamp	File Hash	malware confirmed by
		VirusTotal
Oct 30 2013 09:25:10AM	364be14fd1629644b1b7e87a8222573dfc79373ef9ea0be40c41d48b6c3faa86	zeus
Oct 30 2013 09:25:10AM	364be14fd1629644b1b7e87a8222573dfc79373ef9ea0be40c41d48b6c3faa86	zeus
Oct 30 2013 07:55:14AM		cryptolocker
Oct 30 2013 07:55:11AM	003c64fa11ea18a00c3e0bf2adfa1a2b80287fb072d1f8108d1d55cbda17e60cb	cryptolocker
Oct 30 2013 07:55:11AM	003c64fa11ea18a00c3e0bf2adfa1a2b80287fb072d1f8108d1d55cbda17e60cb	cryptolocker
Oct 30 2013 07:55:08AM	8b000da81d4c44c68890506f80ec9274ff35e224cbab1100547930e90178223c	unknown malware
Oct 30 2013 07:55:08AM	e9020b510466e0fc800acf3adeda4fd81a77e29cc63f2b7fc08f24560e69	zeus
Oct 30 2013 06:48:03AM	N/A – agent health check event	N/A – agent health check event

- We stopped CryptoLocker from executing and infecting the machine.
- The machine is still owned by Zeus and is still downloading new malware but...

We Stopped CryptoLocker

CUSTOMER CONFIDENTIAL



To clarify, we were in low enforcement mode on this host in the customer environment. Therefore they had no mechanism in place outside of their AV to protect them from Zeus, but because they applied our CryptoBlocker rule in block mode, the host was not compromised by CryptoLocker. It is however compromised by Zeus.

What can I do about a Zeus infection using Bit9?

```
Directory of C:\Documents and Settings\Administrator\Application Data
11/28/2013  11:48 AM    <DIR>          Adobe
11/16/2012  02:56 PM    <DIR>          Identities
11/16/2012  04:49 PM    <DIR>          Macromedia
11/21/2012  09:15 AM    <DIR>          Odana
11/28/2013  11:45 AM    <DIR>          Sun
              0 File(s)   0 bytes
              5 Dir(s)  36,744,691,712 bytes free

C:\Documents and Settings\Administrator\Application Data>dir Odana
Volume in drive C has no label.
Volume Serial Number is 6C9A-8459

Directory of C:\Documents and Settings\Administrator\Application Data\Odana
11/21/2012  09:15 AM    <DIR>          .
11/21/2012  09:15 AM    <DIR>          .
11/21/2012  09:15 AM           444,928 p2vij.exe
              1 File(s)   444,928 bytes
              2 Dir(s)  36,744,691,712 bytes free
```

CUSTOMER CONFIDENTIAL



Speaking of Zeus. What does a Zeus infection look like? How can we investigate a Zeus infection? How can we defend against it?

Above you see a command prompt displaying a successful Zeus infection on one of my test hosts. In the next few slides we will go in depth into the workflow of detecting and blocking a typical Zeus infection in your environment.

Please keep in mind. This is for Incident response and Triage only, not forensics.

Why do I care about Zeus?

◆ What is Zeus?

- Zeus or Zbot is Trojan malware that runs on Windows.
- Spread mainly through drive-by downloads, exploit kits, and phishing attacks.
- First identified in ~July 2007
- In 2009 estimates of compromised computers were in the millions, ~3.6 million in the United States alone.
- In 2010, the FBI indicated a major international cybercrime network using Zeus to steal ~\$70 Million.
- As of May 2013, the source code and compiled binaries of Zeus were being hosted on GitHub.
- Zeus Trojan-controlled machines have been found in 196 countries, including isolated states such as North Korea.
- The five countries with most infected machines are Egypt, the United States, Mexico, Saudi Arabia, and Turkey.

◆ What Does Zeus do?

- It is most often used to steal banking information and usernames and passwords from browsers.
- It is also used to install the CryptoLocker ransomware.

CUSTOMER CONFIDENTIAL



Above is a few metrics about Zeus. Basically it is a piece of malicious software that gathers browser credentials and sends them to a remote server for later use.

This is the most common infection I have dealt with at financial institutions in the past 5 years.

It is now one of the most popular CryptoLocker delivery systems.

