



THREATCONNECT™

Open Source Malware Lab

March 9, 2016

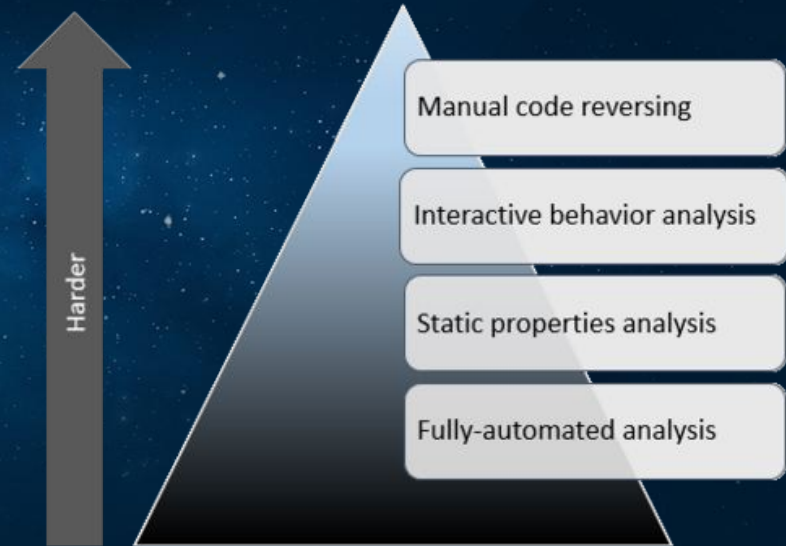
Director of Research Innovation

Research Team

ThreatConnect, Inc.

Why Do I Need A Malware Analysis Lab?

- Malware Research
 - Automated Malware Analysis (AMA)
 - First of four major stages
 - AMA can include second stage
- Enhanced Threat Intelligence
 - Analysis of malware in your enterprise
 - Stage of malware hunting process
- Network Defense
 - Network Traffic
 - Inbound Email
 - Host Intrusion Detection System
- Fun!!!



<https://zeltser.com/mastering-4-stages-of-malware-analysis/>

Malware Analysis Process Entry Points



File



URL



PCAP



Memory
Image

Open Source Malware Analysis Tools



Cuckoo
Sandbox



Thug



Bro



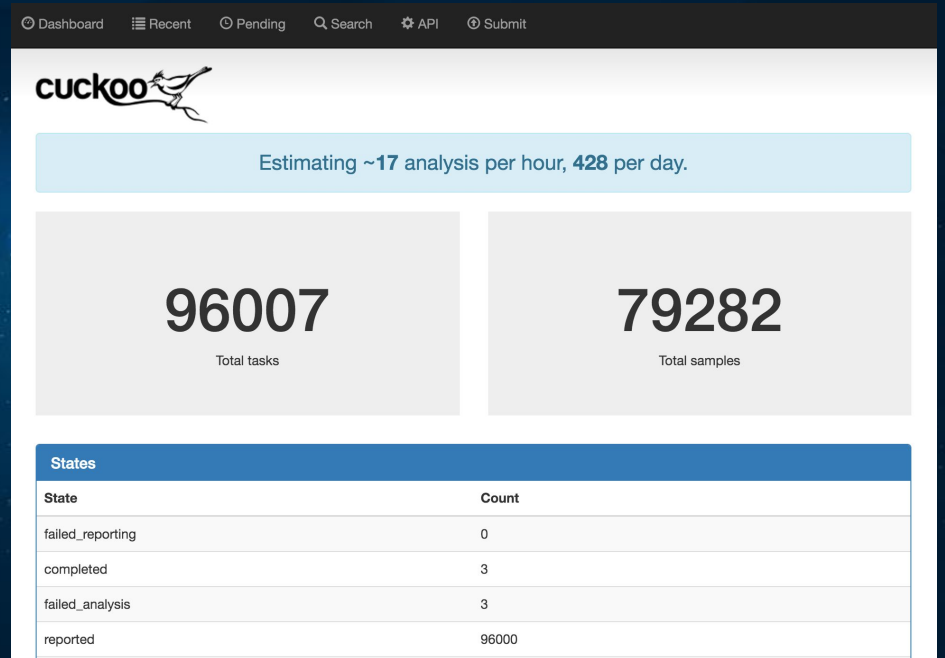
Volatility



Cuckoo Sandbox

Static and Dynamic File Analysis

- A controlled, safe environment
- Leverages
 - Virtual machines
 - Bare metal computers
- Running malware
- Observing its behavior
- Dynamic malware analysis
- May also perform static malware analysis



