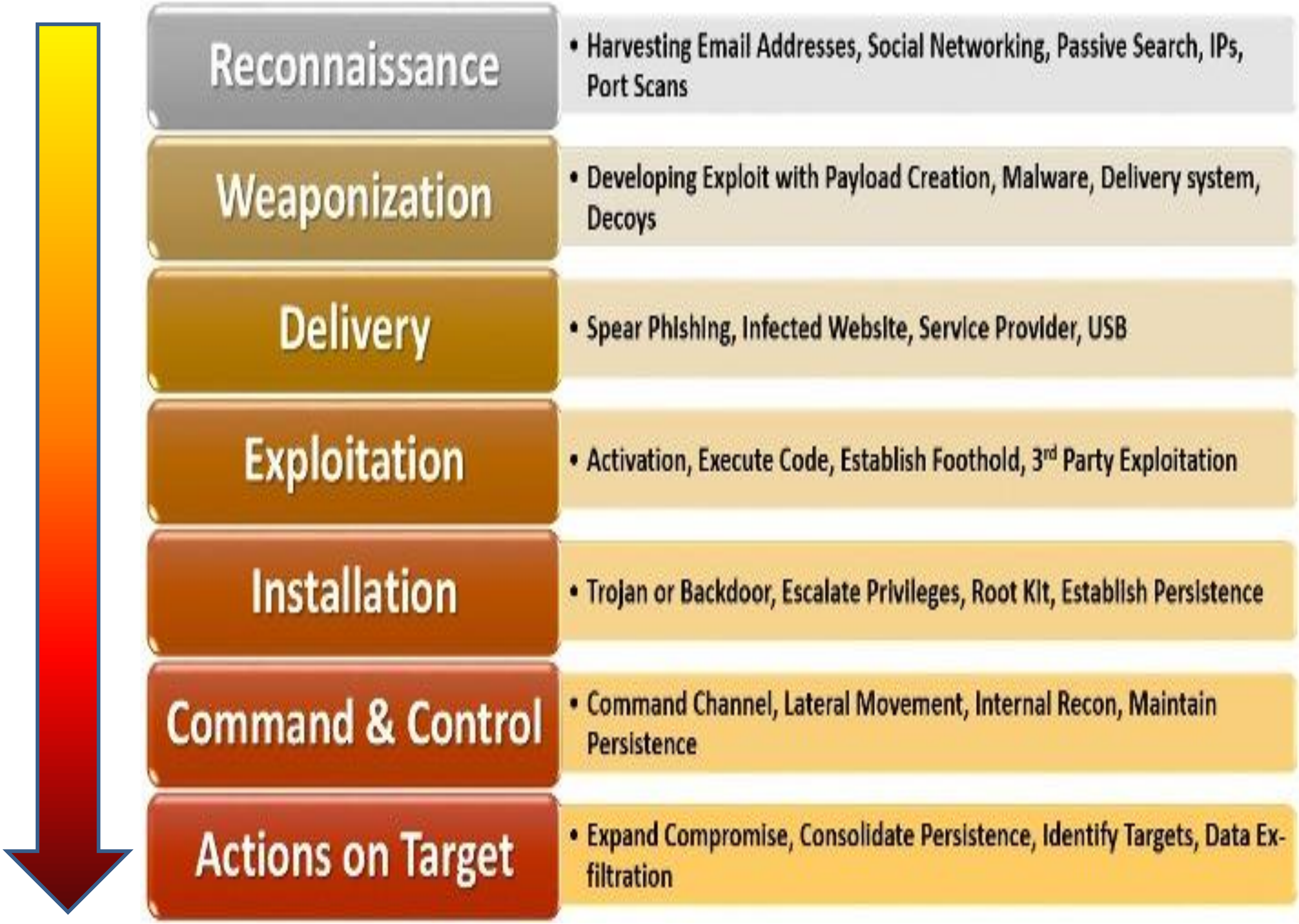
Agile Defensive Technologies

IOC Bucket, LLC

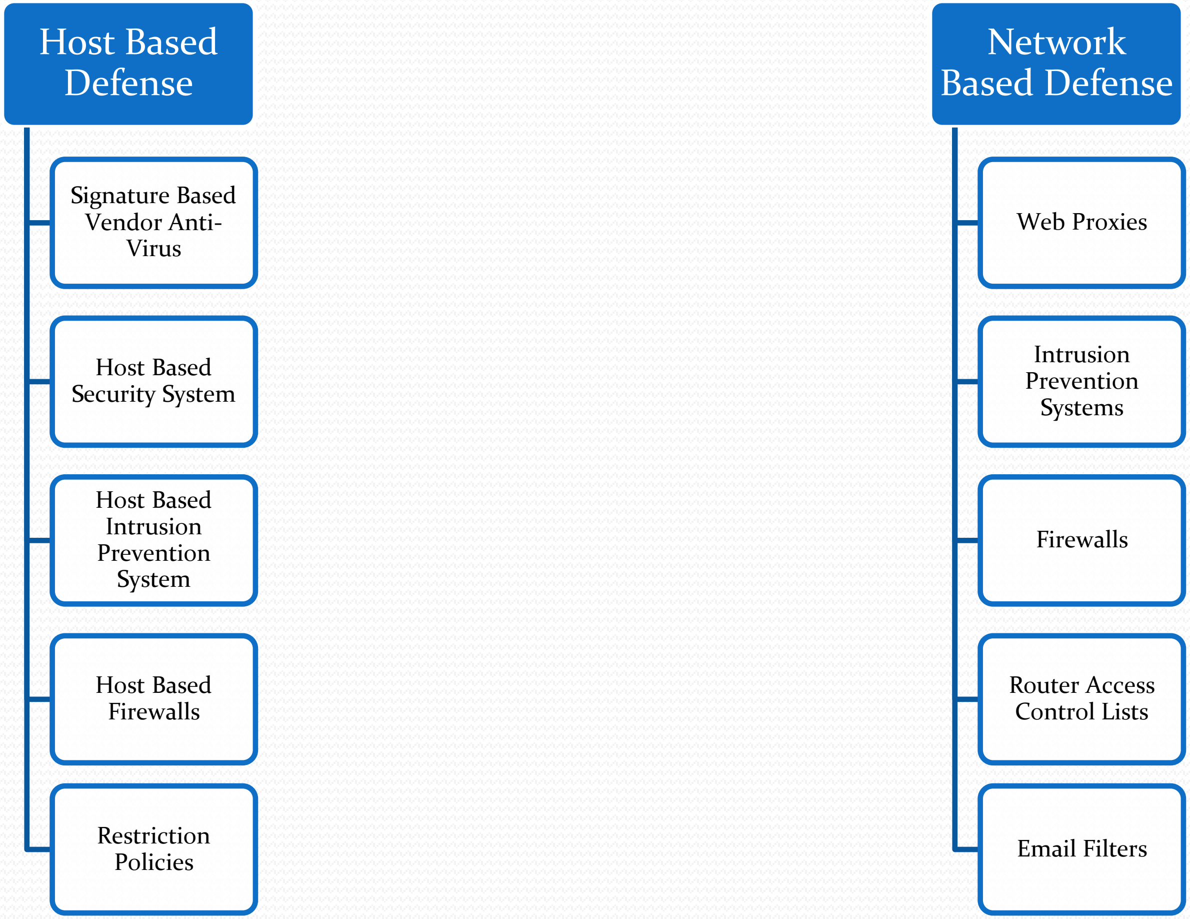
Agenda

- Anatomy of the Attack
- Defense in Depth Capabilities
- Evading Detection through 2014
- Indicators of Compromise (IOC's) what are they?
- Discovering, Building, and Responding with Indicators
- Employing Organizational Intelligence and Open Source Intelligence
- Targeted Hunting Operations with IOC's
- COTS solutions for proactive defense



Reconnaissance	• Harvesting Email Addresses, Social Networking, Passive Search, IPs, Port Scans
Weaponization	• Developing Exploit with Payload Creation, Malware, Delivery system, Decoys
Delivery	• Spear Phishing, Infected Website, Service Provider, USB
Exploitation	• Activation, Execute Code, Establish Foothold, 3rd Party Exploitation
Installation	• Trojan or Backdoor, Escalate Privileges, Root Kit, Establish Persistence
Command & Control	• Command Channel, Lateral Movement, Internal Recon, Maintain Persistence
Actions on Target	• Expand Compromise, Consolidate Persistence, Identify Targets, Data Ex-filtration

Defense In Depth



- Host Based Defense
  - Signature Based Vendor Anti-Virus
  - Host Based Security System
  - Host Based Intrusion Prevention System
  - Host Based Firewalls
  - Restriction Policies
- Network Based Defense
  - Web Proxies
  - Intrusion Prevention Systems
  - Firewalls
  - Router Access Control Lists
  - Email Filters

Current Capabilities and Limitations

- Current Defensive Posture is Reactive
  - Access Control Lists
  - Detection Definitions
  - DNS Blackhole
  - Blacklisting Email Domains
  - File hashes used for malicious file detection
    - Ex. ”MD5: 9051c29972c935649d8fa4b823e54dea”
- These adversary attributes can be easily modified to avoid detection and bypass security countermeasures.

Evasion in 2014

- Memory Injection
- Signature Manipulation(Encoding or Packing)
- Double Encryption
- Traffic Blending(HTTPS, HTTP, DNS)
- PowerShell Injection
- Load Order Hijacking
- Rootkits/Bootkits
- Executable Patching
- Process Hollowing

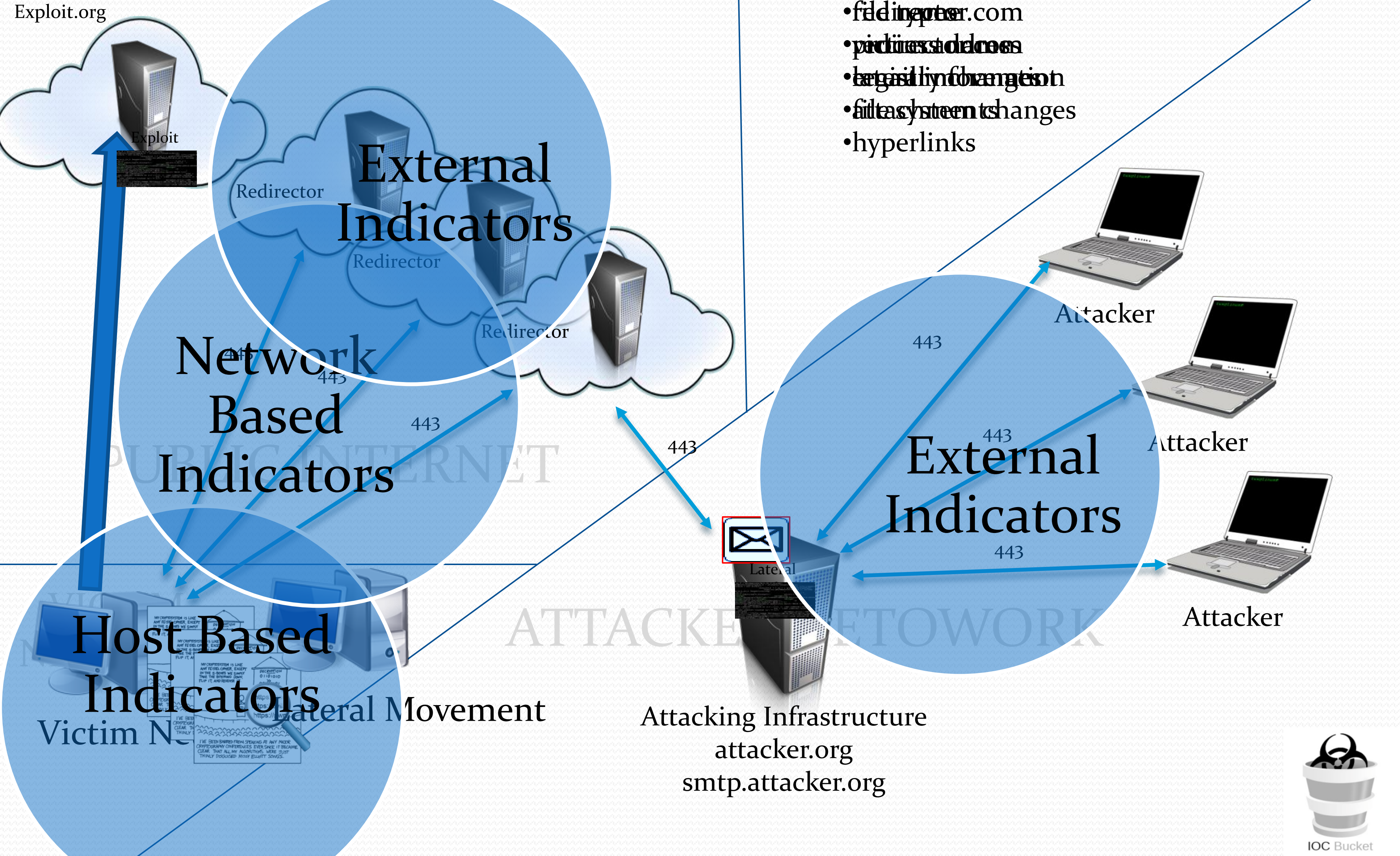
Evasion Demo

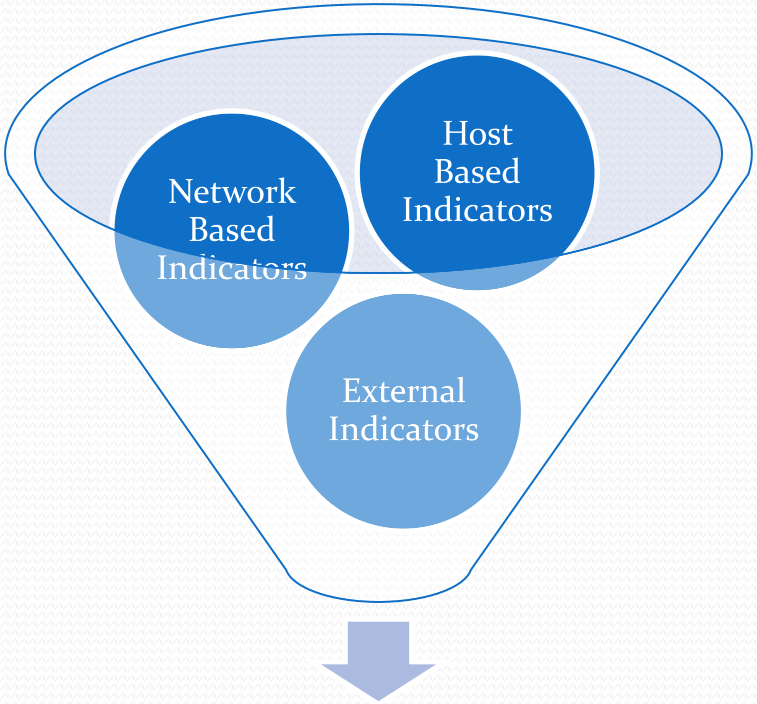
IOC…What are they?

- IOC Stands for Indicators of Compromise
- Collection of forensic elements…Bread Crumbs
  - Example File or Process attributes
  - The more of these you have the better
- Dynamic detection mechanisms are needed to detect and mitigate Advanced Persistent Threat

INDICATORS

- [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - hyperlinks





Indicators of Compromise (IOC)

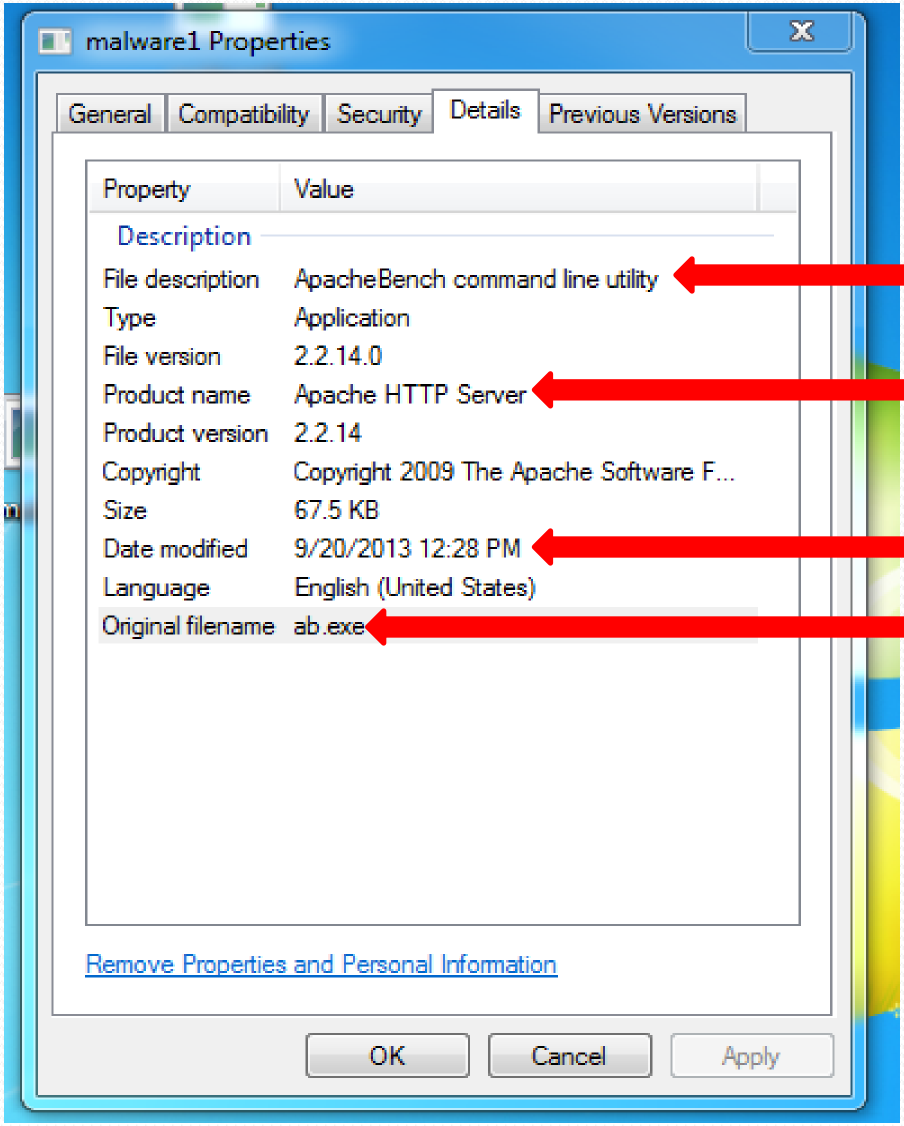
Open IOC

- OpenIOC format developed by Mandiant Corporation
- Indicators
  - The IOC identifies only attacker activity.
  - The IOC is *inexpensive* to evaluate .
  - The IOC is *expensive* for the attacker to evade.
  - Chain multiple artifacts together into one comprehensive signature