Zeus Is Often Paired with CryptoLocker

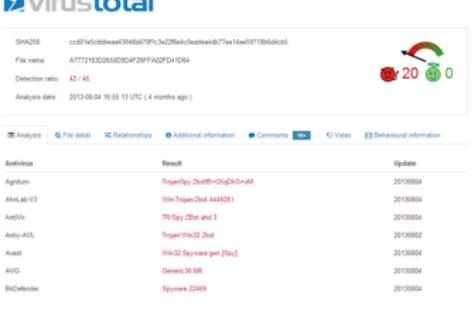
Where did I get Zeus?

- <https://zeustracker.abuse.ch/monitor.php?filter=filesonline>



How do I know it is Zeus?

- <https://www.virustotal.com/en/file/ccd01e5cbbbeaa43648d470f1c3e22f8e4c0eadea4db77ee14ae59718b6d4cb5/analysis/>



CUSTOMER CONFIDENTIAL
Bit9

For our demo today, I am using real malware. I went to Zeus tracker, a well known source to find Zeus command servers and other Zeus related information.

I then did what most of your users do. I kept clicking on random crap until I got my host infected.

At this point I saved the executable and zipped it up for later usage. Going forward I will be depositing this zipped malware on each of my hosts in my environment and trying to execute it from there.

The piece of malware I was able to infect myself with on an unprotected windows XP system is to the right. Bit9 marks it with a low trust rating already but in case you wanted a third party opinion, I have uploaded it to virustotal and received a 42 of 46 rating for Zeus.

I think we can all agree, this is Zeus, this is real, and I should not click on bad links when my system is unprotected. ☺

How do different enforcement levels effect my IR ability?

The screenshot shows a software interface titled "Policies". At the top, there are filter options: "Group By" set to "(none)", "Descending", and "Show/Hide Filter", "Show/Hide Columns", "Export to CSV", and "Refresh Page". Below this is a "Filters" section with an "Add filter" dropdown and checkboxes for "Allow Upgrades" (checked) and "Yes" (checked). Buttons for "Apply", "Cancel", and "Reset" are also present. The main area displays a table with the following data:

Action	Policy	Connected Enforcement	Disconnected Enforcement	Total	Connected
<input type="checkbox"/>	doors unlocked	Low (Monitor Unapproved)	Low (Monitor Unapproved)	1	1
<input type="checkbox"/>	lockdown	High (Block Unapproved)	High (Block Unapproved)	6	1
<input type="checkbox"/>	say pretty please	Medium (Prompt Unapproved)	Medium (Prompt Unapproved)	1	1
<input type="checkbox"/>	you shall not pass	High (Block Unapproved)	High (Block Unapproved)	0	0

At the bottom left, it says "4 items" and "Page 1/1". On the right, there is a "25" dropdown and a "rows per page" checkbox. A "CUSTOMER CONFIDENTIAL" watermark is at the bottom left, and the Bit9 logo is at the bottom right.

Before we go into what Zeus looks like from the console and host, lets talk a bit about my Bit9 setup. Above are all of the policies I have in my environment. We will be using these in the demo today.

I am not using monitor mode because it is out of scope for remediation at this moment. I honestly do not use monitor mode because low enforcement gives me the same visibility as monitor mode but with the added ability of global banning.

Hosts we will be using in demo

Computer Name	Connected	Policy Status	Upgrade Status	Connected Enforcement	Disconnected Enforcement	IP Address	Policy	Operating System
WORKGROUP\PARCLIENTWIN7	<input checked="" type="radio"/>	Up to date	Up to date	Medium (Prompt Unapproved)	Medium (Prompt Unapproved)	192.168.32.101	say pretty please	Windows 7
WORKGROUP\PARSERV	<input checked="" type="radio"/>	Up to date	Up to date	High (Block Unapproved)	High (Block Unapproved)	::1	lockdown	Windows Server 2008
WORKGROUP\PPAR-55DAB9A30	<input checked="" type="radio"/>	Up to date	Up to date	Low (Monitor Unapproved)	Low (Monitor Unapproved)	192.168.32.102	doors unlocked	Windows XP

CUSTOMER CONFIDENTIAL  Bit9

These are the hosts I am using today. I have a windows 2k8r2 server running sqlexpress and bit9. I have nothing else security wise installed. The firewall is off, and my server shares no roles on my domain besides being the bit9 server.

I have a windows7 client and a windows XP client.

My win7 client is in medium enforcement or what I call block and ask mode. It will prompt the user for block or approve permissions for unapproved files.

My XP client is in low enforcement mode and will let anything not on my ban list install.

