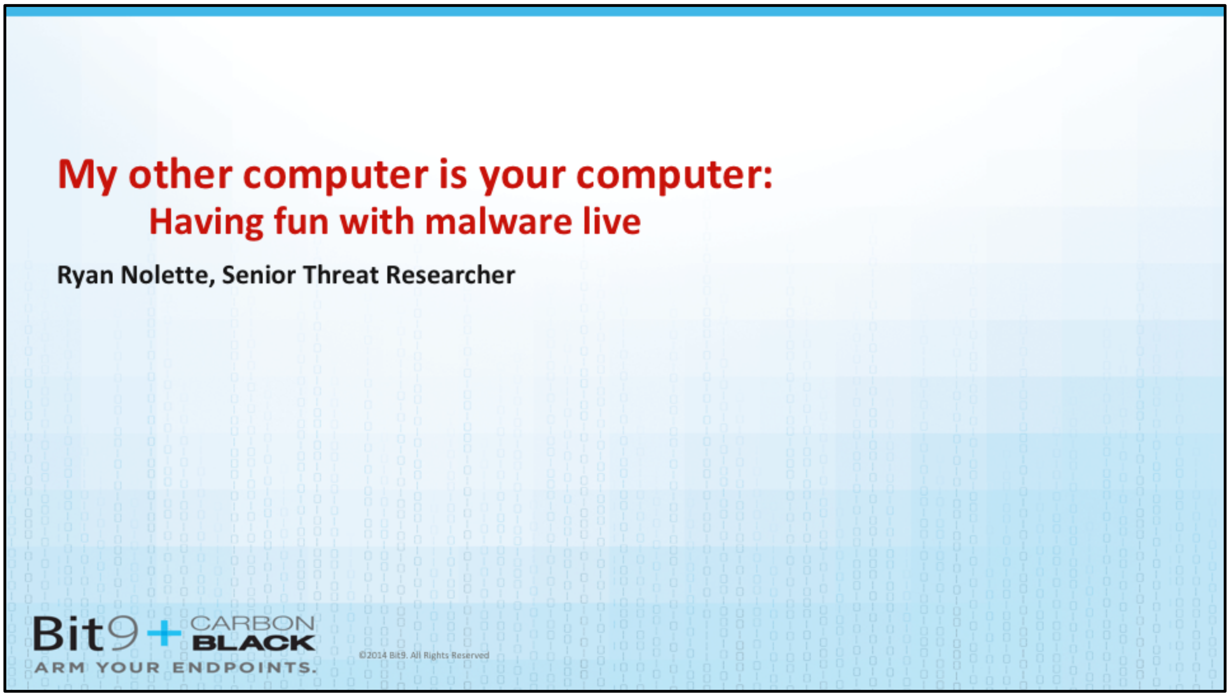
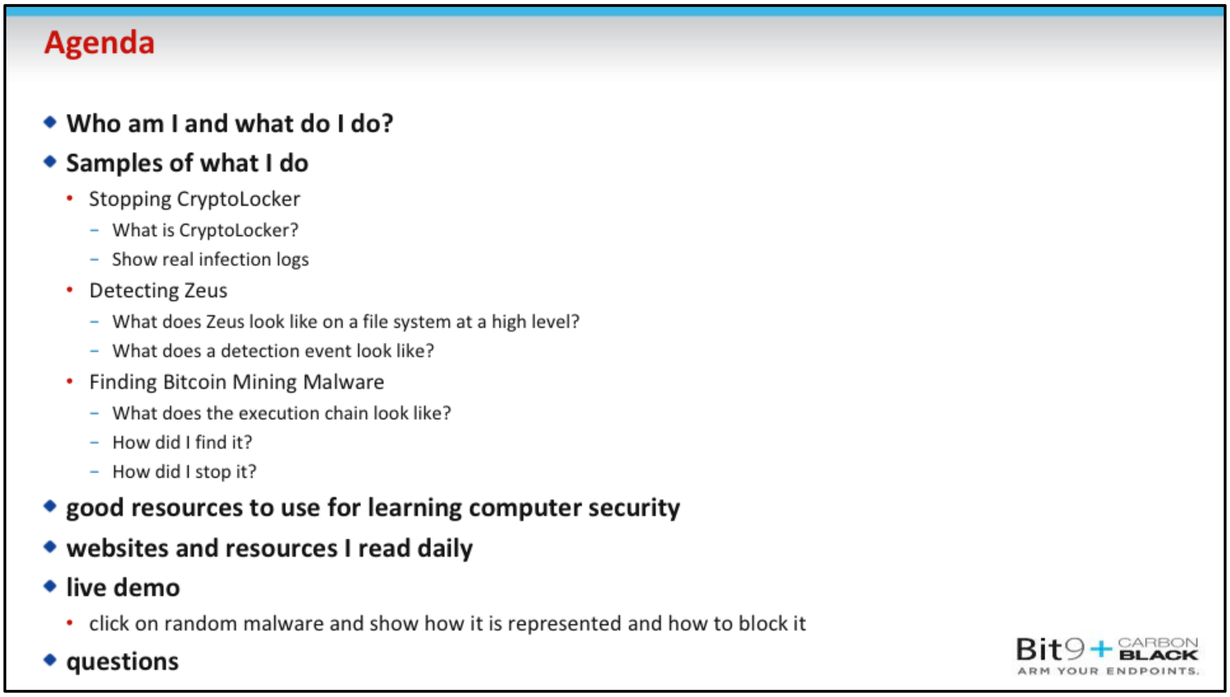