More Than Just Dynamic Analysis

Strings

```
$Info: This file is packed with the UPX executable  
packer http://upx.sf.net $  
$Id: UPX 3.91 Copyright (C) 1996-2013 the UPX Team.  
All Rights Reserved. $
```

AV Detections

```
TrendMicro: OSX_KeRanger.A  
ESET-NOD32: OSX/Filecoder.KeRanger.A  
Kaspersky: UDS:DangerousObject.Multi.Generic
```


More Than Just Dynamic Analysis

Strings

```
$Info: This file is packed with the UPX executable  
packer http://upx.sf.net $  
$Id: UPX 3.91 Copyright (C) 1996-2013 the UPX Team.  
All Rights Reserved. $
```

AV Detections

```
TrendMicro: OSX_KeRanger.A  
ESET-NOD32: OSX/Filecoder.KeRanger.A  
Kaspersky: UDS:DangerousObject.Multi.Generic
```

More Than Just Dynamic Analysis

Strings

```
$Info: This file is packed with the UPX executable  
packer http://upx.sf.net $  
$Id: UPX 3.91 Copyright (C) 1996-2013 the UPX Team.  
All Rights Reserved. $
```

AV Detections

```
TrendMicro: OSX_KeRanger.A  
ESET-NOD32: OSX/Filecoder.KeRanger.A  
Kaspersky: UDS:DangerousObject.Multi.Generic
```

More Than Just Dynamic Analysis

Strings

```
$Info: This file is packed with the UPX executable  
packer http://upx.sf.net $  
$Id: UPX 3.91 Copyright (C) 1996-2013 the UPX Team.  
All Rights Reserved. $
```

AV Detections

```
TrendMicro: OSX_KeRanger.A  
ESET-NOD32: OSX/Filecoder.KeRanger.A  
Kaspersky: UDS:DangerousObject.Multi.Generic
```

More Than Just Dynamic Analysis

Sections

```
Name Addr Ent MD5
.rsrc 532480 3.59 7ce8cbef10f26dfef328a35f2c724cd5
52 files found
```

Resources

```
data RT_VERSION
3519388073965d5b6bae77135c36786f6f8e6882099a88504fba
d3ed9b9c9687 99 files found
```

File Metadata

```
Timestamp: 2016-03-07 09:41:34
First Seen: 2016-03-07 09:42:47 95c231bb, web, RU
```

More Than Just Dynamic Analysis

Sections

```
Name Addr Ent MD5
.rsrc 532480 3.59 7ce8cbef10f26dfef328a35f2c724cd5
52 files found
```

Resources

```
data RT_VERSION
3519388073965d5b6bae77135c36786f6f8e6882099a88504fba
d3ed9b9c9687 99 files found
```

File Metadata

```
Timestamp: 2016-03-07 09:41:34
First Seen: 2016-03-07 09:42:47 95c231bb, web, RU
```

More Than Just Dynamic Analysis

Sections

```
Name Addr Ent MD5
.rsrc 532480 3.59 7ce8cbef10f26dfef328a35f2c724cd5
52 files found
```

Resources

```
data RT_VERSION
3519388073965d5b6bae77135c36786f6f8e6882099a88504fba
d3ed9b9c9687 99 files found
```

File Metadata

```
Timestamp: 2016-03-07 09:41:34
First Seen: 2016-03-07 09:42:47 95c231bb, web, RU
```

More Than Just Dynamic Analysis

Sections

```
Name Addr Ent MD5
.rsrc 532480 3.59 7ce8cbef10f26dfef328a35f2c724cd5
52 files found
```