IOC the Methodology NOT the File

- IOC can detect entropy injected via human creativity
- Looking for methodology:
  - Look for specific locations in the file system.
  - Look for sets of artifacts left by tools or toolkits.
  - Look for signs of adversary activity that does not fit normal system user usage

Attribute Indicator Collection



Property	Value
Description	
File description	ApacheBench command line utility
Type	Application
File version	2.2.14.0
Product name	Apache HTTP Server
Product version	2.2.14
Copyright	Copyright 2009 The Apache Software F...
Size	67.5 KB
Date modified	9/20/2013 12:28 PM
Language	English (United States)
Original filename	ab.exe

File Description Name Always the Same

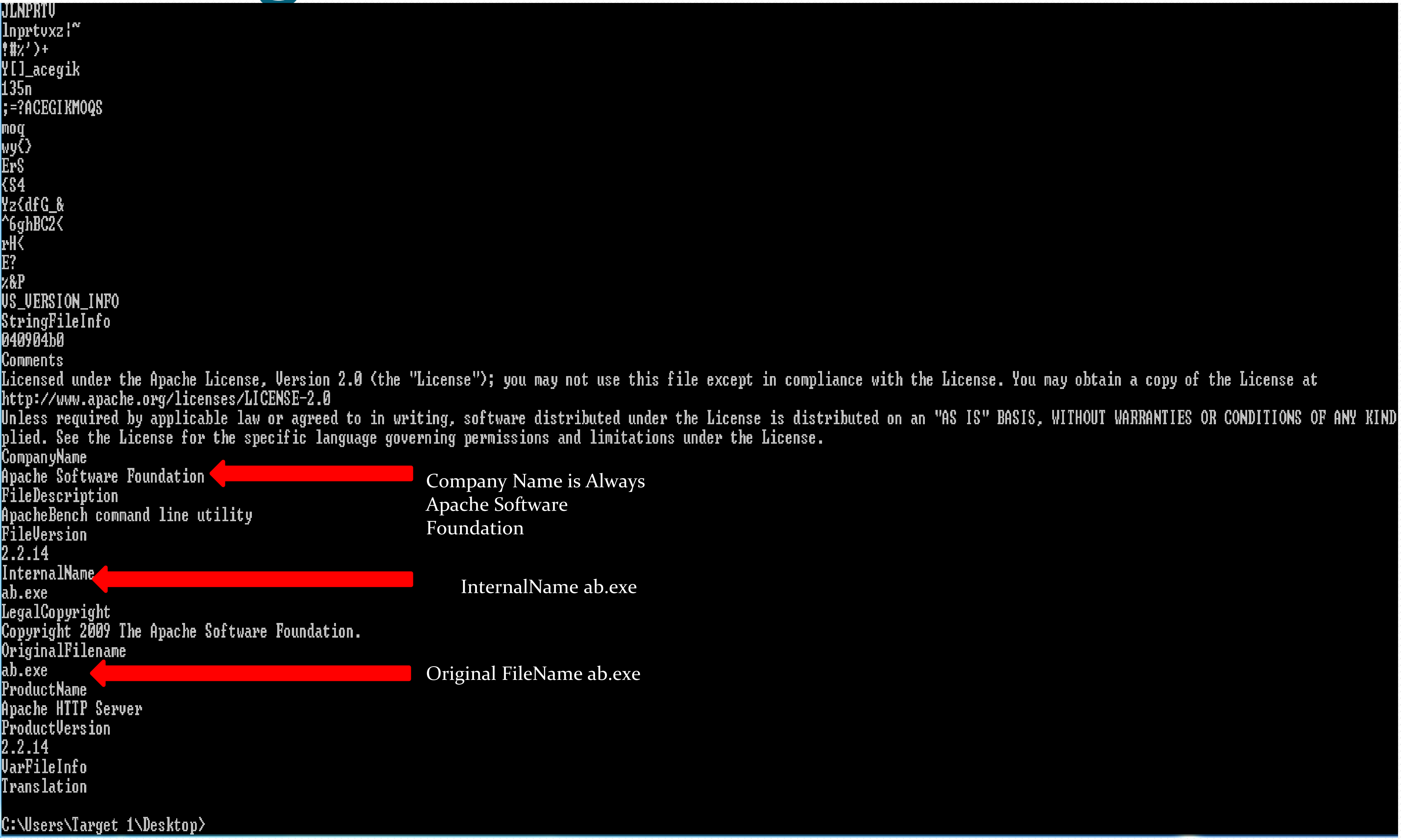
Product Name Always the Same

MACE Attributes Make Good Indicators

Original FileName is Always ab.exe

IOC Bucket

Strings Indicators



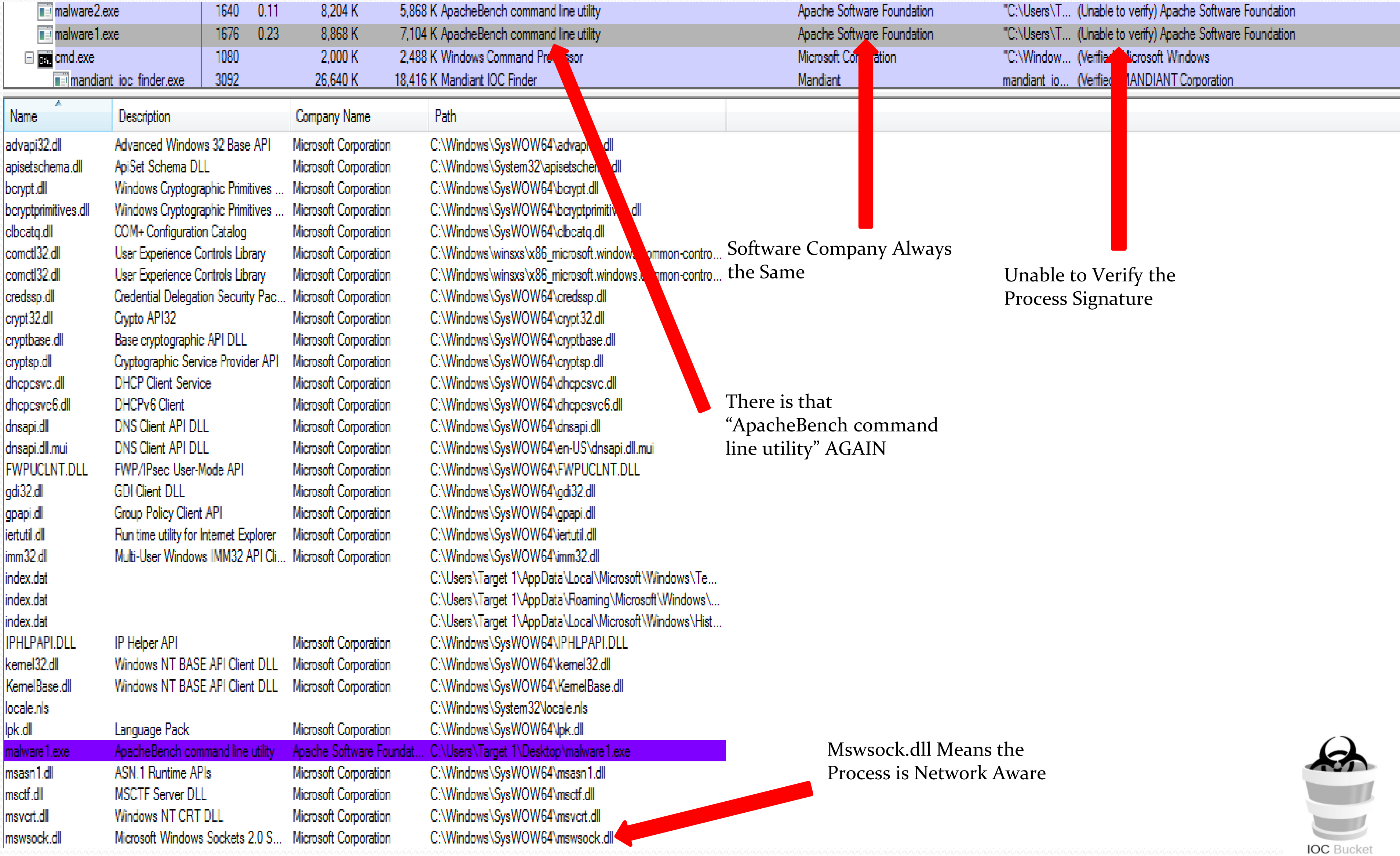
```
JLNPRTV
lnprtvxz¦~
!#%')+
Y[]_acegik
135n
;=?ACEGIKMOQS
moq
wy()
ErS
(S4
Yz(dfG_&
^6ghBC2(
rH(
E?
%&P
VS_VERSION_INFO
StringFileInfo
040904b0
Comments
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at
http://www.apache.org/licenses/LICENSE-2.0
Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND
plied. See the License for the specific language governing permissions and limitations under the License.
CompanyName
Apache Software Foundation
FileDescription
ApacheBench command line utility
FileVersion
2.2.14
InternalName
ab.exe
LegalCopyright
Copyright 2009 The Apache Software Foundation.
OriginalFilename
ab.exe
ProductName
Apache HTTP Server
ProductVersion
2.2.14
VarFileInfo
Translation

C:\Users\Target 1\Desktop>
```

Company Name is Always
Apache Software
Foundation

InternalName ab.exe

Original FileName ab.exe

Process Attributes



malware2.exe	1640	0.11	8,204 K	5,868 K	ApacheBench command line utility	Apache Software Foundation	"C:\Users\T...	(Unable to verify) Apache Software Foundation
malware1.exe	1676	0.23	8,868 K	7,104 K	ApacheBench command line utility	Apache Software Foundation	"C:\Users\T...	(Unable to verify) Apache Software Foundation
cmd.exe	1080		2,000 K	2,488 K	Windows Command Processor	Microsoft Corporation	"C:\Window...	(Verified) Microsoft Windows
mandiant_ioc_finder.exe	3092		26,640 K	18,416 K	Mandiant IOC Finder	Mandiant	mandiant_io...	(Verified) MANDIANT Corporation

Name	Description	Company Name	Path
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\SysWOW64\advapi32.dll
apisetschema.dll	ApiSet Schema DLL	Microsoft Corporation	C:\Windows\System32\apisetschema.dll
bcrypt.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\SysWOW64\bcrypt.dll
bcryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\SysWOW64\bcryptprimitives.dll
clbcatq.dll	COM+ Configuration Catalog	Microsoft Corporation	C:\Windows\SysWOW64\clbcatq.dll
comctl32.dll	User Experience Controls Library	Microsoft Corporation	C:\Windows\winsxs\x86_microsoft.windows.common-contro...
comctl32.dll	User Experience Controls Library	Microsoft Corporation	C:\Windows\winsxs\x86_microsoft.windows.common-contro...
credssp.dll	Credential Delegation Security Pac...	Microsoft Corporation	C:\Windows\SysWOW64\credssp.dll
crypt32.dll	Crypto API32	Microsoft Corporation	C:\Windows\SysWOW64\crypt32.dll
cryptbase.dll	Base cryptographic API DLL	Microsoft Corporation	C:\Windows\SysWOW64\cryptbase.dll
cryptsp.dll	Cryptographic Service Provider API	Microsoft Corporation	C:\Windows\SysWOW64\cryptsp.dll
dhcpcsvc.dll	DHCP Client Service	Microsoft Corporation	C:\Windows\SysWOW64\dhcpcsvc.dll
dhcpcsvc6.dll	DHCPv6 Client	Microsoft Corporation	C:\Windows\SysWOW64\dhcpcsvc6.dll
dnsapi.dll	DNS Client API DLL	Microsoft Corporation	C:\Windows\SysWOW64\dnsapi.dll
dnsapi.dll.mui	DNS Client API DLL	Microsoft Corporation	C:\Windows\SysWOW64\en-US\dnsapi.dll.mui
FWPUCLNT.DLL	FWP/IPsec User-Mode API	Microsoft Corporation	C:\Windows\SysWOW64\FWPUCLNT.DLL
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\SysWOW64\gdi32.dll
gpapi.dll	Group Policy Client API	Microsoft Corporation	C:\Windows\SysWOW64\gpapi.dll
iertutil.dll	Run time utility for Internet Explorer	Microsoft Corporation	C:\Windows\SysWOW64\iertutil.dll
imm32.dll	Multi-User Windows IMM32 API Cli...	Microsoft Corporation	C:\Windows\SysWOW64\imm32.dll
index.dat			C:\Users\Target 1\AppData\Local\Microsoft\Windows\Te...
index.dat			C:\Users\Target 1\AppData\Roaming\Microsoft\Windows\...
index.dat			C:\Users\Target 1\AppData\Local\Microsoft\Windows\Hist...
IPHLPAPI.DLL	IP Helper API	Microsoft Corporation	C:\Windows\SysWOW64\IPHLPAPI.DLL
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\SysWOW64\kernel32.dll
KernelBase.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\SysWOW64\KernelBase.dll
locale.nls			C:\Windows\System32\locale.nls
lpk.dll	Language Pack	Microsoft Corporation	C:\Windows\SysWOW64\lpk.dll
malware1.exe	ApacheBench command line utility	Apache Software Foundat...	C:\Users\Target 1\Desktop\malware1.exe
msasn1.dll	ASN.1 Runtime APIs	Microsoft Corporation	C:\Windows\SysWOW64\msasn1.dll
msctf.dll	MSCTF Server DLL	Microsoft Corporation	C:\Windows\SysWOW64\msctf.dll
msvcrt.dll	Windows NT CRT DLL	Microsoft Corporation	C:\Windows\SysWOW64\msvcrt.dll
mswsock.dll	Microsoft Windows Sockets 2.0 S...	Microsoft Corporation	C:\Windows\SysWOW64\mswsock.dll