High Enforcement Block of Unapproved File

Timestamp	Priority	Type	Subtype	Source
Dec 5 2013 06:06:54 PM	Notice	Policy Enforcement	Execution block (unapproved file)	WORKGROUP\XPPAR-55DAB9A30
Dec 5 2013 06:06:29 PM	Notice	Discovery	New unapproved file to computer	WORKGROUP\XPPAR-55DAB9A30
Dec 5 2013 06:06:29 PM	Info	Discovery	New file on network	WORKGROUP\XPPAR-55DAB9A30

Description

```
File 'c:\documents and settings\administrator\desktop\zeus_binary_a7772183d2650d94f26fa02f641d64.exe' [zeus_binary_a7772183d2650d94f26fa02f641d64.exe] [CC001...D4CB5] was blocked because it was unapproved.
Computer WORKGROUP\XPPAR-55DAB9A30 discovered new file 'c:\documents and settings\administrator\desktop\zeus_binary_a7772183d2650d94f26fa02f641d64.exe' [zeus_binary_a7772183d2650d94f26fa02f641d64.exe] [CC001...D4CB5].
Server discovered new file 'c:\documents and settings\administrator\desktop\zeus_binary_a7772183d2650d94f26fa02f641d64.exe' [zeus_binary_a7772183d2650d94f26fa02f641d64.exe] [CC001...D4CB5].
```

CUSTOMER CONFIDENTIAL

Bit9

When I changed my XP machine into High enforcement mode and clicked on that bad file. As you have guessed, nothing happened. Bit9 blocked this unapproved file from executing automatically.

We can move on from here not worry about the file. Though I will say that in the next few examples we will see bad things happen because of the enforcements I will choose. I will explain everything in more detail as I go, but I wanted to point out that on this high enforcement machine, even though the file has been blocked from running, it is still on the host and should be removed. I suggest removal from each host in scope once you complete your scoping.

Medium Enforcement Block by user, console view

Timestamp	Priority	Type	Subtype	Source
Dec 5 2013 06:12:56 PM	Info	Policy Enforcement	Execution block (unapproved file)	WORKGROUP\XPPAR-55DAB9A30
Dec 5 2013 06:12:56 PM	Info	Policy Enforcement	Execution prompt block (unapproved file)	WORKGROUP\XPPAR-55DAB9A30
Dec 5 2013 06:10:47 PM	Info	Computer Management	Agent Enforcement Level changed	WORKGROUP\XPPAR-55DAB9A30
Dec 5 2013 06:10:15 PM	Info	Computer Management	Computer modified	WORKGROUP\XPPAR-55DAB9A30
Dec 5 2013 06:10:15 PM	Info	Computer Management	Agent policy changed	WORKGROUP\XPPAR-55DAB9A30
Dec 5 2013 06:06:54 PM	Info	Policy Enforcement	Execution block (unapproved file)	WORKGROUP\XPPAR-55DAB9A30
Dec 5 2013 06:06:29 PM	Info	Discovery	New unapproved file to computer	WORKGROUP\XPPAR-55DAB9A30
Dec 5 2013 06:06:29 PM	Info	Discovery	New file on network	WORKGROUP\XPPAR-55DAB9A30

Description

File 'c:\documents and settings\administrator\Desktop\zeus_binary_a7772183d2650d9d4f26ffa02f441d64.exe' [CC001...-D4CB5] was blocked because it was unapproved.
 File 'c:\documents and settings\administrator\Desktop\zeus_binary_a7772183d2650d9d4f26ffa02f441d64.exe' [zeus_binary_a7772183d2650d9d4f26ffa02f441d64.exe] [CC001...-D4CB5] was blocked because of user response.
 Computer 'WORKGROUP\XPPAR-55DAB9A30' changed Enforcement Level from 'High (Block Unapproved)' to 'Medium (Prompt Unapproved)'.
 Computer 'WORKGROUP\XPPAR-55DAB9A30' was moved into the policy 'say pretty please' by 'admin'.
 Computer 'WORKGROUP\XPPAR-55DAB9A30' changed policies from 'lockdown' to 'say pretty please'.
 File 'c:\documents and settings\administrator\Desktop\zeus_binary_a7772183d2650d9d4f26ffa02f441d64.exe' [zeus_binary_a7772183d2650d9d4f26ffa02f441d64.exe] [CC001...-D4CB5] was blocked because it was unapproved.
 Computer WORKGROUP\XPPAR-55DAB9A30 discovered new file 'c:\documents and settings\administrator\Desktop\zeus_binary_a7772183d2650d9d4f26ffa02f441d64.exe' [zeus_binary_a7772183d2650d9d4f26ffa02f441d64.exe] [CC001...-D4CB5].
 Server discovered new file 'c:\documents and settings\administrator\Desktop\zeus_binary_a7772183d2650d9d4f26ffa02f441d64.exe' [zeus_binary_a7772183d2650d9d4f26ffa02f441d64.exe] [CC001...-D4CB5].