Resources

```
data RT_VERSION
3519388073965d5b6bae77135c36786f6f8e6882099a88504fba
d3ed9b9c9687 99 files found
```

File Metadata

```
Timestamp: 2016-03-07 09:41:34
First Seen: 2016-03-07 09:42:47 95c231bb, web, RU
```

More Than Just Dynamic Analysis

Sections

```
Name Addr Ent MD5
.rsrc 532480 3.59 7ce8cbef10f26dfce328a35f2c724cd5
52 files found
```

Resources

```
data RT_VERSION
3519388073965d5b6bae77135c36786f6f8e6882099a88504fba
d3ed9b9c9687 99 files found
```

File Metadata

```
Timestamp: 2016-03-07 09:41:34
First Seen: 2016-03-07 09:42:47 95c231bb, web, RU
```


More Than Just Dynamic Analysis

Sections

```
Name Addr Ent MD5
.rsrc 532480 3.59 7ce8cbef10f26dfef328a35f2c724cd5
52 files found
```

Resources

```
data RT_VERSION
3519388073965d5b6bae77135c36786f6f8e6882099a88504fba
d3ed9b9c9687 99 files found
```

File Metadata

```
Timestamp: 2016-03-07 09:41:34
First Seen: 2016-03-07 09:42:47 95c231bb, web, RU
```

More Than Just Dynamic Analysis

Sections

```
Name Addr Ent MD5
.rsrc 532480 3.59 7ce8cbef10f26dfef328a35f2c724cd5
52 files found
```

Resources

```
data RT_VERSION
3519388073965d5b6bae77135c36786f6f8e6882099a88504fba
d3ed9b9c9687 99 files found
```

File Metadata

```
Timestamp: 2016-03-07 09:41:34
First Seen: 2016-03-07 09:42:47 95c231bb, web, RU
```

More Than Just Dynamic Analysis

Sections

```
Name Addr Ent MD5
.rsrc 532480 3.59 7ce8cbef10f26dfef328a35f2c724cd5
52 files found
```

Resources

```
data RT_VERSION
3519388073965d5b6bae77135c36786f6f8e6882099a88504fba
d3ed9b9c9687 99 files found
```

File Metadata

```
Timestamp: 2016-03-07 09:41:34
First Seen: 2016-03-07 09:42:47 95c231bb, web, RU
```

Cuckoo Sandbox Flavors

Plain Vanilla
Version 1.2 (Stable)

Next Generation
Version 2.0 RC1

Cuckoo Modified
(brad-accuvant / spender-sanbox)

Cuckoo Modified

- Normalization of file and registry paths
- 64bit analysis
- Service monitoring
- Extended API
- Tor for outbound network connections
- Malheur integration

Cuckoo Next Generation

- Support for:
 - MacOS X
 - Linux
 - Android
- Integrations:
 - Suricata
 - Snort
 - Moloch
- SSL decryption
- VPN support
- 64bit analysis
- fun, fun, fun

What if the Malware is VM or Sandbox Aware?