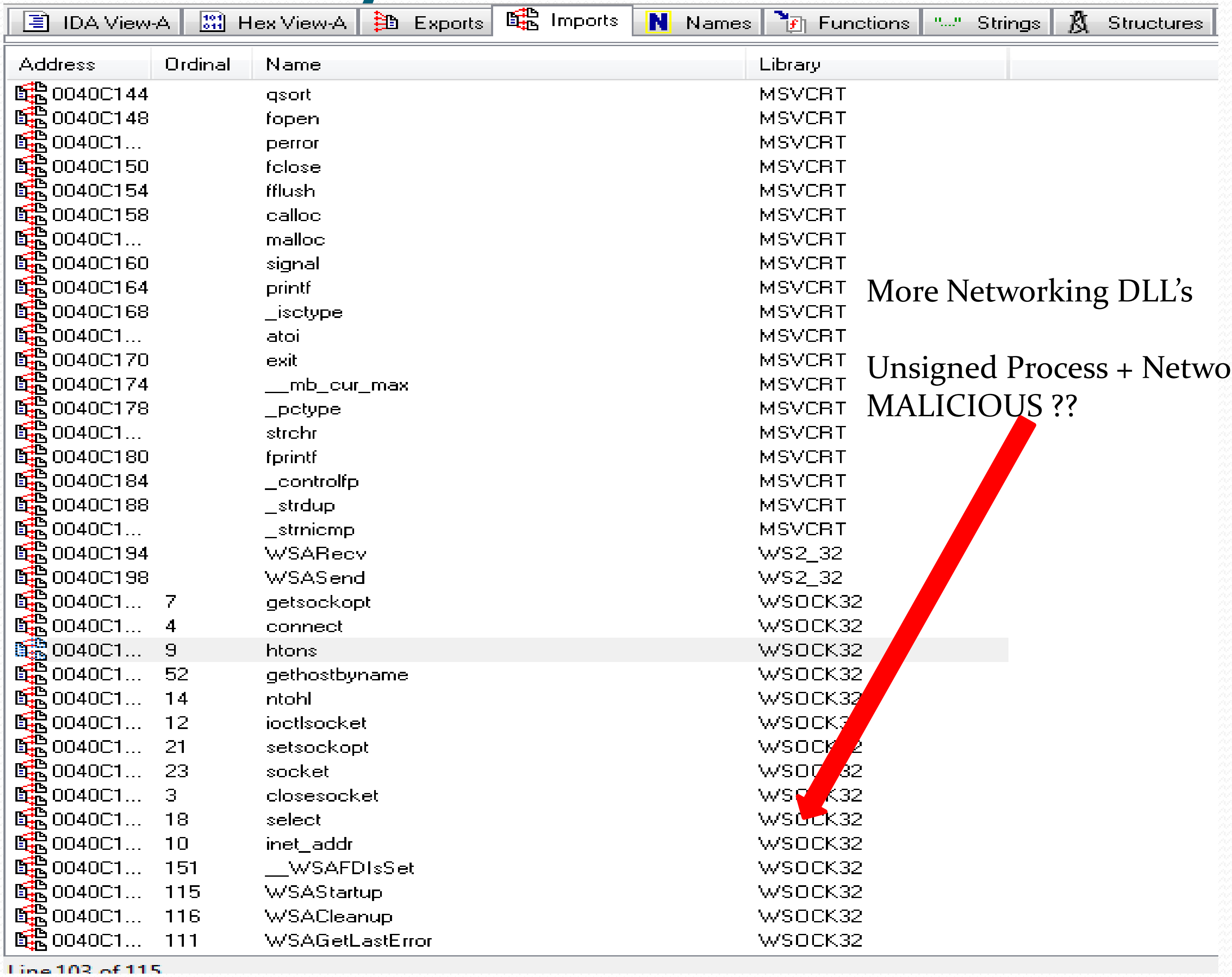
Software Company Always the Same

Unable to Verify the Process Signature

There is that "ApacheBench command line utility" AGAIN

Mswsock.dll Means the Process is Network Aware

Anomaly Attributes



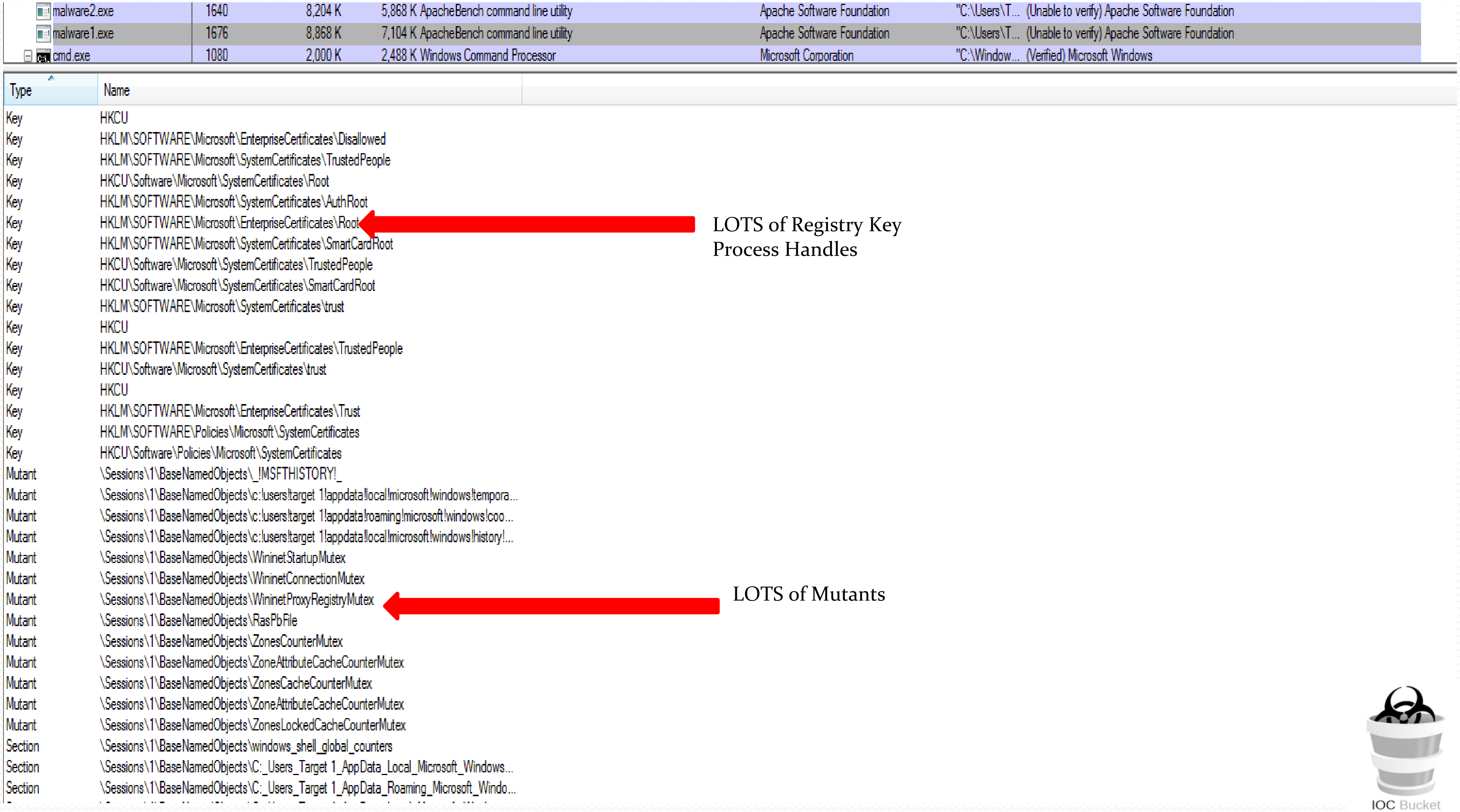
Address	Ordinal	Name	Library
0040C144		qsort	MSVCRT
0040C148		fopen	MSVCRT
0040C1...		perror	MSVCRT
0040C150		fclose	MSVCRT
0040C154		fflush	MSVCRT
0040C158		calloc	MSVCRT
0040C1...		malloc	MSVCRT
0040C160		signal	MSVCRT
0040C164		printf	MSVCRT
0040C168		_isctype	MSVCRT
0040C1...		atoi	MSVCRT
0040C170		exit	MSVCRT
0040C174		__mb_cur_max	MSVCRT
0040C178		_pctype	MSVCRT
0040C1...		strchr	MSVCRT
0040C180		fprintf	MSVCRT
0040C184		_controlfp	MSVCRT
0040C188		_strdup	MSVCRT
0040C1...		_strnicmp	MSVCRT
0040C194		WSARecv	WS2_32
0040C198		WSASend	WS2_32
0040C1...	7	getsockopt	WSOCK32
0040C1...	4	connect	WSOCK32
0040C1...	9	htons	WSOCK32
0040C1...	52	gethostbyname	WSOCK32
0040C1...	14	ntohl	WSOCK32
0040C1...	12	ioctlsocket	WSOCK32
0040C1...	21	setsockopt	WSOCK32
0040C1...	23	socket	WSOCK32
0040C1...	3	closesocket	WSOCK32
0040C1...	18	select	WSOCK32
0040C1...	10	inet_addr	WSOCK32
0040C1...	151	__WSAFDIsSet	WSOCK32
0040C1...	115	WSAStartup	WSOCK32
0040C1...	116	WSACleanup	WSOCK32
0040C1...	111	WSAGetLastError	WSOCK32

Line 103 of 115

More Networking DLL's

Unsigned Process + Networking DLL's == MALICIOUS ??

Handles and Mutex



```
malware2.exe   1640   8,204 K   5,868 K ApacheBench command line utility   Apache Software Foundation   "C:\Users\T...  (Unable to verify) Apache Software Foundation
malware1.exe   1676   8,868 K   7,104 K ApacheBench command line utility   Apache Software Foundation   "C:\Users\T...  (Unable to verify) Apache Software Foundation
cmd.exe        1080   2,000 K   2,488 K Windows Command Processor          Microsoft Corporation        "C:\Window...   (Verified) Microsoft Windows

Type      Name
Key       HKCU
Key       HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Disallowed
Key       HKLM\SOFTWARE\Microsoft\SystemCertificates\TrustedPeople
Key       HKCU\Software\Microsoft\SystemCertificates\Root
Key       HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot
Key       HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Root
Key       HKLM\SOFTWARE\Microsoft\SystemCertificates\SmartCardRoot
Key       HKCU\Software\Microsoft\SystemCertificates\TrustedPeople
Key       HKCU\Software\Microsoft\SystemCertificates\SmartCardRoot
Key       HKLM\SOFTWARE\Microsoft\SystemCertificates\trust
Key       HKCU
Key       HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\TrustedPeople
Key       HKCU\Software\Microsoft\SystemCertificates\trust
Key       HKCU
Key       HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Trust
Key       HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates
Key       HKCU\Software\Policies\Microsoft\SystemCertificates
Mutant    \Sessions\1\BaseNamedObjects\_!MSFTHISTORY!_
Mutant    \Sessions\1\BaseNamedObjects\c:!users!target 1!appdata!local!microsoft!windows!tempora...
Mutant    \Sessions\1\BaseNamedObjects\c:!users!target 1!appdata!roaming!microsoft!windows!coo...
Mutant    \Sessions\1\BaseNamedObjects\c:!users!target 1!appdata!local!microsoft!windows!history!...
Mutant    \Sessions\1\BaseNamedObjects\WininetStartupMutex
Mutant    \Sessions\1\BaseNamedObjects\WininetConnectionMutex
Mutant    \Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex
Mutant    \Sessions\1\BaseNamedObjects\RasPbFile
Mutant    \Sessions\1\BaseNamedObjects\ZonesCounterMutex
Mutant    \Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex
Mutant    \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex
Mutant    \Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex
Mutant    \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex
Section   \Sessions\1\BaseNamedObjects\windows_shell_global_counters
Section   \Sessions\1\BaseNamedObjects\C:_Users_Target 1_AppData_Local_Microsoft_Windows...
Section   \Sessions\1\BaseNamedObjects\C:_Users_Target 1_AppData_Roaming_Microsoft_Windo...
```

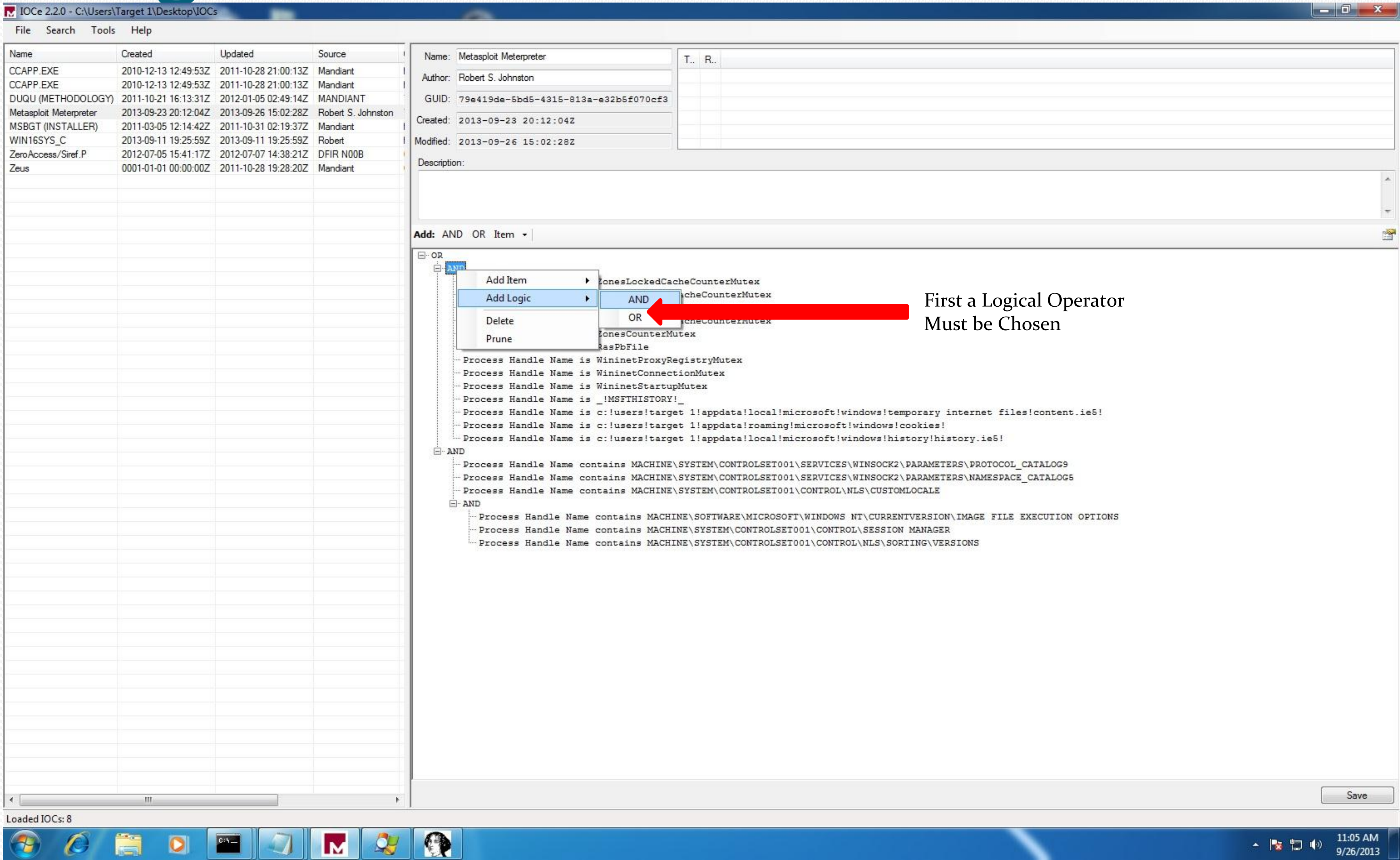
LOTS of Registry Key Process Handles

LOTS of Mutants

Building the IOC

- More than 500 different ways to identify and signature a file
- Series of AND/OR logical expressions differentiate or link indicators in your IOC
- Extremely effective for Incident Response, Identification of lateral movement, Hunting Operations, and Intrusion Detection

Logical Statements



IOCe 2.2.0 - C:\Users\Target 1\Desktop\IOCs

Name	Created	Updated	Source
CCAPP.EXE	2010-12-13 12:49:53Z	2011-10-28 21:00:13Z	Mandiant
CCAPP.EXE	2010-12-13 12:49:53Z	2011-10-28 21:00:13Z	Mandiant
DUQU (METHODOLOGY)	2011-10-21 16:13:31Z	2012-01-05 02:49:14Z	MANDIANT
Metasploit Meterpreter	2013-09-23 20:12:04Z	2013-09-26 15:02:28Z	Robert S. Johnston
MSBGT (INSTALLER)	2011-03-05 12:14:42Z	2011-10-31 02:19:37Z	Mandiant
WIN16SYS_C	2013-09-11 19:25:59Z	2013-09-11 19:25:59Z	Robert
ZeroAccess/Siref.P	2012-07-05 15:41:17Z	2012-07-07 14:38:21Z	DFIR N00B
Zeus	0001-01-01 00:00:00Z	2011-10-28 19:28:20Z	Mandiant

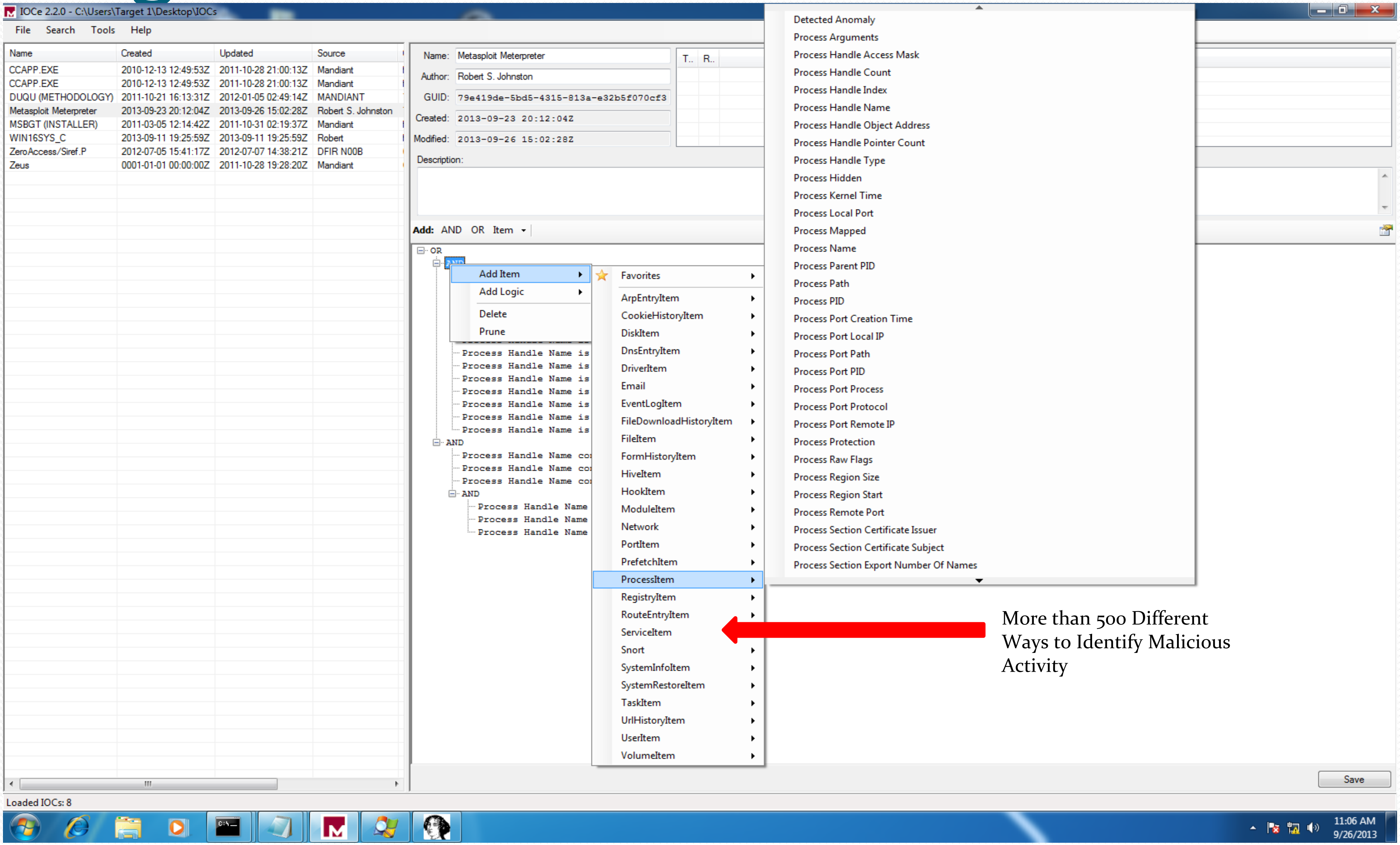
Name: Metasploit Meterpreter
Author: Robert S. Johnston
GUID: 79e419de-5bd5-4315-813a-e32b5f070cf3
Created: 2013-09-23 20:12:04Z
Modified: 2013-09-26 15:02:28Z
Description:

```
OR
  AND
      ZonesLockedCacheCounterMutex
      acheCounterMutex
      acheCounterMutex
      ZonesCounterMutex
      RasPbFile
    Process Handle Name is WininetProxyRegistryMutex
    Process Handle Name is WininetConnectionMutex
    Process Handle Name is WininetStartupMutex
    Process Handle Name is _!MSFTHISTORY!_
    Process Handle Name is c:!users!target 1!appdata!local!microsoft!windows!temporary internet files!content.ie5!
    Process Handle Name is c:!users!target 1!appdata!roaming!microsoft!windows!cookies!
    Process Handle Name is c:!users!target 1!appdata!local!microsoft!windows!history!history.ie5!
  AND
    Process Handle Name contains MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\PROTOCOL_CATALOG9
    Process Handle Name contains MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\NAMESPACE_CATALOG5
    Process Handle Name contains MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\CUSTOMLOCALE
    AND
      Process Handle Name contains MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS
      Process Handle Name contains MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER
      Process Handle Name contains MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS
```