My other computer is your computer:
Having fun with malware live

Ryan Nolette, Senior Threat Researcher

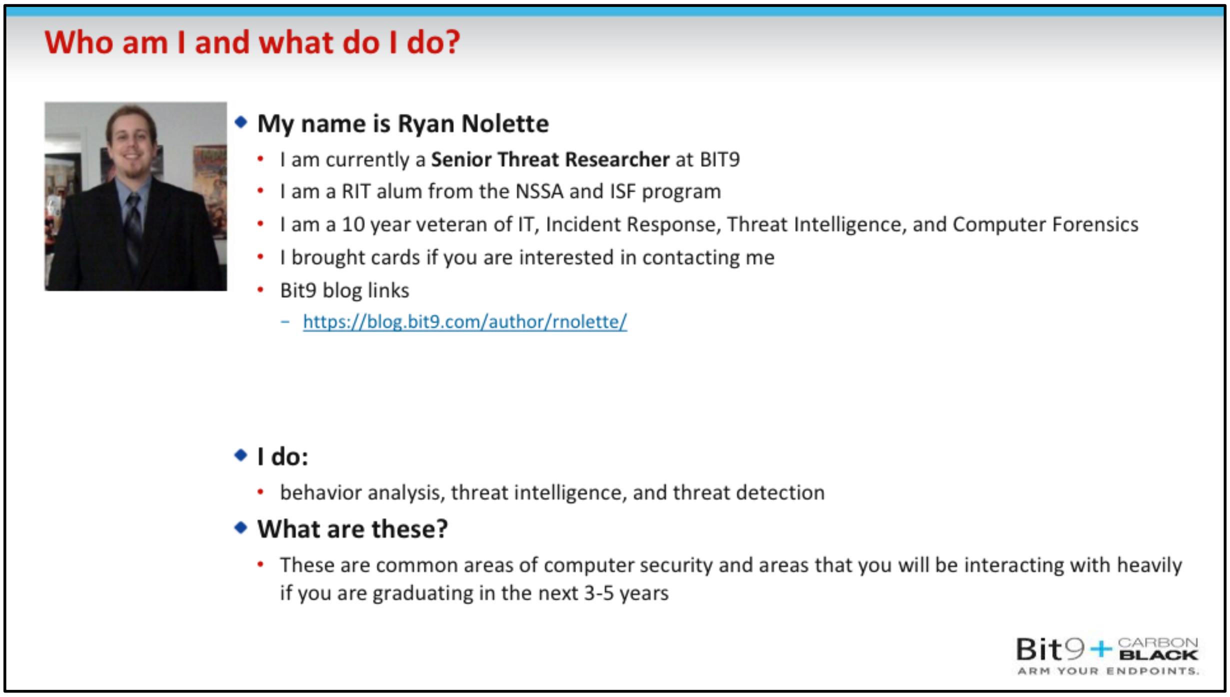
Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.



Agenda

- **Who am I and what do I do?**
- **Samples of what I do**
  - Stopping CryptoLocker
    - What is CryptoLocker?
    - Show real infection logs
  - Detecting Zeus
    - What does Zeus look like on a file system at a high level?
    - What does a detection event look like?
  - Finding Bitcoin Mining Malware
    - What does the execution chain look like?
    - How did I find it?
    - How did I stop it?
- **good resources to use for learning computer security**
- **websites and resources I read daily**
- **live demo**
  - click on random malware and show how it is represented and how to block it
- **questions**

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.



Who am I and what do I do?

- **My name is Ryan Nolette**
  - I am currently a **Senior Threat Researcher** at BIT9
  - I am a RIT alum from the NSSA and ISF program
  - I am a 10 year veteran of IT, Incident Response, Threat Intelligence, and Computer Forensics
  - I brought cards if you are interested in contacting me
  - Bit9 blog links
    - https://blog.bit9.com/author/rnolette/
- **I do:**
  - behavior analysis, threat intelligence, and threat detection
- **What are these?**
  - These are common areas of computer security and areas that you will be interacting with heavily if you are graduating in the next 3-5 years

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

Samples of what I do

- **Bit9**
  - Has 2 primary products that combined create a very useful tool for SecOps and SysAdmins.
    - Bit9
      - Whitelisting
      - Granular protection configuration
      - Ban things from being able to execute by hash, extension, publisher, etc
    - Carbon Black
      - Detection and visibility
      - Ability to leverage many kinds of intelligence feeds to enhance and customize detection

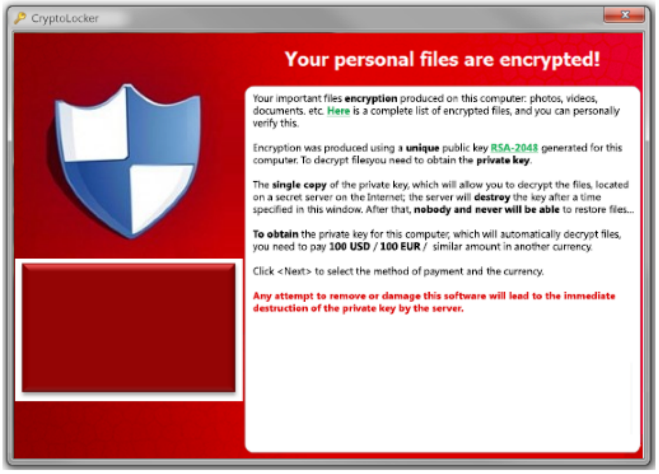
- **My responsibilities**
  - Gather threat intelligence
  - Turn what I learn into actionable information
  - Create behavioral detection rules that customers can use to detect malware

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.

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

What does CryptoLocker look like to the user?



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents. etc. **Here** is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR** / similar amount in another currency.

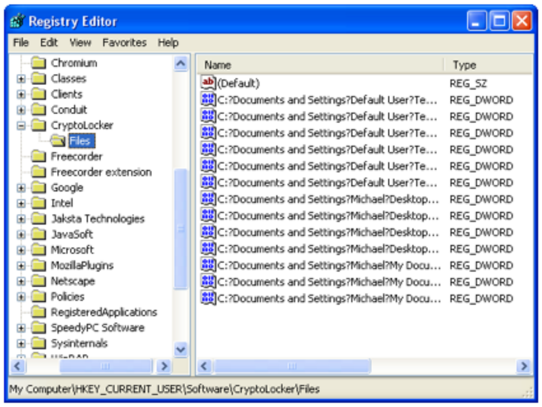
Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