- Pafish (Paranoid Fish)
 - Uses malware's anti-analysis techniques
 - Shows successful and unsuccessful techniques
 - Pinpoint ways to improve sandbox
- VMCloak
 - Automated generation of Windows VM images
 - Ready for use in Cuckoo
 - Obfuscates VM to prevent anti-analysis

```
[ - ] Sandboxie detection
[*] Using sbiedll.dll ... OK

[ - ] Wine detection
[*] Using GetProcAddress(wine_get_unix_file_name) from kernel32.dll ... OK

[ - ] VirtualBox detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key <HKLM\HARDWARE\Description\System "SystemBiosVersion" ... OK
[*] Reg key <HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions ... OK
[*] Reg key <HKLM\HARDWARE\Description\System "VideoBiosVersion" ... traced!
[*] Looking for C:\WINDOWS\system32\drivers\UBoxMouse.sys ... OK

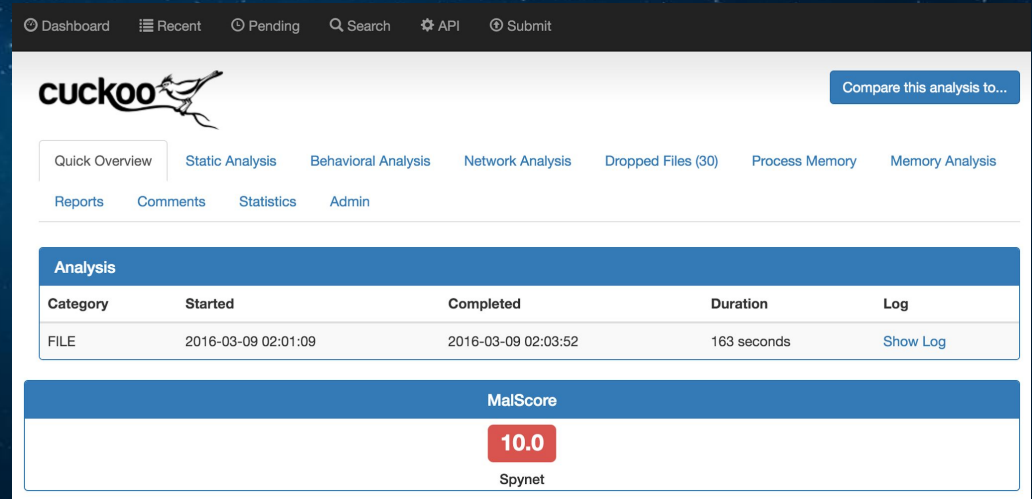
[ - ] VMware detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key <HKLM\SOFTWARE\VMware, Inc.\VMware Tools ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vmmouse.sys ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vmhgfs.sys ... OK

[ - ] Qemu detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key <HKLM\HARDWARE\Description\System "SystemBiosVersion" ... OK

[ - ] Finished, feel free to RE me.
```

Cuckoo Output

- HTML Report
- JSON Report
- MongoDB Output
- Dropped Files
- PCAP
- Memory Image
- Visited URLs



The screenshot displays the Cuckoo Sandbox web interface. At the top, there is a navigation bar with links for Dashboard, Recent, Pending, Search, API, and Submit. The main header features the Cuckoo logo and a "Compare this analysis to..." button. Below the header, there are tabs for "Quick Overview" (selected), Static Analysis, Behavioral Analysis, Network Analysis, Dropped Files (30), Process Memory, and Memory Analysis. Underneath, there are links for Reports, Comments, Statistics, and Admin. The main content area shows an "Analysis" section with a table of results:

Category	Started	Completed	Duration	Log
FILE	2016-03-09 02:01:09	2016-03-09 02:03:52	163 seconds	Show Log

Below the table, there is a "MalScore" section showing a score of **10.0** in a red box, with the source identified as "Spynet".



Thug

Low-Interaction Honeyclient

What is a Low-Interaction Honeyclient?

- Pretends to be a browser
- Trigger a drive-by download
- Capture its payload



<http://previews.123rf.com/images/miceking/miceking1506/miceking150600087/40785514-Honey-Pot-Stock-Vector.jpg>

Wolf in Sheep's Clothing

- User Agent can change
 - Windows, Mac, Linux, Android, iOS
 - Limitless possibilities
 - <http://www.useragentstring.com/pages/useragentstring.php>
 - <http://www.browser-info.net/useragents>
- Simulates vulnerable plugins with configurable versions
 - Flash
 - Java
 - Acrobat Reader (PDF)



