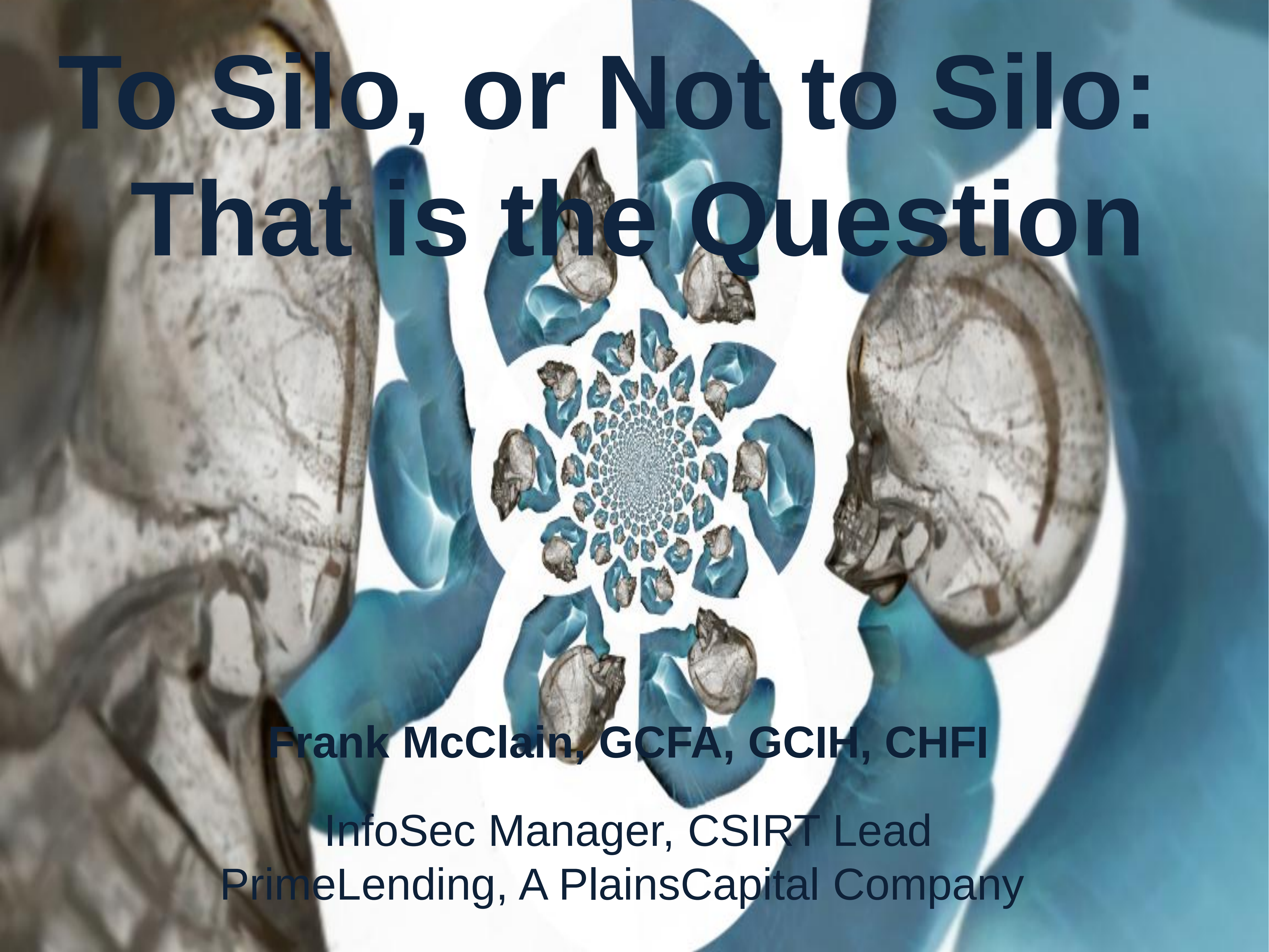
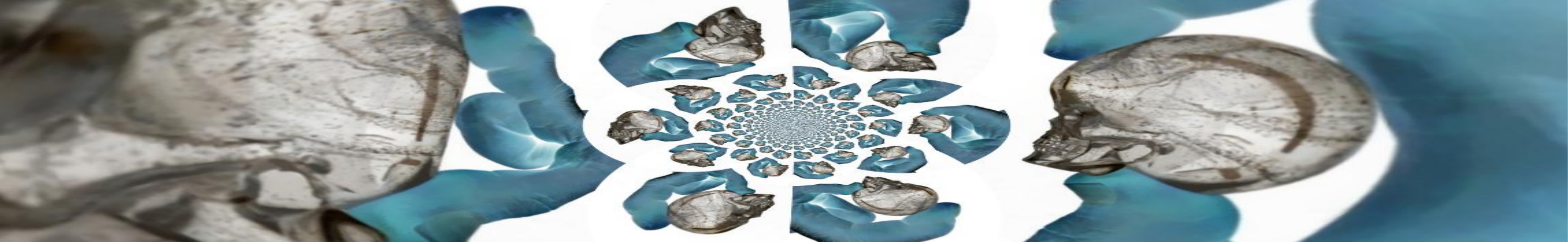


To Silo, or Not to Silo: That is the Question

Frank McClain, GCFA, GCIH, CHFI

InfoSec Manager, CSIRT Lead
PrimeLending, A PlainsCapital Company



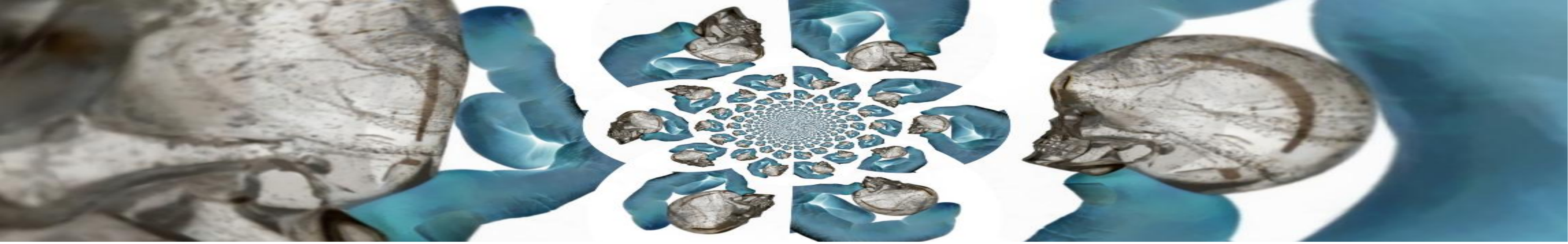
Systems

Network

Cloud

Mobile

One thing in common: All are sources of evidence



DHCP DNS Netflow Firewall

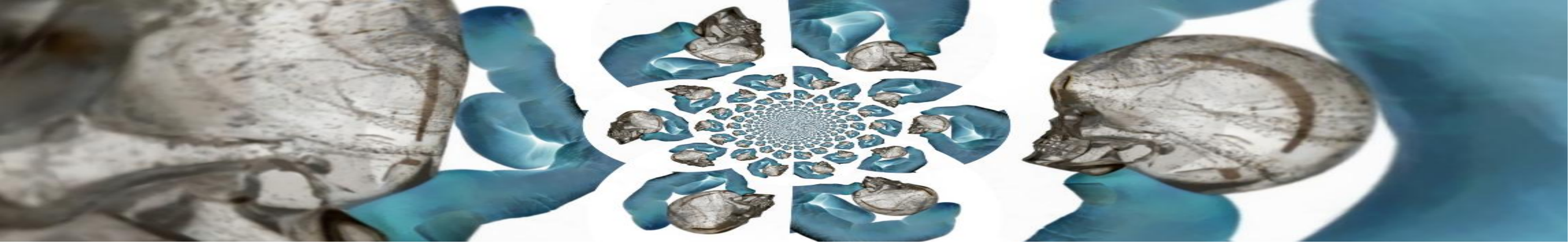
Proxy DLP IDS/IPS NSM

RE RAM Timeline Triage

Disk Image Event Logs HIPS AV

Backups Restore Points Prefetch

Registry VMDK Temp Files Browser Cache



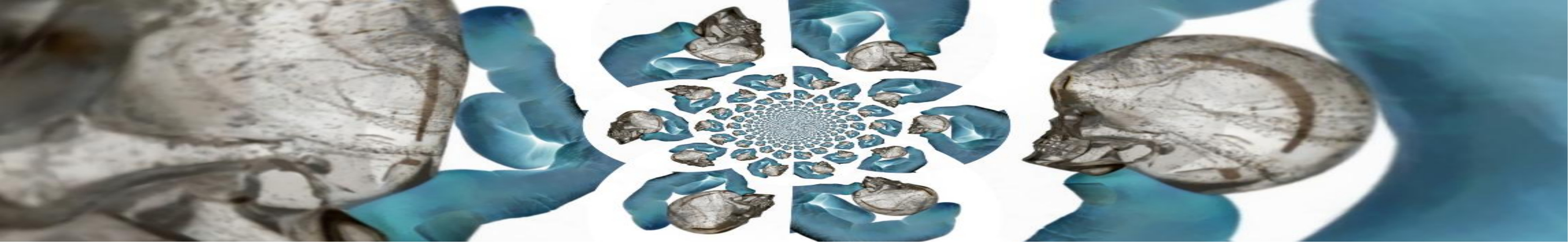
Host

Traditional: Full Disk Imaging, VMDK, Timelines, Registry, Restore Points, Prefetch, Temp Files, Browser Cache, Volatile Data

Event Logs: Antivirus, EMET, System, Application, Firewall, HIPS

Volatile/Focused: Triage (targeted collections), RAM, RE

Advanced: Host monitoring, threat feeds, C2 traffic



Network

Logs: DHCP, DNS, Proxy, Firewall

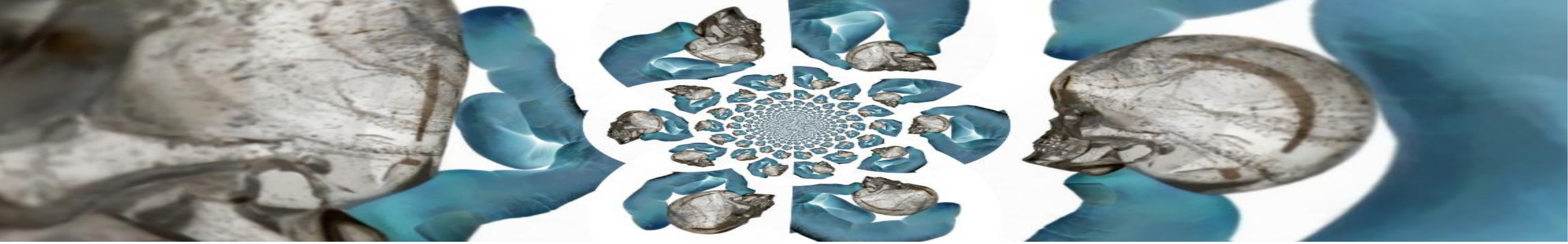
Events: IDS/IPS, Firewall, DLP, WAF

SIEM: Event/System Logs

NSM: Streaming packet capture, ad hoc pcap, netflow

Advanced: Threat feeds, C2 traffic, encrypted binaries

Vulnerability Scans: Historical scan data

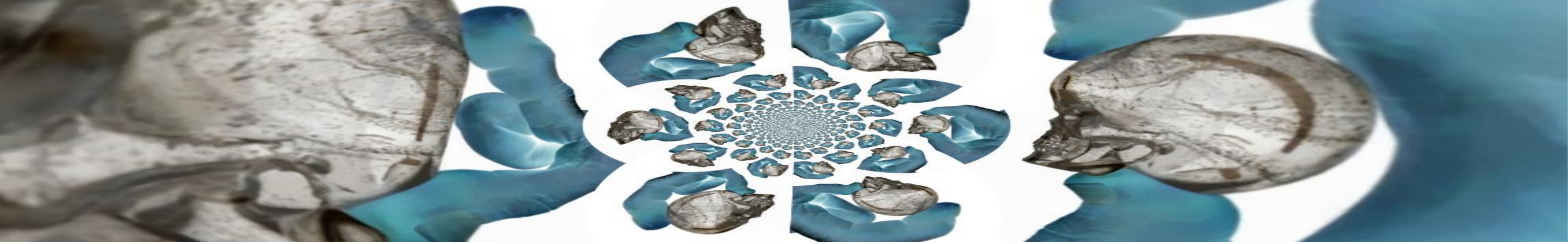


Cloud

Limited data if third-party hosted

VMDK Files

Correlate to activity you “own”

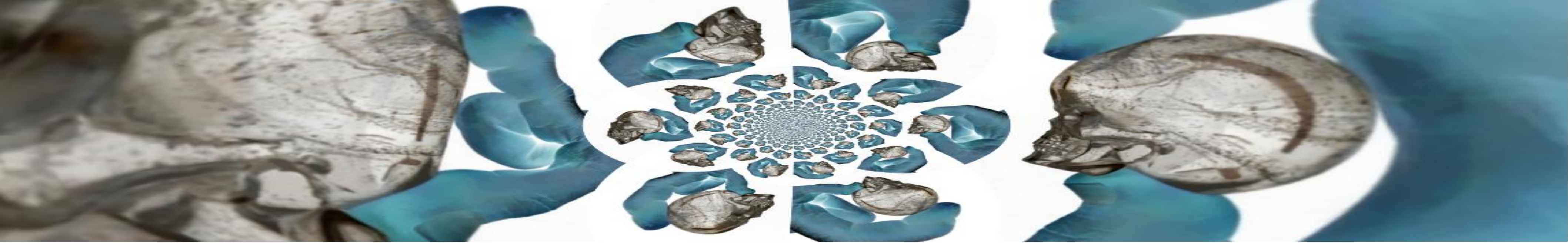


Mobile

Limited access (BYOD)

Correlate to activity you “own”

Always changing/updating

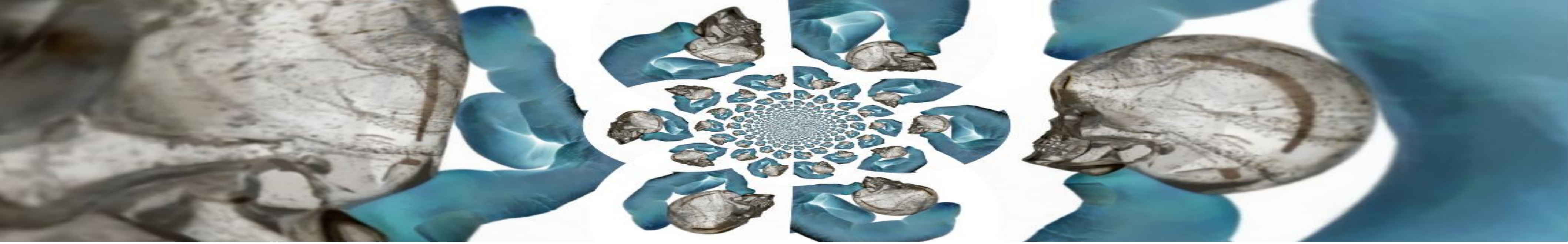


Investigation Trifecta

Observation
(Gather information/evidence, prepare to answer questions)

Interpretation
(Understanding the evidence – you can't jump to this step)

Application
(Putting it all together – resolution/recommendations)



Talk is cheap, show me the money...

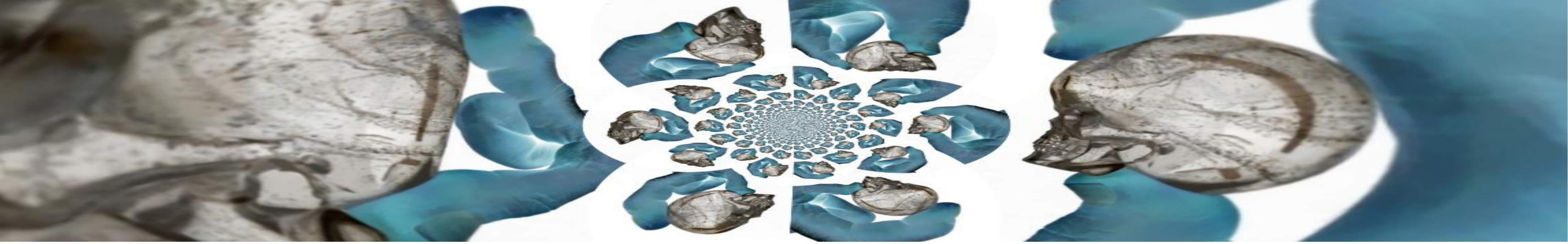
Zbot Infection

Banload Trojan

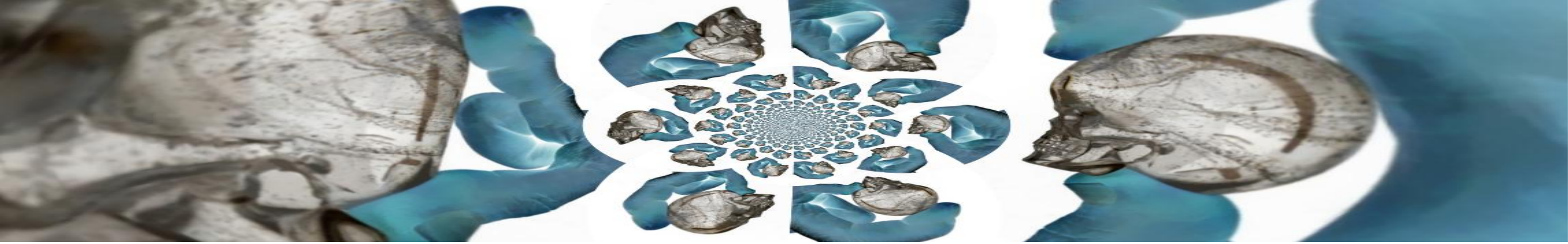
Kuluoz (or Dofoil) Trojan

User Activity

LSASS Child Process

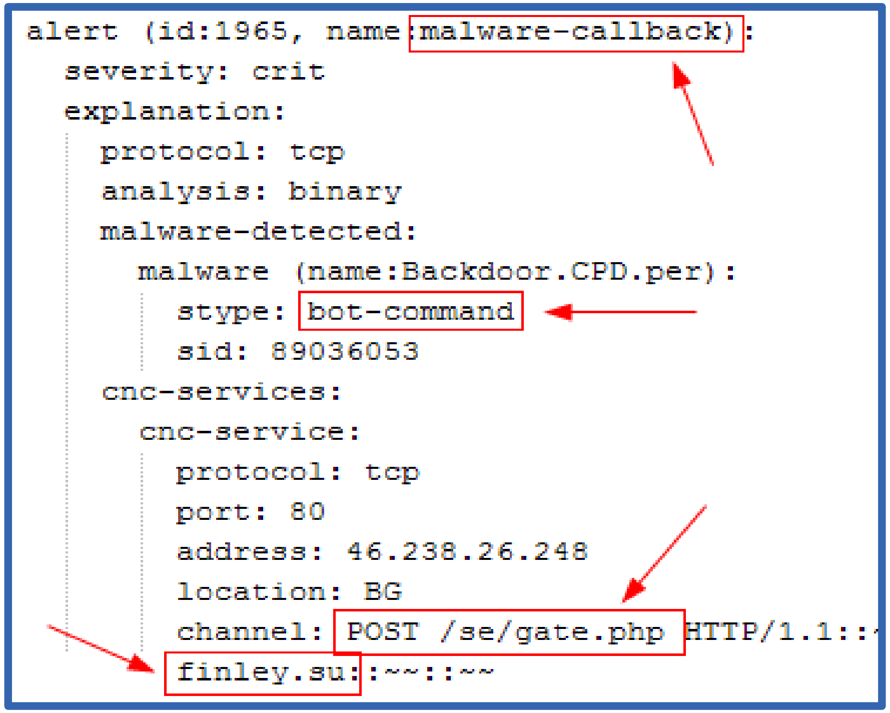


Zbot Infection

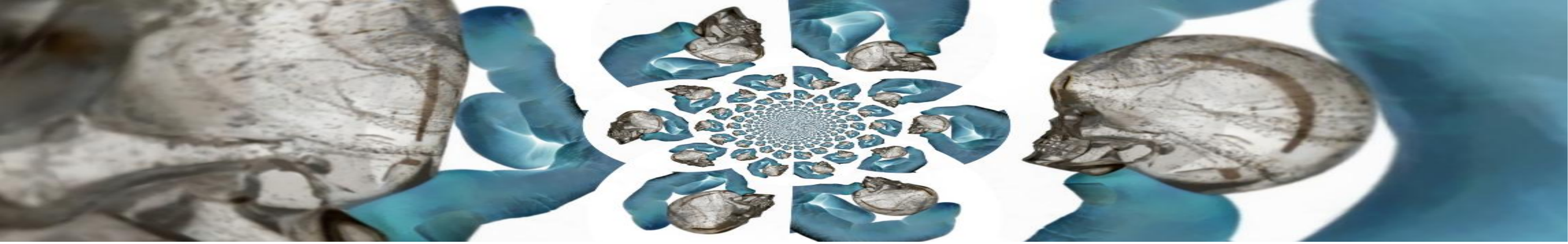


Zbot (1)