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, *.xlsb, *.xlk, *.ppt, *.pptx, *.pptm, *.mdb, *.accdb, *.pst, *.dwg, *.dxf, *.dxg, *.wpd, *.rtf, *.wb2, *.mdf, *.dbf, *.psd, *.pdd, *.eps, *.ai, *.indd, *.cdr, ????????.jpg, ????????.jpe, img_*.jpg, *.dng, *.3fr, *.arw, *.srf, *.sr2, *.bay, *.crw, *.cr2, *.dcr, *.kdc, *.erf, *.mef, *.mrw, *.nef, *.nrw, *.orf, *.raf, *.raw, *.rwl, *.rw2, *.r3d, *.ptx, *.pef, *.srw, *.x3f, *.der, *.cer, *.crt, *.pem, *.pfx, *.p12, *.p7b, *.p7cThe

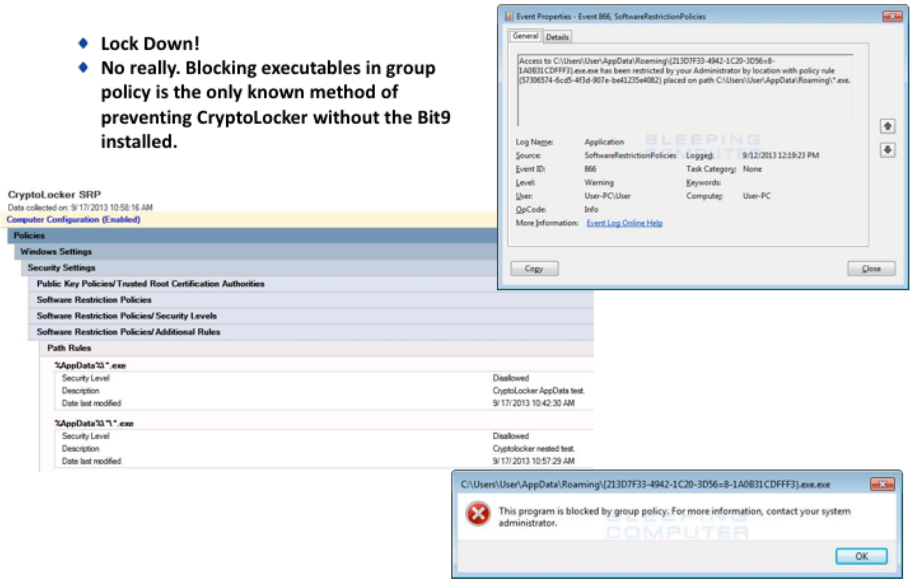


Name	Type
(Default)	REG_SZ
C:?Documents and Settings?Default User?Te...	REG_DWORD
C:?Documents and Settings?Default User?Te...	REG_DWORD
C:?Documents and Settings?Default User?Te...	REG_DWORD
C:?Documents and Settings?Default User?Te...	REG_DWORD
C:?Documents and Settings?Default User?Te...	REG_DWORD
C:?Documents and Settings?Default User?Te...	REG_DWORD
C:?Documents and Settings?Michael?Desktop...	REG_DWORD
C:?Documents and Settings?Michael?Desktop...	REG_DWORD
C:?Documents and Settings?Michael?Desktop...	REG_DWORD
C:?Documents and Settings?Michael?Desktop...	REG_DWORD
C:?Documents and Settings?Michael?My Docu...	REG_DWORD
C:?Documents and Settings?Michael?My Docu...	REG_DWORD
C:?Documents and Settings?Michael?My Docu...	REG_DWORD

My Computer\HKEY_CURRENT_USER\Software\CryptoLocker\Files

How do I stop CryptoLocker?

- Lock Down!
- No really. Blocking executables in group policy is the only known method of preventing CryptoLocker without the Bit9 installed.



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
Description	CryptoLocker AppData test.
Date last modified	9/17/2013 10:42:30 AM

%AppData%**.exe

Security Level	Disallowed
Description	Cryptolocker nested test.
Date last modified	9/17/2013 10:57:29 AM

Event Properties - Event 866, SoftwareRestrictionPolicies

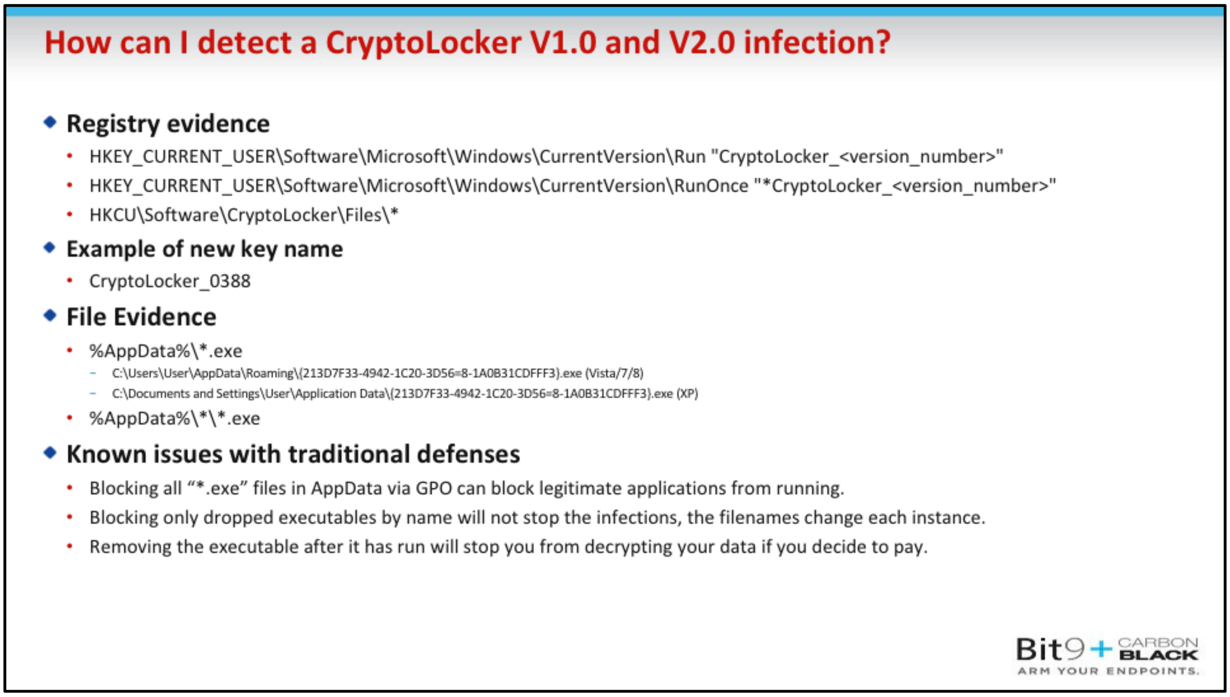
```
Access to C:\Users\User\AppData\Roaming\{213D7F33-4942-1C20-3D56=8-
1A0B31CDFFF3}.exe.exe has been restricted by your Administrator by location with policy rule
{57306574-6cd5-4f3d-907e-be41235e4082} placed on path C:\Users\User\AppData\Roaming\*.exe.
```