Available User Agents

Available User-Agents:

winxpie60	Internet Explorer 6.0	(Windows XP)
winxpie61	Internet Explorer 6.1	(Windows XP)
winxpie70	Internet Explorer 7.0	(Windows XP)
winxpie80	Internet Explorer 8.0	(Windows XP)
winxpchrome20	Chrome 20.0.1132.47	(Windows XP)
winxpfirefox12	Firefox 12.0	(Windows XP)
winxpsafari5	Safari 5.1.7	(Windows XP)
win2kie60	Internet Explorer 6.0	(Windows 2000)
win2kie80	Internet Explorer 8.0	(Windows 2000)
win7ie80	Internet Explorer 8.0	(Windows 7)
win7ie90	Internet Explorer 9.0	(Windows 7)
win7chrome20	Chrome 20.0.1132.47	(Windows 7)
win7chrome40	Chrome 40.0.2214.91	(Windows 7)
win7chrome45	Chrome 45.0.2454.85	(Windows 7)
win7firefox3	Firefox 3.6.13	(Windows 7)
win7safari5	Safari 5.1.7	(Windows 7)
osx10chrome19	Chrome 19.0.1084.54	(MacOS X 10.7.4)
osx10safari5	Safari 5.1.1	(MacOS X 10.7.2)
linuxchrome26	Chrome 26.0.1410.19	(Linux)
linuxchrome30	Chrome 30.0.1599.15	(Linux)
linuxchrome44	Chrome 44.0.2403.89	(Linux)
linuxfirefox19	Firefox 19.0	(Linux)
linuxfirefox40	Firefox 40.0	(Linux)
galaxy2chrome18	Chrome 18.0.1025.166	(Samsung Galaxy S II, Android 4.0.3)
galaxy2chrome25	Chrome 25.0.1364.123	(Samsung Galaxy S II, Android 4.0.3)
galaxy2chrome29	Chrome 29.0.1547.59	(Samsung Galaxy S II, Android 4.1.2)
nexuschrome18	Chrome 18.0.1025.133	(Google Nexus, Android 4.0.4)
ipadchrome33	Chrome 33.0.1750.21	(iPad, iOS 7.1)
ipadchrome35	Chrome 35.0.1916.41	(iPad, iOS 7.1.1)
ipadchrome37	Chrome 37.0.2062.52	(iPad, iOS 7.1.2)
ipadchrome38	Chrome 38.0.2125.59	(iPad, iOS 8.0.2)
ipadchrome39	Chrome 39.0.2171.45	(iPad, iOS 8.1.1)
ipadchrome45	Chrome 45.0.2454.68	(iPad, iOS 8.4.1)
ipadchrome46	Chrome 46.0.2490.73	(iPad, iOS 9.0.2)
ipadsafari7	Safari 7.0	(iPad, iOS 7.0.4)
ipadsafari8	Safari 8.0	(iPad, iOS 8.0.2)
ipadsafari9	Safari 9.0	(iPad, iOS 9.1)

Available User Agents

Available User-Agents:

winxpie60	Internet Explorer 6.0	(Windows XP)
winxpie61	Internet Explorer 6.1	(Windows XP)
winxpie70	Internet Explorer 7.0	(Windows XP)
winxpie80	Internet Explorer 8.0	(Windows XP)
winxpchrome20	Chrome 20.0.1132.47	(Windows XP)
winxpfirefox12	Firefox 12.0	(Windows XP)
winxpsafari5	Safari 5.1.7	(Windows XP)
win2kie60	Internet Explorer 6.0	(Windows 2000)
win2kie80	Internet Explorer 8.0	(Windows 2000)
win7ie80	Internet Explorer 8.0	(Windows 7)
win7ie90	Internet Explorer 9.0	(Windows 7)
win7chrome20	Chrome 20.0.1132.47	(Windows 7)
win7chrome40	Chrome 40.0.2214.91	(Windows 7)
win7chrome45	Chrome 45.0.2454.85	(Windows 7)
win7firefox3	Firefox 3.6.13	(Windows 7)
win7safari5	Safari 5.1.7	(Windows 7)
osx10chrome19	Chrome 19.0.1084.54	(MacOS X 10.7.4)
osx10safari5	Safari 5.1.1	(MacOS X 10.7.2)
linuxchrome26	Chrome 26.0.1410.19	(Linux)
linuxchrome30	Chrome 30.0.1599.15	(Linux)
linuxchrome44	Chrome 44.0.2403.89	(Linux)
linuxfirefox19	Firefox 19.0	(Linux)
linuxfirefox40	Firefox 40.0	(Linux)
galaxy2chrome18	Chrome 18.0.1025.166	(Samsung Galaxy S II, Android 4.0.3)
galaxy2chrome25	Chrome 25.0.1364.123	(Samsung Galaxy S II, Android 4.0.3)
galaxy2chrome29	Chrome 29.0.1547.59	(Samsung Galaxy S II, Android 4.1.2)
nexuschrome18	Chrome 18.0.1025.133	(Google Nexus, Android 4.0.4)
ipadchrome33	Chrome 33.0.1750.21	(iPad, iOS 7.1)
ipadchrome35	Chrome 35.0.1916.41	(iPad, iOS 7.1.1)
ipadchrome37	Chrome 37.0.2062.52	(iPad, iOS 7.1.2)
ipadchrome38	Chrome 38.0.2125.59	(iPad, iOS 8.0.2)
ipadchrome39	Chrome 39.0.2171.45	(iPad, iOS 8.1.1)
ipadchrome45	Chrome 45.0.2454.68	(iPad, iOS 8.4.1)
ipadchrome46	Chrome 46.0.2490.73	(iPad, iOS 9.0.2)
ipadsafari7	Safari 7.0	(iPad, iOS 7.0.4)
ipadsafari8	Safari 8.0	(iPad, iOS 8.0.2)
ipadsafari9	Safari 9.0	(iPad, iOS 9.1)

