



Using Indicators of Compromise to Find Evil and Fight Crime

GFIRST
August 11, 2011



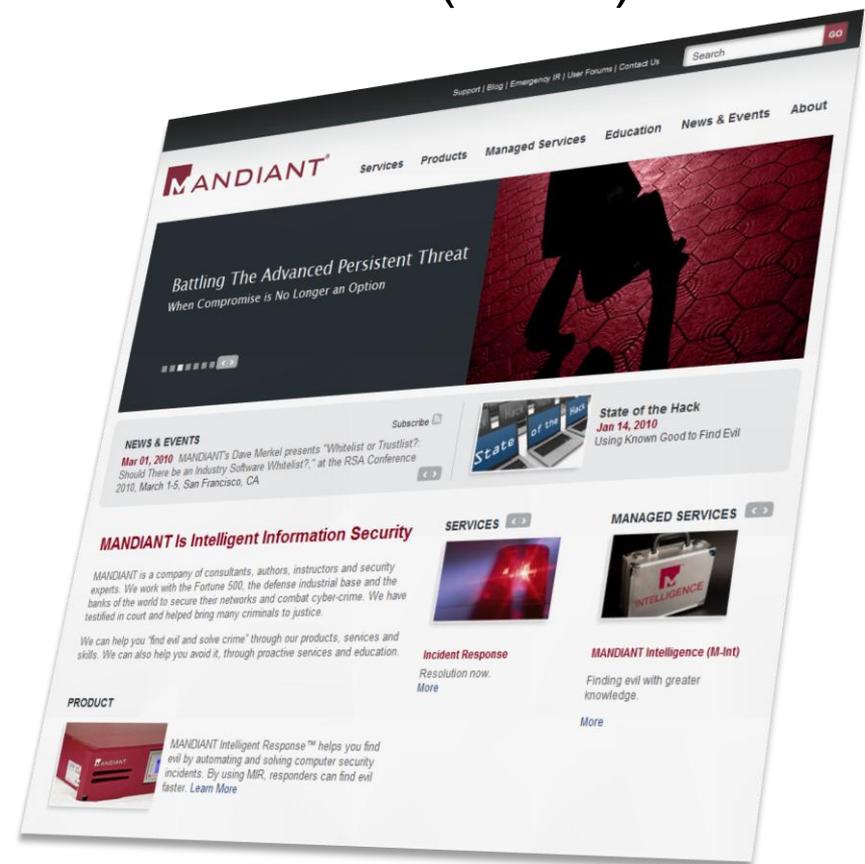
- “Old School” Incident Response

- Introduction to Indicators of Compromise (IOCs)
 - and OpenIOC

- OpenIOC based Incident Response Case Study

- Wrapping Up

- “Find Evil, Solve Crime.”
- VISA Qualified Incident Response Assessor (QIRA)
- APT and CDT experts
- Located in
 - Washington
 - New York
 - Los Angeles
 - San Francisco
 - Reston, VA
- Services, software, and education



Our Team: Industry Leaders



- 10 years average information security experience
- Over 50% of consultants hold “Top Secret” clearances
- 9 security books authored or co-authored
- 10% testified as subject matter experts

Books



Articles and interviews



Presentations



David Ross

- Technical Director
 - Managed Services
- Enterprise IR Specialist
 - The bigger, the better
- Created OpenIOC
- Responded to over a half million hosts
 - Last year alone

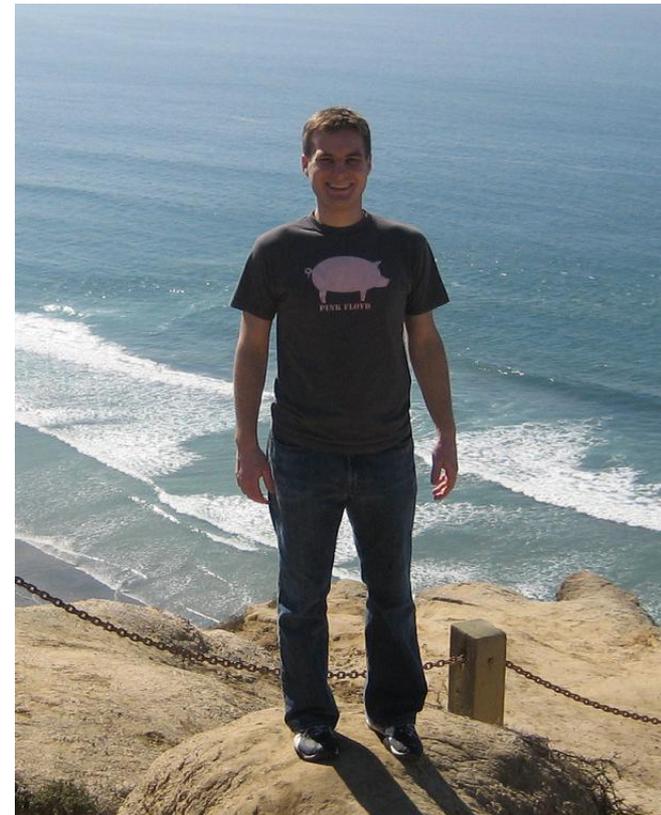


Chris Bream

- Manager / Operations Lead
 - Managed Services

- Six years of Federal information security auditing
 - Used to recite FISMA in his sleep