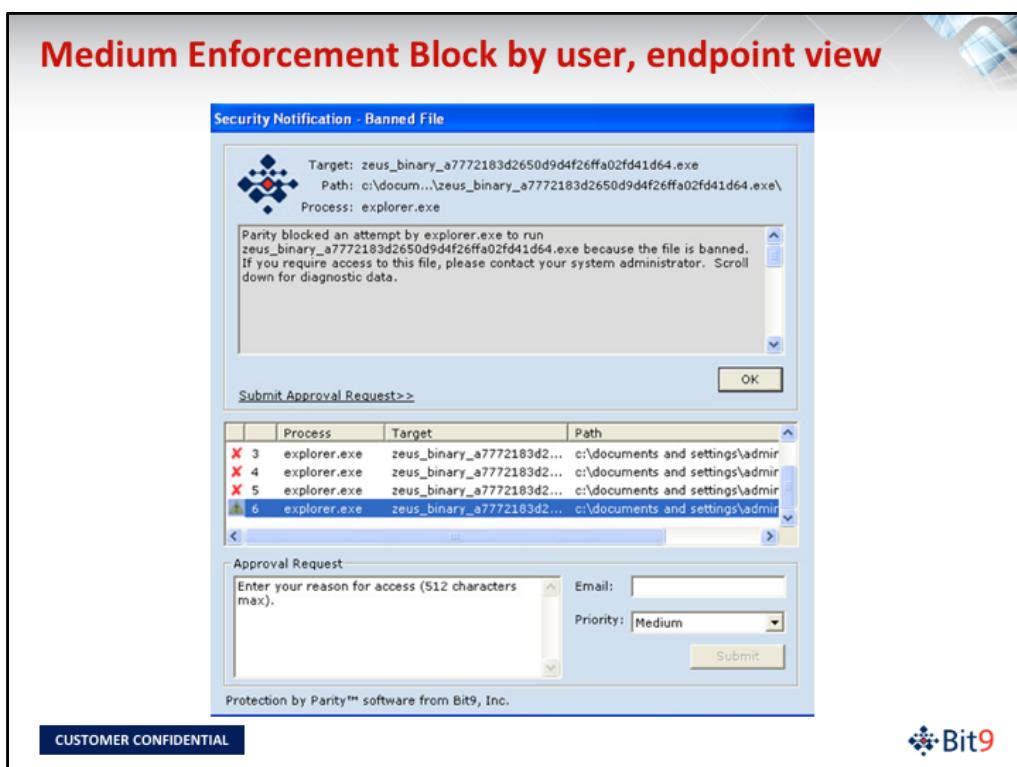
CUSTOMER CONFIDENTIAL

 Bit9

Now this is where things can get tricky. Medium enforcement mode gives the user power to block or approved unapproved files based on whatever criteria they user deems necessary. This is pretty much the same decision making that led to the file being downloaded in the first place in most cases so keep in mind that a user can still be infected in this enforcement mode if they approve everything and it has not yet been global banned.

Above you will see me click on the malware and try to execute it. I get a prompt message and I choose to block the file from running. This is what you will see in the console from that event.

Medium Enforcement Block by user, endpoint view



This is the flipside to the block. The user is prompted with a screen similar to the one above and can choose to block or approve the file.

Low enforcement Zeus Infection (no preventive block rule)



CUSTOMER CONFIDENTIAL

Bit9

Now I have switched my Xp client into low enforcement mode with no server side block rule. This is all the user will see after executing the malware. Nothing. They have no idea they were infected.