Thug Output

- Payload Files
- Other Content Files
- Visited URLs
- MongoDB Output
- Elasticsearch Output
- HPFeeds
- MAEC
- Native Report Format



Bro

Network Analysis Framework

What is Bro?

- Network Security Monitoring (NSM) Framework
- Processes
 - Live Packet Capture
 - Recorded Packet Capture (PCAP)
- Series of scripts
- Output Bro logs
- Packaged with a large group of scripts
- Rich community of open source scripts
- Write your own Bro script for specific needs

Bro in Action

- Analysis Target: Документ.xls
- PCAP Source: <https://www.hybrid-analysis.com/>
- SHA1: 09229cc895c15db0c8900211ef4e76918b2ccda1
- What can we learn from PCAP only?

conn.log

```
$ cat conn.log | bro-cut -c uid id.orig_h id.resp_h id.resp_p proto service |
sed -e 's/#fields//g' | grep -v '#' | column -t
```

uid	id.orig_h	id.resp_h	id.resp_p	proto	service
CeJmNF34xN03NtSGnj	fe80::e1f1:a1d3:450a:e764	ff02::16	0	icmp	-
CNlSS928ab78QnKSL3	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CBmkph31212thohefd	192.168.56.18	224.0.0.252	5355	udp	dns
C0LkngQTWe8rv01j	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CdtvgM2r45S8DlASng	192.168.56.18	224.0.0.252	5355	udp	dns
CinmLMpcwJQtXFcja	192.168.56.18	8.8.8.8	53	udp	dns
C0Rpek4S51GPbs1CWg	192.168.56.18	185.26.97.121	80	tcp	http
C0KY1k4E1knNFN5ZWg	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CPu2nu12Xvles4NUj	192.168.56.18	224.0.0.252	5355	udp	dns
C54Xtu1NVmeI4cEZja	192.168.56.18	89.108.101.61	5651	tcp	-
CL6bhh3vEUaIF6sVfd	192.168.56.18	90.156.241.111	80	tcp	http
CI7bFMWiKtPXjkkm3	192.168.56.18	8.8.8.8	53	udp	dns
Cdc37M2hosjXx7dwog	192.168.56.18	80.234.32.33	5651	tcp	-
CyHRbg2kJVuoL9X7	fe80::e1f1:a1d3:450a:e764	ff02::1:2	547	udp	-

conn.log

```
$ cat conn.log | bro-cut -c uid id.orig_h id.resp_h id.resp_p proto service |
sed -e 's/#fields//g' | grep -v '#' | column -t
```