Log Name:	Application		
Source:	SoftwareRestrictionPolicies	Logged:	9/12/2013 12:19:23 PM
Event ID:	866	Task Category:	None
Level:	Warning	Keywords:	
User:	User-PC\User	Computer:	User-PC
OpCode:	Info		
More Information:	Event Log Online Help		

C:\Users\User\AppData\Roaming\{213D7F33-4942-1C20-3D56=8-1A0B31CDFFF3}.exe.exe

This program is blocked by group policy. For more information, contact your system administrator.

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

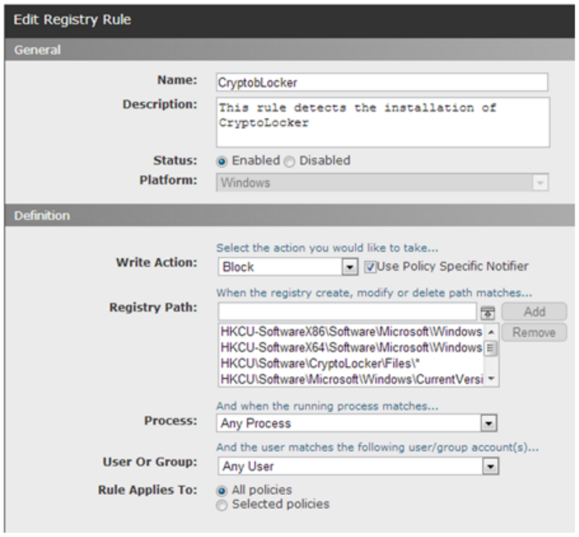


How can I detect a CryptoLocker V1.0 and V2.0 infection?

- **Registry evidence**
  - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "CryptoLocker_<version_number>"
  - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "*CryptoLocker_<version_number>"
  - HKCU\Software\CryptoLocker\Files\*
- **Example of new key name**
  - CryptoLocker_0388
- **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.

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

CryptoBlocker in console



Edit Registry Rule

General

Name: CryptobLocker

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:
```
HKCU-SoftwareX86\Software\Microsoft\Windows
HKCU-SoftwareX64\Software\Microsoft\Windows
HKCU\Software\CryptoLocker\Files\*
HKCU\Software\Microsoft\Windows\CurrentVersi
```

And when the running process matches...

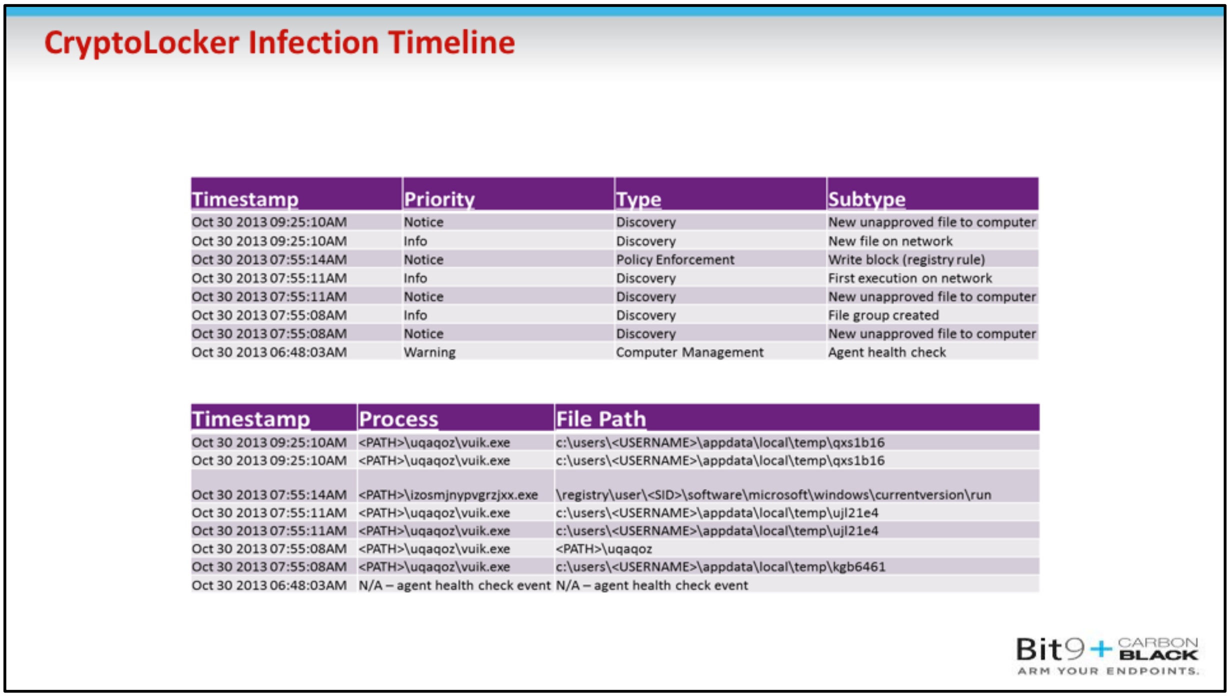
Process: Any Process

And the user matches the following user/group account(s)...