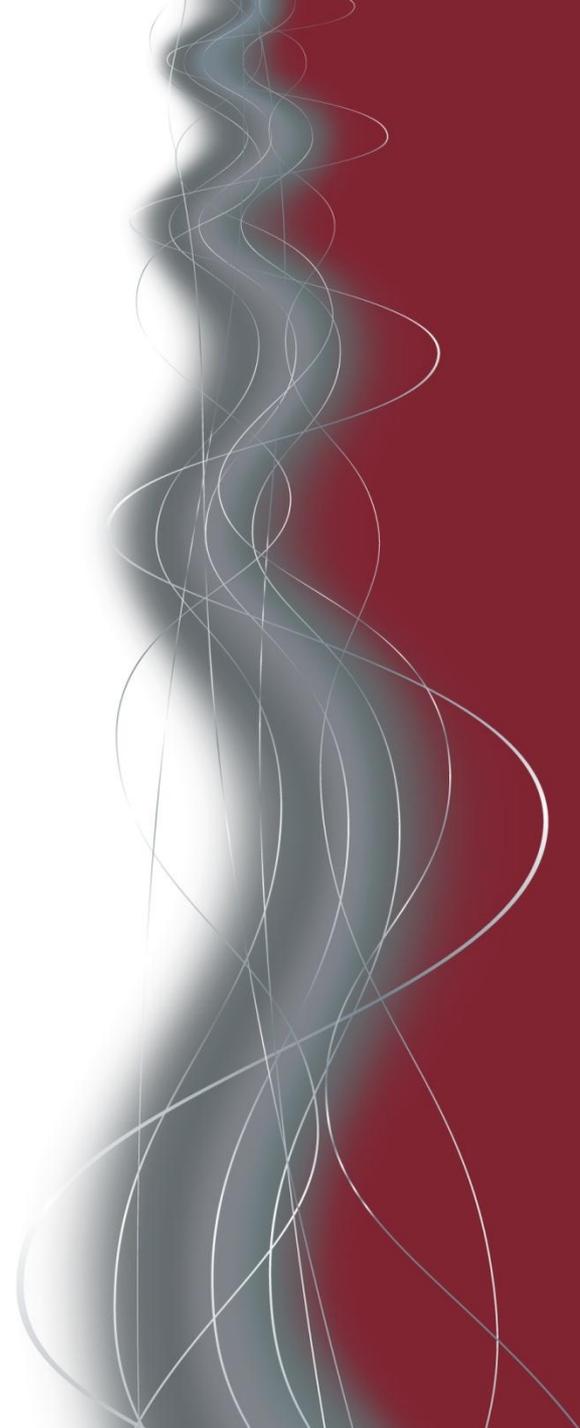
- SysAdmin background



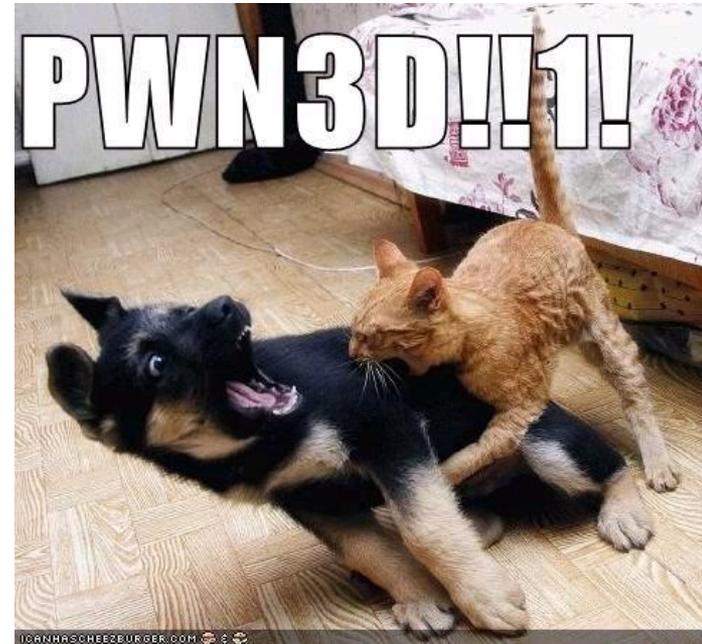
All information is derived
from MANDIANT observations
in unclassified environments.

Some information has been sanitized to
protect our clients' interests.