Low enforcement Zeus Infection (no preventive block rule)

```
Volume Serial Number is 6C9A-8459
Directory of C:\Documents and Settings\Administrator\Application Data
01/28/2013 11:48 AM <DIR> Adobe
11/16/2012 02:56 PM <DIR> Identities
11/21/2012 09:15 AM <DIR> Macros
11/21/2012 09:15 AM <DIR> Odama
0 File(s) 0 bytes
5 Dir(s) 36,744,691,712 bytes free
C:\Documents and Settings\Administrator\Application Data>dir Odama
Volume in drive C has no label
Volume Serial Number is 6C9A-8459
Directory of C:\Documents and Settings\Administrator\Application Data\Odama
11/21/2012 09:15 AM <DIR> .
11/21/2012 09:15 AM <DIR> ..
11/21/2012 09:15 AM 444,928 pyj.exe
2 Dir(s) 36,744,691,712 bytes free
C:\Documents and Settings\Administrator\Application Data>
```

CUSTOMER CONFIDENTIAL



This is what happened to the infected host. Above I can verify the Zeus malware has fully installed on this system and is actively running without the user's knowledge or the company's consent.

Zeus Infection viewed from Bit9 Console (Medium Enforcement malicious file approved by user)

<input type="checkbox"/>	Dec 5 2013 06:15:47 PM	Notice	Discovery	New unapproved file to computer	WORKGROUP\XPPAR-55DAB9A30
<input type="checkbox"/>	Dec 5 2013 06:15:47 PM	Info	Discovery	New file on network	WORKGROUP\XPPAR-55DAB9A30
<input type="checkbox"/>	Dec 5 2013 06:15:47 PM	Notice	Policy Enforcement	Report execution (custom rule)	WORKGROUP\XPPAR-55DAB9A30
<input type="checkbox"/>	Dec 5 2013 06:15:49 PM	Info	Discovery	File group created	WORKGROUP\XPPAR-55DAB9A30
<input type="checkbox"/>	Dec 5 2013 06:15:49 PM	Notice	Policy Enforcement	Report execution (custom rule)	WORKGROUP\XPPAR-55DAB9A30
<input type="checkbox"/>	Dec 5 2013 06:15:49 PM	Notice	Discovery	New unapproved file to computer	WORKGROUP\XPPAR-55DAB9A30
<input type="checkbox"/>	Dec 5 2013 06:14:56 PM	Info	Discovery	New file on network	WORKGROUP\XPPAR-55DAB9A30
<input type="checkbox"/>	Dec 5 2013 06:14:55 PM	Info	Policy Enforcement	Execution prompt allowed (unapproved file)	WORKGROUP\XPPAR-55DAB9A30

Computer WORKGROUP\XPPAR-55DAB9A30 discovered new file 'c:\documents and settings\administrator\local settings\temp\lmp5f931ba2.bat' [4BF2B...DBCA2].

Server discovered new file 'c:\documents and settings\administrator\local settings\temp\lmp5f931ba2.bat' [4BF2B...DBCA2].

File 'c:\windows\system32\cmd.exe' [62A8E...55E84] was executed.

Installation group was created for the file 'c:\documents and settings\administrator\Desktop\zeus_binary_a7772183d2650d9d4f26ffa02fd41d64.exe\zeus_binary_a7772183d2650d9d4f26ffa02fd41d64.exe' [CCD01...D4CB5].

File 'c:\windows\system32\cmd.exe' [62A8E...55E84] was executed.

Computer WORKGROUP\XPPAR-55DAB9A30 discovered new file 'c:\documents and settings\administrator\application data\odama\piy\piy.exe' [C1E31...53583].

Server discovered new file 'c:\documents and settings\administrator\application data\odama\piy\piy.exe' [C1E31...53583].

File 'c:\documents and settings\administrator\Desktop\zeus_binary_a7772183d2650d9d4f26ffa02fd41d64.exe\zeus_binary_a7772183d2650d9d4f26ffa02fd41d64.exe' [CCD01...D4CB5] was approved because of user response.

CUSTOMER CONFIDENTIAL

Bit9

What happens if we were to approve the file in medium enforcement? The same thing that happens to the low enforcement machine without a block rule. The host becomes infected. This is a view of the infection from the console.

How can I scope the infection?

- ◆ How was I notified of the infection in the first place?
- ◆ Initial Triage Scoping
 - Is this a one off infection?
 - Is this a campaign?
 - How many machines are infected?
 - When did this happen?
 - How long have they been infected?
 - How did I get these metrics?
 - How long did it take me to scope this incident?
- ◆ Where did the infection come from (browser, email, download, etc.)?
- ◆ How do I stop the infection and spread of the malware?
- ◆ How do I stop this infection in the future?