User Or Group: Any User

Rule Applies To: ● All policies ○ Selected policies

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

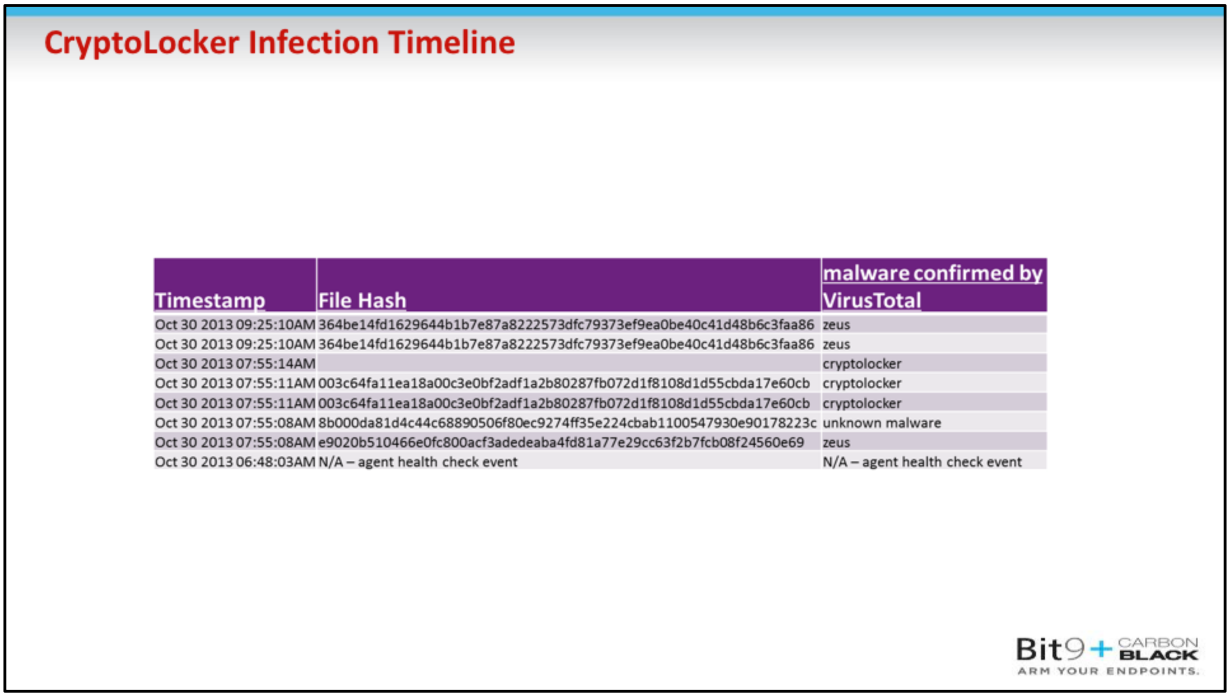


CryptoLocker Infection Timeline

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>\izosmjnypvgrzjxx.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\ujl21e4
Oct 30 2013 07:55:11AM	<PATH>\uqaqoz\vuik.exe	c:\users\<USERNAME>\appdata\local\temp\ujl21e4
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

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.



CryptoLocker Infection Timeline

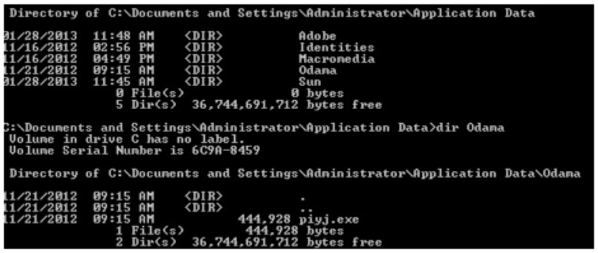
Timestamp	File Hash	malware confirmed by VirusTotal
Oct 30 2013 09:25:10AM	364be14fd1629644b1b7e87a8222573dfc79373ef9ea0be40c41d48b6c3faa86	zeus
Oct 30 2013 09:25:10AM	364be14fd1629644b1b7e87a8222573dfc79373ef9ea0be40c41d48b6c3faa86	zeus
Oct 30 2013 07:55:14AM		cryptolocker
Oct 30 2013 07:55:11AM	003c64fa11ea18a00c3e0bf2adf1a2b80287fb072d1f8108d1d55cbda17e60cb	cryptolocker
Oct 30 2013 07:55:11AM	003c64fa11ea18a00c3e0bf2adf1a2b80287fb072d1f8108d1d55cbda17e60cb	cryptolocker
Oct 30 2013 07:55:08AM	8b000da81d4c44c68890506f80ec9274ff35e224cbab1100547930e90178223c	unknown malware
Oct 30 2013 07:55:08AM	e9020b510466e0fc800acf3adedeaba4fd81a77e29cc63f2b7fcb08f24560e69	zeus
Oct 30 2013 06:48:03AM	N/A – agent health check event	N/A – agent health check event

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

What can I do about a Zeus infection?

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.



```
 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
11/16/2012  04:49 PM    <DIR>          Macromedia
11/21/2012  09:15 AM    <DIR>          Odama
01/28/2013  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 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 piyj.exe
               1 File(s)        444,928 bytes
               2 Dir(s)  36,744,691,712 bytes free
```

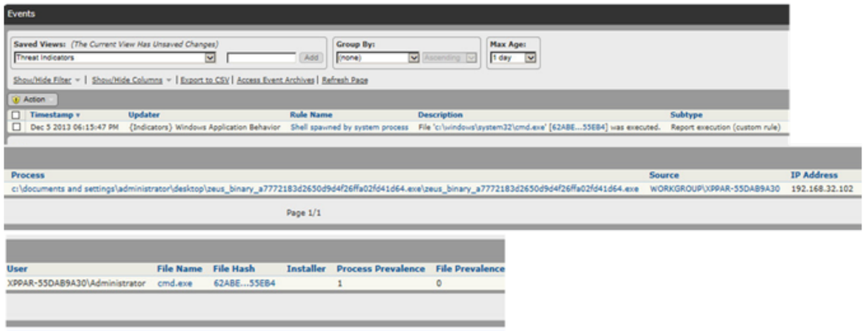
What Does Zeus do?