Trigger: Alert from malware detection platform, for C2 traffic:

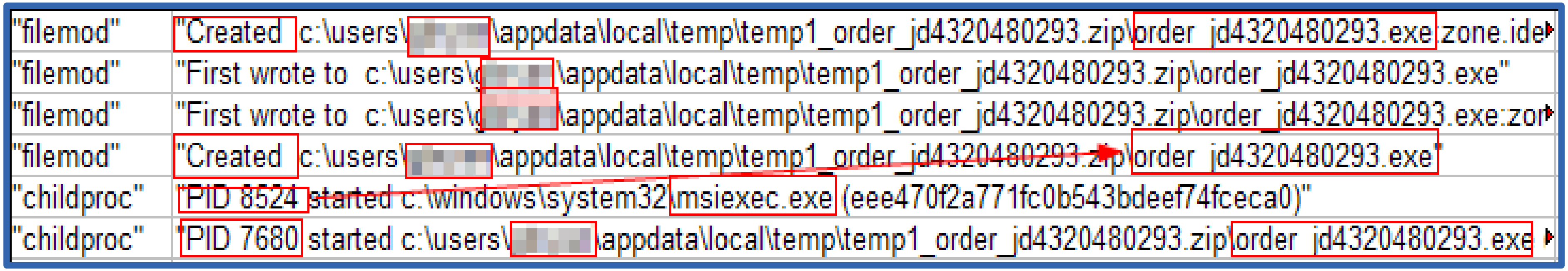


```
alert (id:1965, name:malware-callback):
  severity: crit
  explanation:
    protocol: tcp
    analysis: binary
    malware-detected:
      malware (name:Backdoor.CPD.per):
        stype: bot-command
        sid: 89036053
    cnc-services:
      cnc-service:
        protocol: tcp
        port: 80
        address: 46.238.26.248
        location: BG
        channel: POST /se/gate.php HTTP/1.1::
        finley.su::~~::~~
```

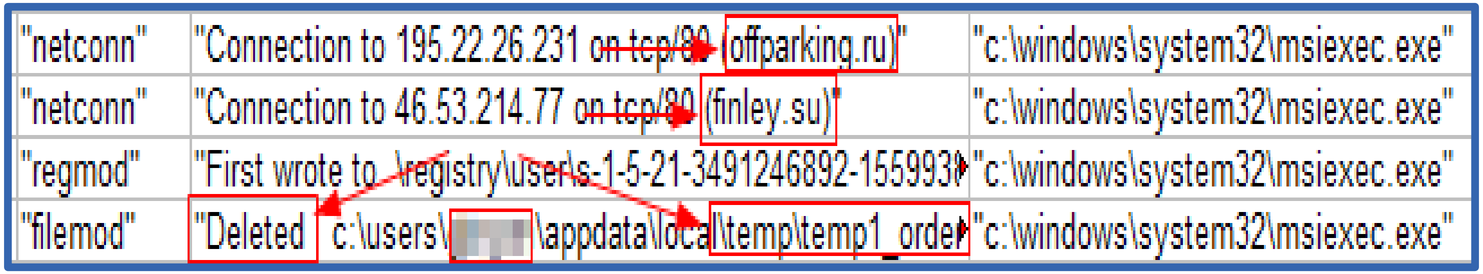


Zbot (2)

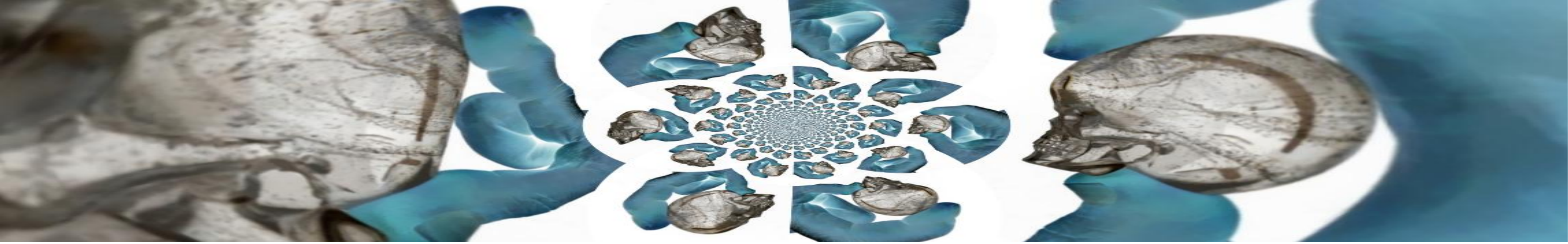
Filesystem: Point of Infection, malware self-cleanup



"filemod"	"Created c:\users\[redacted]\appdata\local\temp\temp1_order_jd4320480293.zip\order_jd4320480293.exe:zone.ide
"filemod"	"First wrote to c:\users\[redacted]\appdata\local\temp\temp1_order_jd4320480293.zip\order_jd4320480293.exe"
"filemod"	"First wrote to c:\users\[redacted]\appdata\local\temp\temp1_order_jd4320480293.zip\order_jd4320480293.exe:zor
"filemod"	"Created c:\users\[redacted]\appdata\local\temp\temp1_order_jd4320480293.zip\order_jd4320480293.exe"
"childproc"	"PID 8524 started c:\windows\system32\msiexec.exe (eee470f2a771fc0b543bdeef74fceca0)"
"childproc"	"PID 7680 started c:\users\[redacted]\appdata\local\temp\temp1_order_jd4320480293.zip\order_jd4320480293.exe

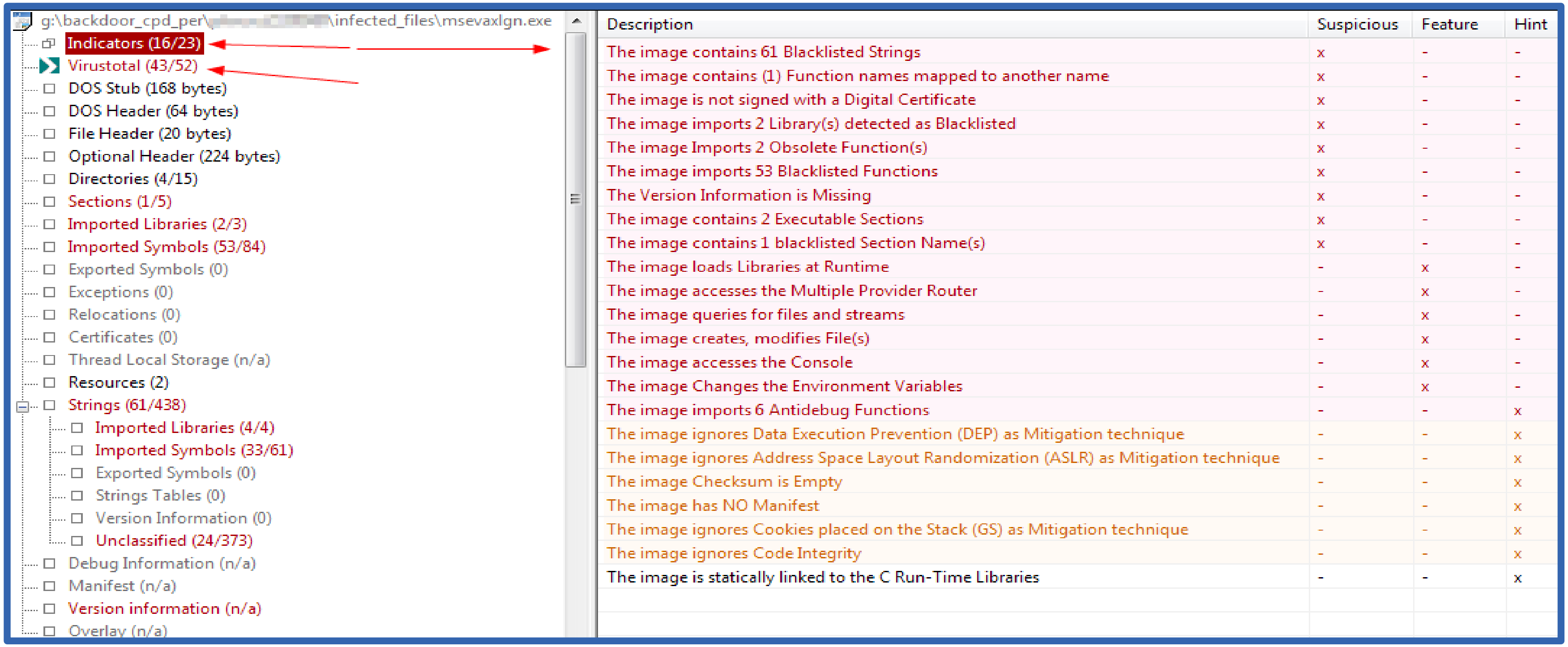


"netconn"	"Connection to 195.22.26.231 on tcp/80 (offparking.ru)"	"c:\windows\system32\msiexec.exe"
"netconn"	"Connection to 46.53.214.77 on tcp/80 (finley.su)"	"c:\windows\system32\msiexec.exe"
"regmod"	"First wrote to \registry\user\s-1-5-21-3491246892-155993	"c:\windows\system32\msiexec.exe"
"filemod"	"Deleted c:\users\[redacted]\appdata\local\temp\temp1_order	"c:\windows\system32\msiexec.exe"



Zbot (3)

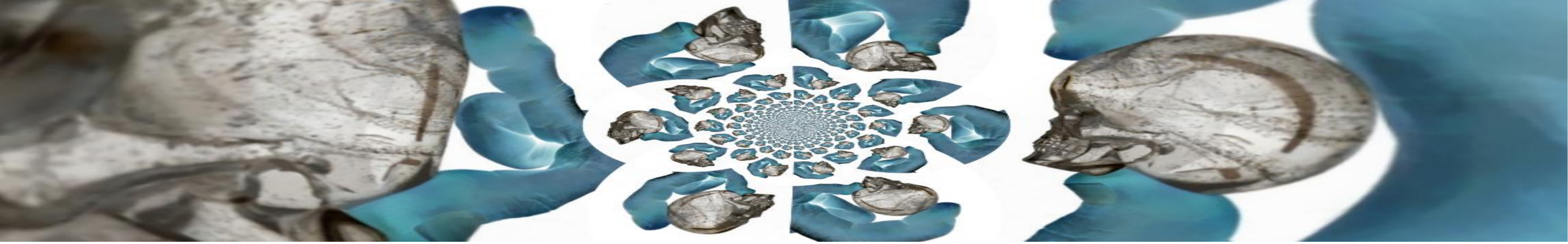
Binary Analysis: (order_jd4320480293.exe, msevaxlgn.exe, mssuhin.exe, msyaam.exe) - all with the same hash



g:\backdoor_cpd_per\[redacted]\infected_files\msevaxlgn.exe

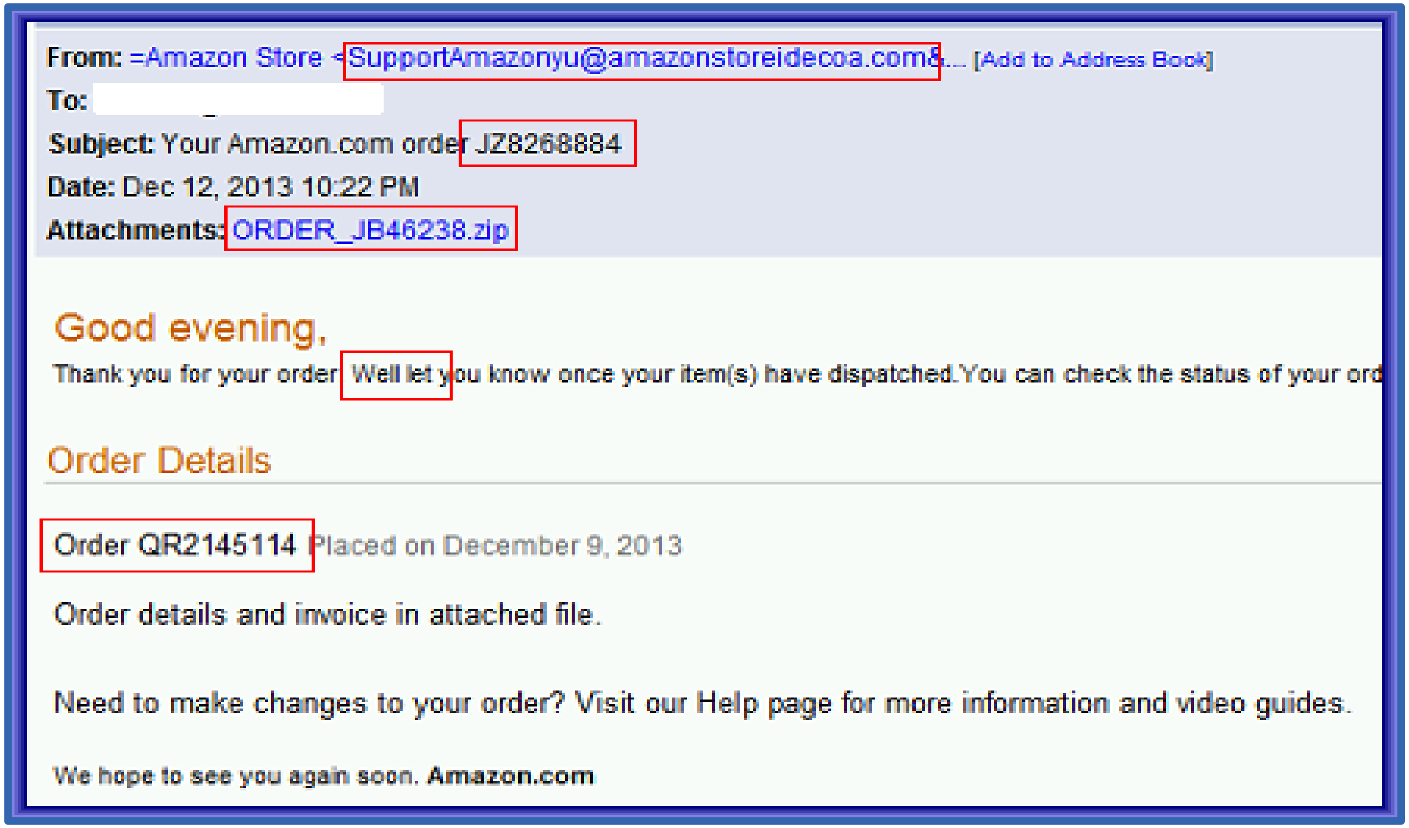
- Indicators (16/23)
- Virustotal (43/52)
- □ DOS Stub (168 bytes)
- □ DOS Header (64 bytes)
- □ File Header (20 bytes)
- □ Optional Header (224 bytes)
- □ Directories (4/15)
- □ Sections (1/5)
- □ Imported Libraries (2/3)
- □ Imported Symbols (53/84)
- □ Exported Symbols (0)
- □ Exceptions (0)
- □ Relocations (0)
- □ Certificates (0)
- □ Thread Local Storage (n/a)
- □ Resources (2)
- □ Strings (61/438)
  - □ Imported Libraries (4/4)
  - □ Imported Symbols (33/61)
  - □ Exported Symbols (0)
  - □ Strings Tables (0)
  - □ Version Information (0)
  - □ Unclassified (24/373)
- □ Debug Information (n/a)
- □ Manifest (n/a)
- □ Version information (n/a)
- □ Overlay (n/a)

Description	Suspicious	Feature	Hint
The image contains 61 Blacklisted Strings	x	-	-
The image contains (1) Function names mapped to another name	x	-	-
The image is not signed with a Digital Certificate	x	-	-
The image imports 2 Library(s) detected as Blacklisted	x	-	-
The image Imports 2 Obsolete Function(s)	x	-	-
The image imports 53 Blacklisted Functions	x	-	-
The Version Information is Missing	x	-	-
The image contains 2 Executable Sections	x	-	-
The image contains 1 blacklisted Section Name(s)	x	-	-
The image loads Libraries at Runtime	-	x	-
The image accesses the Multiple Provider Router	-	x	-
The image queries for files and streams	-	x	-
The image creates, modifies File(s)	-	x	-
The image accesses the Console	-	x	-
The image Changes the Environment Variables	-	x	-
The image imports 6 Antidebug Functions	-	-	x
The image ignores Data Execution Prevention (DEP) as Mitigation technique	-	-	x
The image ignores Address Space Layout Randomization (ASLR) as Mitigation technique	-	-	x
The image Checksum is Empty	-	-	x
The image has NO Manifest	-	-	x
The image ignores Cookies placed on the Stack (GS) as Mitigation technique	-	-	x
The image ignores Code Integrity	-	-	x
The image is statically linked to the C Run-Time Libraries	-	-	x



Zbot (5)

Vector: Personal email via the web...



From: =Amazon Store <SupportAmazonyu@amazonstoreidecoa.com&... [Add to Address Book]

To: [redacted]

Subject: Your Amazon.com order JZ8268884

Date: Dec 12, 2013 10:22 PM

Attachments: ORDER_JB46238.zip

Good evening,

Thank you for your order. Well let you know once your item(s) have dispatched.You can check the status of your ord

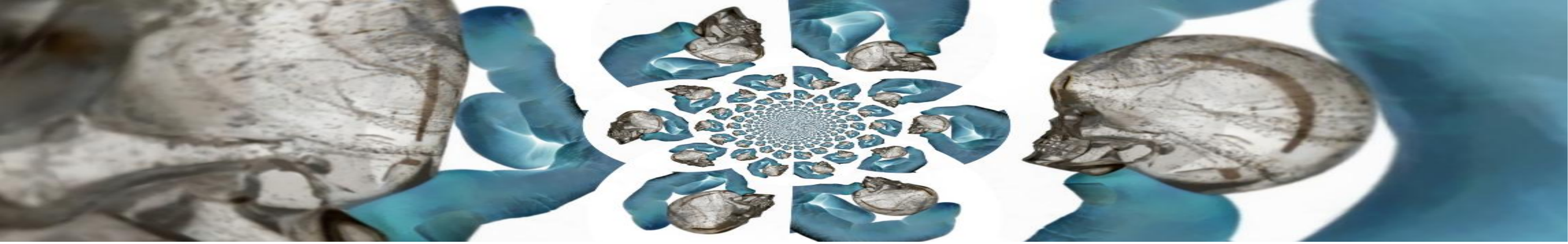
Order Details

Order QR2145114 Placed on December 9, 2013

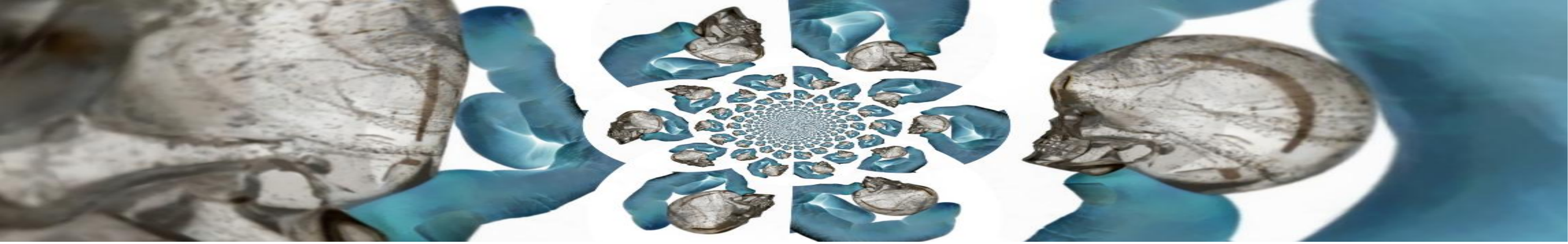
Order details and invoice in attached file.