“Old School” Incident Response

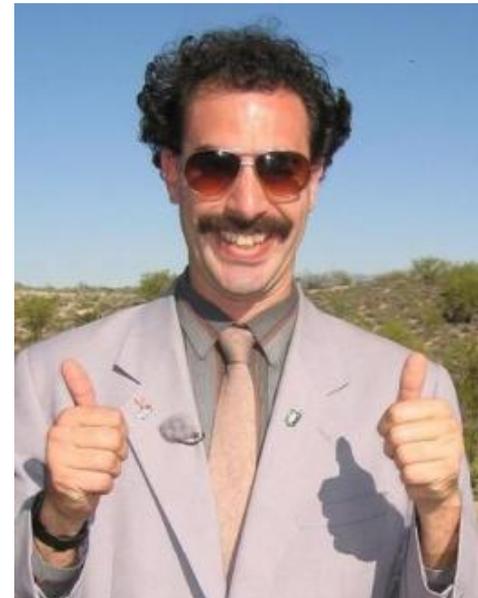


- Law enforcement notifies your agency or company
 - One specific system is compromised
 - Out of 30,000 systems in your enterprise
 - No further details
- Where do you start?
- How do you identify the malware?
- How do you identify malware variants?
- How do you tell other people how to find the malware?



- Hard drive forensics
 - Acquire system
 - Forensic processing
 - Identify malware and attacker activity
- Software management/inventory tool for suspicious files
- Historical log analysis
- Submit malware samples to anti-virus vendor
- Block malicious network traffic

- Reverse engineer malware
 - Identify two bad C2 domain names
- Search network logs traffic to C2 domains
- Use software management tool to search for evil filenames and MD5s
- No new systems found
- Case Closed...Great Success!



- Analyst missed malware on a host
 - Did not have the latest indicators
- Network engineers missed a compromised host
 - Static on conference line so they **misheard** a subdomain
- Attackers returned using C2 from last month
 - Listed in a text file on someone's desktop
- Analyst missed attacker in activity in event log
 - Fat-fingered an event message when searching

- Full timeline of events
- In-depth forensic analysis
 - Keyword searching
 - Search unallocated space
 - Identify deleted data files involved in theft
- Effective at finding malware on an individual basis

- Difficult to codify and share information
 - Massive lists of information in various formats/repositories
 - Inconsistent understanding of compromise across teams
 - Inconsistent analysis of hosts
- Difficult to maintain information for later
- Information provides no context
- Many tools that actually store information are in a proprietary format

FAIL

Lists lose relevance

You can't determine why you were looking for the keyword, or what else is related to that keyword.

Lists are too rigid

Need to look for a new keyword type? You need to make a new list.

Introduction to Indicators of Compromise (IOCs) and OpenIOC



Indicator of Compromise

- Raw Intelligence
 - MD5s
 - File names
 - Packer types
 - Registry keys
 - Mutexes
 - DNS strings
 - IP Addresses

OpenIOC

- Organized Intelligence
 - Highly Tactical
 - Logically grouped
 - Extendable
 - Built in XML

What can IOCs describe?

- Anything!
 - Malware
 - File attributes
 - Registry attributes
 - Process attributes
 - Network attributes
 - Persistence Methods
 - Tactics and Techniques
 - The color of your shirt and the length of your shoelaces!

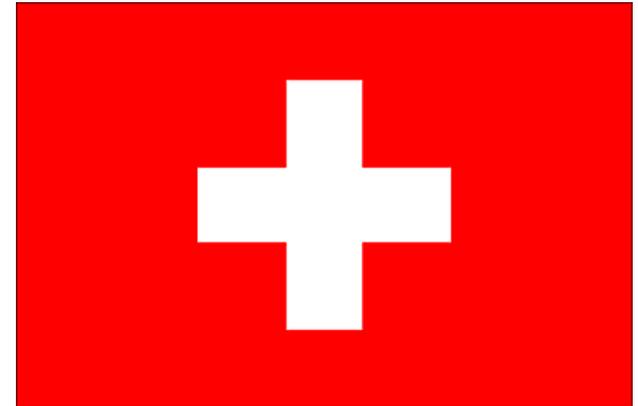
- Provides Context by including metadata



Why did we create OpenIOC?

- Recognized gap in intelligence sharing
 - Hard to capture and share intelligence internally
 - Impossible to capture and share intelligence externally
- One format for any platform
- Turn data into intelligence
 - Provide context, not just information
- Eliminate lists!!
- Provide an open standard to share data
 - This was an after thought, actually.

- Does not require any product
- Easily converts to needed formats
 - Xpath
 - Lucene
 - Word reports
 - Pie charts
 - 'grep lists'
 - It is just XML
- Easy to create and edit with IOCe™



http://www.mandiant.com/products/free_software/ioce/

The screenshot shows the IOCe 2.1.100 application window. The left pane displays a list of indicators with columns for Name and GUID. The 'WIRE (BACKDOOR)' indicator is selected. The right pane shows the details for this indicator, including its Name, Author (Mandiant), GUID, and a detailed description. Below the description, the 'Definition' section shows a complex logical expression for the indicator's detection rules.