uid	id.orig_h	id.resp_h	id.resp_p	proto	service
CeJmNF34xN03NtSGnj	fe80::e1f1:a1d3:450a:e764	ff02::16	0	icmp	-
CNlSS928ab78QnKSL3	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CBmkph31212thohefd	192.168.56.18	224.0.0.252	5355	udp	dns
C0LkngQTWe8rv01j	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CdtvgM2r45S8DlASng	192.168.56.18	224.0.0.252	5355	udp	dns
CinmLMpcwJQtXFcja	192.168.56.18	8.8.8.8	53	udp	dns
C0Rpek4S51GPbs1CWg	192.168.56.18	185.26.97.121	80	tcp	http
C0KY1k4E1knNFN5ZWg	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CPu2nu12Xvles4NUj	192.168.56.18	224.0.0.252	5355	udp	dns
C54Xtu1NVmeI4cEZja	192.168.56.18	89.108.101.61	5651	tcp	-
CL6bhh3vEUaIF6sVfd	192.168.56.18	90.156.241.111	80	tcp	http
CI7bFMWiKtPXjkkm3	192.168.56.18	8.8.8.8	53	udp	dns
Cdc37M2hosjXx7dwog	192.168.56.18	80.234.32.33	5651	tcp	-
CyhRbgt2kJVuoL9X7	fe80::e1f1:a1d3:450a:e764	ff02::1:2	547	udp	-

conn.log

```
$ cat conn.log | bro-cut -c uid id.orig_h id.resp_h id.resp_p proto service |
sed -e 's/#fields//g' | grep -v '#' | column -t
```

uid	id.orig_h	id.resp_h	id.resp_p	proto	service
CeJmNF34xN03NtSGnj	fe80::e1f1:a1d3:450a:e764	ff02::16	0	icmp	-
CNlSS928ab78QnKSL3	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CBmkph31212thohefd	192.168.56.18	224.0.0.252	5355	udp	dns
C0LkngQTWe8rv01j	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CdtvgM2r45S8DlASng	192.168.56.18	224.0.0.252	5355	udp	dns
CinmLMpcwJQtXFcja	192.168.56.18	8.8.8.8	53	udp	dns
C0Rpek4S51GPbs1CWg	192.168.56.18	185.26.97.121	80	tcp	http
C0KY1k4E1knNFN5ZWg	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CPu2nu12Xvles4NUj	192.168.56.18	224.0.0.252	5355	udp	dns
C54Xtu1NVmeI4cEZja	192.168.56.18	89.108.101.61	5651	tcp	-
CL6bhh3vEUaIF6sVfd	192.168.56.18	90.156.241.111	80	tcp	http
CI7bFMWiKtPXjkkm3	192.168.56.18	8.8.8.8	53	udp	dns
Cdc37M2hosjXx7dwog	192.168.56.18	80.234.32.33	5651	tcp	-
CyHRbg2kJVuoL9X7	fe80::e1f1:a1d3:450a:e764	ff02::1:2	547	udp	-

conn.log

```
$ cat conn.log | bro-cut -c uid id.orig_h id.resp_h id.resp_p proto service |
sed -e 's/#fields//g' | grep -v '#' | column -t
```

uid	id.orig_h	id.resp_h	id.resp_p	proto	service
CeJmNF34xN03NtSGnj	fe80::e1f1:a1d3:450a:e764	ff02::16	0	icmp	-
CNlSS928ab78QnKSL3	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CBmkph31212thohefd	192.168.56.18	224.0.0.252	5355	udp	dns
C0LkngQTWe8rv01j	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CdtvgM2r45S8DlASng	192.168.56.18	224.0.0.252	5355	udp	dns
CinmLMpcwJQtXFcja	192.168.56.18	8.8.8.8	53	udp	dns
C0Rpek4S51GPbs1CWg	192.168.56.18	185.26.97.121	80	tcp	http
C0KY1k4E1knNFN5ZWg	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CPu2nu12Xvles4NUj	192.168.56.18	224.0.0.252	5355	udp	dns
C54Xtu1NVmeI4cEZja	192.168.56.18	80.108.101.61	5651	tcp	-
CL6bhh3vEUaIF6sVfd	192.168.56.18	90.156.241.111	80	tcp	http
CI7bFMWiKtPXjkkm3	192.168.56.18	8.8.8.8	53	udp	dns
Cdc37M2hosjXx7dwog	192.168.56.18	80.234.32.33	5651	tcp	-
CyHRbgT2kJVuoL9X7	fe80::e1f1:a1d3:450a:e764	ff02::1:2	547	udp	-