Need to make changes to your order? Visit our Help page for more information and video guides.

We hope to see you again soon. **Amazon.com**

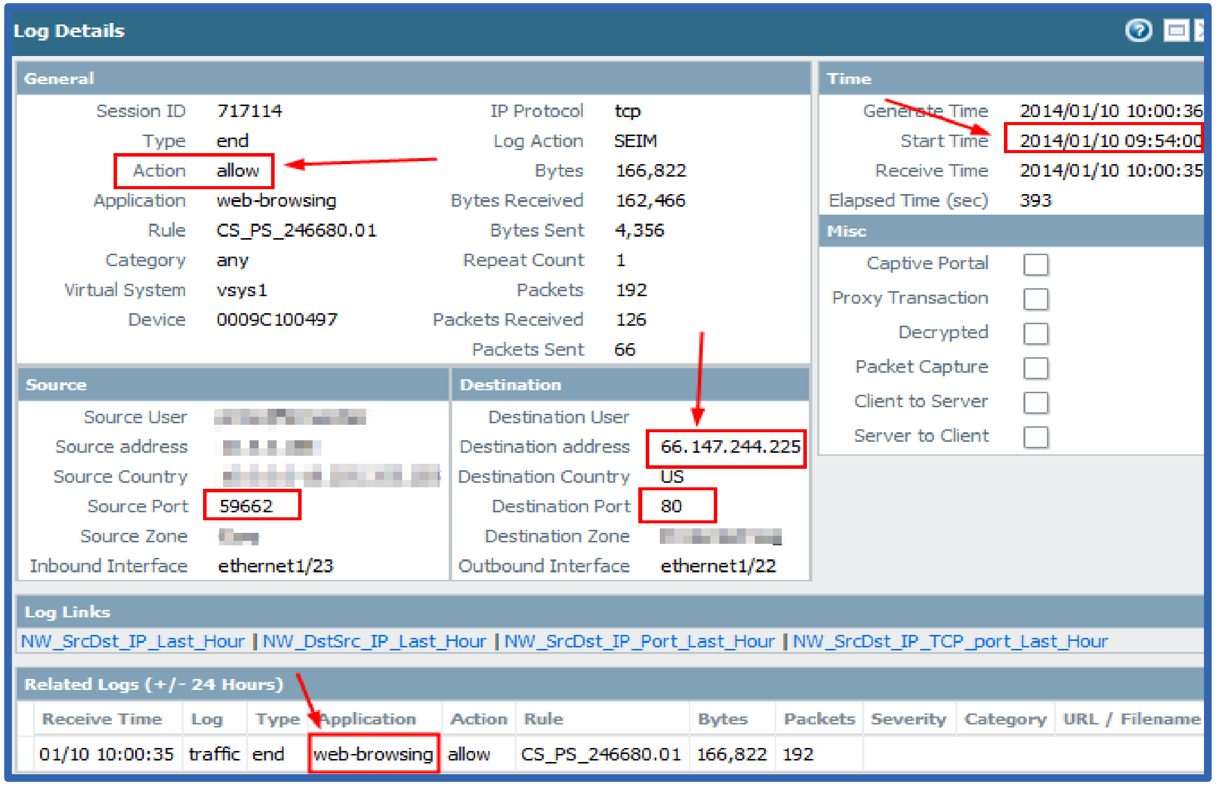


Banload Trojan



Banload (1)

Trigger: Alert on potentially malicious web traffic (allowed)
Firewall Log Details



Log Details

General

Session ID	717114	IP Protocol	tcp
Type	end	Log Action	SEIM
Action	allow	Bytes	166,822
Application	web-browsing	Bytes Received	162,466
Rule	CS_PS_246680.01	Bytes Sent	4,356
Category	any	Repeat Count	1
Virtual System	vsys1	Packets	192
Device	0009C100497	Packets Received	126
		Packets Sent	66

Time

Generate Time	2014/01/10 10:00:36
Start Time	2014/01/10 09:54:00
Receive Time	2014/01/10 10:00:35
Elapsed Time (sec)	393

Misc

Captive Portal	□
Proxy Transaction	□
Decrypted	□
Packet Capture	□
Client to Server	□
Server to Client	□

Source

Source User	[redacted]
Source address	[redacted]
Source Country	[redacted]
Source Port	59662
Source Zone	[redacted]
Inbound Interface	ethernet1/23

Destination

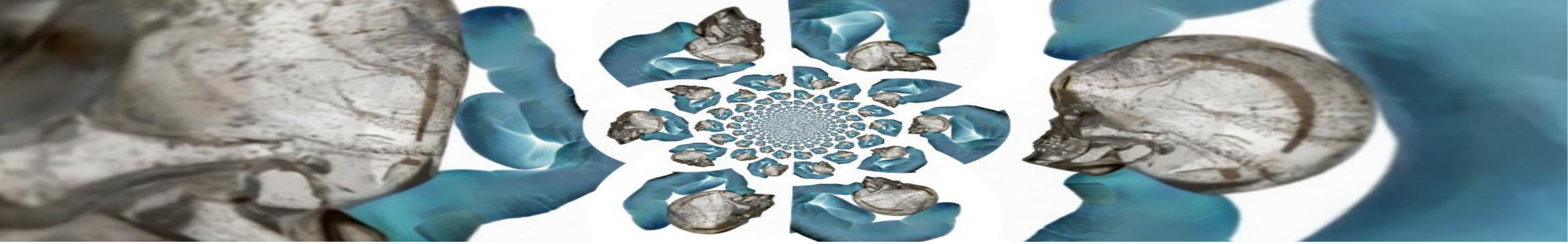
Destination User	
Destination address	66.147.244.225
Destination Country	US
Destination Port	80
Destination Zone	[redacted]
Outbound Interface	ethernet1/22

Log Links

NW_SrcDst_IP_Last_Hour | NW_DstSrc_IP_Last_Hour | NW_SrcDst_IP_Port_Last_Hour | NW_SrcDst_IP_TCP_port_Last_Hour

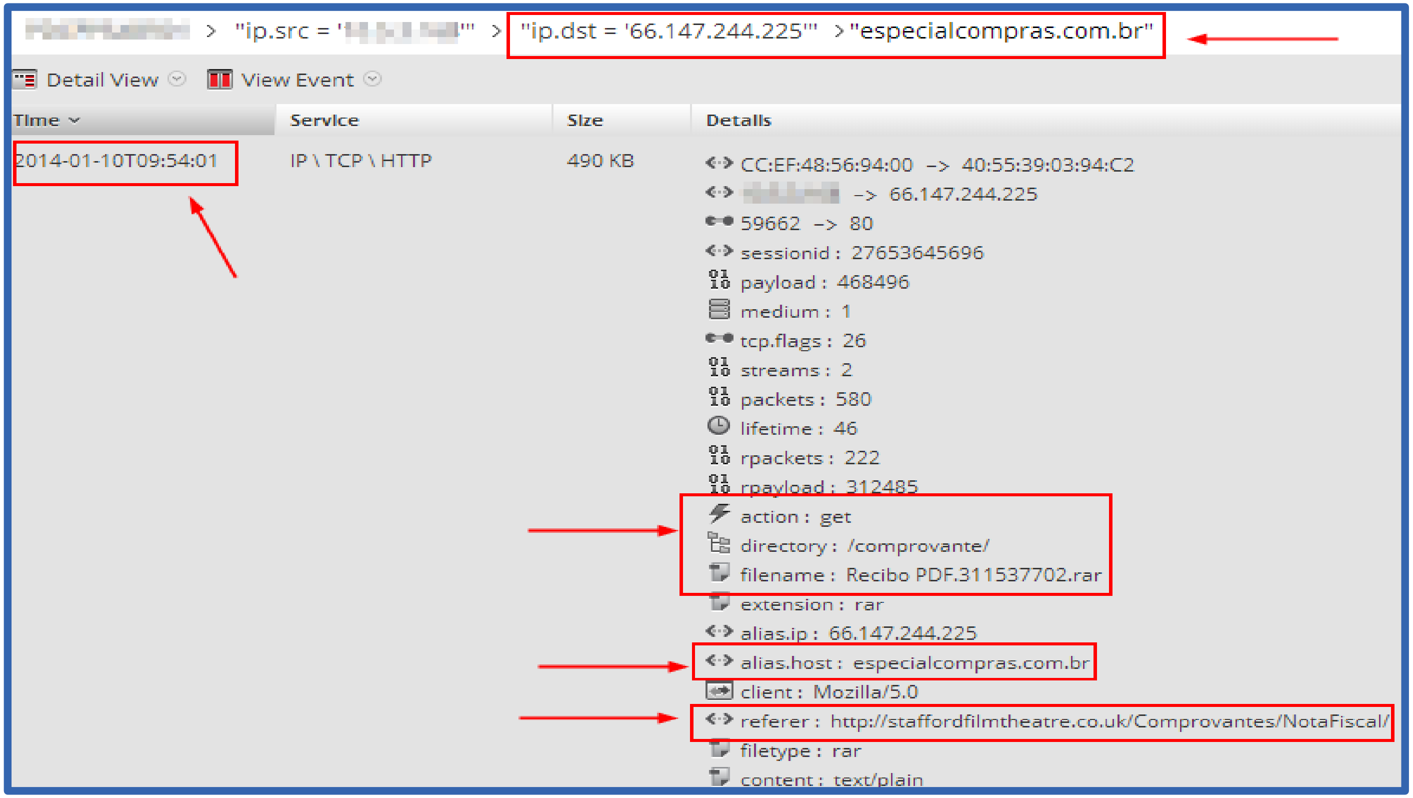
Related Logs (+/- 24 Hours)

Receive Time	Log	Type	Application	Action	Rule	Bytes	Packets	Severity	Category	URL / Filename
01/10 10:00:35	traffic	end	web-browsing	allow	CS_PS_246680.01	166,822	192			



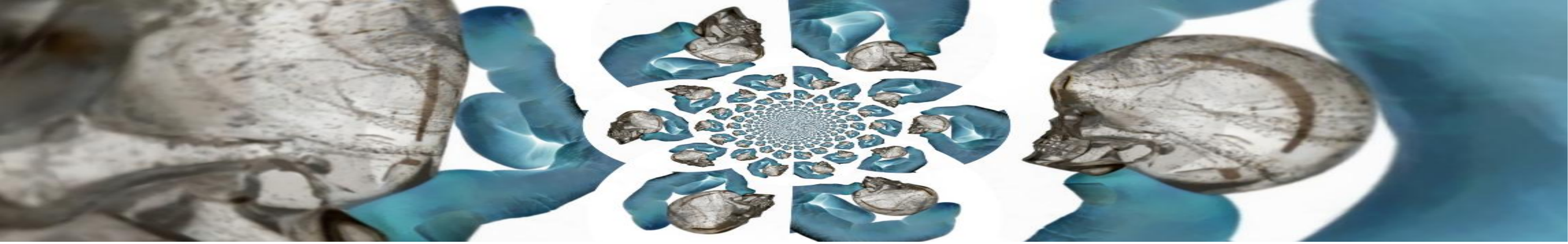
Banload (2)

NSM: Streaming PCAP – What is the traffic?



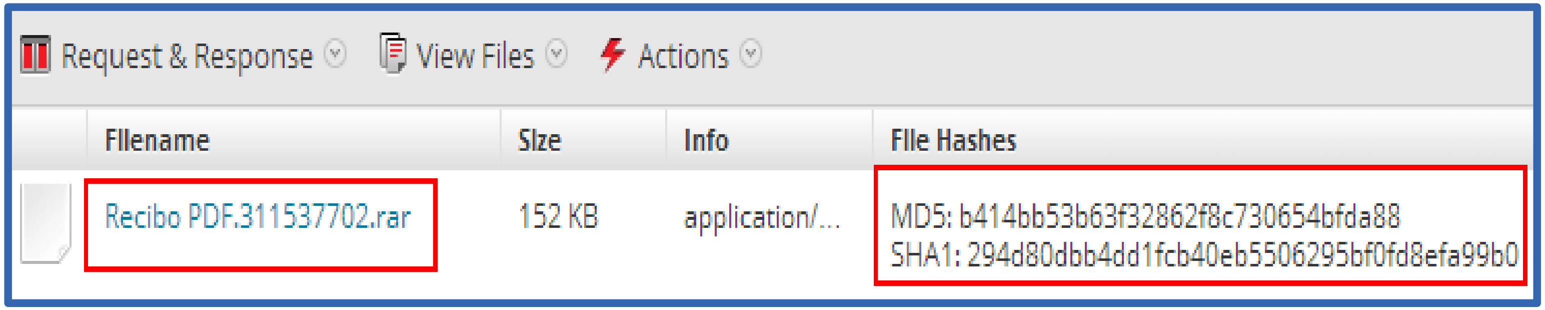
[redacted] > "ip.src = '[redacted]'" > "ip.dst = '66.147.244.225'" > "especialcompras.com.br"

Time	Service	Size	Details
2014-01-10T09:54:01	IP \ TCP \ HTTP	490 KB	CC:EF:48:56:94:00 -> 40:55:39:03:94:C2 [redacted] -> 66.147.244.225 59662 -> 80 sessionid : 27653645696 payload : 468496 medium : 1 tcp.flags : 26 streams : 2 packets : 580 lifetime : 46 rpackets : 222 rpayload : 312485 action : get directory : /comprovante/ filename : Recibo PDF.311537702.rar extension : rar alias.ip : 66.147.244.225 alias.host : especialcompras.com.br client : Mozilla/5.0 referer : http://staffordfilmtheatre.co.uk/Comprovantes/NotaFiscal/ filetype : rar content : text/plain

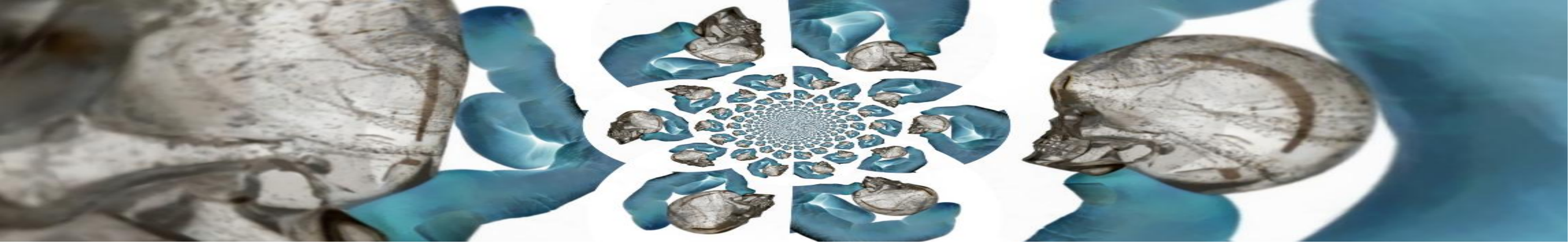


Banload (3)

NSM: Streaming PCAP – File Extraction

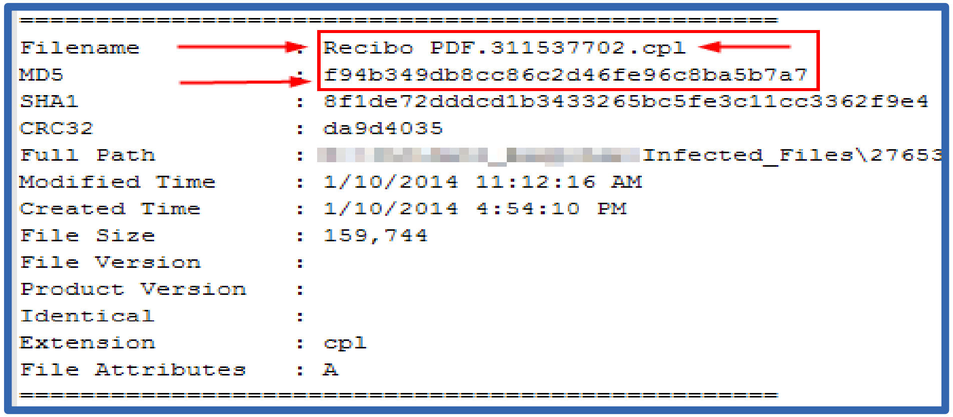


	Filename	Size	Info	File Hashes
	Recibo PDF.311537702.rar	152 KB	application/...	MD5: b414bb53b63f32862f8c730654bfda88 SHA1: 294d80dbb4dd1fcb40eb5506295bf0fd8efa99b0

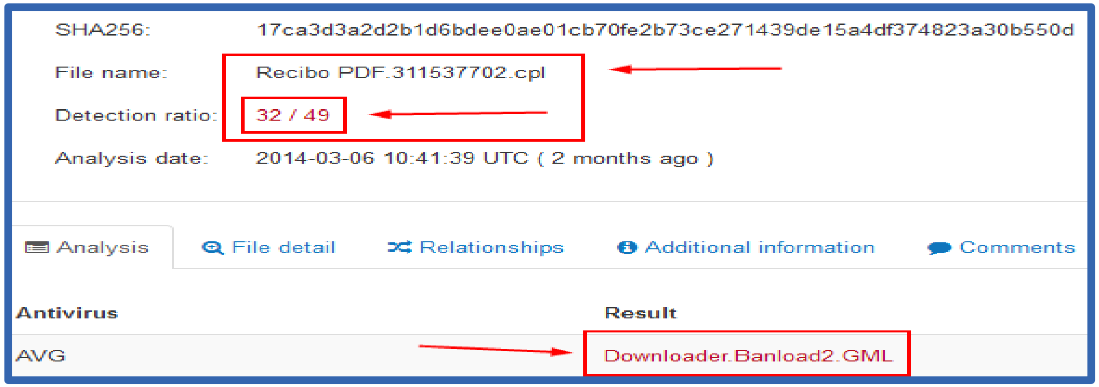


Banload (4)

Binary Analysis – Unpacked File, Hash, Malware



```
==================================================
Filename          : Recibo PDF.311537702.cpl
MD5               : f94b349db8cc86c2d46fe96c8ba5b7a7
SHA1              : 8f1de72dddcd1b3433265bc5fe3c11cc3362f9e4
CRC32             : da9d4035
Full Path         : [redacted]Infected_Files\27653
Modified Time     : 1/10/2014 11:12:16 AM
Created Time      : 1/10/2014 4:54:10 PM
File Size         : 159,744
File Version      :
Product Version   :
Identical         :
Extension         : cpl
File Attributes   : A
==================================================
```