CUSTOMER CONFIDENTIAL



Now that we have a confirmed infected endpoint, how about we start this IR?

ask above questions

Let's answer a few of these really quickly using the bit9 console.

How was I notified of the infection in the first place?

◆ Bit9 Detection ATI's

- Home » Events
- Saved Views >> Threat Indicators

The screenshot shows the Bit9 Detection ATI's interface. At the top, there is a search bar with 'Saved Views: (The Current View Has Unsaved Changes)' and dropdown menus for 'Threat Indicators' (selected), 'Group By: (none)', and 'Max Age: 1 day'. Below the search bar are buttons for 'Show/Hide Filter', 'Show/Hide Columns', 'Export to CSV', 'Access Event Archives', and 'Refresh Page'. A yellow 'Action' button is highlighted. The main table has columns: Timestamp, Updater, Rule Name, Description, and Subtype. One row is shown: 'Dec 5 2013 06:15:47 PM (Indicators) Windows Application Behavior Shell spawned by system process File 'c:\windows\system32\cmd.exe' [62ABE...55EB4] was executed. Report execution (custom rule)'. Below the table, there is a 'Process' section with a table showing 'Source' (WORKGROUP\XPPAR-55DAB9A30) and 'IP Address' (192.168.32.102). The table has columns: User, File Name, File Hash, Installer, Process Prevalence, and File Prevalence. One row is shown: 'XPPAR-55DAB9A30\Administrator cmd.exe 62ABE...55EB4 1 0 0'. At the bottom left is a 'CUSTOMER CONFIDENTIAL' box, and at the bottom right is the Bit9 logo.

Bit9 Detection alerted us of the infection to the XP client. Zeus has a unique behavior that sets off our ‘Shell Spawned by System Process’ ATI.

After checking the “Threat Indicators” View in the console, I notice an alert for a file that I am unaware of. I should probably look into this event further.

explain columns seen here

Initial Triage Scoping

- ◆ Is this a one off infection?
 - yes
- ◆ Is this a campaign?
 - no
- ◆ How many machines are infected?
 - 1
- ◆ When did this happen?
 - Dec 5 2013 06:14:55 PM
- ◆ How long have they been infected?
 - This host was infected between 12/5/13_06:14:55PM-112/5/13_06:41:33PM
 - A total dwell time of ~27 minutes
- ◆ How did I get these metrics?
 - The events page of the console
- ◆ How long did it take me to scope this incident?
 - ~1 minute
- ◆ How can I confirm all of this?
 - Search All File Instances

Find Files

Files with SHA-256: ccd01e5cbbeaa43648d470f1c3e22f8e4cdeacea4db77ee14ae59718b6d4cb5

Action	Date Created	Computer	File Name	Publisher or Company	User Name	Trust	Threat	Local State	Global State
<input type="checkbox"/>	Dec 05 2013 06:05:29PM	WORKGROUP\X99AR-55DAB9A30	zeus_binary_x77721820265009476F025541d4.exe	PressCloud			Banned	Banned	

1 item

Page 1/1

25 rows per page

CUSTOMER CONFIDENTIAL

Bit9

Now that we have been alerted to a suspicious behavior, lets answer some typical IR questions about this event for IR scoping.

go over above questions

We can see from the All File Instance page that this is a one off unique event and we should probably ban the file globally.

Where did the infection come from?

- ◆ A user specified download via the browser
- ◆ How do we know?
 - First seen path:
 - c:\documents and settings\administrator\desktop\zeus_binary_a7772183d2650d9d4f26ffa02fd41d64.exe\
 - Parent process
 - c:\windows\explorer.exe
 - » This means the malware was most likely downloaded as an archive file and executed via double clicking on the executable.
 - Confirmable by looking at agent cache of first seen host
 - Confirmable if you have an archive tracking rule (.zip, .rar, .tar, etc.)
 - » If this was downloaded as an executable and self-executed the parent process would be the application that downloaded the file (browser, email, etc.)

File Details	
General	
First Seen Name:	zeus_binary_a7772183d2650d9d4f26ffa02fd41d64.exe
First Seen Date:	Dec 5 2013 06:06:55 PM
Last Updated:	Dec 5 2013 06:06:55 PM
First Seen Path:	c:\documents and settings\administrator\desktop\zeus_binary_a7772183d2650d9d4f26ffa02fd41d64.exe\

CUSTOMER CONFIDENTIAL



Before I show you how to ban this file, let's discuss where it came from

explain above

How do I stop the infection and spread of the malware?