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

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

Zeus Is Often Paired with CryptoLocker

- Detection rule I wrote that detects Zeus installation



Events

Saved Views: *(The Current View Has Unsaved Changes)* Threat Indicators

Group By: (none) Ascending

Max Age: 1 day

Add
Show/Hide Filter | Show/Hide Columns | Export to CSV | Access Event Archives | Refresh Page
Action

□	Timestamp ▾	Updater	Rule Name	Description	Subtype
□	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)

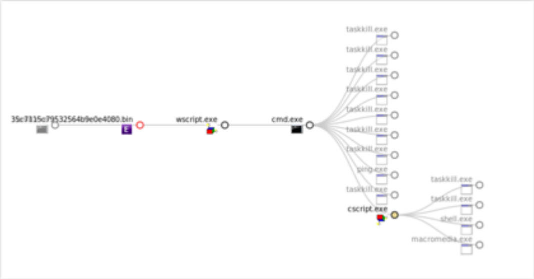
Process	Source	IP Address
c:\documents and settings\administrator\desktop\zeus_binary_a7772183d2650d9d4f26ffa02fd41d64.exe\zeus_binary_a7772183d2650d9d4f26ffa02fd41d64.exe	WORKGROUP\XPPAR-55DAB9A30	192.168.32.102

Page 1/1

User	File Name	File Hash	Installer	Process Prevalence	File Prevalence
XPPAR-55DAB9A30\Administrator	cmd.exe	62ABE...55EB4		1	0

Finding Bitcoin Mining Malware

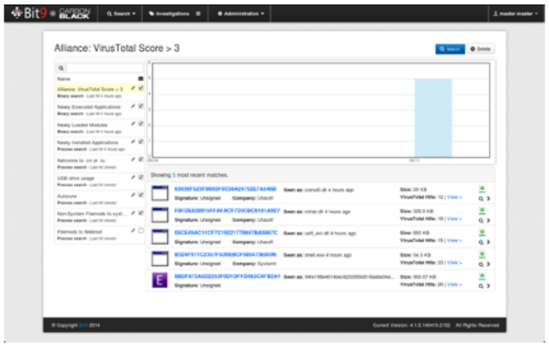
What does the execution chain look like?



- From the Carbon Black process analysis of the file "94fe198e4614bec6233585d518adde34a01dc0a35c7115c79532564b9e0e4080.bin" we are able to see it spawn of the processes: Wscript.exe, Cmd.exe, Taskkill.exe, Cscript.exe, Ping.exe
- If we then drill into each of these child processes we can see that "csscript.exe" spawned 3 processes: Taskkill.exe, Shell.exe, Macromedia.exe

How did I find it?

- Right away I can see 5 matches for files in my environment that have a VirusTotal rating of 4 or more.



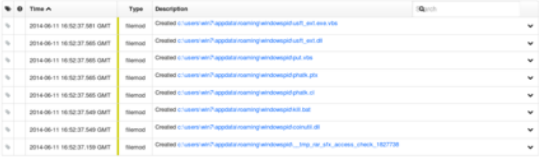
Alliance: VirusTotal Score > 3

Showing 5 most recent matches.

Finding Bitcoin Mining Malware

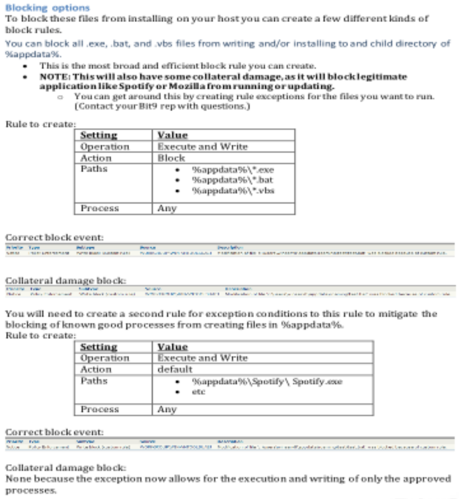
What did it do?

- According to the analysis page the above snippet is just the tip of the iceberg. There were 1805 file modifications, 63 module loads, 4 registry modifications, and 2 child processes spawned just from this file alone. These counts do not include everything done by the child processes spawned.



Time ^	Type	Description
2014-06-11 16:52:37.581 GMT	filemod	Created c:\users\win7\appdata\roaming\windowspid\usft_ext.exe.vbs
2014-06-11 16:52:37.565 GMT	filemod	Created c:\users\win7\appdata\roaming\windowspid\usft_ext.dll
2014-06-11 16:52:37.565 GMT	filemod	Created c:\users\win7\appdata\roaming\windowspid\put.vbs
2014-06-11 16:52:37.565 GMT	filemod	Created c:\users\win7\appdata\roaming\windowspid\phatk.ptx
2014-06-11 16:52:37.565 GMT	filemod	Created c:\users\win7\appdata\roaming\windowspid\phatk.cl
2014-06-11 16:52:37.549 GMT	filemod	Created c:\users\win7\appdata\roaming\windowspid\kill.bat
2014-06-11 16:52:37.549 GMT	filemod	Created c:\users\win7\appdata\roaming\windowspid\coinutil.dll
2014-06-11 16:52:37.159 GMT	filemod	Created c:\users\win7\appdata\roaming\windowspid\__tmp_rar_sfx_access_check_1827738

How did I stop it?



Blocking options

To block these files from installing on your host you can create a few different kinds of block rules.

You can block all .exe, .bat, and .vbs files from writing and/or installing to and child directory of %appdata%.

- This is the most broad and efficient block rule you can create.
- **NOTE: This will also have some collateral damage, as it will block legitimate application like Spotify or Mozilla from running or updating.**
    - You can get around this by creating rule exceptions for the files you want to run. (Contact your Bit9 rep with questions.)

Rule to create:

Setting	Value
Operation	Execute and Write
Action	Block
Paths	• %appdata%*.exe • %appdata%*.bat • %appdata%*.vbs
Process	Any

Correct block event:

[illegible]

Collateral damage block:

[illegible]

You will need to create a second rule for exception conditions to this rule to mitigate the blocking of known good processes from creating files in %appdata%.
Rule to create:

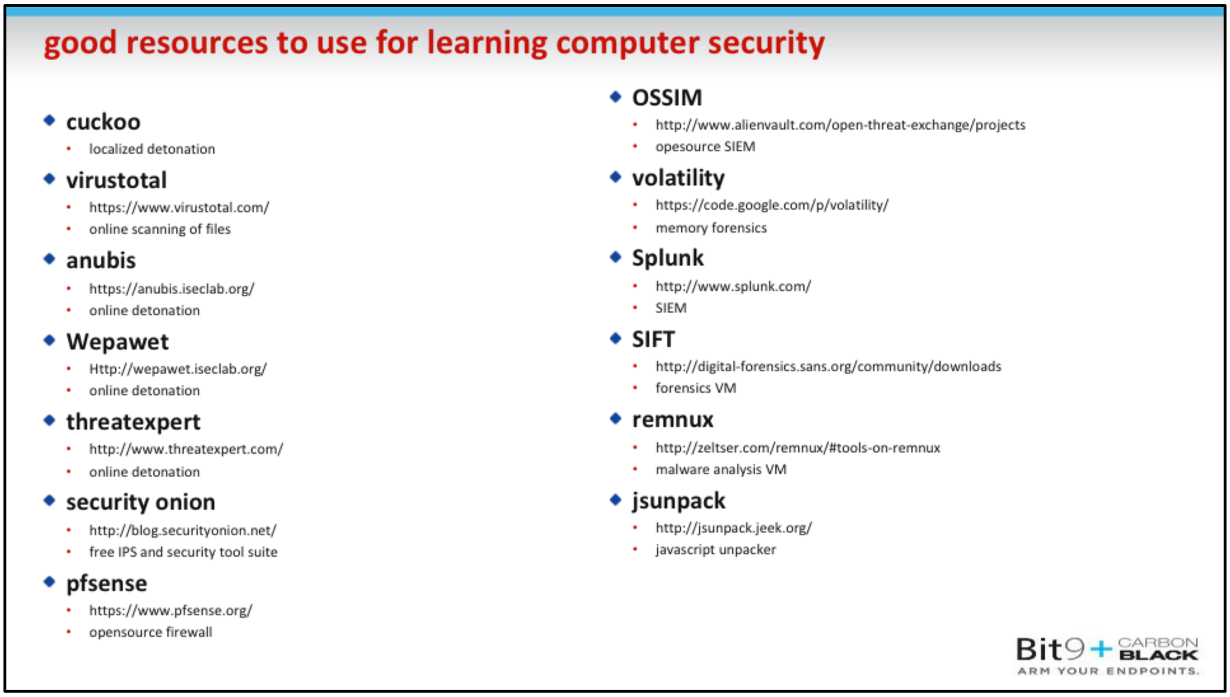
Setting	Value
Operation	Execute and Write
Action	default
Paths	• %appdata%\Spotify\ Spotify.exe • etc
Process	Any

Correct block event:

[illegible]

Collateral damage block:
None because the exception now allows for the execution and writing of only the approved processes.

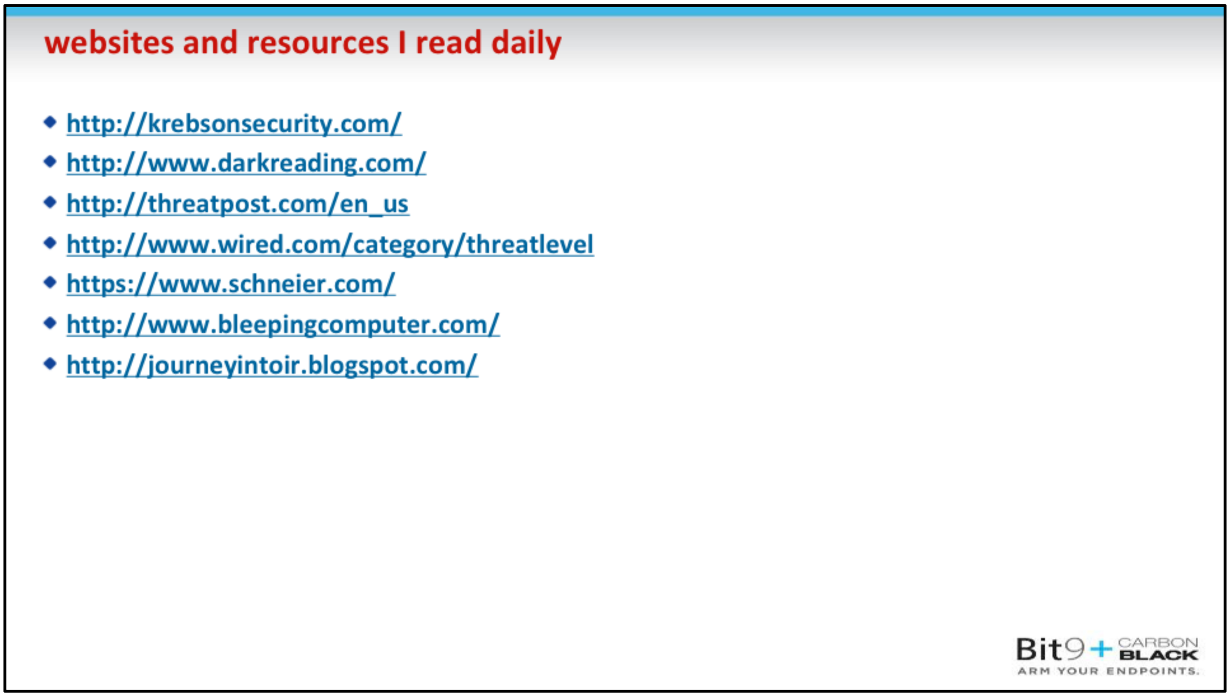
ARM YOUR ENDPOINTS.



good resources to use for learning computer security

- **cuckoo**
  - localized detonation
- **virustotal**
  - https://www.virustotal.com/
  - online scanning of files
- **anubis**
  - https://anubis.iseclab.org/
  - online detonation
- **Wepawet**
  - Http://wepawet.iseclab.org/
  - online detonation
- **threatexpert**
  - http://www.threatexpert.com/
  - online detonation
- **security onion**
  - http://blog.securityonion.net/
  - free IPS and security tool suite
- **pfsense**
  - https://www.pfsense.org/
  - opensource firewall
- **OSSIM**
  - http://www.alienvault.com/open-threat-exchange/projects
  - opesource SIEM
- **volatility**
  - https://code.google.com/p/volatility/
  - memory forensics
- **Splunk**
  - http://www.splunk.com/
  - SIEM
- **SIFT**
  - http://digital-forensics.sans.org/community/downloads
  - forensics VM
- **remnux**
  - http://zeltser.com/remnux/#tools-on-remnux
  - malware analysis VM
- **jsunpack**
  - http://jsunpack.jeek.org/
  - javascript unpacker