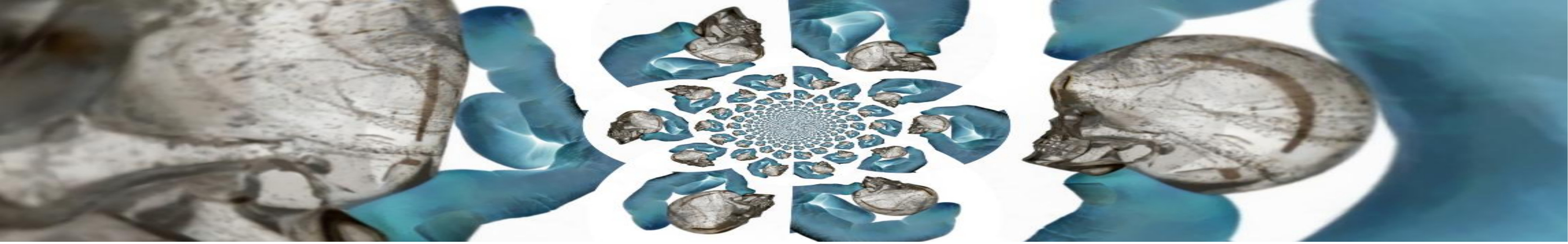
SHA256: 17ca3d3a2d2b1d6bdee0ae01cb70fe2b73ce271439de15a4df374823a30b550d

File name: Recibo PDF.311537702.cpl

Detection ratio: 32 / 49

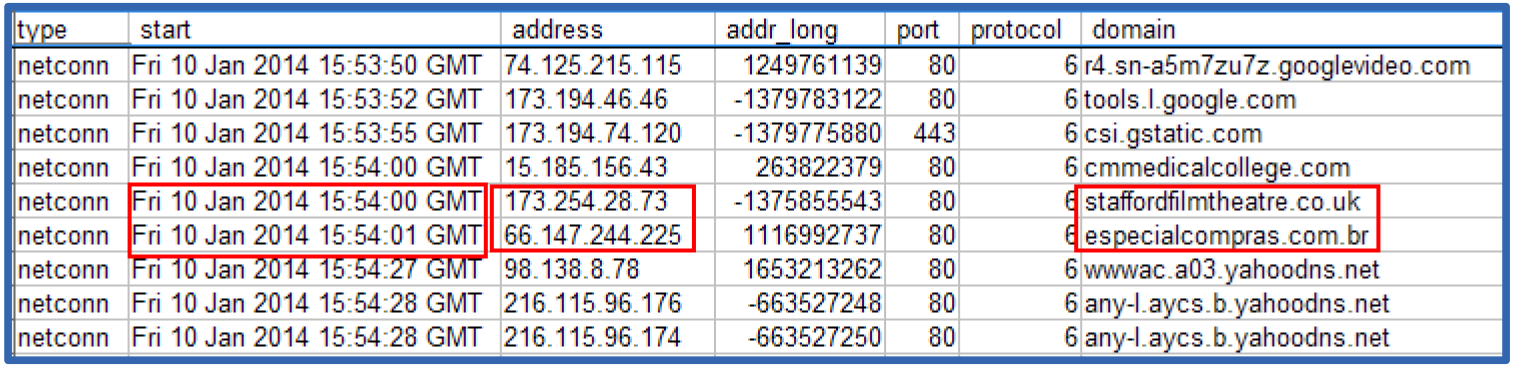
Analysis date: 2014-03-06 10:41:39 UTC (2 months ago)

Antivirus	Result
AVG	Downloader.Banload2.GML

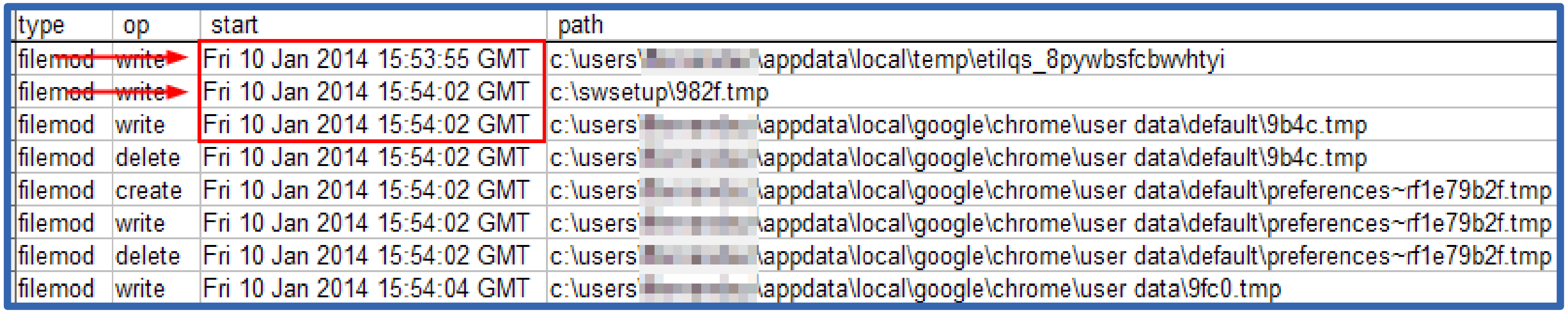


Banload (5)

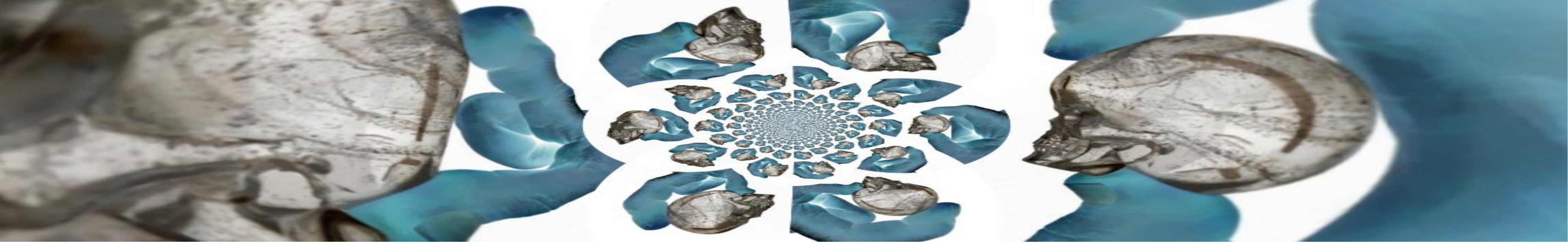
Host Analysis: Connection established? Malware launched?



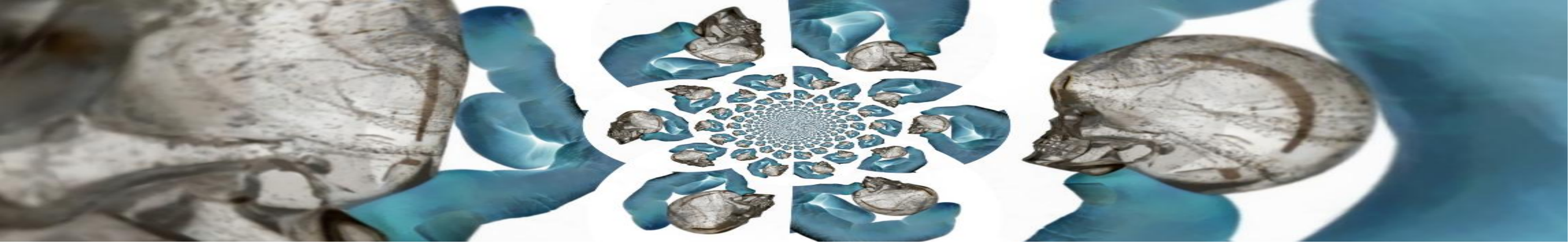
type	start	address	addr_long	port	protocol	domain
netconn	Fri 10 Jan 2014 15:53:50 GMT	74.125.215.115	1249761139	80	6	r4.sn-a5m7zu7z.googlevideo.com
netconn	Fri 10 Jan 2014 15:53:52 GMT	173.194.46.46	-1379783122	80	6	tools.l.google.com
netconn	Fri 10 Jan 2014 15:53:55 GMT	173.194.74.120	-1379775880	443	6	csi.gstatic.com
netconn	Fri 10 Jan 2014 15:54:00 GMT	15.185.156.43	263822379	80	6	cmmedicalcollege.com
netconn	Fri 10 Jan 2014 15:54:00 GMT	173.254.28.73	-1375855543	80	6	staffordfilmtheatre.co.uk
netconn	Fri 10 Jan 2014 15:54:01 GMT	66.147.244.225	1116992737	80	6	especialcompras.com.br
netconn	Fri 10 Jan 2014 15:54:27 GMT	98.138.8.78	1653213262	80	6	wwwac.a03.yahoodns.net
netconn	Fri 10 Jan 2014 15:54:28 GMT	216.115.96.176	-663527248	80	6	any-l.aycs.b.yahoodns.net
netconn	Fri 10 Jan 2014 15:54:28 GMT	216.115.96.174	-663527250	80	6	any-l.aycs.b.yahoodns.net



type	op	start	path
filemod	write	Fri 10 Jan 2014 15:53:55 GMT	c:\users\[redacted]\appdata\local\temp\etilqs_8pywbsfcbwhtyi
filemod	write	Fri 10 Jan 2014 15:54:02 GMT	c:\swsetup\982f.tmp
filemod	write	Fri 10 Jan 2014 15:54:02 GMT	c:\users\[redacted]\appdata\local\google\chrome\user data\default\9b4c.tmp
filemod	delete	Fri 10 Jan 2014 15:54:02 GMT	c:\users\[redacted]\appdata\local\google\chrome\user data\default\9b4c.tmp
filemod	create	Fri 10 Jan 2014 15:54:02 GMT	c:\users\[redacted]\appdata\local\google\chrome\user data\default\preferences~rf1e79b2f.tmp
filemod	write	Fri 10 Jan 2014 15:54:02 GMT	c:\users\[redacted]\appdata\local\google\chrome\user data\default\preferences~rf1e79b2f.tmp
filemod	delete	Fri 10 Jan 2014 15:54:02 GMT	c:\users\[redacted]\appdata\local\google\chrome\user data\default\preferences~rf1e79b2f.tmp
filemod	write	Fri 10 Jan 2014 15:54:04 GMT	c:\users\[redacted]\appdata\local\google\chrome\user data\9fc0.tmp

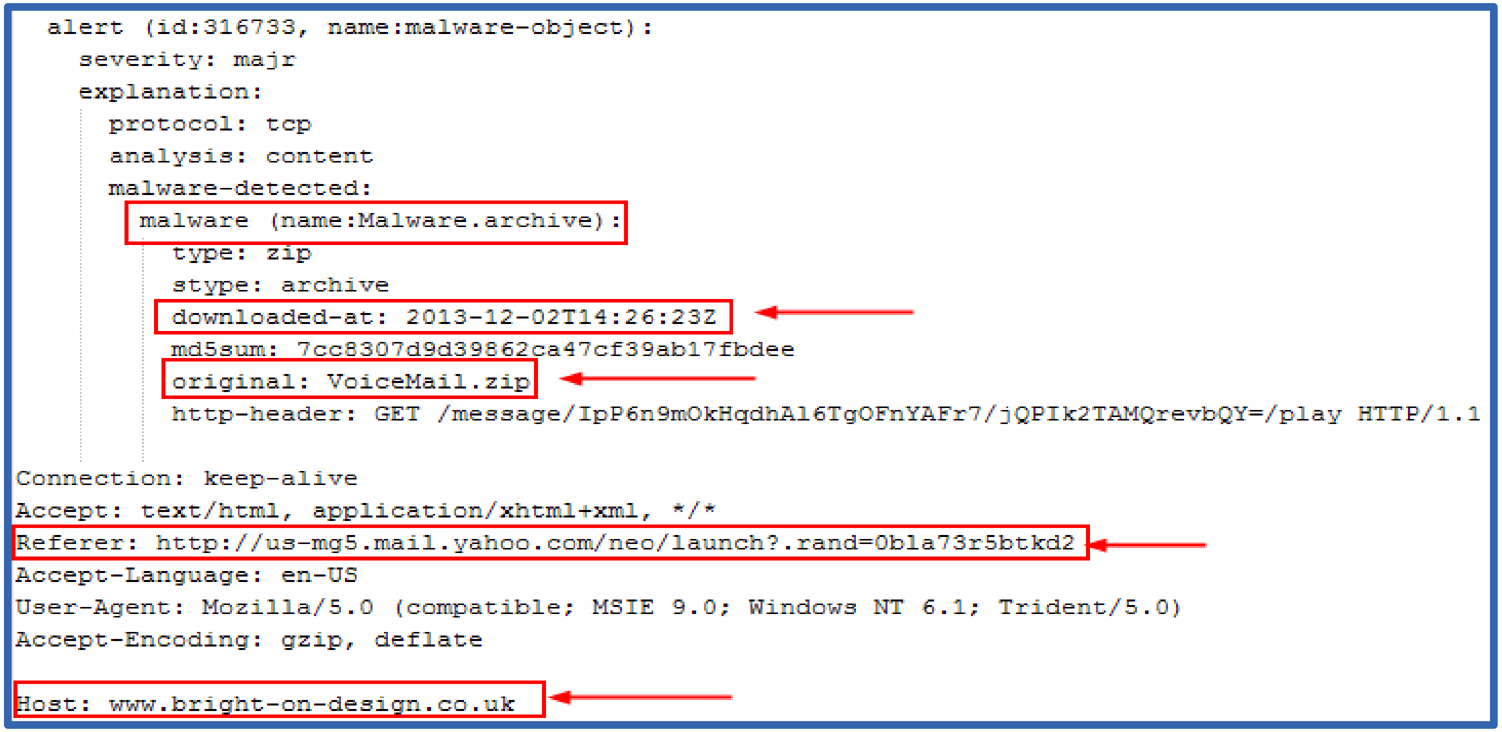


Kuluoz (Dofoil) Trojan

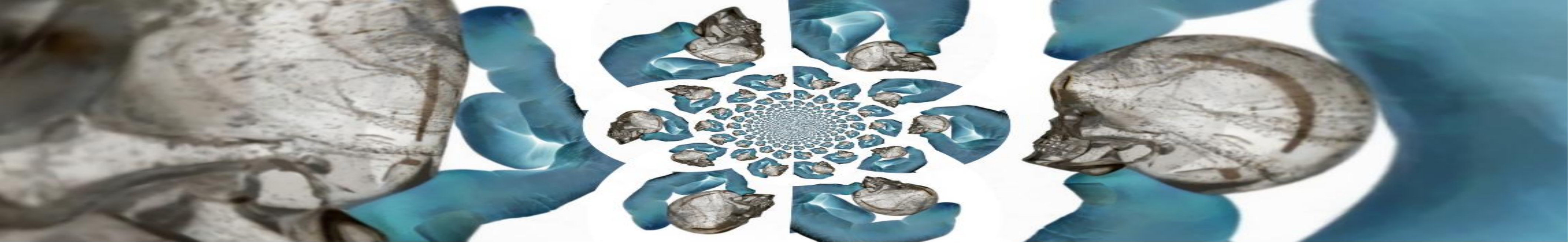


Kuluoz (1)

Trigger: Alert on potentially malicious web traffic, allowed

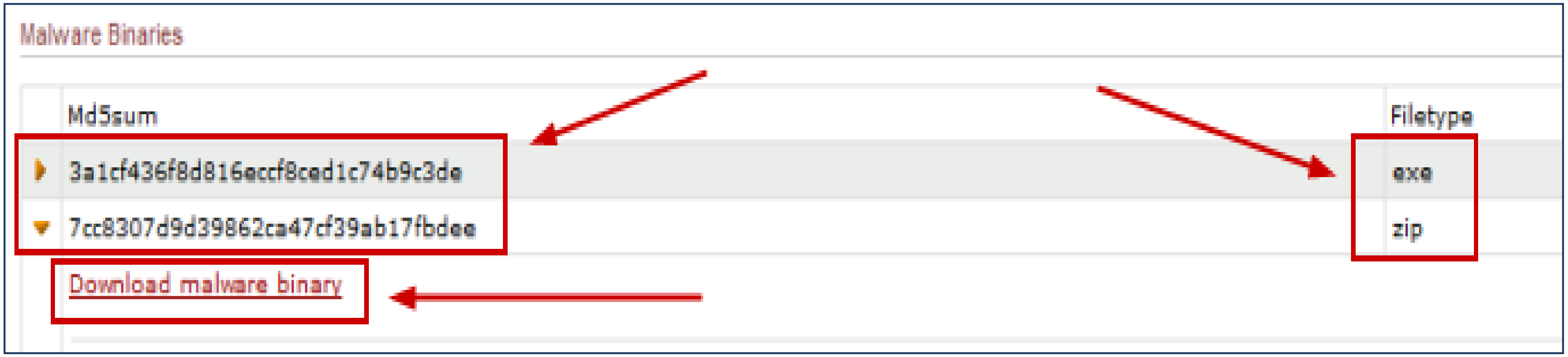


```
  alert (id:316733, name:malware-object):
    severity: majr
    explanation:
      protocol: tcp
      analysis: content
      malware-detected:
        malware (name:Malware.archive):
          type: zip
          stype: archive
          downloaded-at: 2013-12-02T14:26:23Z
          md5sum: 7cc8307d9d39862ca47cf39ab17fbdee
          original: VoiceMail.zip
          http-header: GET /message/IpP6n9mOkHqdhAl6TgOFnYAFr7/jQPIk2TAMQrevbQY=/play HTTP/1.1

Connection: keep-alive
Accept: text/html, application/xhtml+xml, */*
Referer: http://us-mg5.mail.yahoo.com/neo/launch?.rand=0bla73r5btkd2
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
Accept-Encoding: gzip, deflate

Host: www.bright-on-design.co.uk
```



Kuluoz (2)

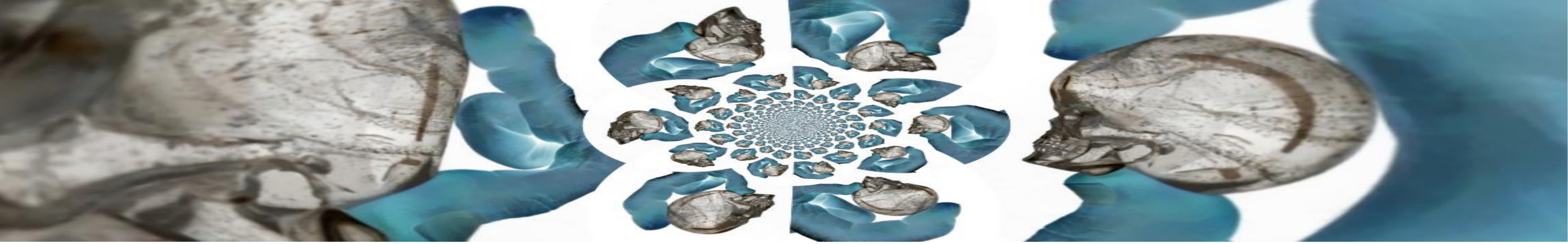
Malware Alert Details



Malware Binaries

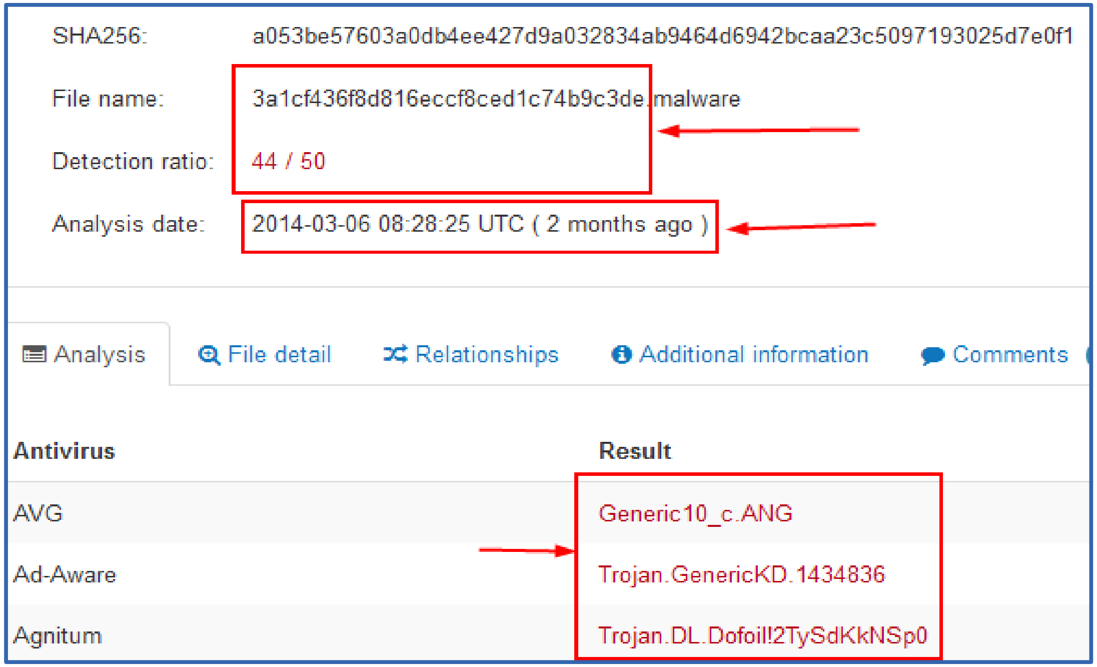
	Md5sum	Filetype
▶	3a1cf436f8d816eccf8ced1c74b9c3de	exe
▼	7cc8307d9d39862ca47cf39ab17fbdee	zip