Name	GUID
UPS (BACKDOOR)	923ad6a8-8e18-4857-
UPS (BACKDOOR)	92aba776-c7bd-4182-
UPS (BACKDOOR)	93919b00-6fca-4000-t
UPS (BACKDOOR)	a9fd1e0f-8157-45ab-9
UPS (BACKDOOR)	c4a3e76c-99ef-47de-e
UPS (BACKDOOR)	c4e849be-801a-419f-f
UPS (BACKDOOR)	d7b04d9d-0b70-41bb-
UPS (BACKDOOR)	ebaae701-e40c-454c-
UPS (UNKNOWN)	75c63169-32f7-476e-t
W32TIMESVC (BACKDOO...	17c2a4c9-7f35-4c48-f
WIADBYLD (GINA REPL...	964d3df4-a537-4be0-f
WINCTL (KEYLOGGER)	d5c6e568-8acc-491a-
WINDBGCONFG (BACKD...	1bfd8ef5-e8d4-4d75-9
WINDOWS (BACKDOOR)	0a0c7038-8e98-4d23-
WININSTALLER (BACKD...	7efe63c5-5ad6-4fab-9
WINML32 (BACKDOOR)	75ece49b-b2c3-43d4-
WINNETM (BACKDOOR)	ef4663bc-cd6e-4f6d-8
WINSK (BACKDOOR)	8a2bf01b-cfa0-477a-a
WINSRV32 (UNKNOWN)	6f7e285d-3992-4f46-9
WINSYS3 (DOWNLOADER)	331de78b-26cb-496-f
WINZF32 (BACKDOOR)	99b7829-1a62-4b91-f
WIRE (BACKDOOR)	5fb6558a-c78e-4ac1-
WMDMSVC (BACKDOOR)	2d80b2f2-d7ab-485e-f
WSDBG (BACKDOOR)	f0c43bff-df2e-4298-b0
WUAUCLT (BACKDOOR)	e47827f5-d022-4156-t
WWW (UNKNOWN)	bfa86294-3537-4663-t
Y29 (BACKDOOR)	9b24b25f-03b4-4038-e
Y29 (BACKDOOR)	9fcfb253-767c-41d8-b
Y29 (BACKDOOR)	dbde89a6-2879-400f-e
Y29 (DOWNLOADER)	a686fa30-792a-4d63-e

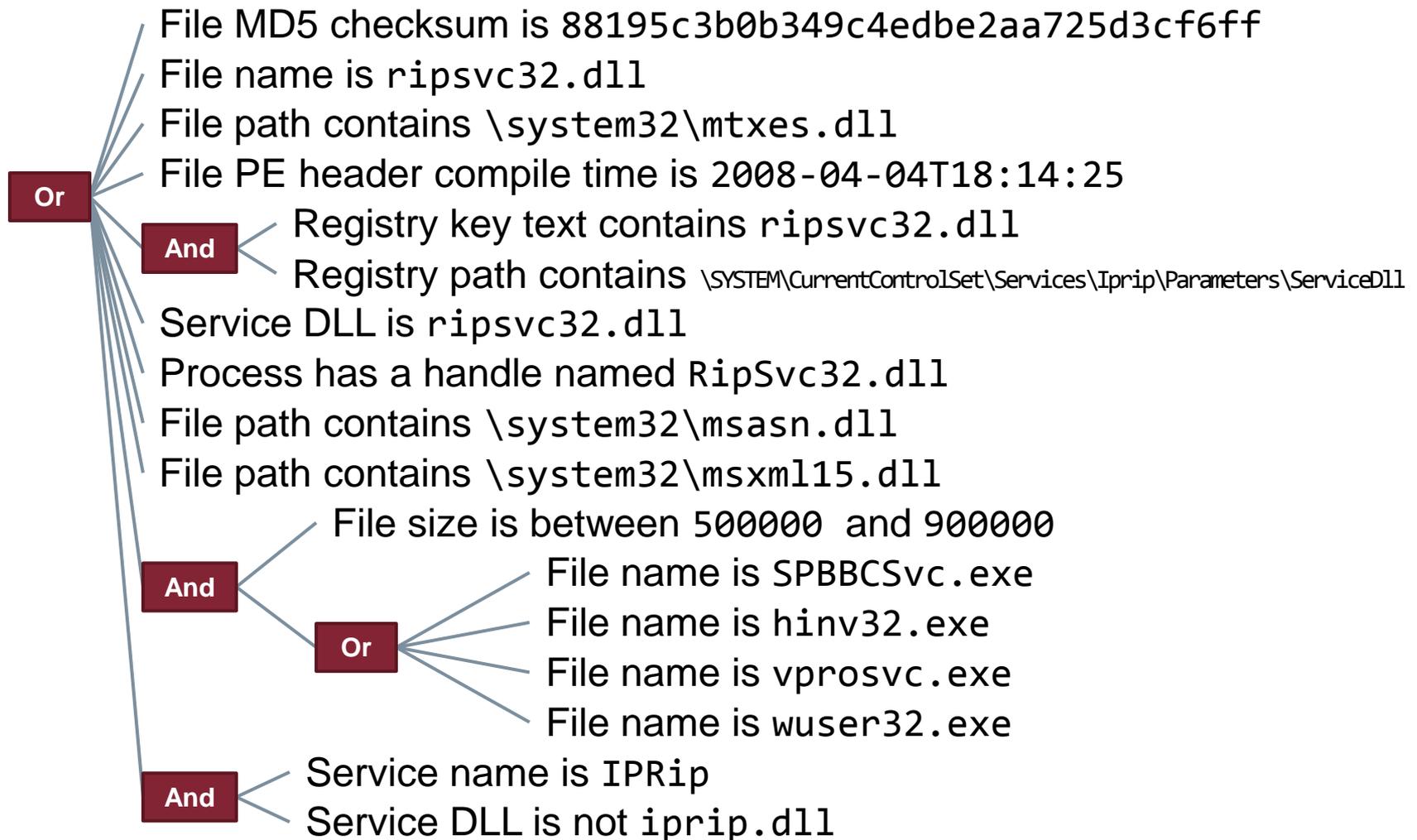
Name: WIRE (BACKDOOR)
Author: Mandiant
GUID: 5fb6558a-c78e-4ac1-8fb9-624df871f