First a Logical Operator
Must be Chosen

Loaded IOCs: 8

Signature Statements



IOCe 2.2.0 - C:\Users\Target 1\Desktop\IOCs

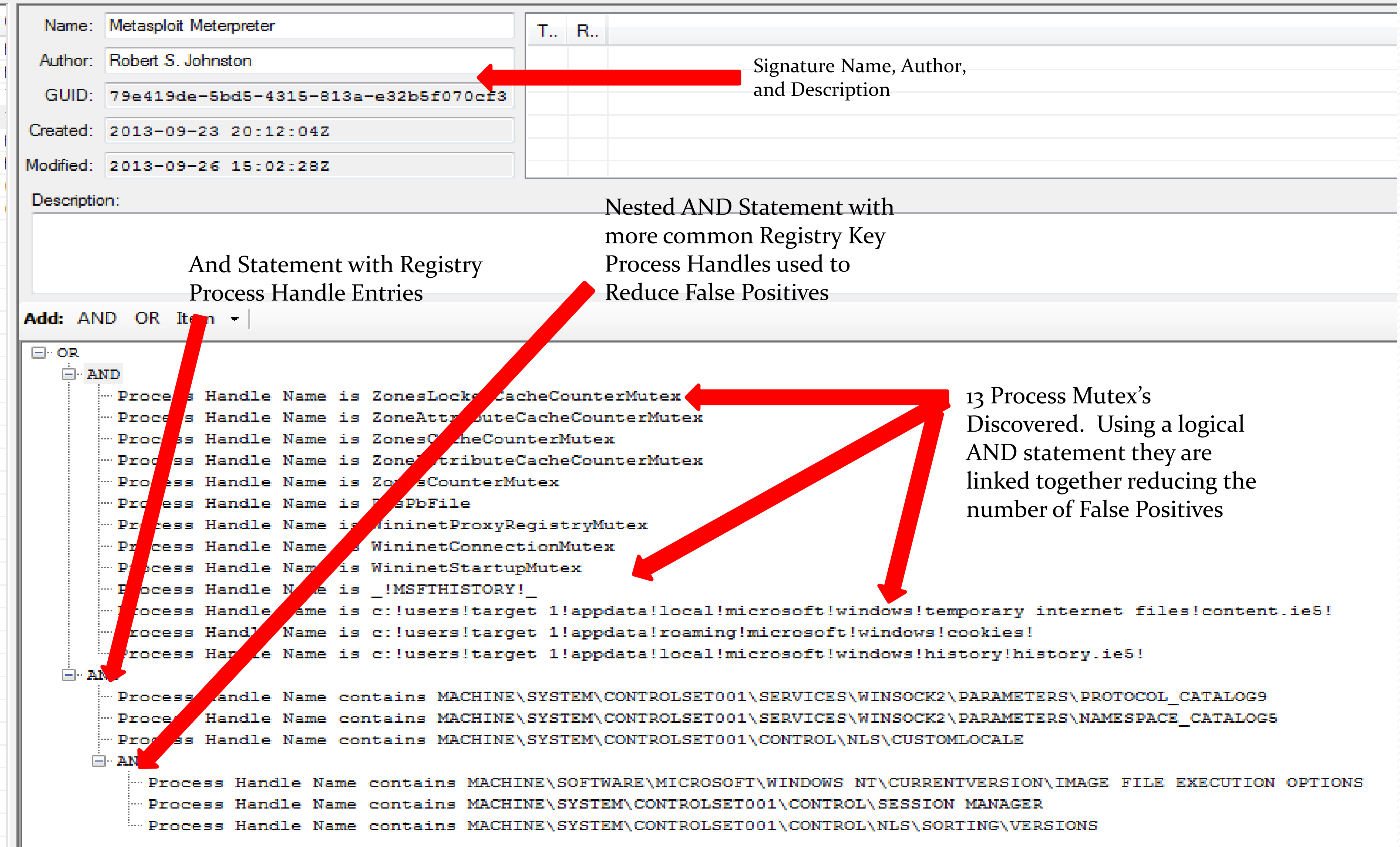
Name	Created	Updated	Source
CCAPP.EXE	2010-12-13 12:49:53Z	2011-10-28 21:00:13Z	Mandiant
CCAPP.EXE	2010-12-13 12:49:53Z	2011-10-28 21:00:13Z	Mandiant
DUQU (METHODOLOGY)	2011-10-21 16:13:31Z	2012-01-05 02:49:14Z	MANDIANT
Metasploit Meterpreter	2013-09-23 20:12:04Z	2013-09-26 15:02:28Z	Robert S. Johnston
MSBGT (INSTALLER)	2011-03-05 12:14:42Z	2011-10-31 02:19:37Z	Mandiant
WIN16SYS_C	2013-09-11 19:25:59Z	2013-09-11 19:25:59Z	Robert
ZeroAccess/Siref.P	2012-07-05 15:41:17Z	2012-07-07 14:38:21Z	DFIR N00B
Zeus	0001-01-01 00:00:00Z	2011-10-28 19:28:20Z	Mandiant

Name: Metasploit Meterpreter
Author: Robert S. Johnston
GUID: 79e419de-5bd5-4315-813a-e32b5f070cf3
Created: 2013-09-23 20:12:04Z
Modified: 2013-09-26 15:02:28Z
Description:

Loaded IOCs: 8

More than 500 Different Ways to Identify Malicious Activity

Metasploit Meterpreter IOC



Name: Metasploit Meterpreter

Author: Robert S. Johnston

GUID: 79e419de-5bd5-4315-813a-e32b5f070cf3

Created: 2013-09-23 20:12:04Z

Modified: 2013-09-26 15:02:28Z

Description:

```
⊟ OR
  ⊟ AND
      Process Handle Name is ZonesLockedCacheCounterMutex
      Process Handle Name is ZoneAttributeCacheCounterMutex
      Process Handle Name is ZonesCacheCounterMutex
      Process Handle Name is ZoneAttributeCacheCounterMutex
      Process Handle Name is ZonesCounterMutex
      Process Handle Name is RasPbFile
      Process Handle Name is WininetProxyRegistryMutex
      Process Handle Name is WininetConnectionMutex
      Process Handle Name is WininetStartupMutex
      Process Handle Name is _!MSFTHISTORY!_
      Process Handle Name is c:!users!target 1!appdata!local!microsoft!windows!temporary internet files!content.ie5!
      Process Handle Name is c:!users!target 1!appdata!roaming!microsoft!windows!cookies!
      Process Handle Name is c:!users!target 1!appdata!local!microsoft!windows!history!history.ie5!
  ⊟ AND
      Process Handle Name contains MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\PROTOCOL_CATALOG9
      Process Handle Name contains MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\NAMESPACE_CATALOG5
      Process Handle Name contains MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\CUSTOMLOCALE
    ⊟ AND
        Process Handle Name contains MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS
        Process Handle Name contains MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER
        Process Handle Name contains MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS
```

Signature Name, Author, and Description

Nested AND Statement with more common Registry Key Process Handles used to Reduce False Positives

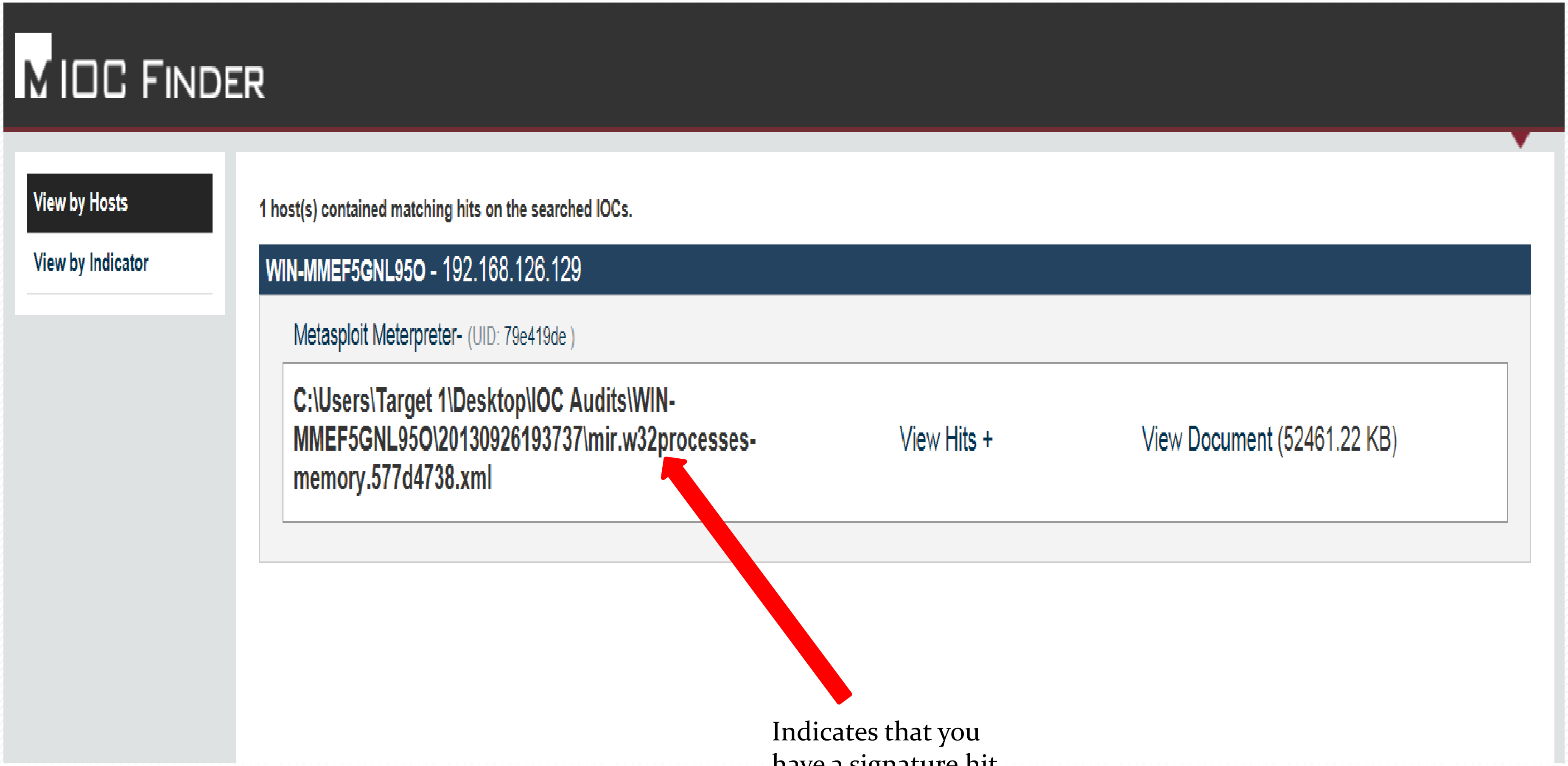
And Statement with Registry Process Handle Entries

13 Process Mutex's Discovered. Using a logical AND statement they are linked together reducing the number of False Positives

Collection and Analysis

- Mandiant Redline/IOC Finder used for both collection and analysis
  - First collect data about the system based upon information outlined in IOC’s. Then compare IOC’s against collected data.
  - Outputs the report in to an HTML format that is easy to conduct analysis on

Proactive Malware Detection



1 host(s) contained matching hits on the searched IOCs.

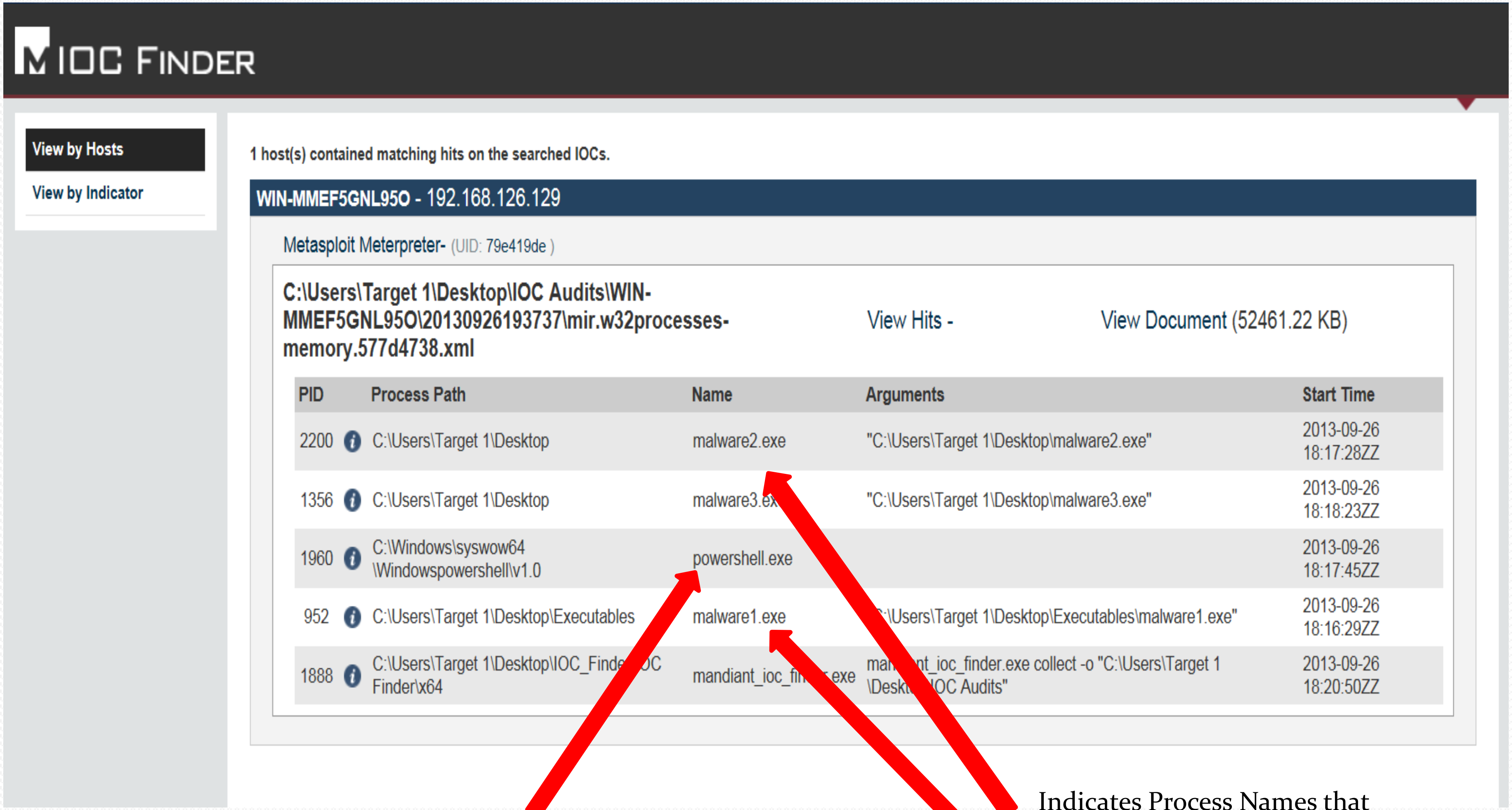
WIN-MMEF5GNL95O - 192.168.126.129

Metasploit Meterpreter- (UID: 79e419de)

C:\Users\Target 1\Desktop\IOC Audits\WIN-MMEF5GNL95O\20130926193737\mir.w32processes-memory.577d4738.xml

Indicates that you have a signature hit AND how it found the signature hit in Process Memory

Proactive Malware Detection



1 host(s) contained matching hits on the searched IOCs.