Download malware binary



Kuluoz (3)

Malware Identification



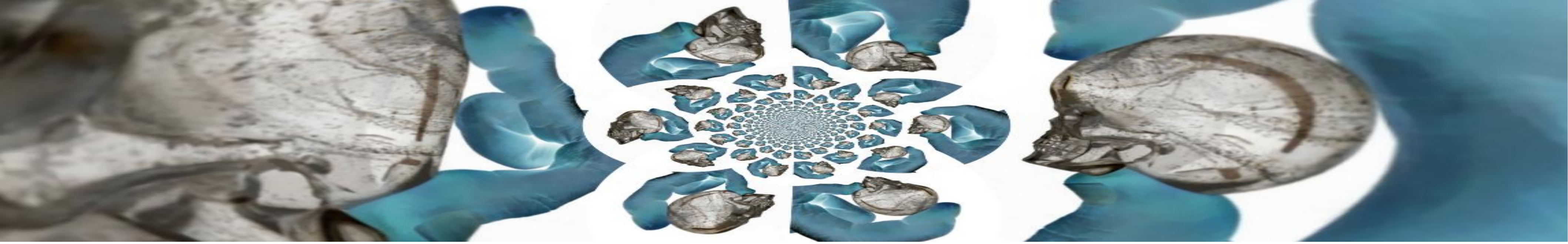
SHA256: a053be57603a0db4ee427d9a032834ab9464d6942bcaa23c5097193025d7e0f1

File name: 3a1cf436f8d816eccf8ced1c74b9c3de.malware

Detection ratio: 44 / 50

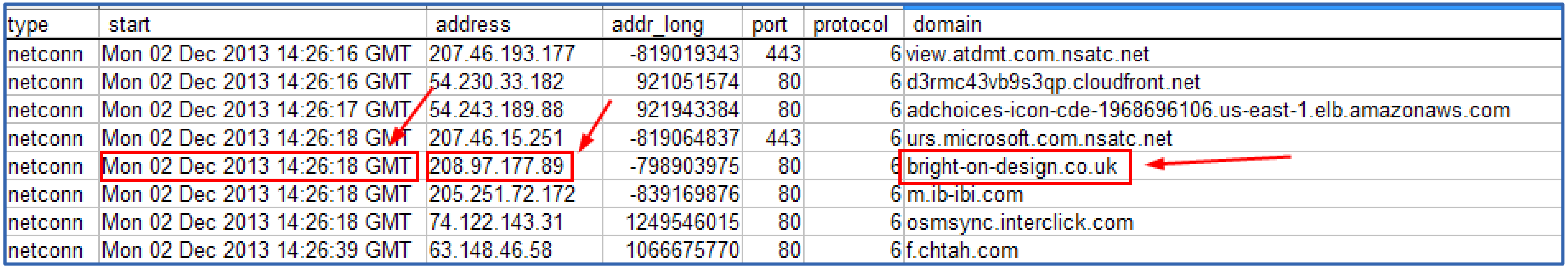
Analysis date: 2014-03-06 08:28:25 UTC (2 months ago)

Antivirus	Result
AVG	Generic10_c.ANG
Ad-Aware	Trojan.GenericKD.1434836
Agnitum	Trojan.DL.Dofoil!2TySdKkNSp0

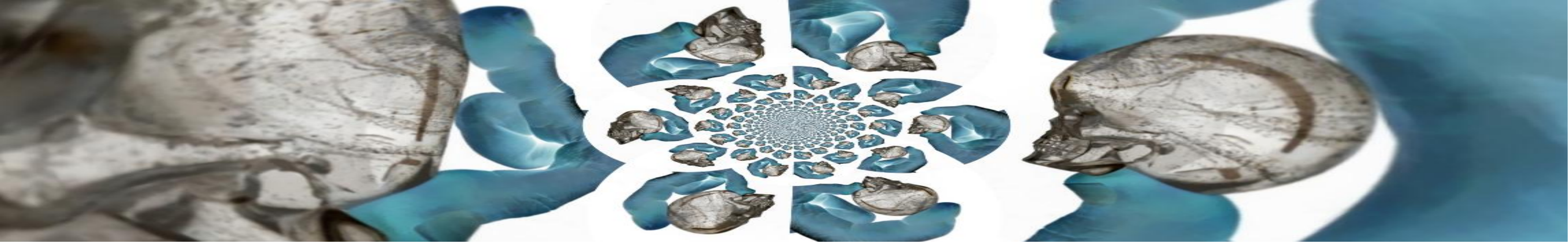


Kuluoz (4)

Host Analysis – Connection complete? Malware detonate?

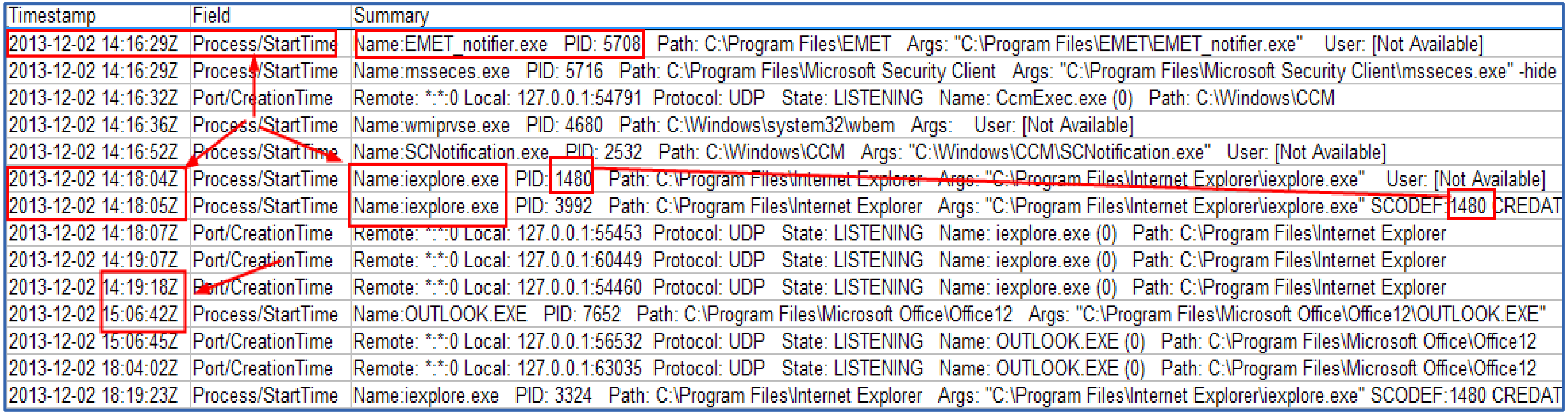


type	start	address	addr_long	port	protocol	domain
netconn	Mon 02 Dec 2013 14:26:16 GMT	207.46.193.177	-819019343	443	6	view.atdmt.com.nsatc.net
netconn	Mon 02 Dec 2013 14:26:16 GMT	54.230.33.182	921051574	80	6	d3rmc43vb9s3qp.cloudfront.net
netconn	Mon 02 Dec 2013 14:26:17 GMT	54.243.189.88	921943384	80	6	adchoices-icon-cde-1968696106.us-east-1.elb.amazonaws.com
netconn	Mon 02 Dec 2013 14:26:18 GMT	207.46.15.251	-819064837	443	6	urs.microsoft.com.nsatc.net
netconn	Mon 02 Dec 2013 14:26:18 GMT	208.97.177.89	-798903975	80	6	bright-on-design.co.uk
netconn	Mon 02 Dec 2013 14:26:18 GMT	205.251.72.172	-839169876	80	6	m.ib-ibi.com
netconn	Mon 02 Dec 2013 14:26:18 GMT	74.122.143.31	1249546015	80	6	osmsync.interclick.com
netconn	Mon 02 Dec 2013 14:26:39 GMT	63.148.46.58	1066675770	80	6	f.chtah.com

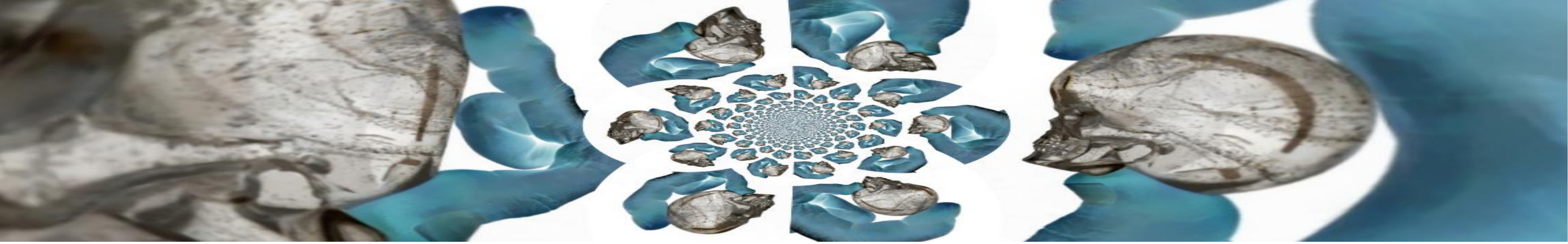


Kuluoz (5)

RAM Analysis – Did malware detonate?

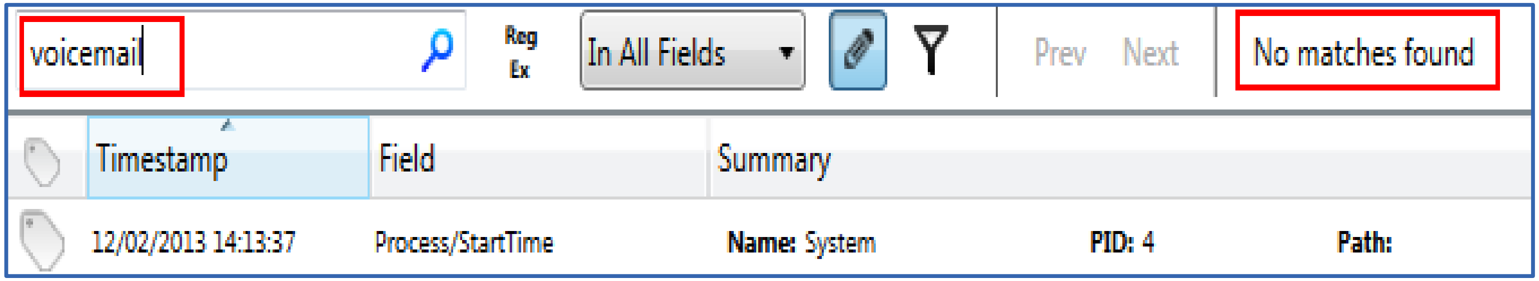


Timestamp	Field	Summary
2013-12-02 14:16:29Z	Process/StartTime	Name:EMET_notifier.exe PID: 5708 Path: C:\Program Files\EMET Args: "C:\Program Files\EMET\EMET_notifier.exe" User: [Not Available]
2013-12-02 14:16:29Z	Process/StartTime	Name:msseces.exe PID: 5716 Path: C:\Program Files\Microsoft Security Client Args: "C:\Program Files\Microsoft Security Client\msseces.exe" -hide
2013-12-02 14:16:32Z	Port/CreationTime	Remote: *:*:0 Local: 127.0.0.1:54791 Protocol: UDP State: LISTENING Name: CcmExec.exe (0) Path: C:\Windows\CCM
2013-12-02 14:16:36Z	Process/StartTime	Name:wmiprvse.exe PID: 4680 Path: C:\Windows\system32\wbem Args: User: [Not Available]
2013-12-02 14:16:52Z	Process/StartTime	Name:SCNotification.exe PID: 2532 Path: C:\Windows\CCM Args: "C:\Windows\CCM\SCNotification.exe" User: [Not Available]
2013-12-02 14:18:04Z	Process/StartTime	Name:iexplore.exe PID: 1480 Path: C:\Program Files\Internet Explorer Args: "C:\Program Files\Internet Explorer\iexplore.exe" User: [Not Available]
2013-12-02 14:18:05Z	Process/StartTime	Name:iexplore.exe PID: 3992 Path: C:\Program Files\Internet Explorer Args: "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:1480 CREDAT
2013-12-02 14:18:07Z	Port/CreationTime	Remote: *:*:0 Local: 127.0.0.1:55453 Protocol: UDP State: LISTENING Name: iexplore.exe (0) Path: C:\Program Files\Internet Explorer
2013-12-02 14:19:07Z	Port/CreationTime	Remote: *:*:0 Local: 127.0.0.1:60449 Protocol: UDP State: LISTENING Name: iexplore.exe (0) Path: C:\Program Files\Internet Explorer
2013-12-02 14:19:18Z	Port/CreationTime	Remote: *:*:0 Local: 127.0.0.1:54460 Protocol: UDP State: LISTENING Name: iexplore.exe (0) Path: C:\Program Files\Internet Explorer
2013-12-02 15:06:42Z	Process/StartTime	Name:OUTLOOK.EXE PID: 7652 Path: C:\Program Files\Microsoft Office\Office12 Args: "C:\Program Files\Microsoft Office\Office12\OUTLOOK.EXE"
2013-12-02 15:06:45Z	Port/CreationTime	Remote: *:*:0 Local: 127.0.0.1:56532 Protocol: UDP State: LISTENING Name: OUTLOOK.EXE (0) Path: C:\Program Files\Microsoft Office\Office12
2013-12-02 18:04:02Z	Port/CreationTime	Remote: *:*:0 Local: 127.0.0.1:63035 Protocol: UDP State: LISTENING Name: OUTLOOK.EXE (0) Path: C:\Program Files\Microsoft Office\Office12
2013-12-02 18:19:23Z	Process/StartTime	Name:iexplore.exe PID: 3324 Path: C:\Program Files\Internet Explorer Args: "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:1480 CREDAT



Kuluoz (6)

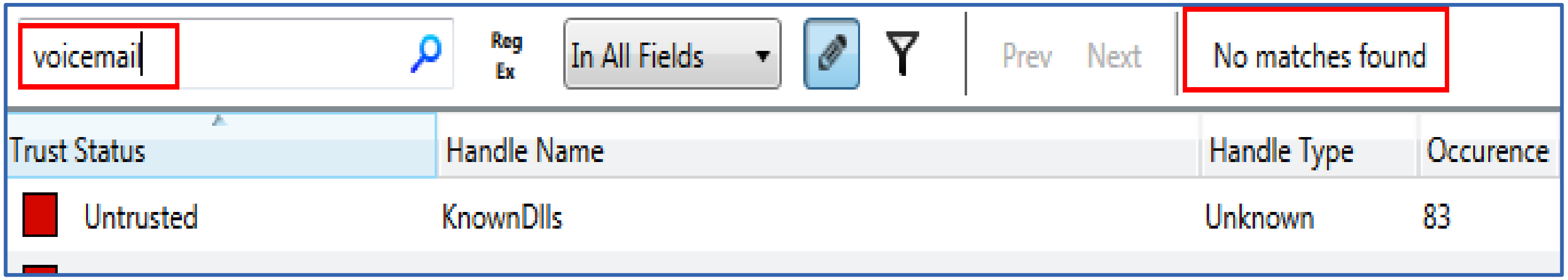
RAM Analysis – Evidence of malware activity?



voicemail

No matches found

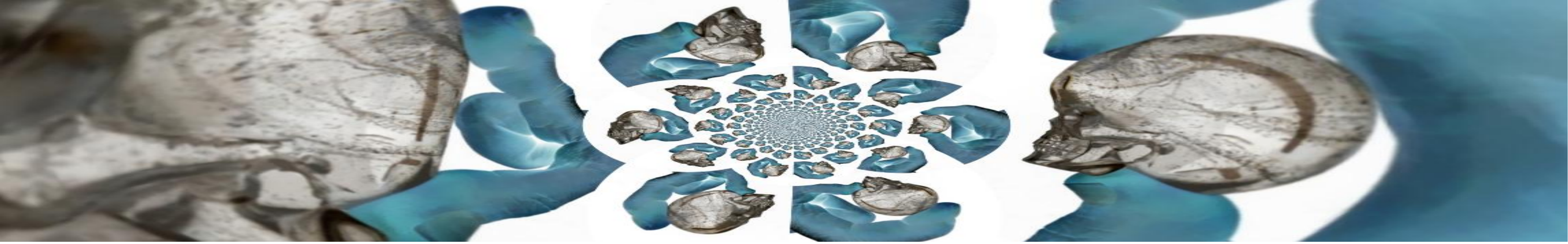
Timestamp	Field	Summary		
12/02/2013 14:13:37	Process/StartTime	**Name:** System	**PID:** 4	**Path:**



voicemail

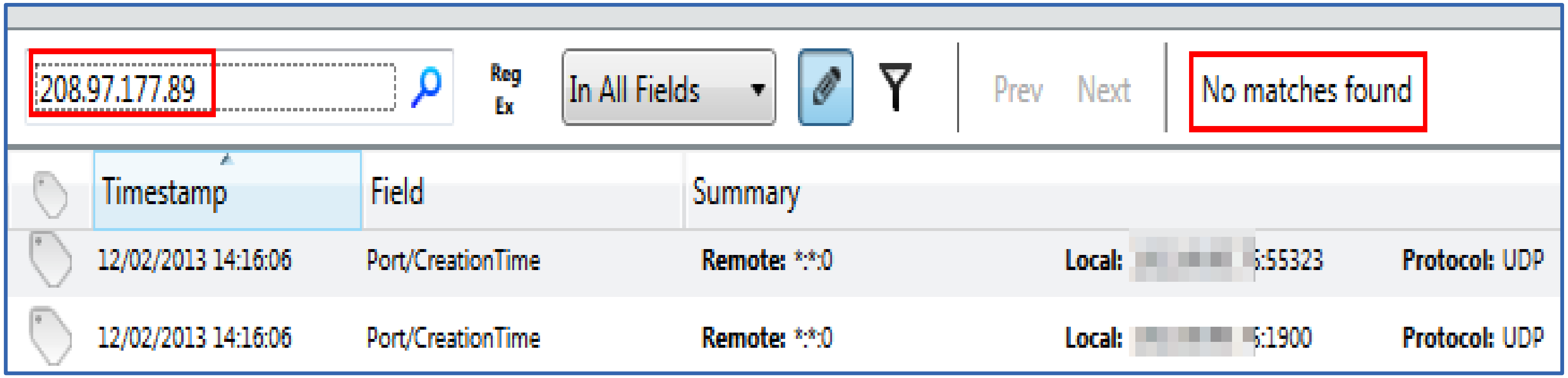
No matches found

Trust Status	Handle Name	Handle Type	Occurence
🟥 Untrusted	KnownDlls	Unknown	83



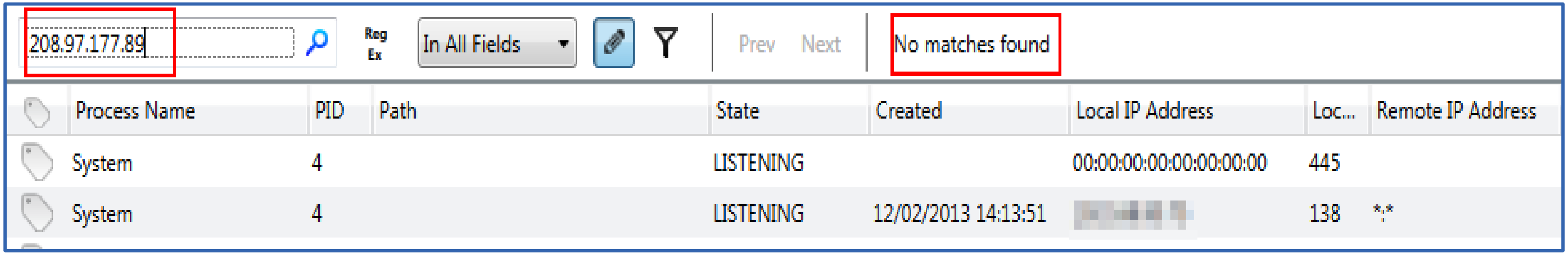
Kuluoz (7)

RAM Analysis – Evidence of malware activity?