Type: threatgroup
Reference: APT
comment: Converted from SignatureList

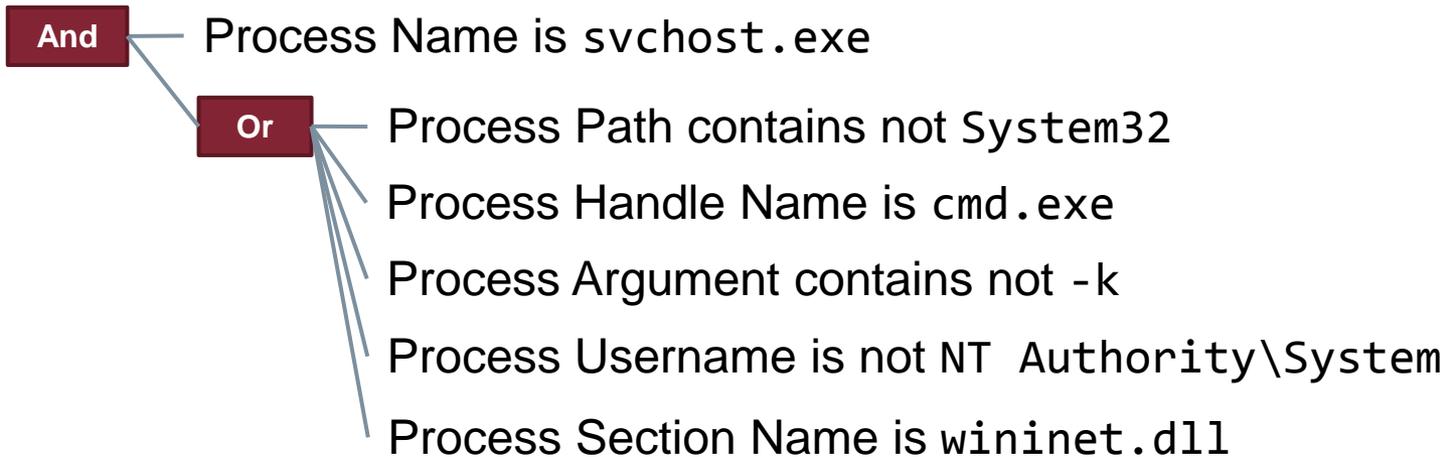
Description:
This malware is a persistent, HTTP-based reverse backdoor. The sample obtained by Mandiant was named wire.scr but the malware will install itself as wks.exe. It persists on a compromised host through registry modifications. It communicates via HTTP. The malware can upload and download files, install additional malware and execute programs.

Add: Definition:
Registry Path contains \SOFTWARE\myid
Registry Path contains \SOFTWARE\thel
Registry Path contains \SOFTWARE\Microsoft\Windows\CurrentV
Registry Path contains \SOFTWARE\Microsoft\Windows\CurrentV
Registry Path contains \SOFTWARE\Microsoft\Windows\CurrentV
Registry Path contains \SOFTWARE\Microsoft\Windows\CurrentV
Process Handle Name is Windows32KernelStart
AND
File Name is wire.scr
OR
File Compile Time contains 1992-06-19T22:22:17Z
File Size is 58368
AND
File Name is invoice.scr
OR
File Size is 59904
File Compile Time contains 1992-06-19T22:22:17Z
AND
Registry Path contains Microsoft\Windows\CurrentVersion\i
Registry Text is 0