◆ Global ban

- This is always my first step when finding unknown or suspicious files in my environment
- Why am I not afraid of banning a good file?
 - Files are guilty until proven innocent
 - With Bit9 I can always easily and quickly un-ban a file

The screenshot shows a list of actions taken by the Bit9 agent. The 'Action' column includes options like 'Approve Locally', 'Remove Local Approval', 'Approve Globally', and 'Ban Globally'. The 'Ban Globally' row is highlighted with a red box. The 'Description' column provides details for each action, such as file paths and error messages. The 'Customer Confidential' logo is visible at the bottom left.

Action	Description
Approve Locally	Upload of file 'c:\documents and settings\all users\application data\b9par\logs\vpqr-55dab9a30-diagnostic-20131205-1819020768.zip' from computer 'WORKGROUP\VPQR-55DAB9A30' completed.
Remove Local Approval	B9par_Agent failed a health check. Task was found Total[2] High[0] Medium[0] Low[1] TestError[1] Options[0x00000003] TotalFailure[2]
Approve Globally	B9par_Agent failed a health check. Task was found Total[2] High[0] Medium[0] Low[1] TestError[1] Options[0x00000003] TotalFailure[2]
Ban Globally	Globally ban checked files in all policies admin requested upload of 'Diagnostic' files from computer 'WORKGROUP\VPQR-55DAB9A30'. Agent detected a problem: C:\Windows\System32\userinit.exe is not signed: Error[0x00920099], Severity[Low], Options[0x00000003] TotalFailure[1] Agent detected that certificate 'Adobe Systems Incorporated Digital ID Class 3 - Microsoft Software Validation v2 Flash Player - FORTNIGHT Adobe Systems Incorporated San Jose California US' is valid. Agent detected that certificate 'Symantec Time Stamping Services CA - G1 Symantec Corporation US' is valid. Agent detected that certificate 'VeriSign Class 3 Primary Certification Authority - G3 (*.c) 2006 VeriSign, Inc.' is valid. Dec 5 2013 06:16:14 PM Agent detected that certificate 'Sun Microsystems, Inc.' Sun Microsystems Digital ID Class 3 - Microsoft Software Validation v2 'Sun Microsystems, Inc.' Palo Alto California US' is valid. Dec 5 2013 06:16:14 PM Agent detected that certificate 'VeriSign Class 3 Code Signing 2010 CA Terms of Use at https://www.verisign.com/ipsa ([1]) VeriSign Trust Network, 'VeriSign, Inc.' US' is valid. Dec 5 2013 06:16:14 PM Agent detected that certificate 'Symantec Time Stamping Services Eigner - G4 Symantec Corporation US' is valid. Dec 5 2013 06:16:14 PM Agent detected that certificate 'VeriSign Class 3 Public Primary Certification Authority - G3 (*.c) 2006 VeriSign, Inc.' is valid. Dec 5 2013 06:15:47 PM Computer WORKGROUP\VPQR-55DAB9A30 discovered new file 'c:\documents and settings\administrator\local settings\temp\mpf931ba2.bat' [48F2B...DBCA2]. Dec 5 2013 06:15:47 PM Server discovered new file 'c:\documents and settings\administrator\local settings\temp\mpf931ba2.bat' [48F2B...DBCA2]. Dec 5 2013 06:15:47 PM File 'c:\windows\system\32\cmd.exe' [624BE...358E4] was executed. Dec 5 2013 06:15:48 PM Installation group was created for the file 'c:\documents and settings\administrator\desktop\zeus_binary_a7772183d2650d940f26fa02f441d64.exe' [CC001...D4C85]. Dec 5 2013 06:15:48 PM File 'c:\windows\system\32\cmd.exe' [624BE...358E4] was executed. Dec 5 2013 06:14:56 PM Computer WORKGROUP\VPQR-55DAB9A30 discovered new file 'c:\documents and settings\administrator\applications\odama\pivj.exe' [C1E31...53583]. Dec 5 2013 06:14:56 PM File 'c:\documents and settings\administrator\applications\odama\pivj.exe' [C1E31...53583] was approved because of user response. Dec 5 2013 06:14:56 PM File 'c:\documents and settings\administrator\applications\odama\pivj.exe' [C1E31...53583] was blocked because it was unapproved. Dec 5 2013 06:14:56 PM File 'c:\documents and settings\administrator\applications\odama\pivj.exe' [C1E31...53583] was blocked because it was unapproved. Dec 5 2013 06:13:58 PM Modification of registry 'Vegary\machine\system\controlset01\services\net\parameters\allowServiceAccess' was allowed. Dec 5 2013 06:13:58 PM Modification of registry 'Vegary\machine\system\controlset01\services\net\parameters\allowServiceAccess' was blocked because it was unapproved. Dec 5 2013 06:12:56 PM File 'c:\documents and settings\administrator\desktop\zeus_binary_a7772183d2650d940f26fa02f441d64.exe' [CC001...D4C85] was blocked because it was unapproved.