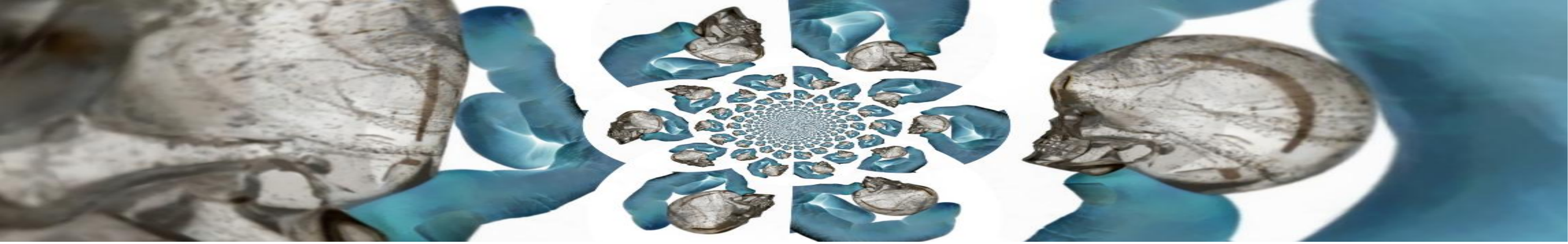
No matches found

Timestamp	Field	Summary		
12/02/2013 14:16:06	Port/CreationTime	**Remote:** *:*:0	**Local:** [redacted]:55323	**Protocol:** UDP
12/02/2013 14:16:06	Port/CreationTime	**Remote:** *:*:0	**Local:** [redacted]:1900	**Protocol:** UDP

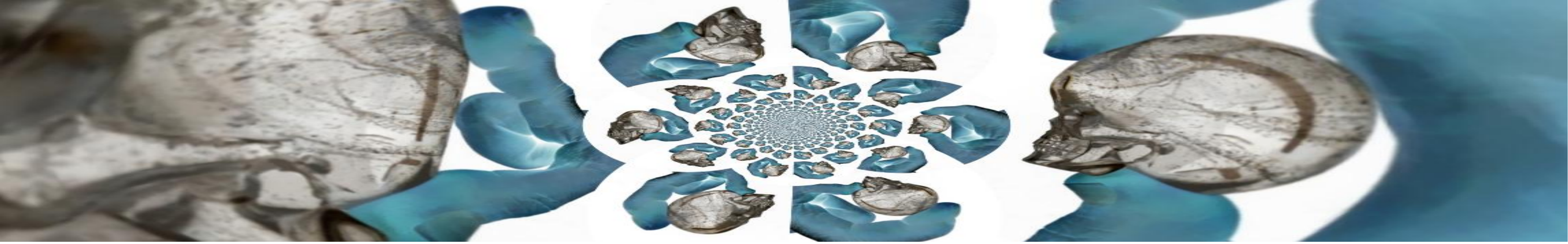


No matches found

Process Name	PID	Path	State	Created	Local IP Address	Loc...	Remote IP Address
System	4		LISTENING		00:00:00:00:00:00:00:00	445	
System	4		LISTENING	12/02/2013 14:13:51	[redacted]	138	*:*



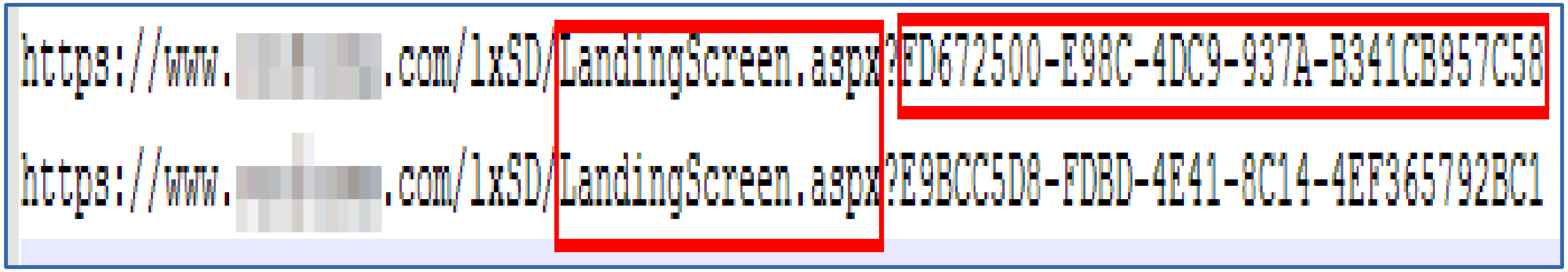
User Activity



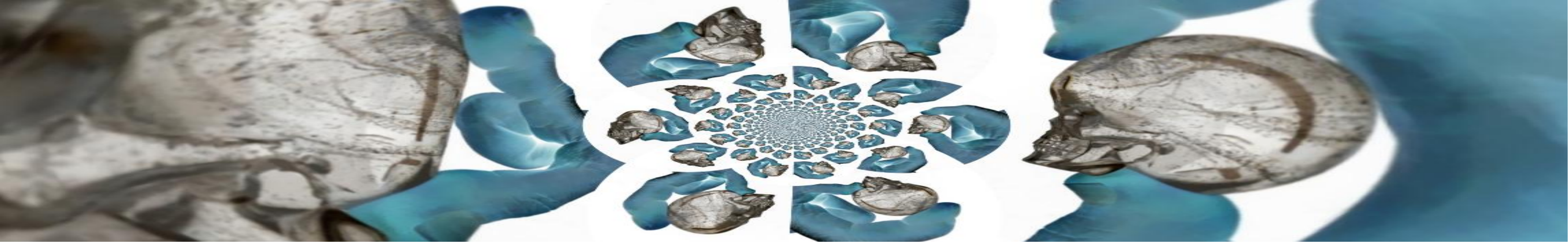
User Activity (1)

Trigger: Report of activity from third-party vendor

Sample Links



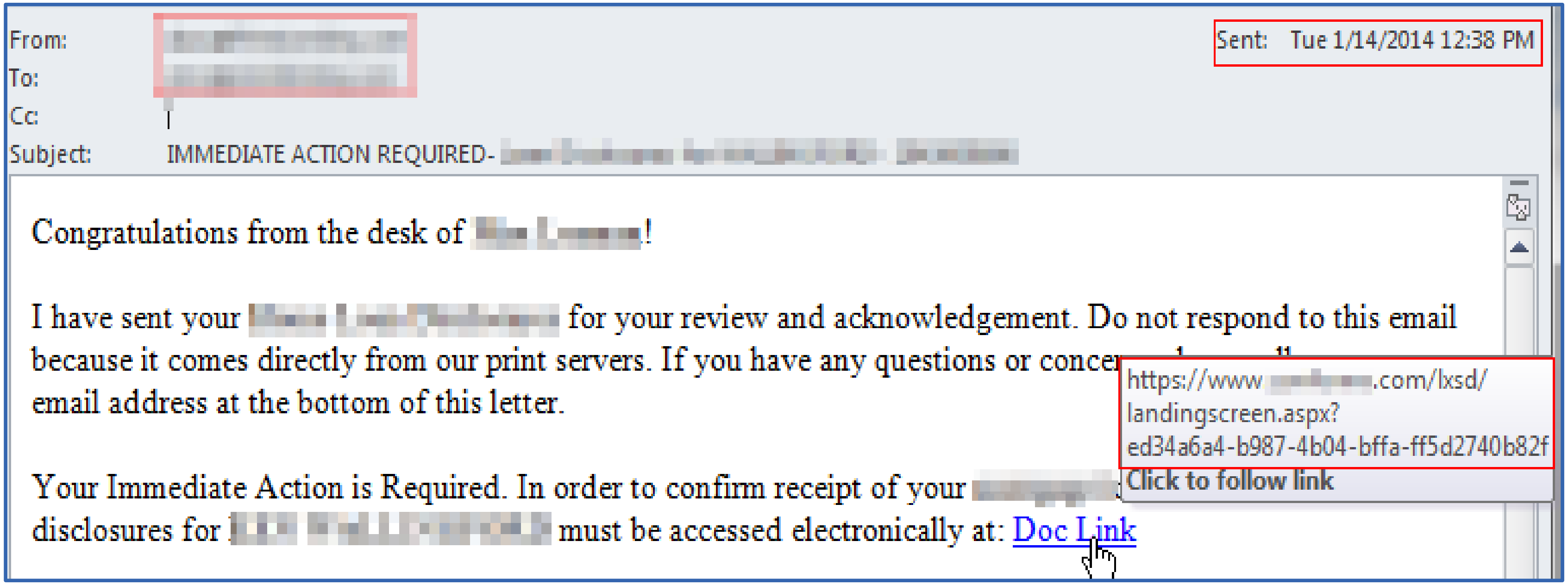
```
https://www.[redacted].com/1xSD/LandingScreen.aspx?FD672500-E98C-4DC9-937A-B341CB957C58
https://www.[redacted].com/1xSD/LandingScreen.aspx?E9BCC5D8-FDBD-4E41-8C14-4EF365792BC1
```



User Activity (2)

Email – Delivery of unique links to user

Extracted from Journaled Archives



From: [redacted]
To: [redacted]
Cc:
Subject: IMMEDIATE ACTION REQUIRED- [redacted]

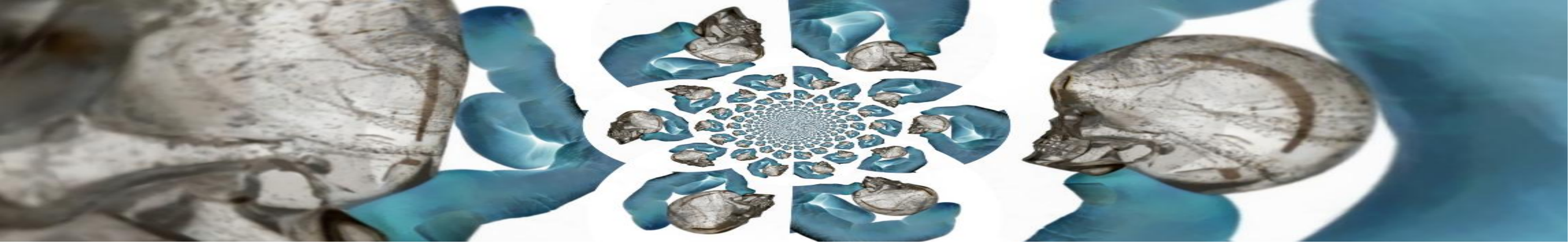
Sent: Tue 1/14/2014 12:38 PM

Congratulations from the desk of [redacted]!

I have sent your [redacted] for your review and acknowledgement. Do not respond to this email because it comes directly from our print servers. If you have any questions or concer
email address at the bottom of this letter.

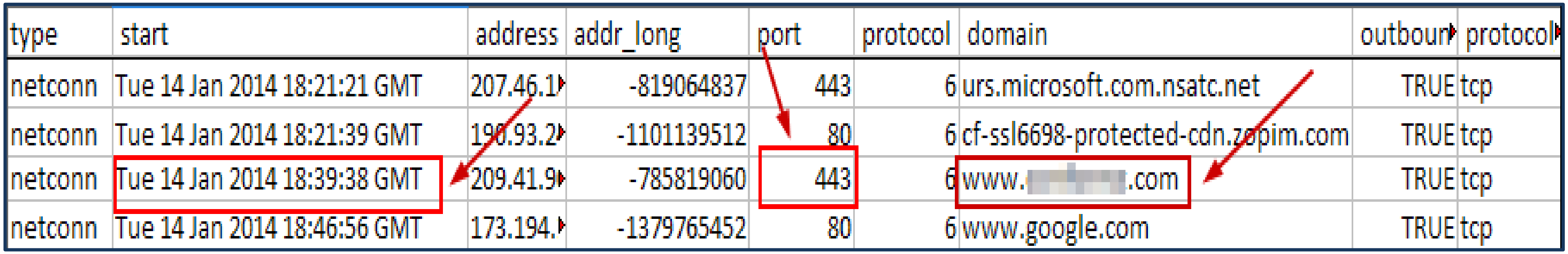
Your Immediate Action is Required. In order to confirm receipt of your [redacted]
disclosures for [redacted] must be accessed electronically at: Doc Link

https://www [redacted] .com/lxsd/landingscreen.aspx?ed34a6a4-b987-4b04-bffa-ff5d2740b82f
Click to follow link

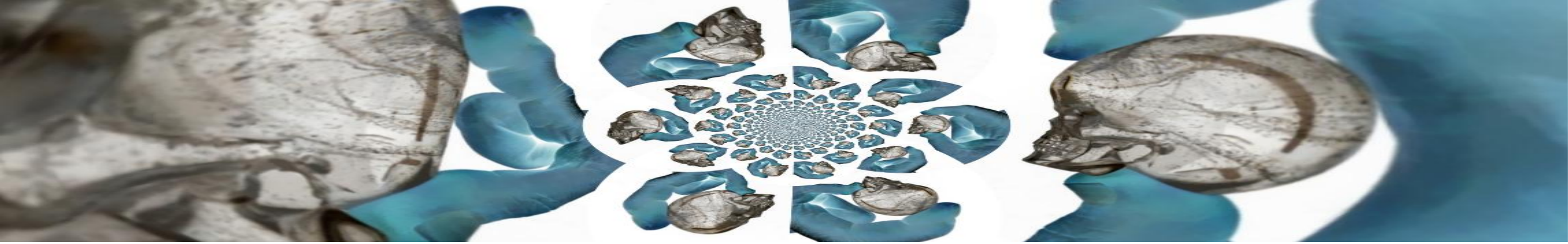


User Activity (3)

Host Analysis – Did the user visit the URL?

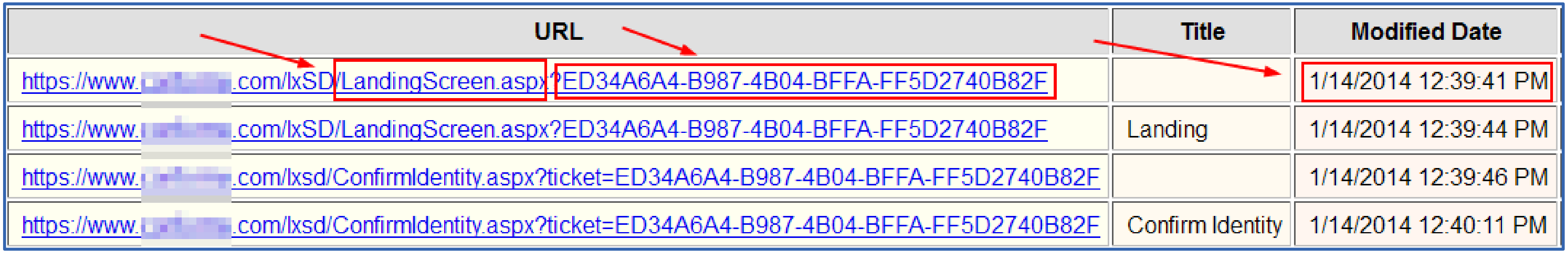


type	start	address	addr_long	port	protocol	domain	outboun	protocol
netconn	Tue 14 Jan 2014 18:21:21 GMT	207.46.1	-819064837	443	6	urs.microsoft.com.nsatc.net	TRUE	tcp
netconn	Tue 14 Jan 2014 18:21:39 GMT	190.93.2	-1101139512	80	6	cf-ssl6698-protected-cdn.zopim.com	TRUE	tcp
netconn	Tue 14 Jan 2014 18:39:38 GMT	209.41.9	-785819060	443	6	www.[redacted].com	TRUE	tcp
netconn	Tue 14 Jan 2014 18:46:56 GMT	173.194.	-1379765452	80	6	www.google.com	TRUE	tcp

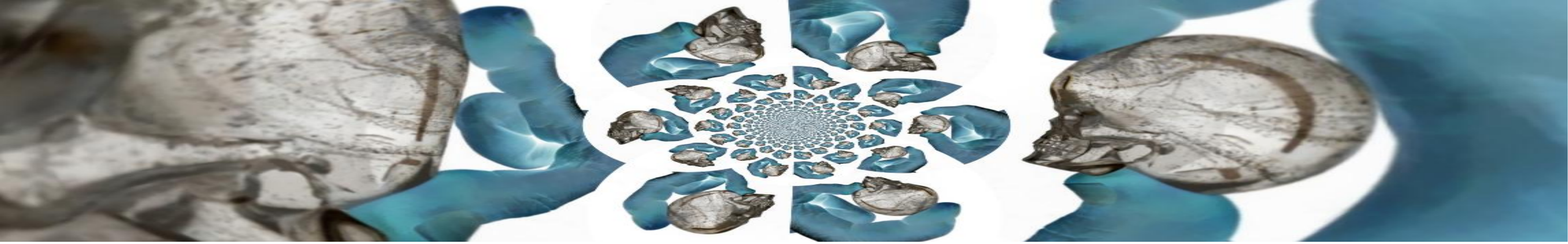


User Activity (4)

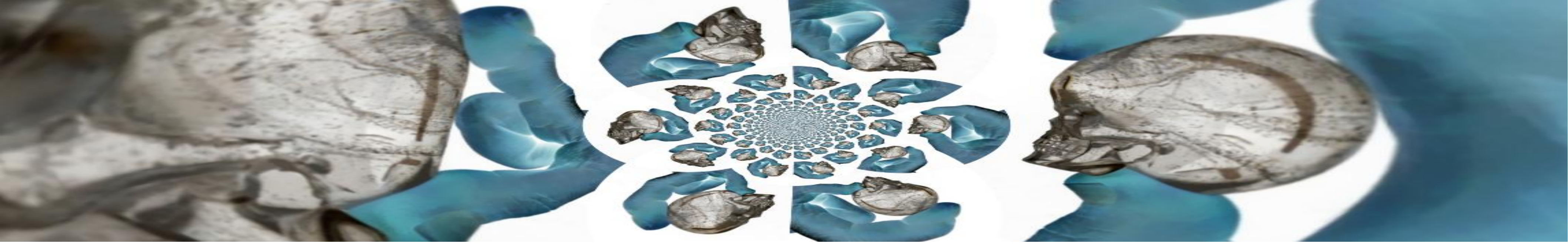
Host Analysis – Targeted Triage on Internet History



URL	Title	Modified Date
https://www.[redacted].com/lxSD/LandingScreen.aspx?ED34A6A4-B987-4B04-BFFA-FF5D2740B82F		1/14/2014 12:39:41 PM
https://www.[redacted].com/lxSD/LandingScreen.aspx?ED34A6A4-B987-4B04-BFFA-FF5D2740B82F	Landing	1/14/2014 12:39:44 PM
https://www.[redacted].com/lxsd/ConfirmIdentity.aspx?ticket=ED34A6A4-B987-4B04-BFFA-FF5D2740B82F		1/14/2014 12:39:46 PM
https://www.[redacted].com/lxsd/ConfirmIdentity.aspx?ticket=ED34A6A4-B987-4B04-BFFA-FF5D2740B82F	Confirm Identity	1/14/2014 12:40:11 PM