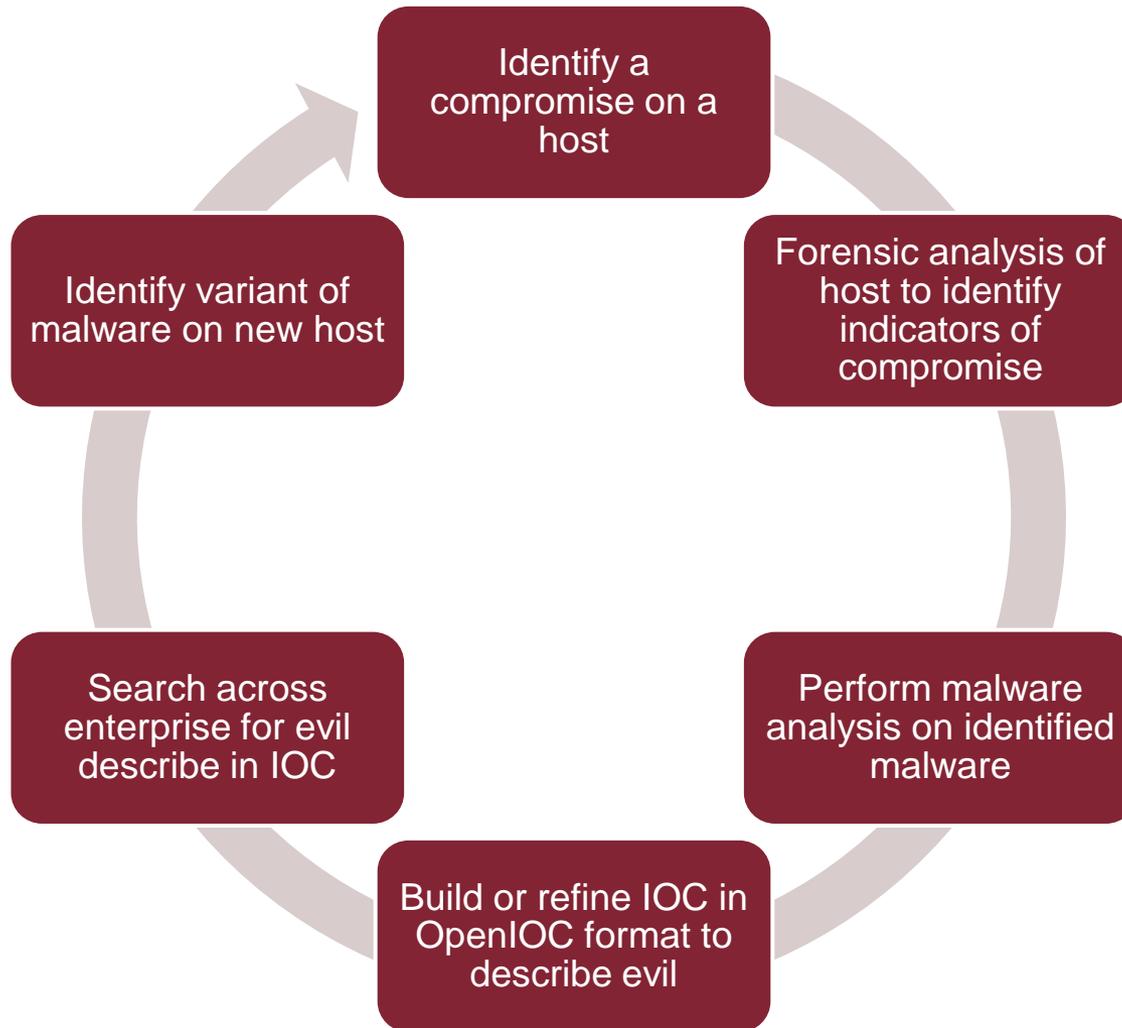
What does an IOC look like?



- “When you see svchost.exe running out of something other than ‘system32’ or it doesn’t have that dash k at the end or it’s not being run as System or...”



How do we create IOCs?



OpenIOC IR Case Study

ORGANIZATION A

- ~ 6,000 endpoints
- Detected malicious activity
- Analyzed initial data based on detection
- Needed to understand scope of the problem

ORGANIZATION B

- ~ 12,000 endpoints
- Notified by law enforcement about one compromise
- Entered Mandiant Managed Service
- Fighting initial compromise
- Managed service identified additional compromise
- Round 2, fight!

Organization A, you've got malware!

- Forensic analysis identified malware on compromised host
- IR team working for Organization A built an IOC

Or

File MD5 Checksum is e132ec5404b891b0919ak3fb852e8c7e
Process Handle Name is UNIQUEEVILTHINGS
Network DNS is level.unholyp1ace.com