WIN-MMEF5GNL95O - 192.168.126.129

Metasploit Meterpreter- (UID: 79e419de)

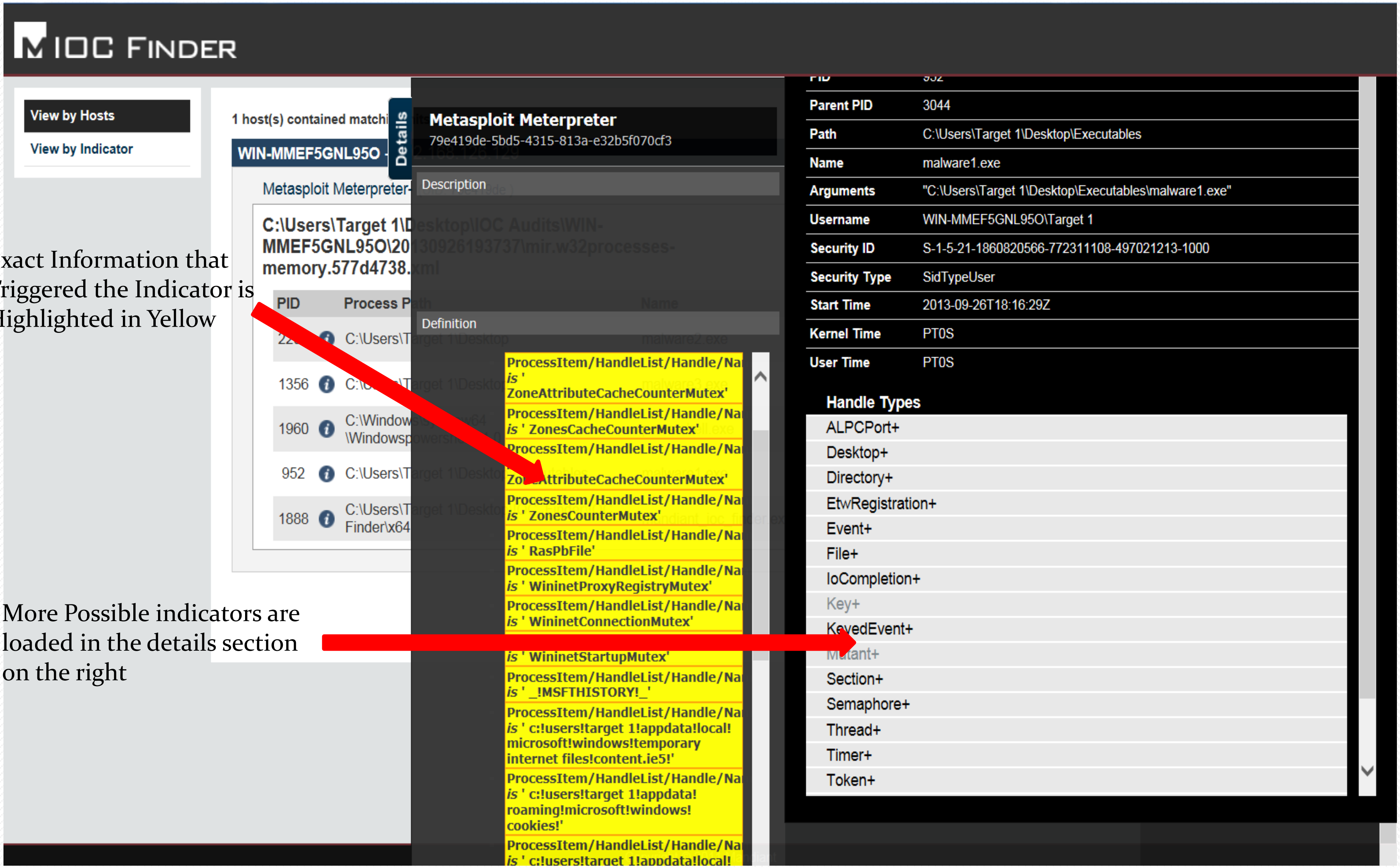
C:\Users\Target 1\Desktop\IOC Audits\WIN-MMEF5GNL95O\20130926193737\mir.w32processes-memory.577d4738.xml View Hits - View Document (52461.22 KB)

PID	Process Path	Name	Arguments	Start Time
2200	C:\Users\Target 1\Desktop	malware2.exe	"C:\Users\Target 1\Desktop\malware2.exe"	2013-09-26 18:17:28ZZ
1356	C:\Users\Target 1\Desktop	malware3.ex	"C:\Users\Target 1\Desktop\malware3.exe"	2013-09-26 18:18:23ZZ
1960	C:\Windows\syswow64 \Windowspowershell\v1.0	powershell.exe		2013-09-26 18:17:45ZZ
952	C:\Users\Target 1\Desktop\Executables	malware1.exe	:\Users\Target 1\Desktop\Executables\malware1.exe"	2013-09-26 18:16:29ZZ
1888	C:\Users\Target 1\Desktop\IOC_Finde OC Finder\x64	mandiant_ioc_fi exe	ma nt_ioc_finder.exe collect -o "C:\Users\Target 1 \Desk IOC Audits"	2013-09-26 18:20:50ZZ

What about PowerShell is this a false Positive???

Indicates Process Names that were hits on your signature

Proactive Malware Detection



C:\Users\Target 1\Desktop\IOC Audits\WIN-MMEF5GNL95O\20130926193737\mir.w32processes-memory.577d4738.xml

PID	Process Path	Name
22	C:\Users\Target 1\Desktop	malware2.exe
1356	C:\Users\Target 1\Desktop	malware3.exe
1960	C:\Windows\System...\x64 \Windowspowershell...	...ll.exe
952	C:\Users\Target 1\Desktop	malware1.exe
1888	C:\Users\Target 1\Desktop Finder\x64	mandiant_ioc_finder.ex

Metasploit Meterpreter
79e419de-5bd5-4315-813a-e32b5f070cf3

Description

Definition

```
ProcessItem/HandleList/Handle/Na
is '
ZoneAttributeCacheCounterMutex'
ProcessItem/HandleList/Handle/Na
is ' ZonesCacheCounterMutex'
ProcessItem/HandleList/Handle/Na

ZoneAttributeCacheCounterMutex'
ProcessItem/HandleList/Handle/Na
is ' ZonesCounterMutex'
ProcessItem/HandleList/Handle/Na
is ' RasPbFile'
ProcessItem/HandleList/Handle/Na
is ' WininetProxyRegistryMutex'
ProcessItem/HandleList/Handle/Na
is ' WininetConnectionMutex'

is ' WininetStartupMutex'
ProcessItem/HandleList/Handle/Na
is ' _!MSFTHISTORY!_'
ProcessItem/HandleList/Handle/Na
is ' c:!users!target 1!appdata!local!
microsoft!windows!temporary
internet files!content.ie5!'
ProcessItem/HandleList/Handle/Na
is ' c:!users!target 1!appdata!
roaming!microsoft!windows!
cookies!'
ProcessItem/HandleList/Handle/Na
is ' c:!users!target 1!appdata!local!
```

PID	952
Parent PID	3044
Path	C:\Users\Target 1\Desktop\Executables
Name	malware1.exe
Arguments	"C:\Users\Target 1\Desktop\Executables\malware1.exe"
Username	WIN-MMEF5GNL95O\Target 1
Security ID	S-1-5-21-1860820566-772311108-497021213-1000
Security Type	SidTypeUser
Start Time	2013-09-26T18:16:29Z
Kernel Time	PT0S
User Time	PT0S

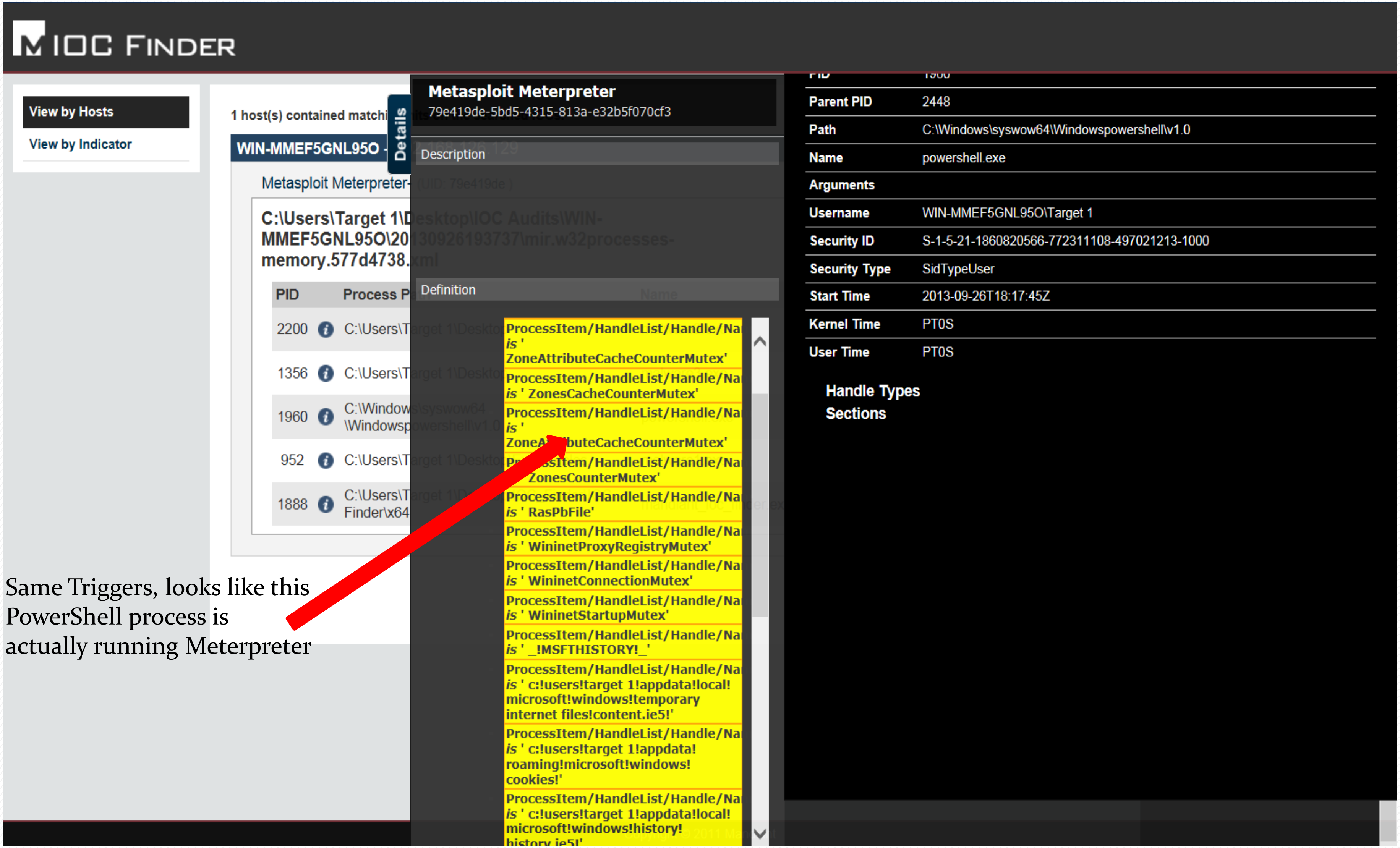
Handle Types

ALPCPort+
Desktop+
Directory+
EtwRegistration+
Event+
File+
IoCompletion+
Key+
KeyedEvent+
Mutant+
Section+
Semaphore+
Thread+
Timer+
Token+

Exact Information that Triggered the Indicator is Highlighted in Yellow

More Possible indicators are loaded in the details section on the right

Lets Investigate that PowerShell Process



1 host(s) contained matchi

WIN-MMEF5GNL95O -

Metasploit Meterpreter-

C:\Users\Target 1\Desktop\IOC Audits\WIN-MMEF5GNL95O\20130926193737\mir.w32processes-memory.577d4738.xml

PID	Process P
2200	C:\Users\Target 1\Deskto
1356	C:\Users\Target 1\Deskto
1960	C:\Windows\syswow64 \Windowspowershell\v1.0
952	C:\Users\Target 1\Deskto
1888	C:\Users\Target 1\D Finder\x64

Metasploit Meterpreter
79e419de-5bd5-4315-813a-e32b5f070cf3

Description

Definition

```
ProcessItem/HandleList/Handle/Na
is ' ZoneAttributeCacheCounterMutex'
ProcessItem/HandleList/Handle/Na
is ' ZonesCacheCounterMutex'
ProcessItem/HandleList/Handle/Na
is ' ZoneAttributeCacheCounterMutex'
ProcessItem/HandleList/Handle/Na
   ZonesCounterMutex'
ProcessItem/HandleList/Handle/Na
is ' RasPbFile'
ProcessItem/HandleList/Handle/Na
is ' WininetProxyRegistryMutex'
ProcessItem/HandleList/Handle/Na
is ' WininetConnectionMutex'
ProcessItem/HandleList/Handle/Na
is ' WininetStartupMutex'
ProcessItem/HandleList/Handle/Na
is ' _!MSFTHISTORY!_'
ProcessItem/HandleList/Handle/Na
is ' c:!users!target 1!appdata!local!microsoft!windows!temporary internet files!content.ie5!'
ProcessItem/HandleList/Handle/Na
is ' c:!users!target 1!appdata!roaming!microsoft!windows!cookies!'
ProcessItem/HandleList/Handle/Na
is ' c:!users!target 1!appdata!local!microsoft!windows!history!history.ie5!'
```

PID	1960
Parent PID	2448
Path	C:\Windows\syswow64\Windowspowershell\v1.0
Name	powershell.exe
Arguments	
Username	WIN-MMEF5GNL95O\Target 1
Security ID	S-1-5-21-1860820566-772311108-497021213-1000
Security Type	SidTypeUser
Start Time	2013-09-26T18:17:45Z
Kernel Time	PT0S
User Time	PT0S

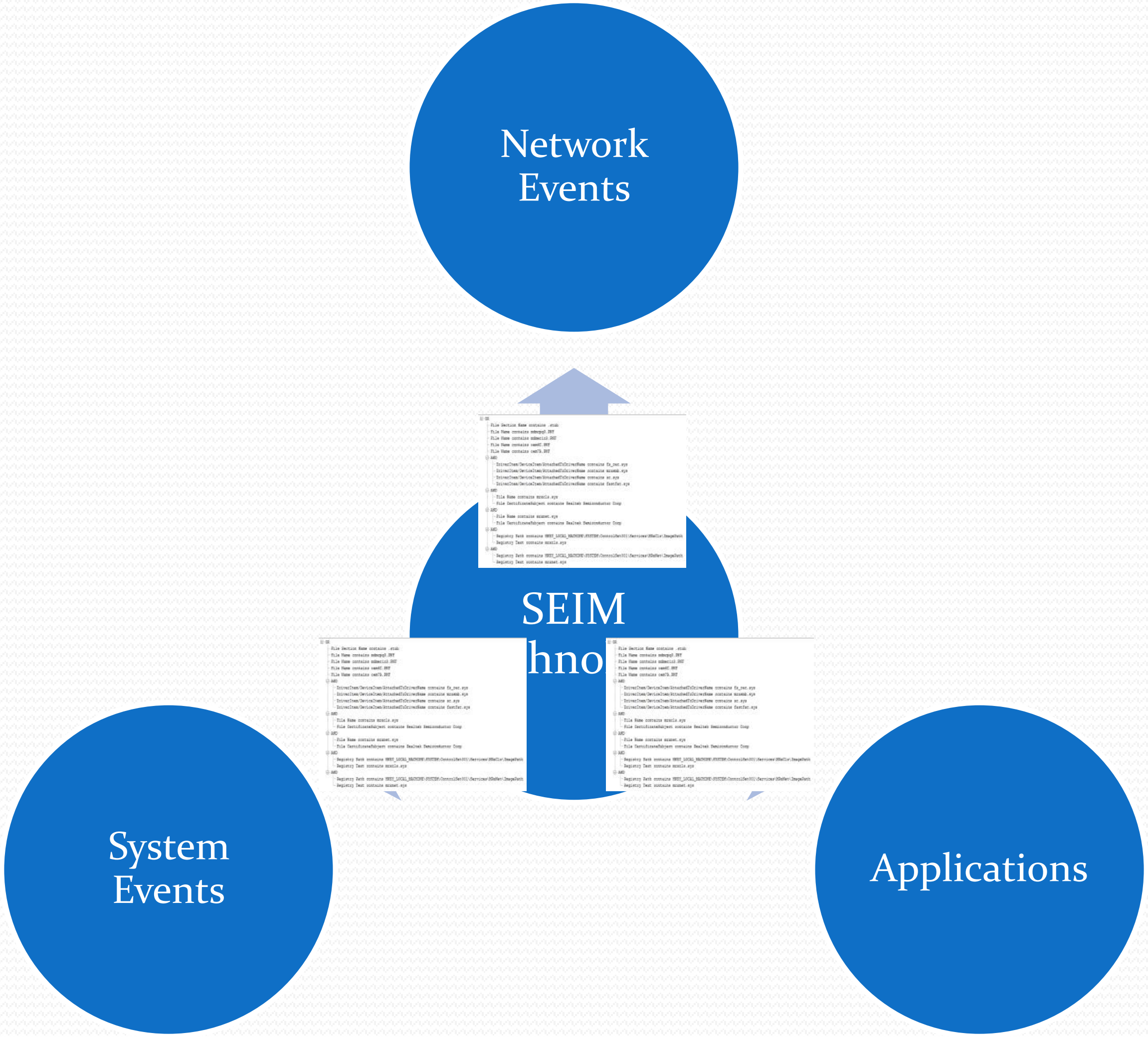
Handle Types
Sections

Same Triggers, looks like this PowerShell process is actually running Meterpreter

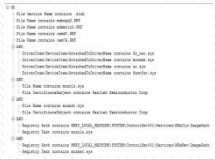
Organizational Intelligence

- Government has the unique capability of Intelligence Collection. In Cyber it can be used to our advantage
- Non Government entities Collection Platforms
- SEIM Technology
  - Understanding your own network
    - Essential Elements of Friendly Information
  - Sensor Feeds
  - Anomaly Detection