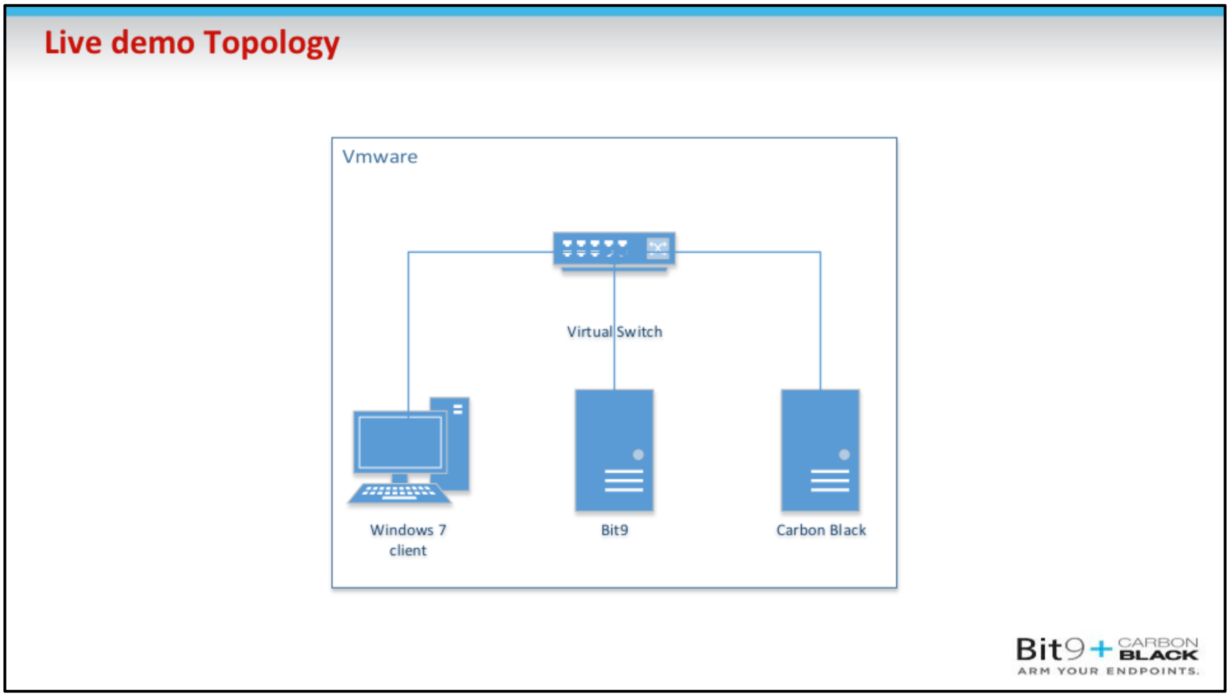
Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.



websites and resources I read daily

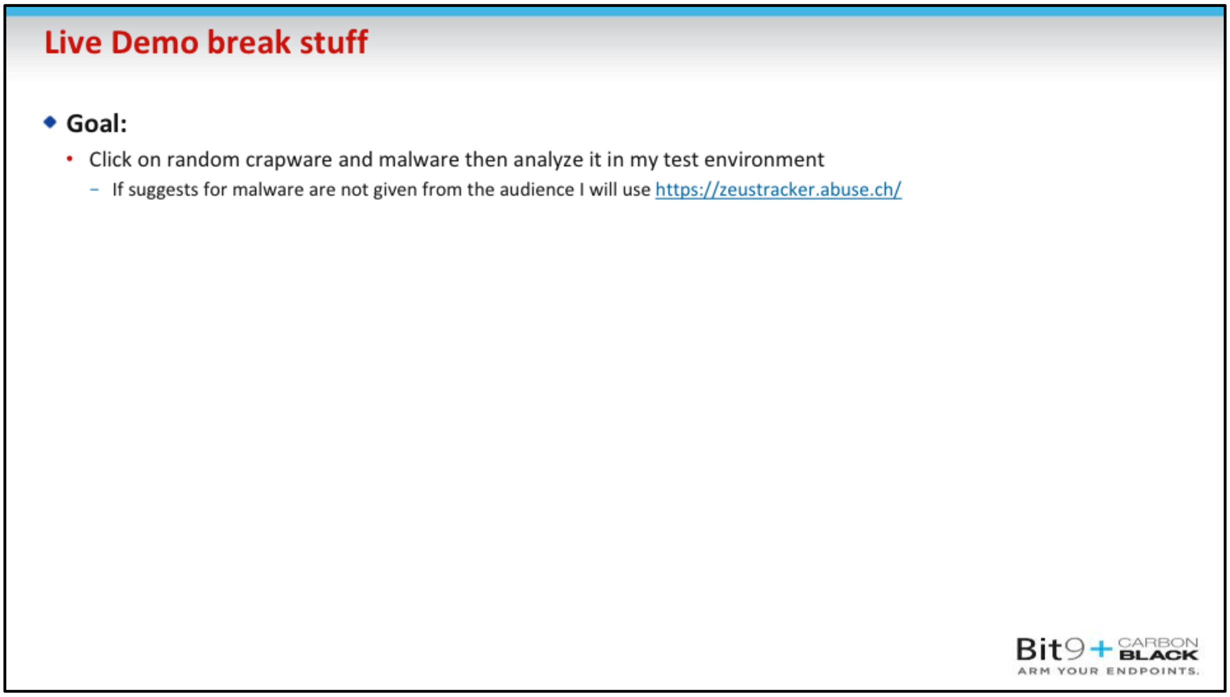
- http://krebsonsecurity.com/
- http://www.darkreading.com/
- http://threatpost.com/en_us
- http://www.wired.com/category/threatlevel
- https://www.schneier.com/
- http://www.bleepingcomputer.com/
- http://journeyintoir.blogspot.com/

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.



Live demo Topology

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.



Live Demo break stuff

- **Goal:**
  - Click on random crapware and malware then analyze it in my test environment
    - If suggests for malware are not given from the audience I will use https://zeustracker.abuse.ch/

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

Questions?

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.