And

Or

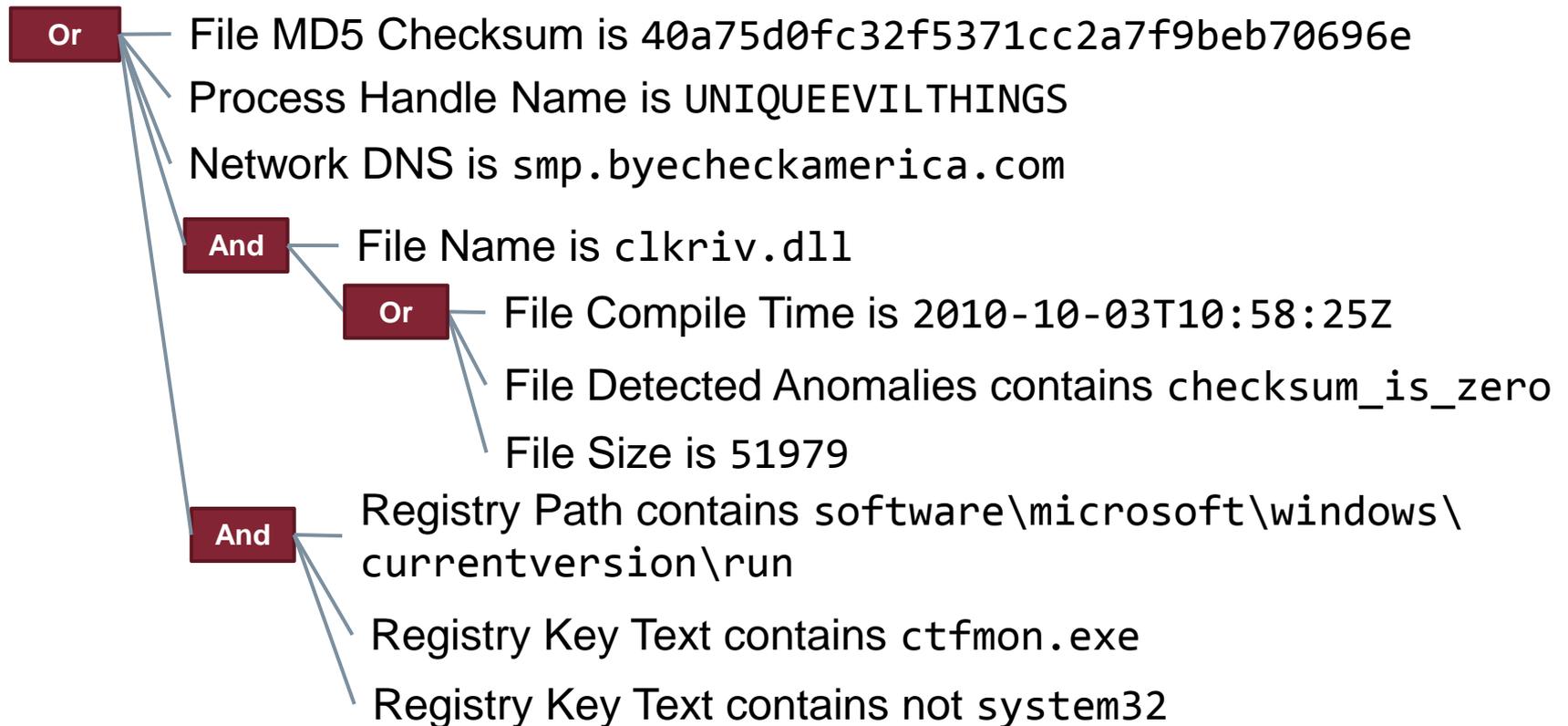
File Name is halysc.dll
File Compile Time is 2010-10-03T10:58:25Z
File Detected Anomalies contains checksum_is_zero
File Size is 51979



Organization B, you've got a funny handle!

- IOC built by Organization A team makes its way to team working for Organization B
- Organization B team sweeps the environment and finds something suspicious
 - “iexplore.exe” process running with a handle “UNIQUEEVILTHINGS”
- Organization B team conducts further analysis on host and identifies:
 - Malicious DLL “clkriv.dll”
 - Malware loader “ctfmon.exe”
 - Loader persistence via registry run key

- Organization B team builds an expanded indicator

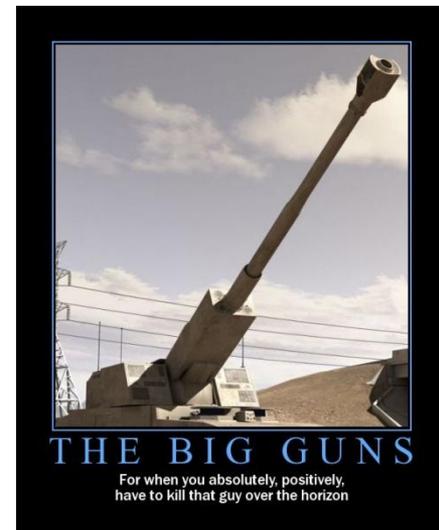


Org A Team brings in the big guns

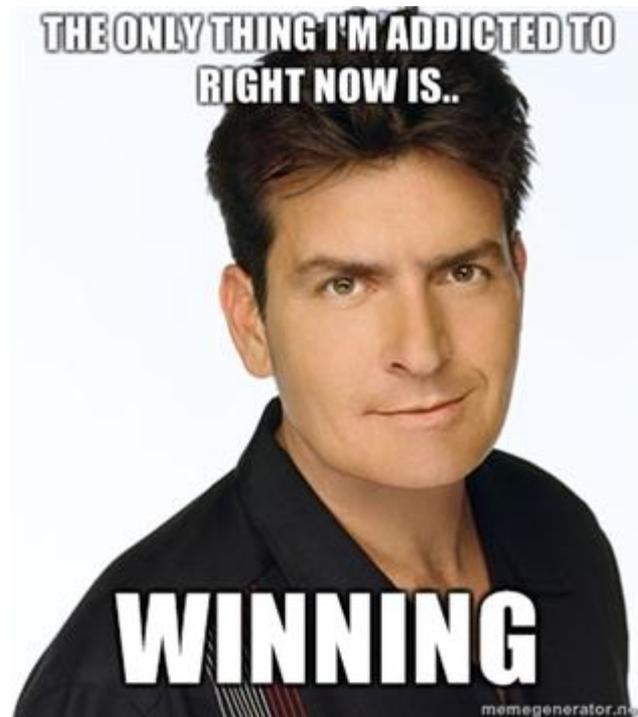
- Organization A's team uses the latest indicator to identify four variants of the DLL
- Calls in malware analysts to review malware
- Identifies a series of imports that, put together, are unique