SIEM Technology

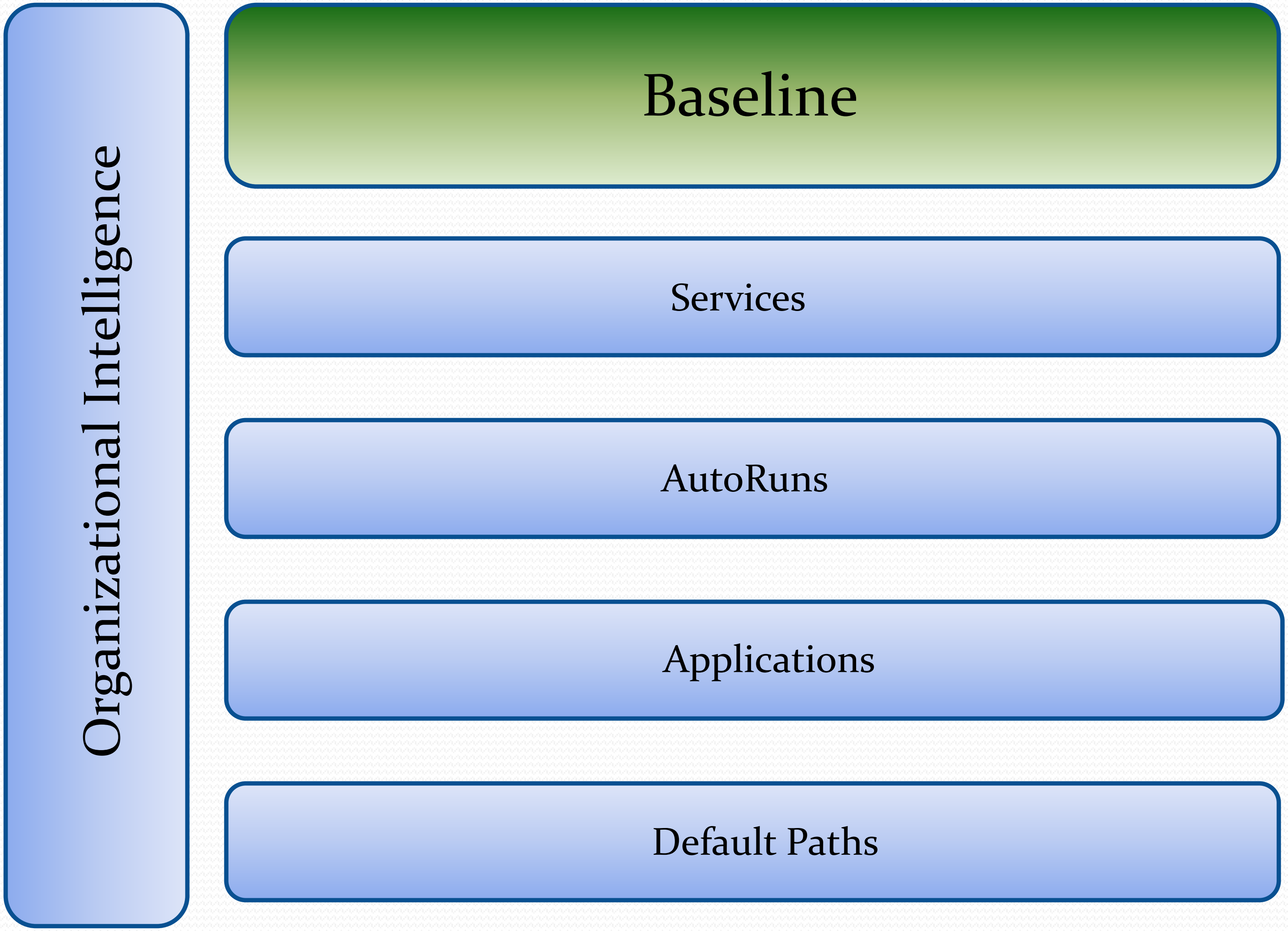


```
OR
  File Section Name contains .stub
  File Name contains mdmcpq3.PNF
  File Name contains mdmeric3.PNF
  File Name contains oem6C.PNF
  File Name contains oem7A.PNF
  AND
    DriverItem/DeviceItem/AttachedToDriverName contains fs_rec.sys
    DriverItem/DeviceItem/AttachedToDriverName contains mrxsmb.sys
    DriverItem/DeviceItem/AttachedToDriverName contains sr.sys
    DriverItem/DeviceItem/AttachedToDriverName contains fastfat.sys
  AND
    File Name contains mrxcls.sys
    File CertificateSubject contains Realtek Semiconductor Corp
  AND
    File Name contains mrxnet.sys
    File CertificateSubject contains Realtek Semiconductor Corp
  AND
    Registry Path contains HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxCls\ImagePath
    Registry Text contains mrxcls.sys
  AND
    Registry Path contains HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxNet\ImagePath
    Registry Text contains mrxnet.sys
```



```
OR
  File Section Name contains .stub
  File Name contains mdmcpq3.PNF
  File Name contains mdmeric3.PNF
  File Name contains oem6C.PNF
  File Name contains oem7A.PNF
  AND
    DriverItem/DeviceItem/AttachedToDriverName contains fs_rec.sys
    DriverItem/DeviceItem/AttachedToDriverName contains mrxsmb.sys
    DriverItem/DeviceItem/AttachedToDriverName contains sr.sys
    DriverItem/DeviceItem/AttachedToDriverName contains fastfat.sys
  AND
    File Name contains mrxcls.sys
    File CertificateSubject contains Realtek Semiconductor Corp
  AND
    File Name contains mrxnet.sys
    File CertificateSubject contains Realtek Semiconductor Corp
  AND
    Registry Path contains HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxCls\ImagePath
    Registry Text contains mrxcls.sys
  AND
    Registry Path contains HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxNet\ImagePath
    Registry Text contains mrxnet.sys
```

IOC Bucket



Organizational Intelligence

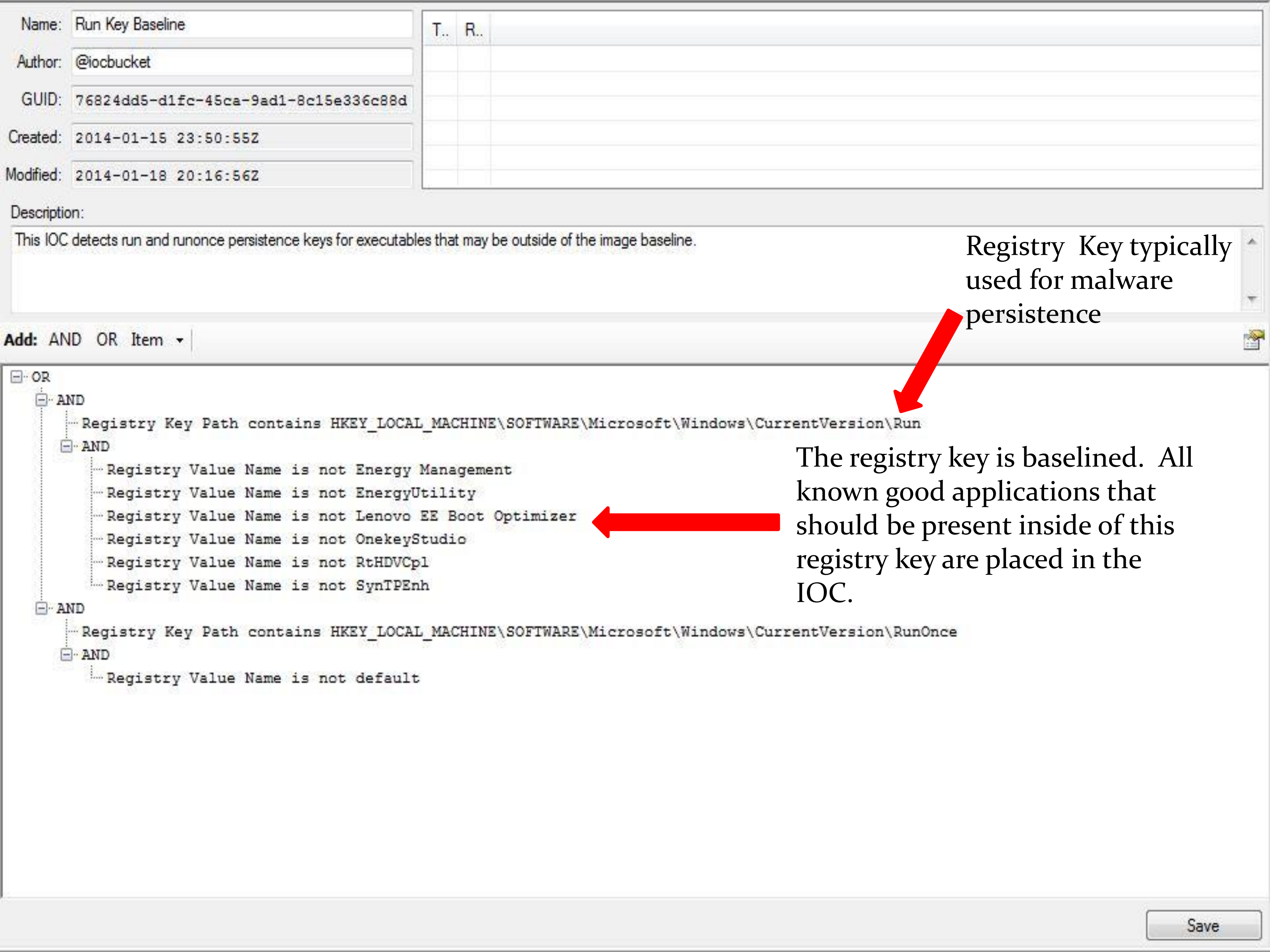
Baseline

Services

AutoRuns

Applications

Default Paths



Name: Run Key Baseline

Author: @iocbucket

GUID: 76824dd5-d1fc-45ca-9ad1-8c15e336c88d

Created: 2014-01-15 23:50:55Z

Modified: 2014-01-18 20:16:56Z

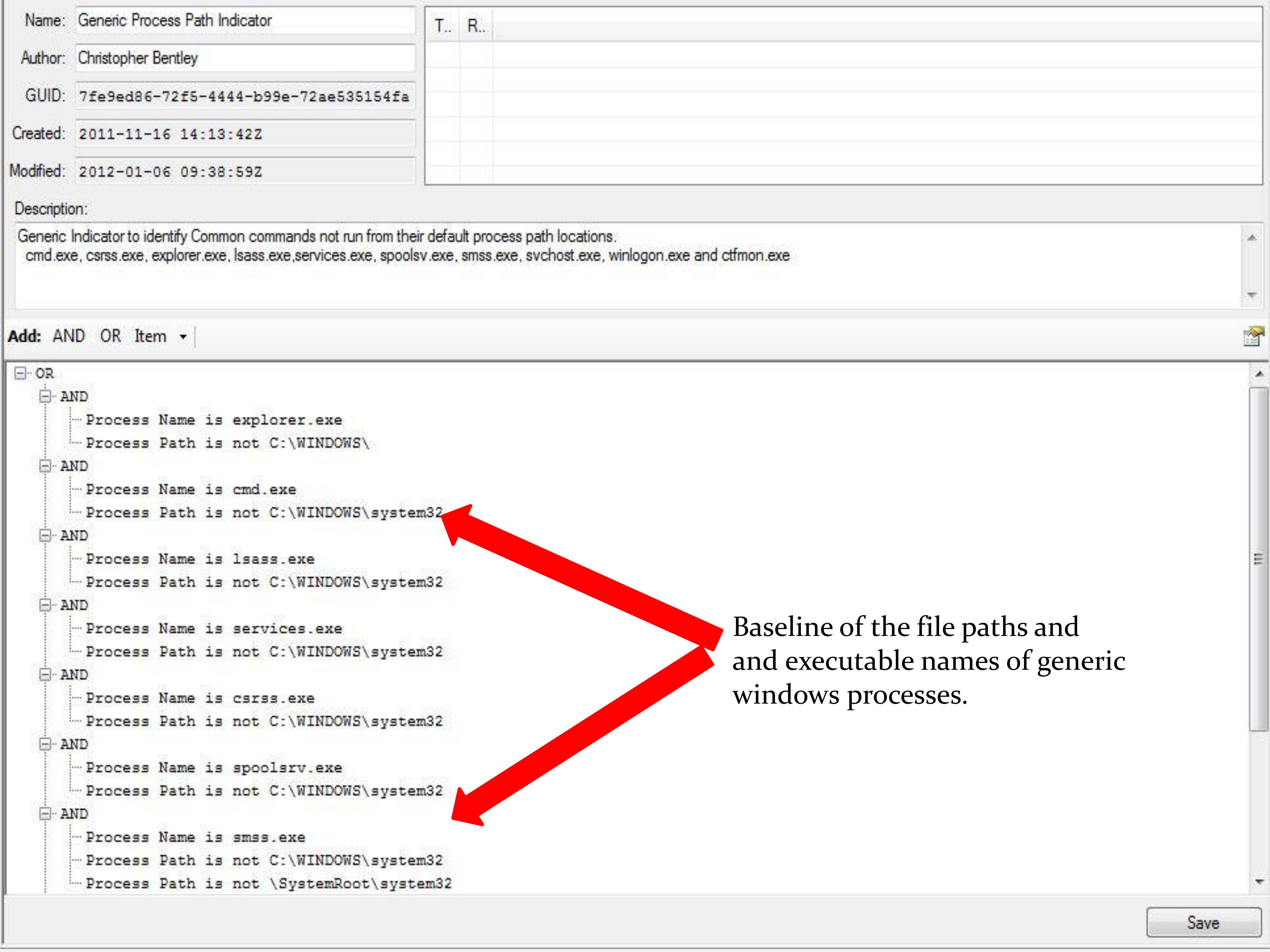
Description:

This IOC detects run and runonce persistence keys for executables that may be outside of the image baseline.

```
OR
  AND
    Registry Key Path contains HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
    AND
      Registry Value Name is not Energy Management
      Registry Value Name is not EnergyUtility
      Registry Value Name is not Lenovo EE Boot Optimizer
      Registry Value Name is not OnekeyStudio
      Registry Value Name is not RtHDVCpl
      Registry Value Name is not SynTPEnh
  AND
    Registry Key Path contains HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
    AND
      Registry Value Name is not default
```

Registry Key typically used for malware persistence

The registry key is baselined. All known good applications that should be present inside of this registry key are placed in the IOC.



Name: Generic Process Path Indicator

Author: Christopher Bentley

GUID: 7fe9ed86-72f5-4444-b99e-72ae535154fa

Created: 2011-11-16 14:13:42Z

Modified: 2012-01-06 09:38:59Z

Description:

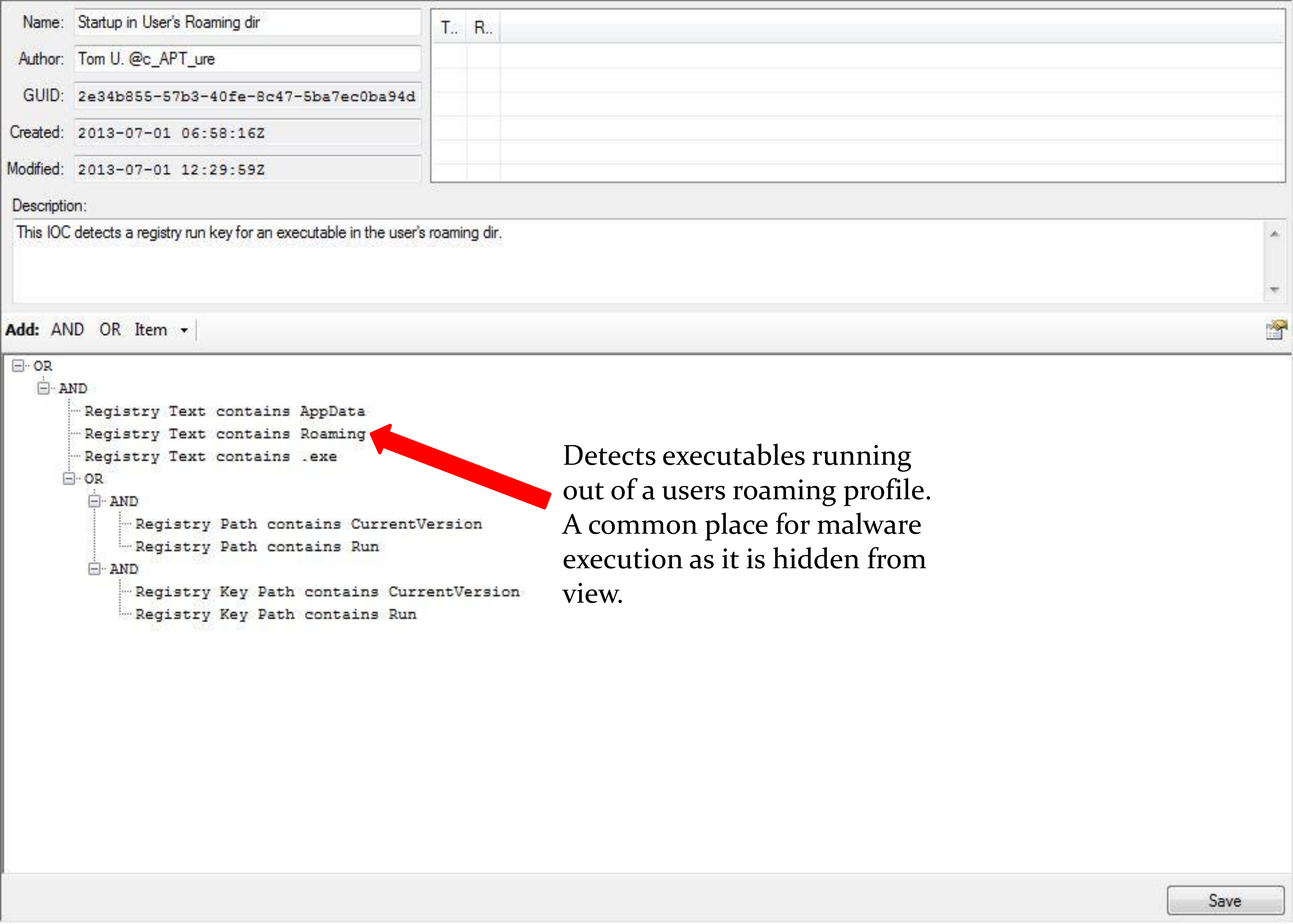
Generic Indicator to identify Common commands not run from their default process path locations.
cmd.exe, csrss.exe, explorer.exe, lsass.exe,services.exe, spoolsv.exe, smss.exe, svchost.exe, winlogon.exe and ctfmon.exe

```
OR
  AND
    Process Name is explorer.exe
    Process Path is not C:\WINDOWS\
  AND
    Process Name is cmd.exe
    Process Path is not C:\WINDOWS\system32
  AND
    Process Name is lsass.exe
    Process Path is not C:\WINDOWS\system32
  AND
    Process Name is services.exe
    Process Path is not C:\WINDOWS\system32
  AND
    Process Name is csrss.exe
    Process Path is not C:\WINDOWS\system32
  AND
    Process Name is spoolsrv.exe
    Process Path is not C:\WINDOWS\system32
  AND
    Process Name is smss.exe
    Process Path is not C:\WINDOWS\system32
    Process Path is not \SystemRoot\system32
```

Baseline of the file paths and
and executable names of generic
windows processes.