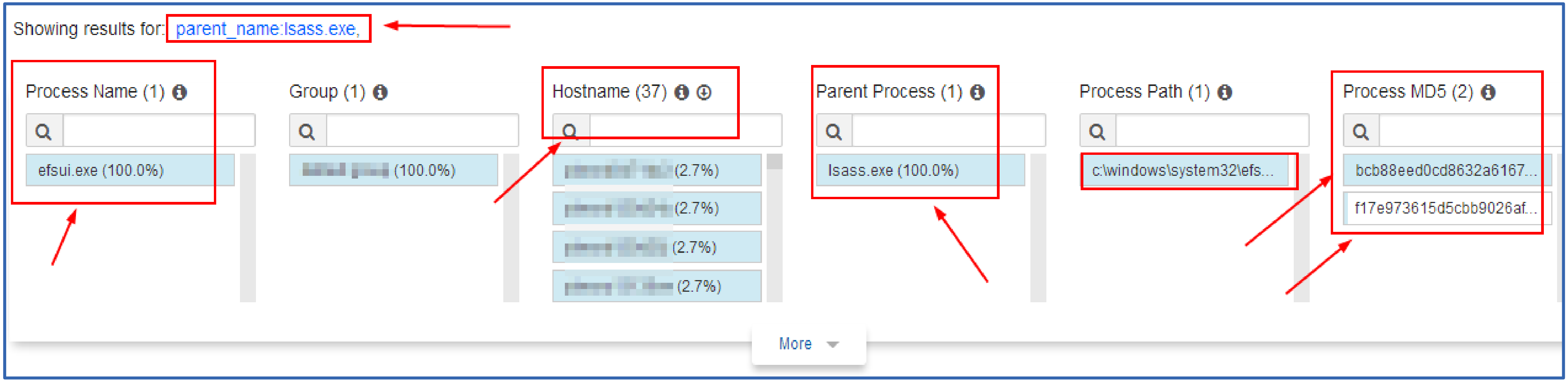
LSASS Child Process



LSASS Child (1)

Trigger: LSASS as Parent Process to EFSUI

Host Query Results



Showing results for: parent_name:lsass.exe,

Process Name (1)

efsui.exe (100.0%)

Group (1)

[redacted] (100.0%)

Hostname (37)

[redacted] (2.7%)

[redacted] (2.7%)

[redacted] (2.7%)

[redacted] (2.7%)

Parent Process (1)

lsass.exe (100.0%)

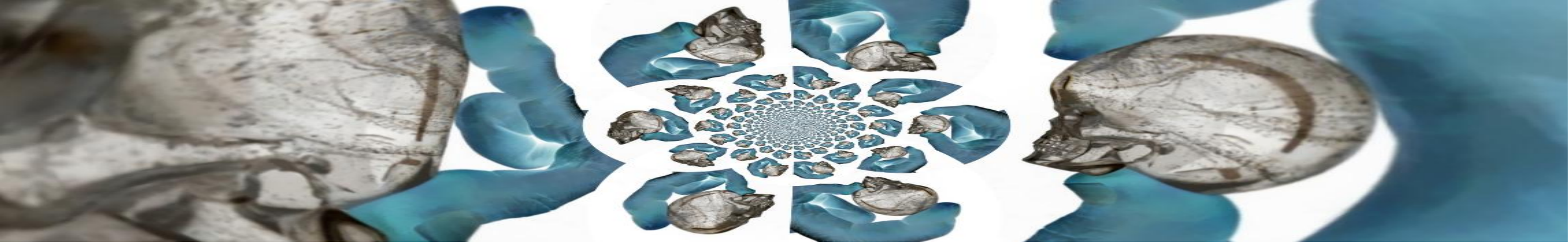
Process Path (1)

c:\windows\system32\efs...

Process MD5 (2)

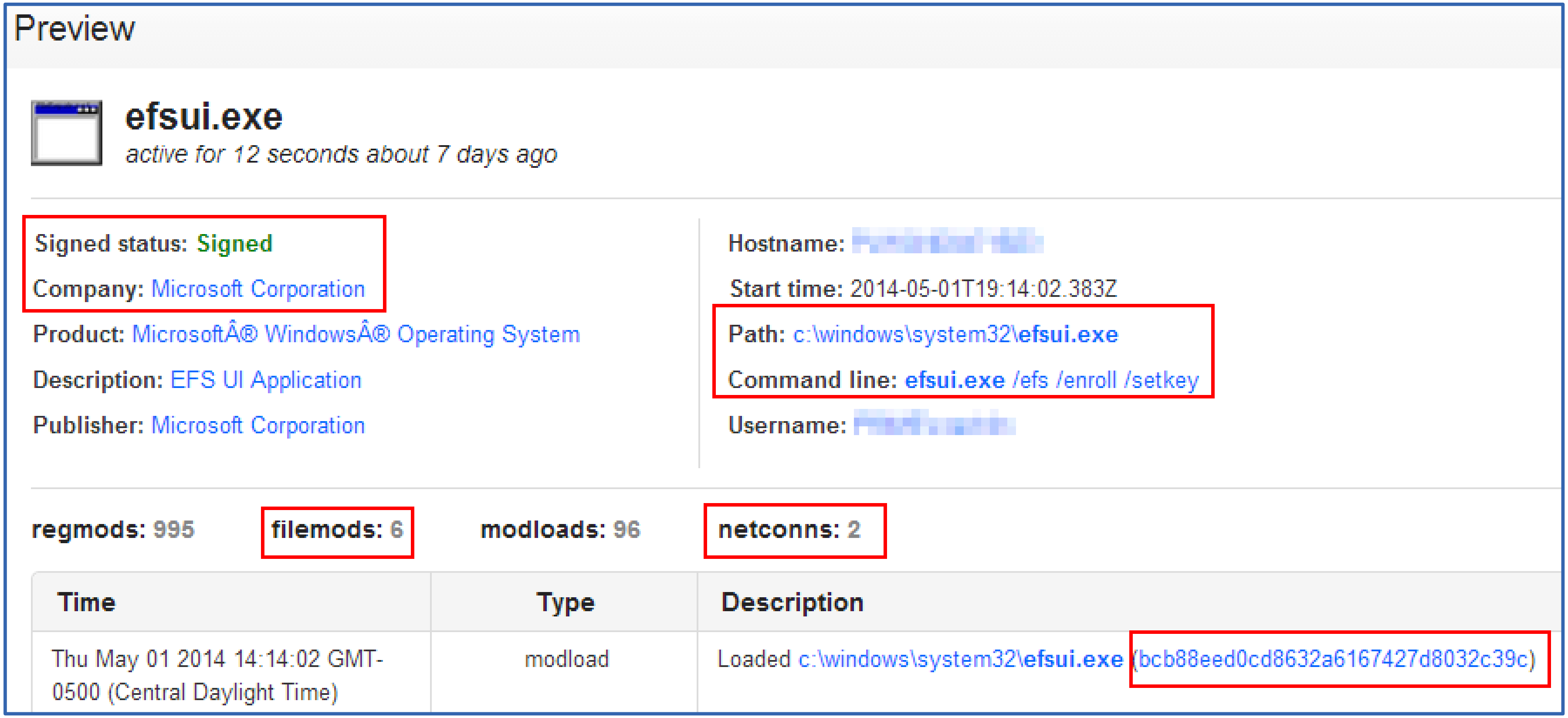
bcb88eed0cd8632a6167...

f17e973615d5cbb9026af...



LSASS Child (2)

Binary Preview (EFSUI) – Looking for anomalies



Preview

efsui.exe

active for 12 seconds about 7 days ago

Signed status: Signed

Company: Microsoft Corporation

Product: MicrosoftÂ® WindowsÂ® Operating System

Description: EFS UI Application

Publisher: Microsoft Corporation

Hostname: [redacted]

Start time: 2014-05-01T19:14:02.383Z

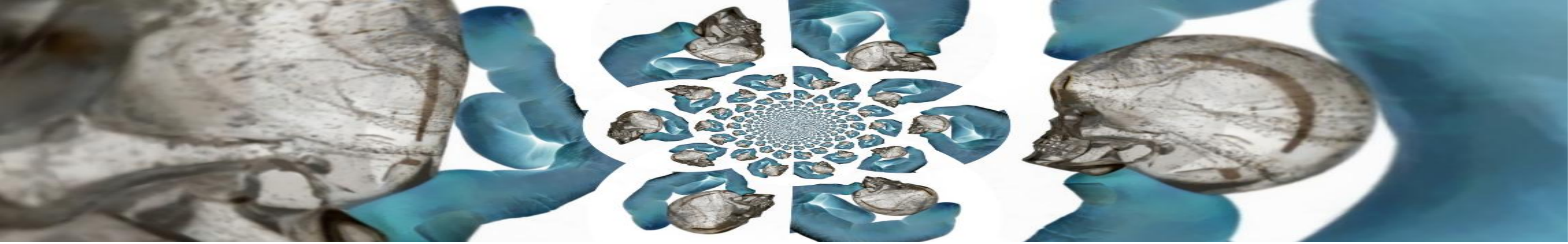
Path: c:\windows\system32\efsui.exe

Command line: efsui.exe /efs /enroll /setkey

Username: [redacted]

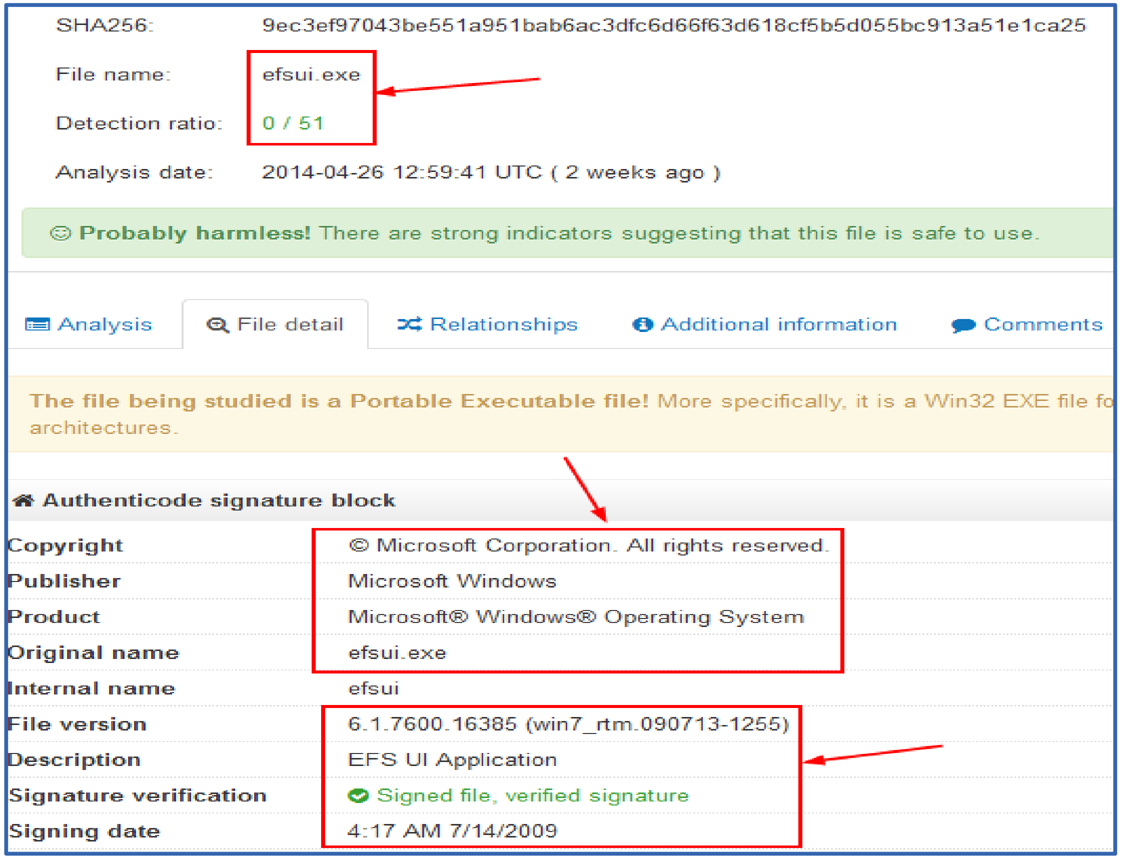
regmods: 995 **filemods:** 6 **modloads:** 96 **netconns:** 2

Time	Type	Description
Thu May 01 2014 14:14:02 GMT-0500 (Central Daylight Time)	modload	Loaded c:\windows\system32\efsui.exe (bcb88eed0cd8632a6167427d8032c39c)



LSASS Child (3)

Binary Analysis – High-level checks against hash



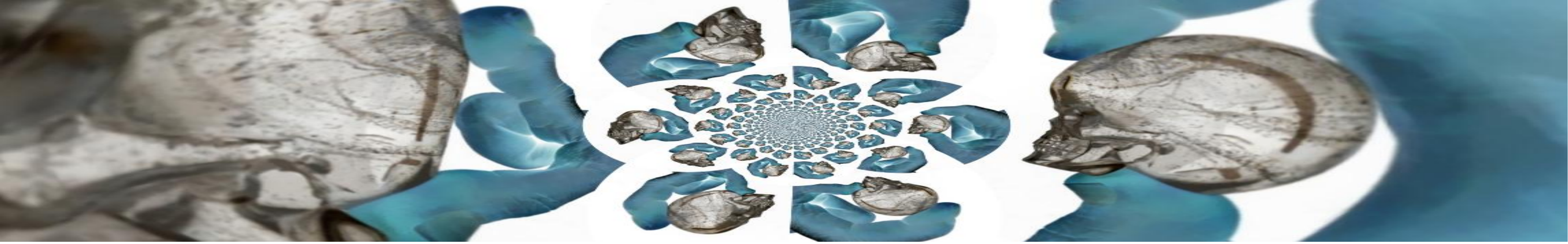
SHA256:	9ec3ef97043be551a951bab6ac3dfc6d66f63d618cf5b5d055bc913a51e1ca25
File name:	efsui.exe
Detection ratio:	0 / 51
Analysis date:	2014-04-26 12:59:41 UTC (2 weeks ago)

☺ **Probably harmless!** There are strong indicators suggesting that this file is safe to use.

The file being studied is a Portable Executable file! More specifically, it is a Win32 EXE file fo architectures.

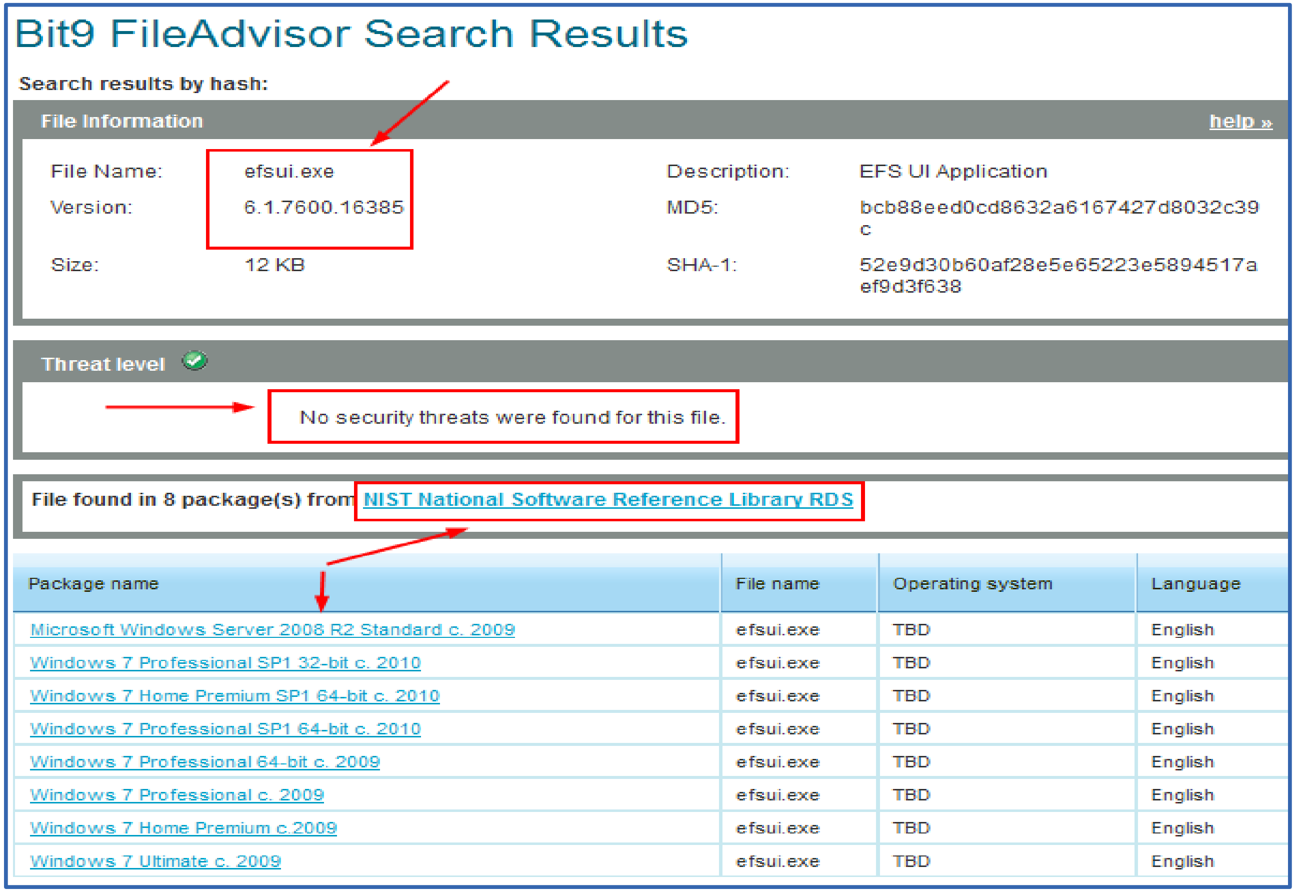
Authenticode signature block

Copyright	© Microsoft Corporation. All rights reserved.
Publisher	Microsoft Windows
Product	Microsoft® Windows® Operating System
Original name	efsui.exe
Internal name	efsui
File version	6.1.7600.16385 (win7_rtm.090713-1255)
Description	EFS UI Application
Signature verification	✓ Signed file, verified signature
Signing date	4:17 AM 7/14/2009



LSASS Child (4)

Binary Analysis – (More) High-level checks against hash



Bit9 FileAdvisor Search Results

Search results by hash:

File Information help »

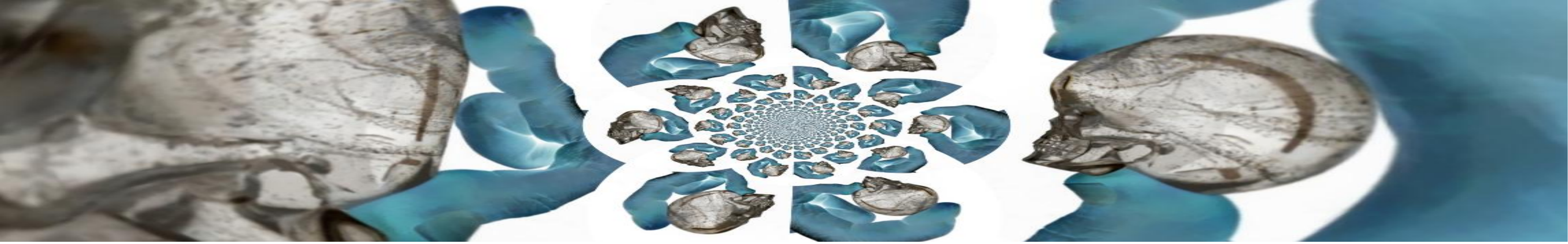
File Name:	efsui.exe	Description:	EFS UI Application
Version:	6.1.7600.16385	MD5:	bcb88eed0cd8632a6167427d8032c39c
Size:	12 KB	SHA-1:	52e9d30b60af28e5e65223e5894517aef9d3f638

Threat level ✓

No security threats were found for this file.