And

- File Import Function is querywindows31filesmigration
- File Import Function is creddeletea
- File Import Function is credpconvertcredential
- File Import Function is credprofileloaded
- File Import Function is getdevicedriverfilenameew
- File Import Function is sendimemessageexa



Finding Evil = Winning

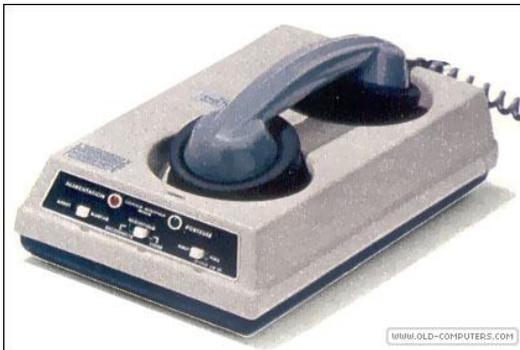


Wrap-up



BEFORE OPENIOC

- List, text files, and spreadsheets, oh my
- Difficult to capture and quantify intelligence
- Information sharing inconsistent



AFTER OPENIOC

- Easy to capture and share intelligence
- Standard format for describing evil
- Better context



- Adoption of the OpenIOC format is not widespread
 - Ok, that *may* be an understatement
- Consolidate your existing data
- Use Mandiant OpenIOCe to capture existing data
 - http://www.mandiant.com/products/free_software/ioce/
- Build tools and process to share IOCs internally
 - We use SVN, really, it's that easy
- Develop scripts and XSLTs to convert IOCs
 - To other software products
 - To reports

- OpenIOC v2.0
 - Node context
 - More descriptors
 - beginswith
 - endswith
 - isregex
 - Term weighting
 - Score hits based on confidence and source
- More free tools for using IOCs
- World domination?



Resources

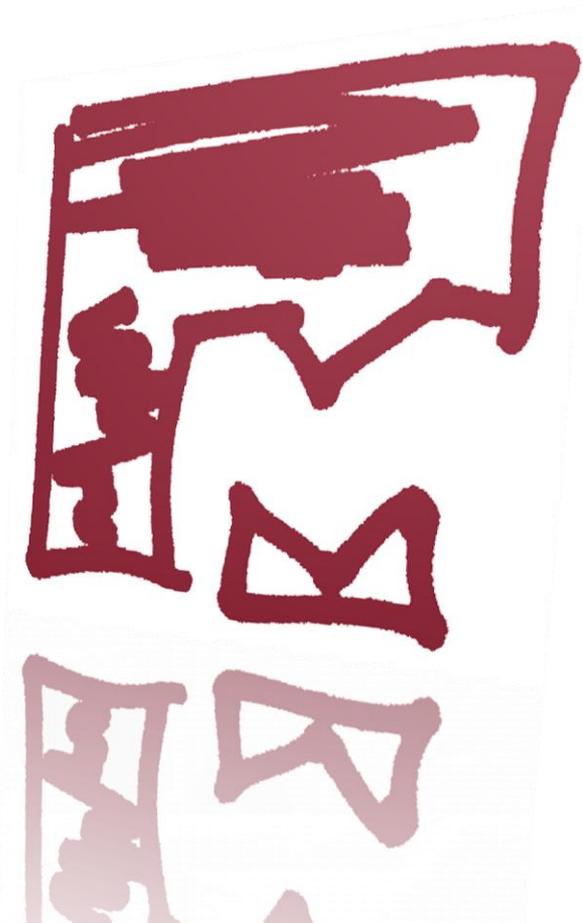




Download the full report

<http://www.mandiant.com>

Redline	answers the question: are you compromised?
Web Historian	browser analysis
Memoryze	memory forensics
Highlighter	log analysis
Red Curtain	malware identifier
IOCe	indicator of compromise editor
OpenIOC	Common language to describe IOCs



STATE OF THE HACK

- Designed for all technical levels
- Case study format
- Illustrates the latest attacks we are seeing



FRESH PRINTS OF MALWARE

- Designed for the technical user
- Case study format
- Digs deeper into the technical aspects of the incidents we respond to



- **Details**
 - October 11-12, 2011
 - Hilton Alexandria Old Town
 - “MANDIANT” room block
 - www.mandiant.com/mircon





Twitter

www.twitter.com/mandiant

LinkedIn

www.linkedin.com/company/mandiant

Facebook

www.facebook.com/mandiantcorp

YouTube

www.youtube.com/mandiantcorp

- Positions in
 - Consulting, federal and managed services
 - Product development
 - Sales
- Locations
 - Washington
 - New York
 - Los Angeles
 - San Francisco
 - Reston, VA
- <http://www.mandiant.com/hireme>

Questions?



- David Ross
 - david.ross@mandiant.com

- Chris Bream
 - chris.bream@mandiant.com

- More MANDIANT info
 - <http://www.mandiant.com/>
 - <http://www.twitter.com/mandiant>
 - info@mandiant.com