Hunting aka anomaly detection

- Hunt: Active Defense measure to “patrol” your network for anomalous activity.
- Requirements
  - IOC Repository
  - Method of Distribution
  - Host Sensor Net
  - Method of Rapid Data Collection
  - Method of IOC Comparison



Name: Startup in User's Roaming dir

Author: Tom U. @c_APT_ure

GUID: 2e34b855-57b3-40fe-8c47-5ba7ec0ba94d

Created: 2013-07-01 06:58:16Z

Modified: 2013-07-01 12:29:59Z

Description:

This IOC detects a registry run key for an executable in the user's roaming dir.

```
OR
  AND
    Registry Text contains AppData
    Registry Text contains Roaming
    Registry Text contains .exe
    OR
      AND
        Registry Path contains CurrentVersion
        Registry Path contains Run
      AND
        Registry Key Path contains CurrentVersion
        Registry Key Path contains Run
```

Detects executables running out of a users roaming profile. A common place for malware execution as it is hidden from view.

Open Source Intelligence

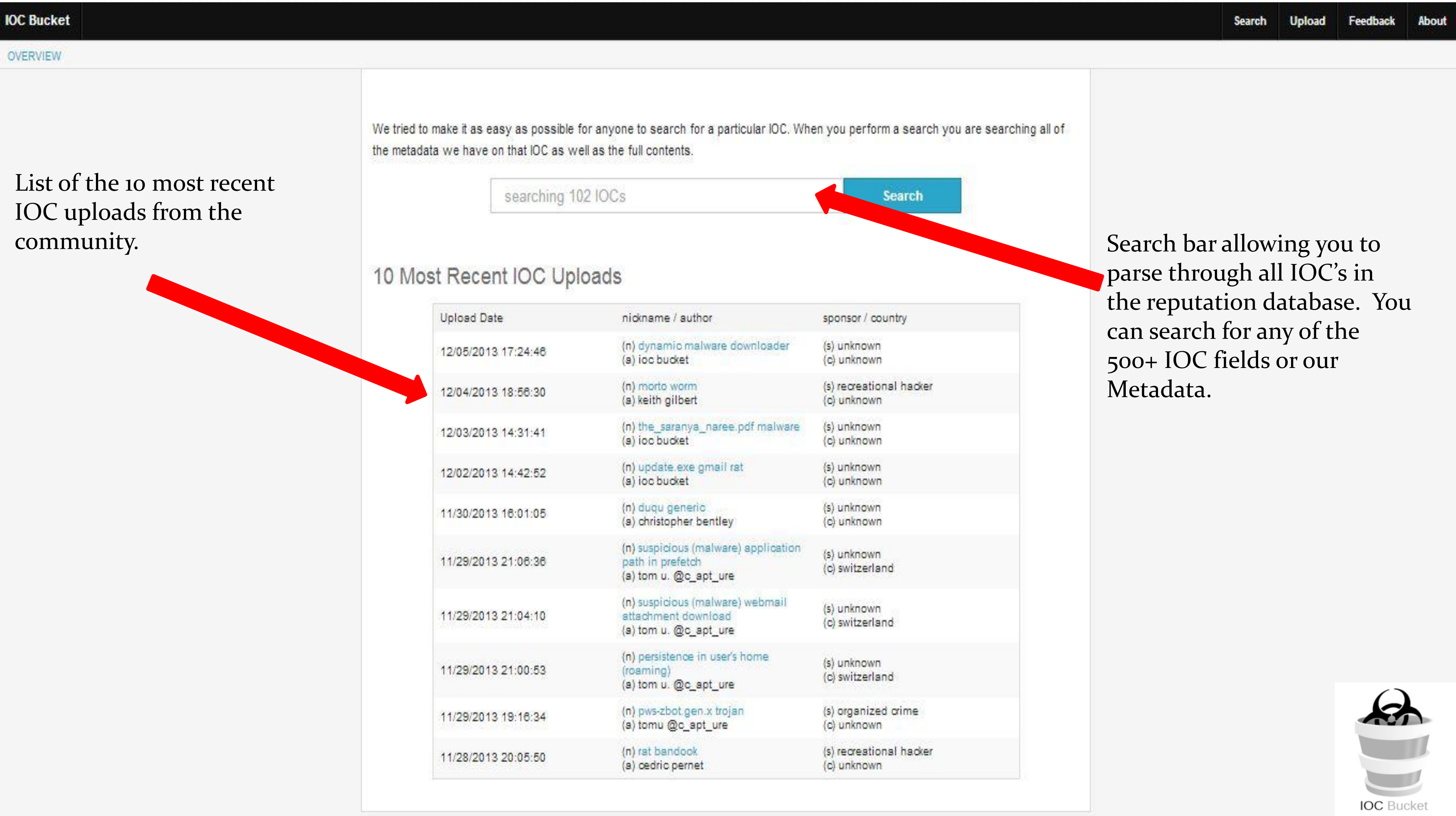
- Global community of security experts dedicated to the sharing of information and intelligence
- Network Security Providers are contributing
- All have been submitted to the community and many more

iocbucket.com

- Largest source of open indicators of compromise on the internet
- Open source Computer Network Counter Intelligence (CNCI) to industrial base
- A centralized open source collection of indicators makes it easy for even the smallest company to attain some intelligence to defend themselves

IOC Bucket

iocbucket.com



We tried to make it as easy as possible for anyone to search for a particular IOC. When you perform a search you are searching all of the metadata we have on that IOC as well as the full contents.

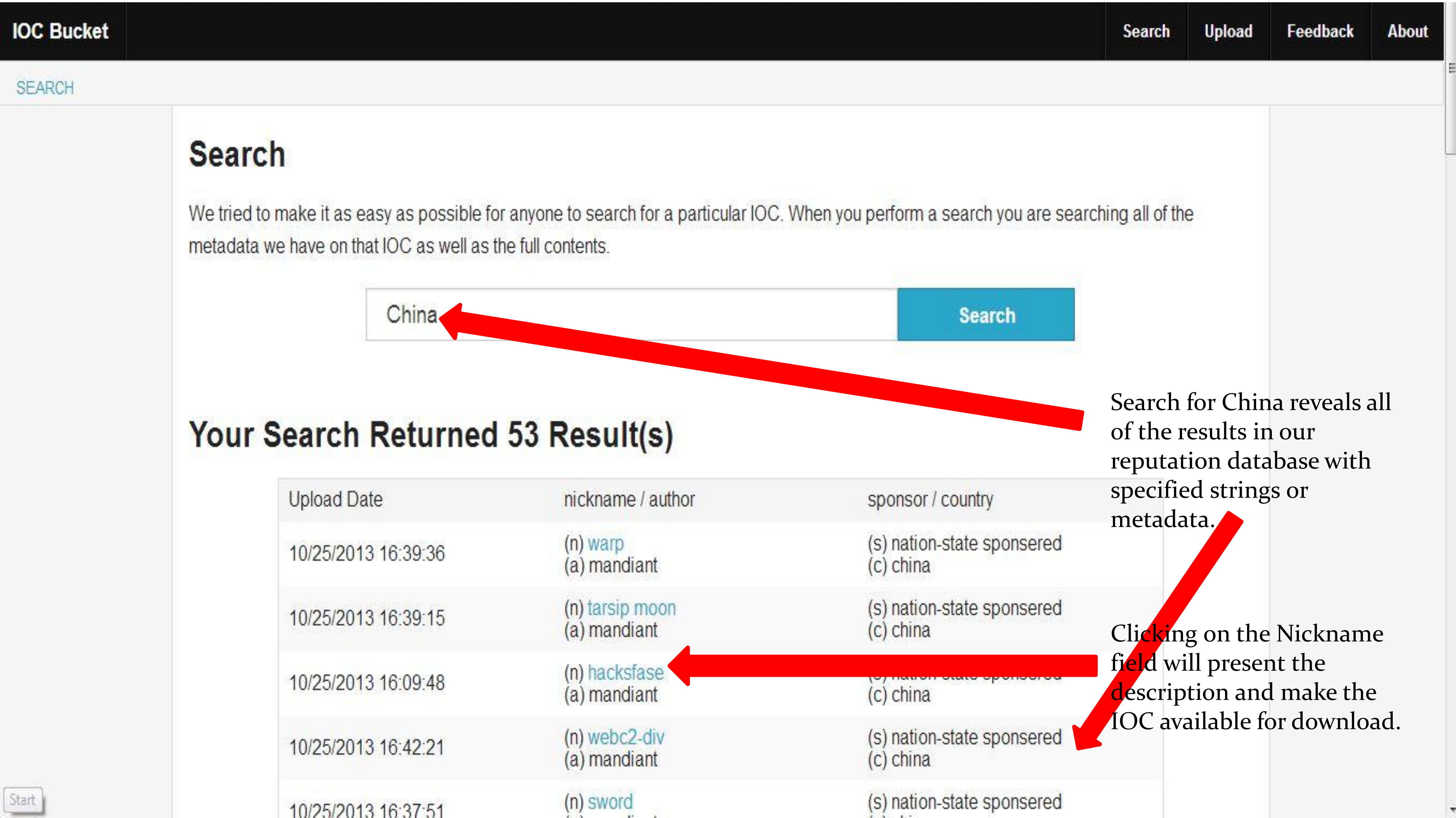
List of the 10 most recent IOC uploads from the community.

Search bar allowing you to parse through all IOC's in the reputation database. You can search for any of the 500+ IOC fields or our Metadata.

10 Most Recent IOC Uploads

Upload Date	nickname / author	sponsor / country
12/05/2013 17:24:46	(n) dynamic malware downloader (a) ioc bucket	(s) unknown (c) unknown
12/04/2013 18:56:30	(n) morto worm (a) keith gilbert	(s) recreational hacker (c) unknown
12/03/2013 14:31:41	(n) the_saranya_naree.pdf malware (a) ioc bucket	(s) unknown (c) unknown
12/02/2013 14:42:52	(n) update.exe gmail rat (a) ioc bucket	(s) unknown (c) unknown
11/30/2013 16:01:05	(n) duqu generic (a) christopher bentley	(s) unknown (c) unknown
11/29/2013 21:06:36	(n) suspicious (malware) application path in prefetch (a) tom u. @c_apt_ure	(s) unknown (c) switzerland
11/29/2013 21:04:10	(n) suspicious (malware) webmail attachment download (a) tom u. @c_apt_ure	(s) unknown (c) switzerland
11/29/2013 21:00:53	(n) persistence in user's home (roaming) (a) tom u. @c_apt_ure	(s) unknown (c) switzerland
11/29/2013 19:16:34	(n) pws-zbot.gen.x trojan (a) tomu @c_apt_ure	(s) organized crime (c) unknown
11/28/2013 20:05:50	(n) rat bandook (a) cedric pernet	(s) recreational hacker (c) unknown

Search Field



Search

We tried to make it as easy as possible for anyone to search for a particular IOC. When you perform a search you are searching all of the metadata we have on that IOC as well as the full contents.

China

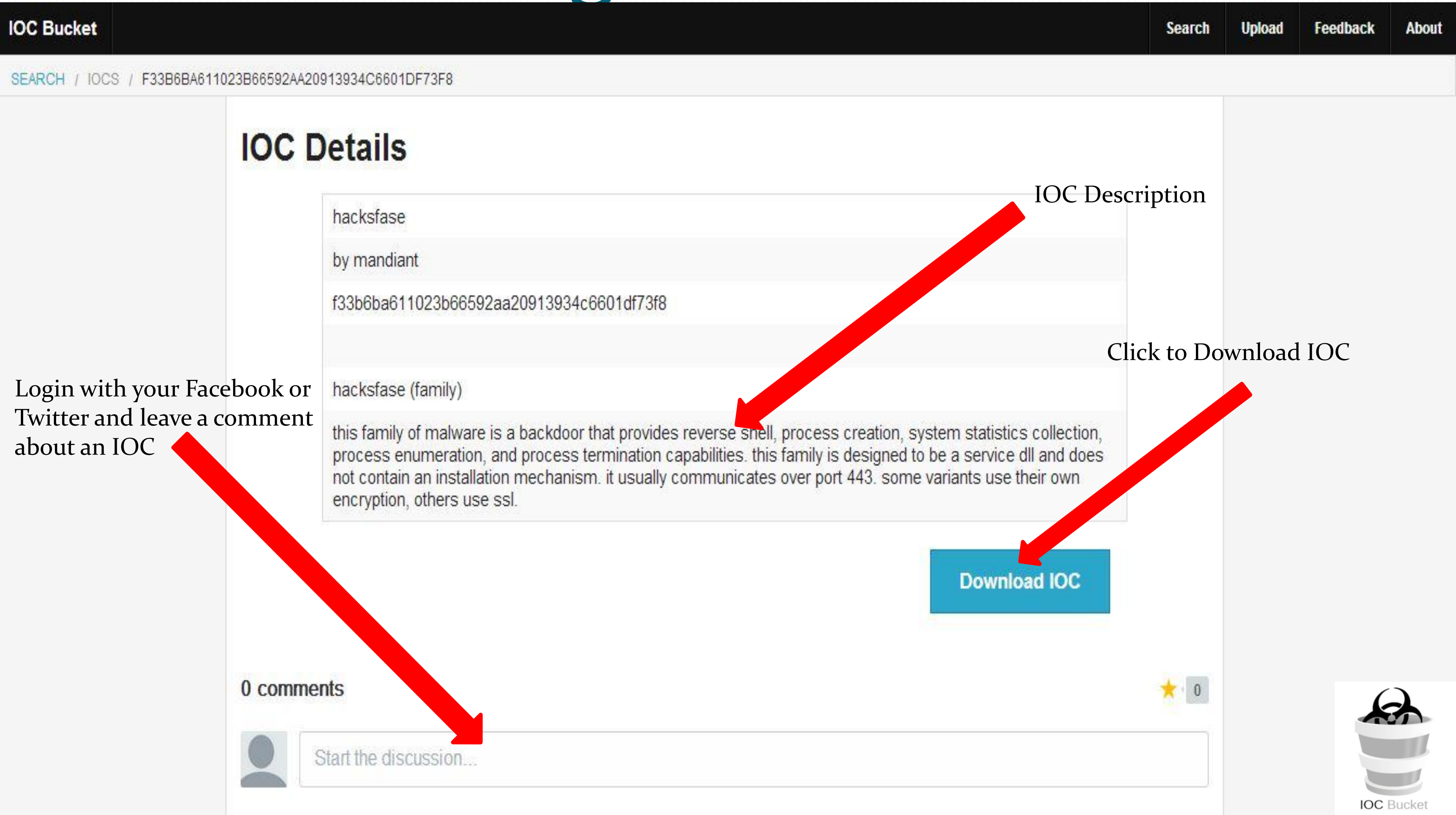
Your Search Returned 53 Result(s)

Upload Date	nickname / author	sponsor / country
10/25/2013 16:39:36	(n) warp (a) mandiant	(s) nation-state sponsered (c) china
10/25/2013 16:39:15	(n) tarsip moon (a) mandiant	(s) nation-state sponsered (c) china
10/25/2013 16:09:48	(n) hacksfase (a) mandiant	(c) china
10/25/2013 16:42:21	(n) webc2-div (a) mandiant	(s) nation-state sponsered (c) china
10/25/2013 16:37:51	(n) sword	(s) nation-state sponsered

Search for China reveals all of the results in our reputation database with specified strings or metadata.

Clicking on the Nickname field will present the description and make the IOC available for download.