CUSTOMER CONFIDENTIAL



The simplest and best solution here is to globally ban the file and all other executables associated with the file. Above is me doing this from the console.

How do I stop this infection in the future?

1. Global Bans of known malicious files

Dec 5 2013 06:35:19 PM	Info	Policy Management	File ban created Ban 'zeus_binary_a7772183d2650d9d4f26ffa02fd41d64.exe' for '[CCD01...D4CB5]' was created by 'admin'.
Dec 5 2013 06:35:19 PM	Info	Policy Management	File ban created Ban 'piyj.exe' for '[C1E31...53583]' was created by 'admin'.

2. Raising Enforcement level to automatically block execution of unapproved files

Global block in the console

Timestamp	Priority	Type	Subtype	Source
Dec 5 2013 06:35:19 PM	Notice	Policy Enforcement	Execution block (banned file)	WORKGROUP\XPPAR-55DAB9A30

Description
File 'c:\documents and settings\administrator\desktop\zeus_binary_a7772183d2650d9d4f26ffa02fd41d64.exe' [CCD01...D4CB5] was blocked because it was banned.

Global Block Screen on Medium Enforcement

Global Block Screen on Low Enforcement

CUSTOMER CONFIDENTIAL

Bit9

Now that we have this file banned, we can see from both the console, an endpoint in medium enforcement, and an endpoint in low enforcement that the malware cannot execute any longer.

explain above

Recap

◆ Today we went over

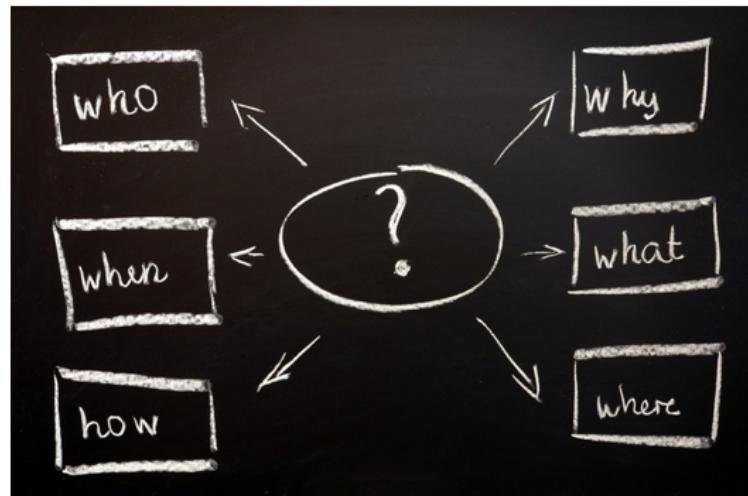
- A few things everyone knows we can do
 - Whitelisting
 - Baseline drift
 - Different enforcement modes
- A few things you may not know Bit9 can do
 - Network Integration (Bit9 Connectors)
 - Detection
- CryptoLocker
 - What is it?
 - How can I stop it using Bit9?
- Zeus
 - What is it?
 - Why do we care?
- IR using Bit9
 - How to find bad behavior using Bit9
 - How different enforcement levels effect your IR
 - How was I notified of the infection in the first place?
 - » Initial Triage Scoping
 - » Is this a one off infection?
 - » Is this a campaign?
 - » How many machines are infected?
 - » When did this happen?
 - » How long have they been infected?
 - » How did I get these metrics?
 - » How long did it take me to scope this incident?
 - Where did the infection come from (browser, email, download, etc.)?
 - How do I stop the infection and spread of the malware?
 - How do I stop this infection in the future?

CUSTOMER CONFIDENTIAL



recap

Questions?



CUSTOMER CONFIDENTIAL

Bit9

questions