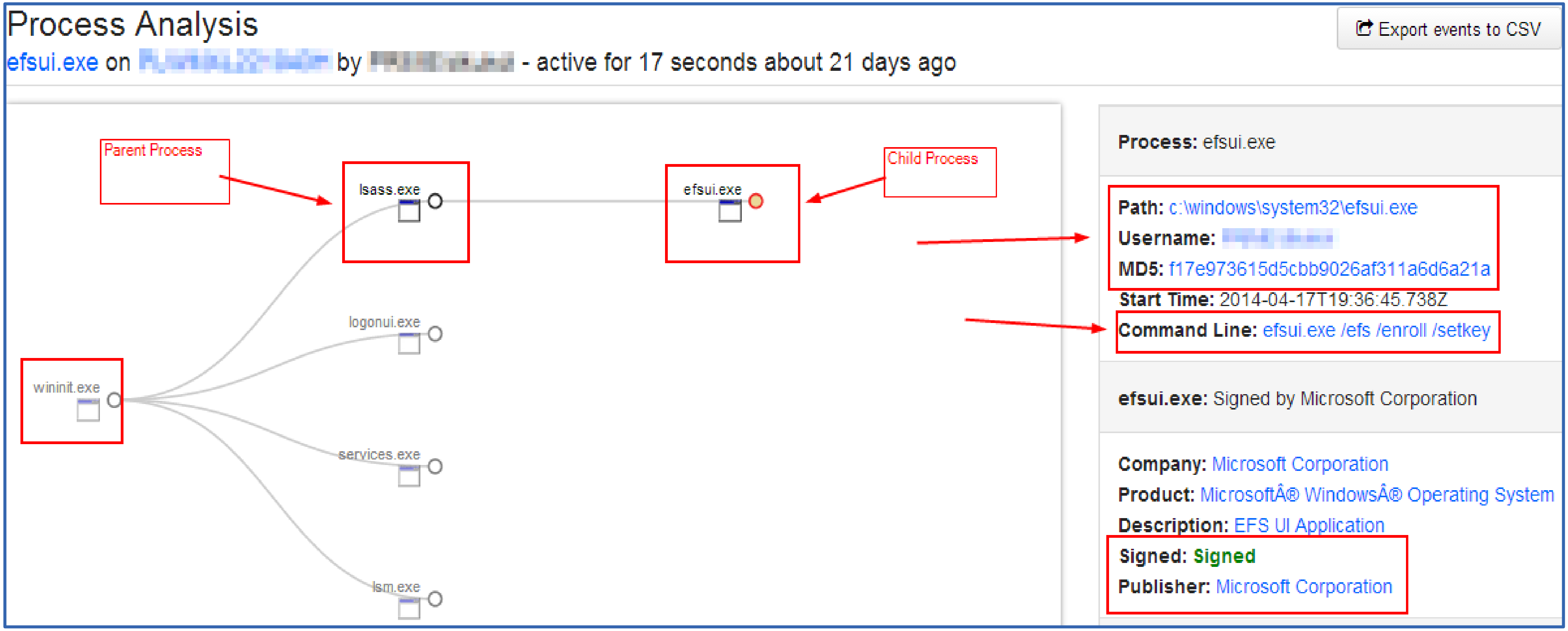
File found in 8 package(s) from NIST National Software Reference Library RDS

Package name	File name	Operating system	Language
Microsoft Windows Server 2008 R2 Standard c. 2009	efsui.exe	TBD	English
Windows 7 Professional SP1 32-bit c. 2010	efsui.exe	TBD	English
Windows 7 Home Premium SP1 64-bit c. 2010	efsui.exe	TBD	English
Windows 7 Professional SP1 64-bit c. 2010	efsui.exe	TBD	English
Windows 7 Professional 64-bit c. 2009	efsui.exe	TBD	English
Windows 7 Professional c. 2009	efsui.exe	TBD	English
Windows 7 Home Premium c.2009	efsui.exe	TBD	English
Windows 7 Ultimate c. 2009	efsui.exe	TBD	English



LSASS Child (5)

Host Analysis – What activity is occurring?



Process Analysis

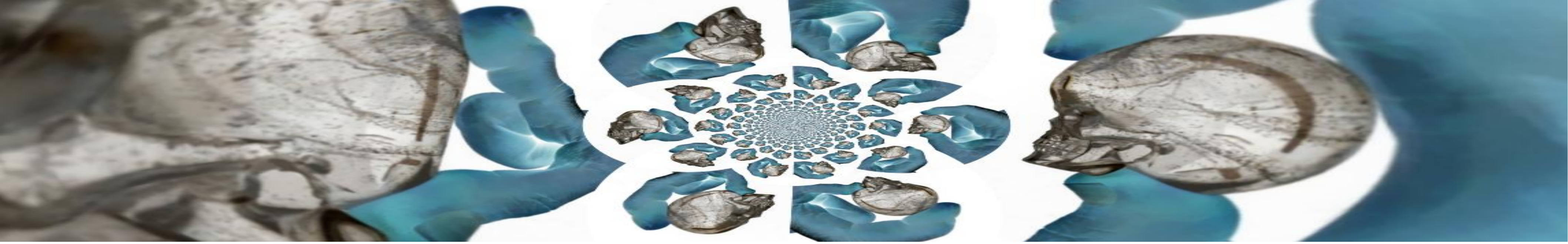
efsui.exe on [redacted] by [redacted] - active for 17 seconds about 21 days ago

Process: efsui.exe

Path: c:\windows\system32\efsui.exe
Username: [redacted]
MD5: f17e973615d5cbb9026af311a6d6a21a
Start Time: 2014-04-17T19:36:45.738Z
Command Line: efsui.exe /efs /enroll /setkey

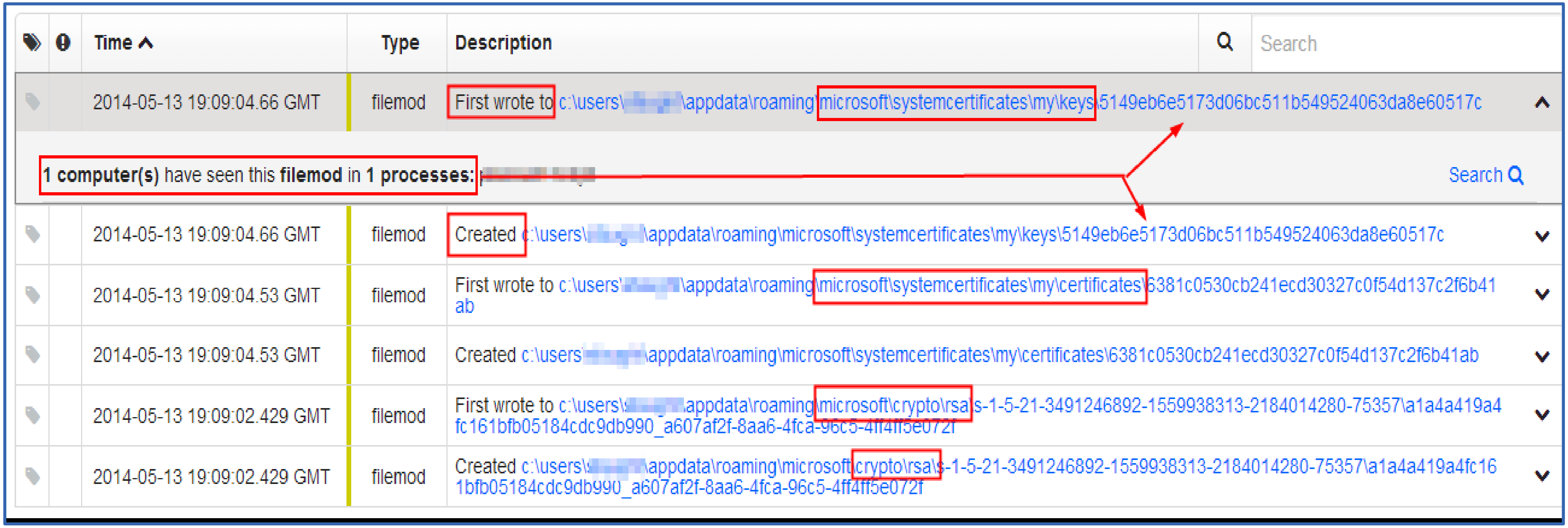
efsui.exe: Signed by Microsoft Corporation

Company: Microsoft Corporation
Product: MicrosoftÂ® WindowsÂ® Operating System
Description: EFS UI Application
Signed: Signed
Publisher: Microsoft Corporation

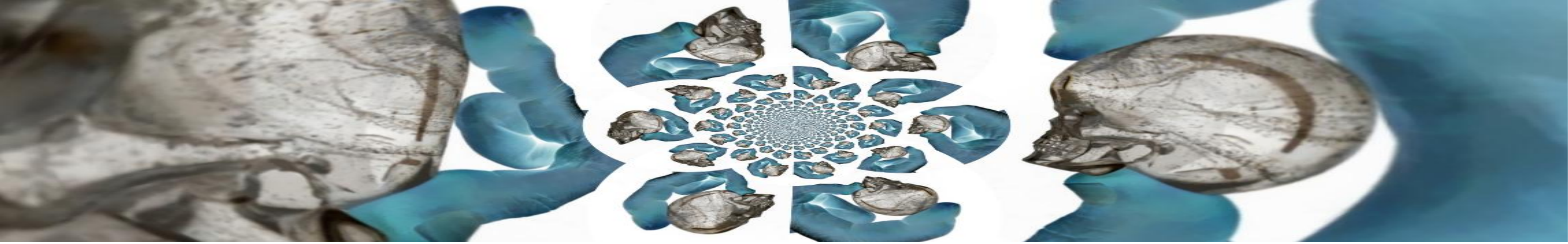


LSASS Child (6)

Host Analysis – File Activity for EFSUI

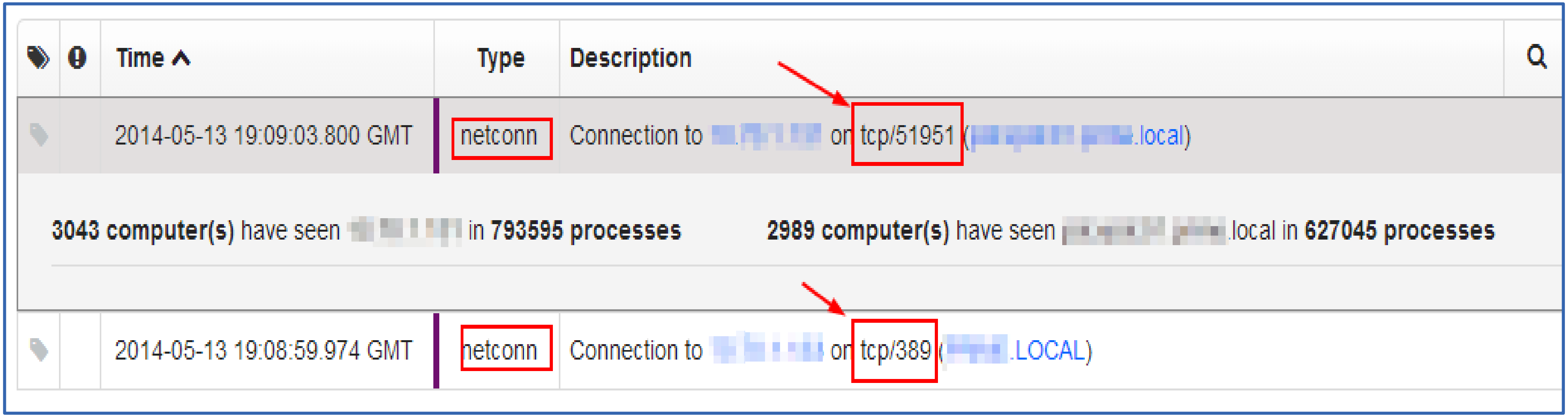


🏷	!	Time ^	Type	Description
🏷		2014-05-13 19:09:04.66 GMT	filemod	First wrote to c:\users\[redacted]\appdata\roaming\microsoft\systemcertificates\my\keys\5149eb6e5173d06bc511b549524063da8e60517c
		1 computer(s) have seen this filemod in 1 processes: [redacted]		Search
🏷		2014-05-13 19:09:04.66 GMT	filemod	Created c:\users\[redacted]\appdata\roaming\microsoft\systemcertificates\my\keys\5149eb6e5173d06bc511b549524063da8e60517c
🏷		2014-05-13 19:09:04.53 GMT	filemod	First wrote to c:\users\[redacted]\appdata\roaming\microsoft\systemcertificates\my\certificates\6381c0530cb241ecd30327c0f54d137c2f6b41ab
🏷		2014-05-13 19:09:04.53 GMT	filemod	Created c:\users\[redacted]\appdata\roaming\microsoft\systemcertificates\my\certificates\6381c0530cb241ecd30327c0f54d137c2f6b41ab
🏷		2014-05-13 19:09:02.429 GMT	filemod	First wrote to c:\users\[redacted]\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-3491246892-1559938313-2184014280-75357\a1a4a419a4fc161bfb05184cdc9db990_a607af2f-8aa6-4fca-96c5-4ff4ff5e072f
🏷		2014-05-13 19:09:02.429 GMT	filemod	Created c:\users\[redacted]\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-3491246892-1559938313-2184014280-75357\a1a4a419a4fc161bfb05184cdc9db990_a607af2f-8aa6-4fca-96c5-4ff4ff5e072f

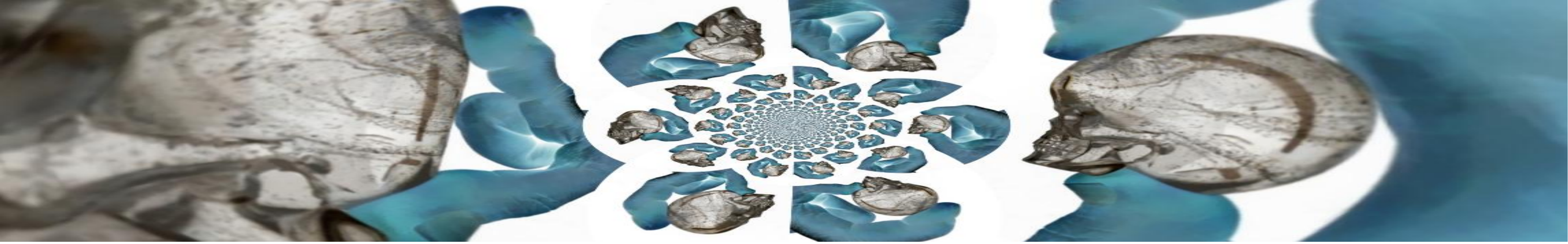


LSASS Child (7)

Host Analysis – Network connections for EFSUI



Time ^	Type	Description
2014-05-13 19:09:03.800 GMT	netconn	Connection to [redacted] on tcp/51951 ([redacted].local)
3043 computer(s) have seen [redacted] in **793595 processes**		**2989 computer(s)** have seen [redacted].local in **627045 processes**
2014-05-13 19:08:59.974 GMT	netconn	Connection to [redacted] on tcp/389 ([redacted].LOCAL)



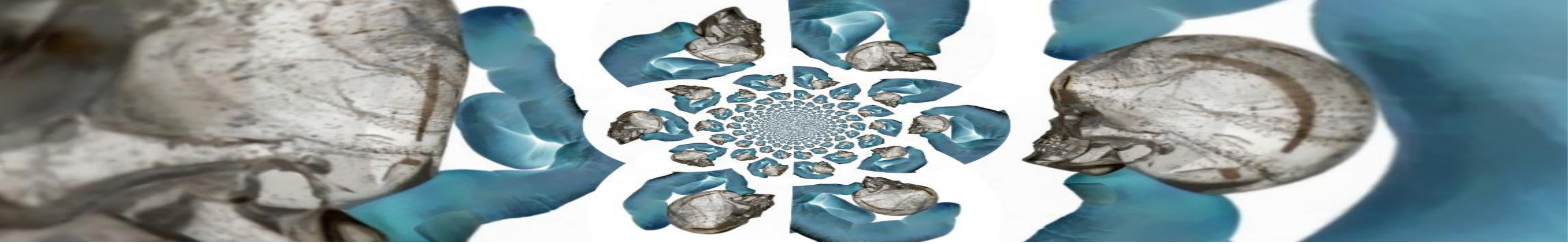
Thoughts to Think About

Every decision is a **risk** decision

Every evidence type may not exist

Lack of knowledge is a hindrance

Ignoring evidence increases risk

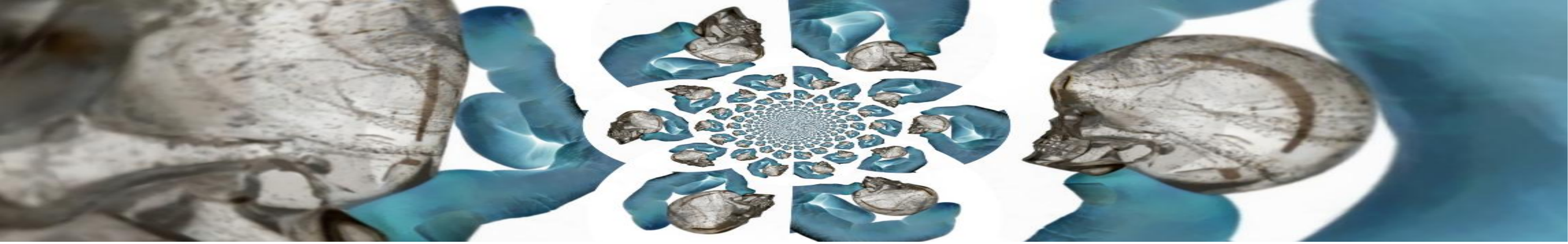


Drinking My Own Medicine

Observation: Many types and sources of evidence

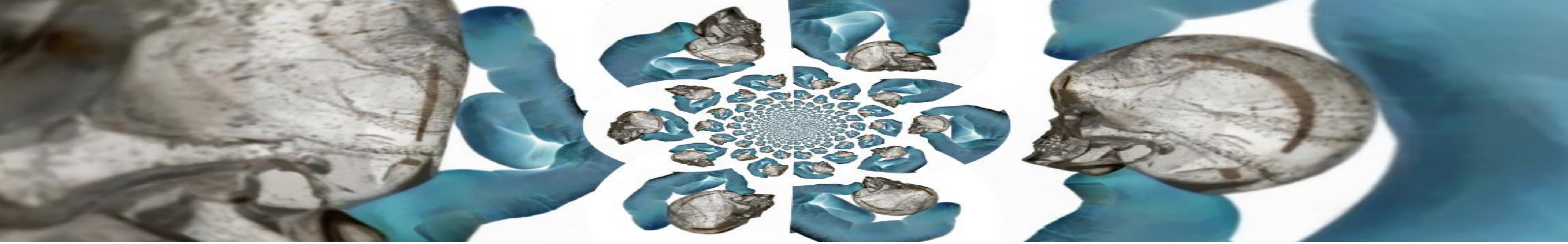
Interpretation: Important to understand them all

Application: Use whenever available and appropriate



No tools, files, registry hives, packets, emails,
restore points, logs, or applications were hurt
in the making of this presentation.

Resources/Tools used just for this presentation include:
PEStudio, VirusTotal, Bit9 File Advisor, Redline



Yes, that's a skull, Horatio. It's a time for introspection.

Write-ups about the Zbot infection and LSASS spawn are available on my blog: forensicaliente.blogspot.com

I'm open for questions and conversation: @littlemac042