Downloading



IOC Details

hacksfase

by mandiant

f33b6ba611023b66592aa20913934c6601df73f8

hacksfase (family)

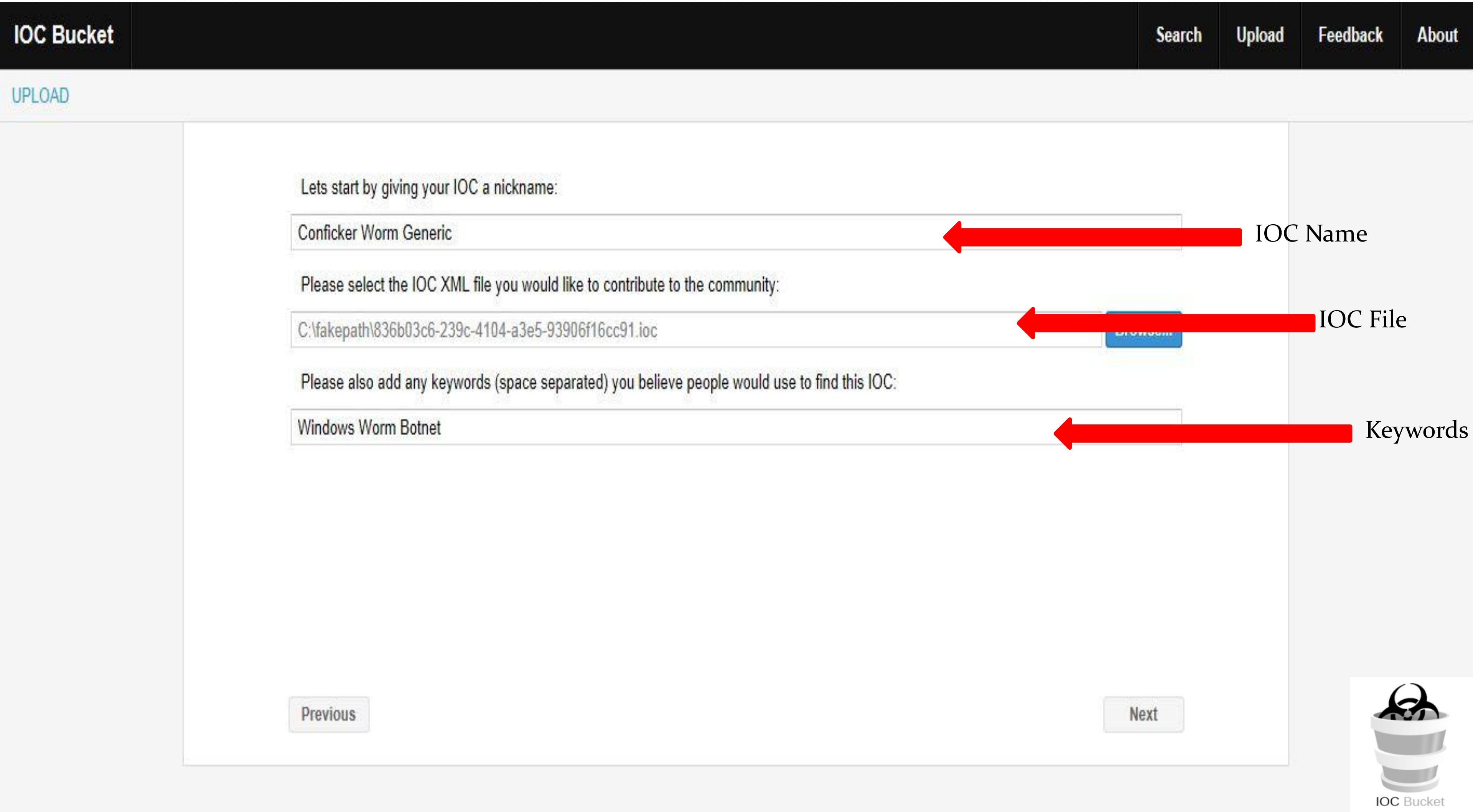
this family of malware is a backdoor that provides reverse shell, process creation, system statistics collection, process enumeration, and process termination capabilities. this family is designed to be a service dll and does not contain an installation mechanism. it usually communicates over port 443. some variants use their own encryption, others use ssl.

IOC Description

Click to Download IOC

Login with your Facebook or Twitter and leave a comment about an IOC

Uploading



Lets start by giving your IOC a nickname:

Conficker Worm Generic

Please select the IOC XML file you would like to contribute to the community:

C:\fakepath\836b03c6-239c-4104-a3e5-93906f16cc91.ioc

Please also add any keywords (space separated) you believe people would use to find this IOC:

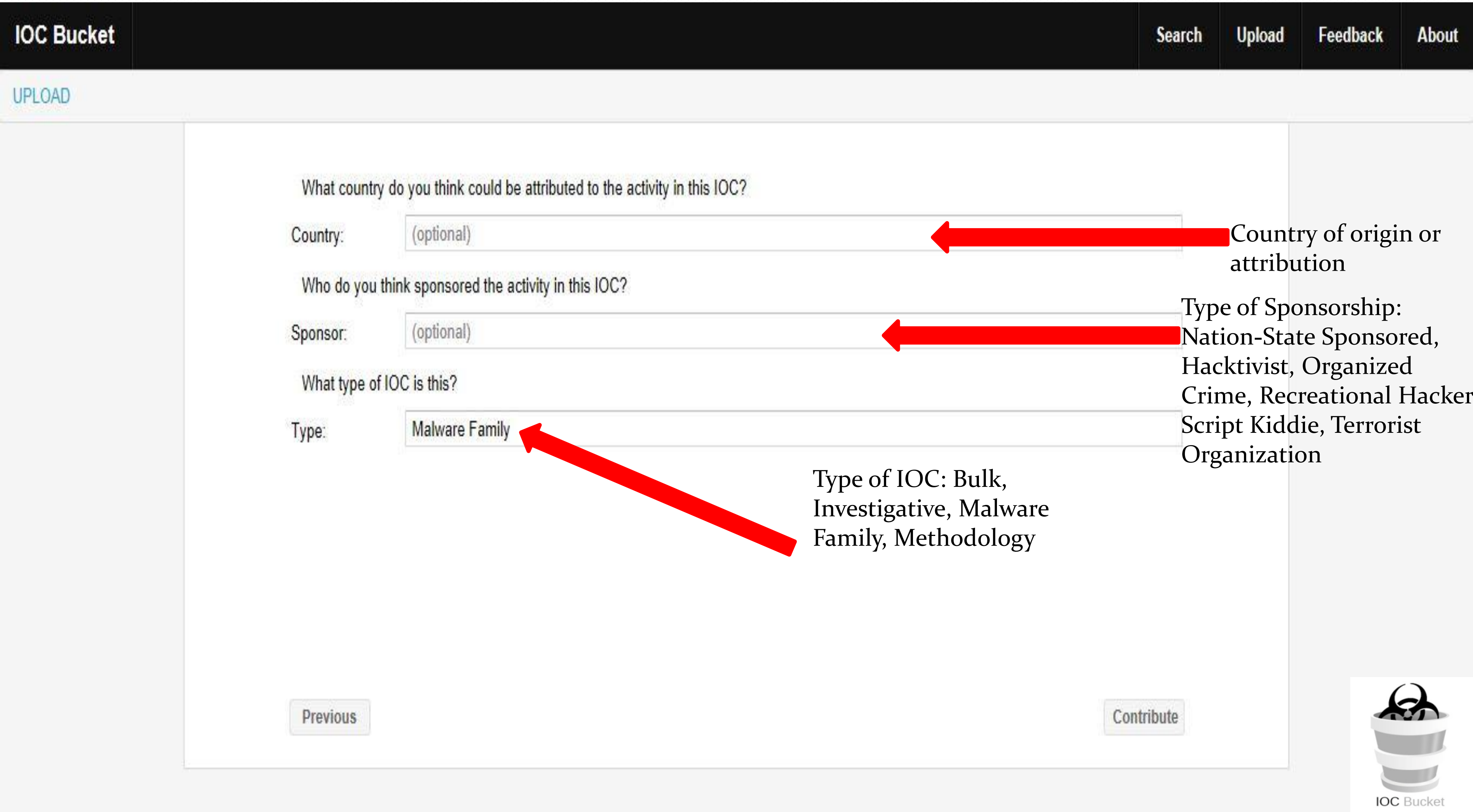
Windows Worm Botnet

IOC Name

IOC File

Keywords

Metadata



What country do you think could be attributed to the activity in this IOC?

Country: (optional)

Who do you think sponsored the activity in this IOC?

Sponsor: (optional)

What type of IOC is this?

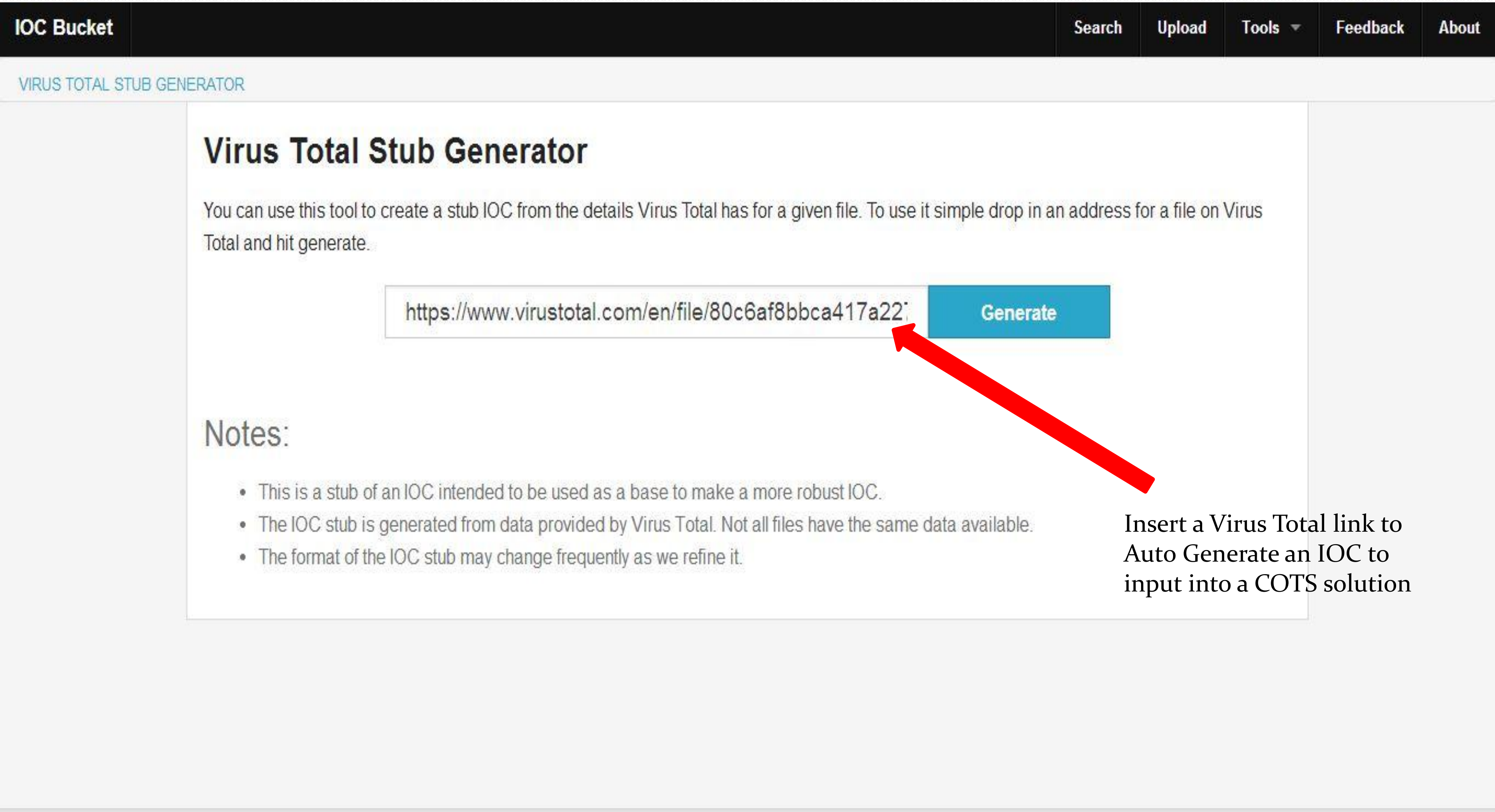
Type: Malware Family

Country of origin or attribution

Type of Sponsorship: Nation-State Sponsored, Hacktivist, Organized Crime, Recreational Hacker Script Kiddie, Terrorist Organization

Type of IOC: Bulk, Investigative, Malware Family, Methodology

Virus Total IOC Generator



Virus Total Stub Generator

You can use this tool to create a stub IOC from the details Virus Total has for a given file. To use it simple drop in an address for a file on Virus Total and hit generate.

https://www.virustotal.com/en/file/80c6af8bbca417a227

Notes:

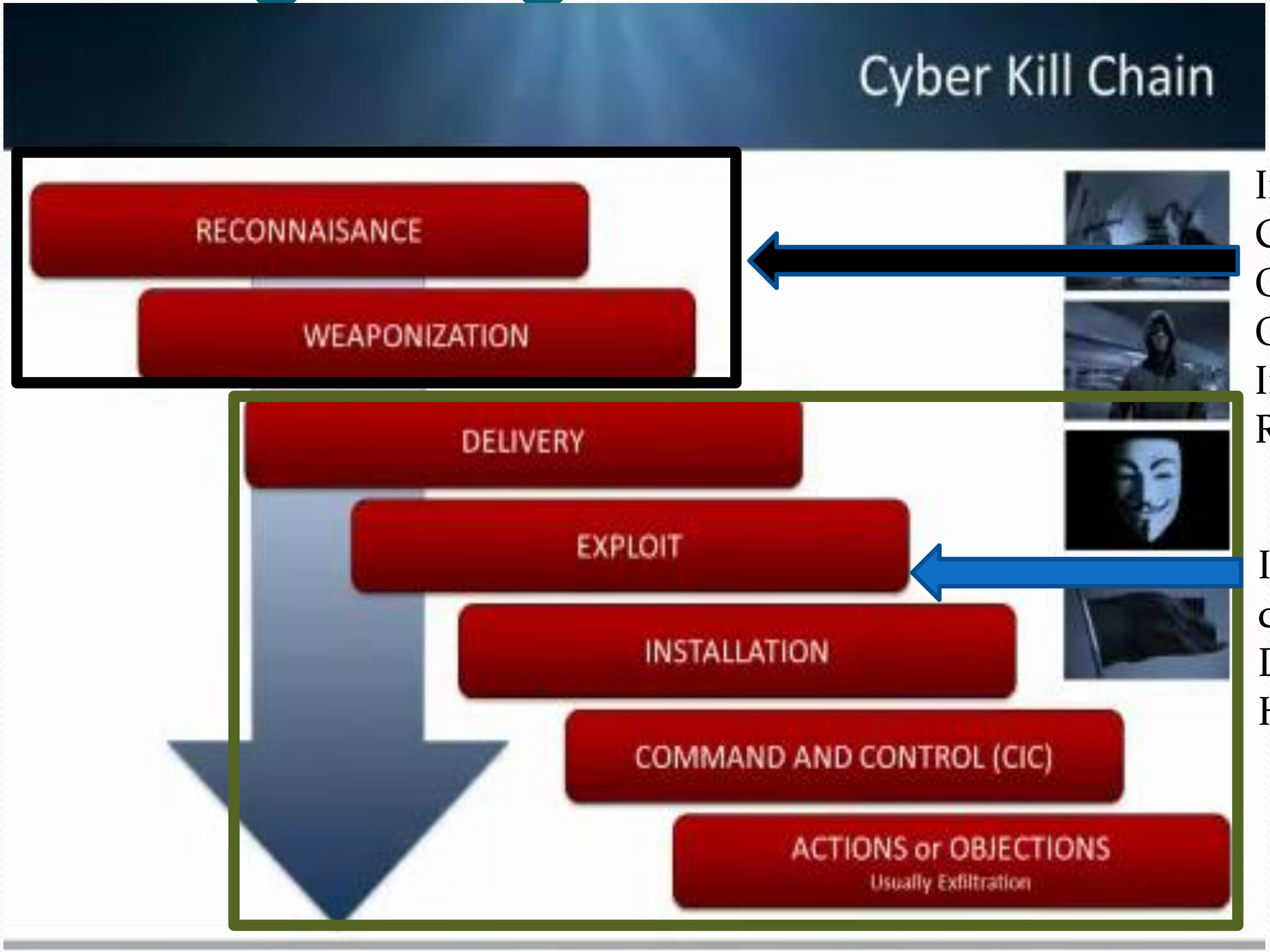
- This is a stub of an IOC intended to be used as a base to make a more robust IOC.
- The IOC stub is generated from data provided by Virus Total. Not all files have the same data available.
- The format of the IOC stub may change frequently as we refine it.

Insert a Virus Total link to Auto Generate an IOC to input into a COTS solution

Future Outlook

- In the next 6 to 8 months iocbucket.com will be the largest online database of OpenIOC’s, Yara Rules, CybOX, Snort, etc…
- Malwr.com Rule Generation
- Sandbox Rule Generation

Integrating Intel and Defense



Cyber Kill Chain

RECONNAISANCE

WEAPONIZATION

DELIVERY

EXPLOIT

INSTALLATION

COMMAND AND CONTROL (CIC)

ACTIONS or OBJECTIONS

Usually Exfiltration

Intelligence Collected via Organizational and Open Source Intelligence Resources.

IOC Signatures to conduct Intrusion Detection and Hunting Operations

COTS Solutions Integrating IOC’s

- Mandiant
  - IOC Finder
  - IOC Editor
  - Redline
- CloudHash Security Host Sentinel
- McAfee Real Time (Tanium)
- Splunk
- CyTech Solutions Cypher
- Many more probably can’t name them all

Questions

@iocbucket

IOC Bucket

IOC Bucket