conn.log

```
$ cat conn.log | bro-cut -c uid id.orig_h id.resp_h id.resp_p proto service |
sed -e 's/#fields//g' | grep -v '#' | column -t
```

uid	id.orig_h	id.resp_h	id.resp_p	proto	service
CeJmNF34xN03NtSGnj	fe80::e1f1:a1d3:450a:e764	ff02::16	0	icmp	-
CNlSS928ab78QnKSL3	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CBmkph31212thohefd	192.168.56.18	224.0.0.252	5355	udp	dns
C0LkngQTWe8rv01j	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CdtvgM2r45S8DlASng	192.168.56.18	224.0.0.252	5355	udp	dns
CinmLMpcwJQtXFcja	192.168.56.18	8.8.8.8	53	udp	dns
C0Rpek4S51GPbs1CWg	192.168.56.18	185.26.97.121	80	tcp	http
C0KY1k4E1knNFN5ZWg	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CPu2nu12Xvles4NUj	192.168.56.18	224.0.0.252	5355	udp	dns
C54Xtu1NVmeI4cEZja	192.168.56.18	89.108.101.61	5651	tcp	-
CL6bhh3vEUaIF6sVfd	192.168.56.18	90.156.241.111	80	tcp	http
CI7bFMWiKtPXjkkm3	192.168.56.18	8.8.8.8	53	udp	dns
Cdc37M2hosjXx7dwog	192.168.56.18	80.234.32.33	5651	tcp	-
CyHRbg2kJVuoL9X7	fe80::e1f1:a1d3:450a:e764	ff02::1:2	547	udp	-

dns.log

```
$ cat dns.log | bro-cut -c query qtype_name answers rcode_name |  
grep 'NOERROR\|fields' | sed -e 's/#fields//g' | column -t
```

query	qtype_name	answers	rcode_name
s01.yapfiles.ru	A	185.26.97.121,136.243.132.31,78.47.0.98,136.243.132.30,185.26.97.120	NOERROR
rmansys.ru	A	90.156.241.111	NOERROR

The screenshot shows the yapfiles.ru website interface. At the top, there is a search bar with the text "Поиск...", a "Найти" button, and a "Везде" dropdown menu. Below the search bar, there are links for "Справка", "RSS", "B", and "Добавить файл избранное". A notification box on the right states: "Ваш IP адрес 77.247.181.165 заблокирован. Доступ ограничен. Если вы считаете это ошибкой, напишите письмо на адрес yapbox@gmail.com". The main navigation bar includes "Главная / Видео", "Музыка", "Картинки", "Флэш", and "Мои файлы". Below this, there is a "Рекомендуем к просмотру" section with a video player showing a car on a road. The video title is "Держись, Маш!" and it has 18656 views and 2 comments. To the right of the video player, there are three video thumbnails: "Арабское такси" (02:36), "Весы" (01:05), and "SPASM live at Obscene Extreme Fest" (03:24). At the bottom, there is a "Новые" section and a "Категории" dropdown menu.

ЯП ФАЙЛЫ
Удобный и бесплатный сервис для хранения и публикации медиа-файлов.
[Подробнее »](#)

Поиск...
Везде ▾ Найти

Справка RSS B **Добавить файл**

избранное

Ваш IP адрес 77.247.181.165 заблокирован. Доступ ограничен. Если вы считаете это ошибкой, напишите письмо на адрес yapbox@gmail.com

Главная / Видео

Видео Музыка Картинки Флэш Мои файлы

Рекомендуем к просмотру ↓ Страницы: 1 2 3

"Держись, Маш!" ★★★★★
07.03.2016 10:38 просмотры: 18656 комментарии: 2 InGrit

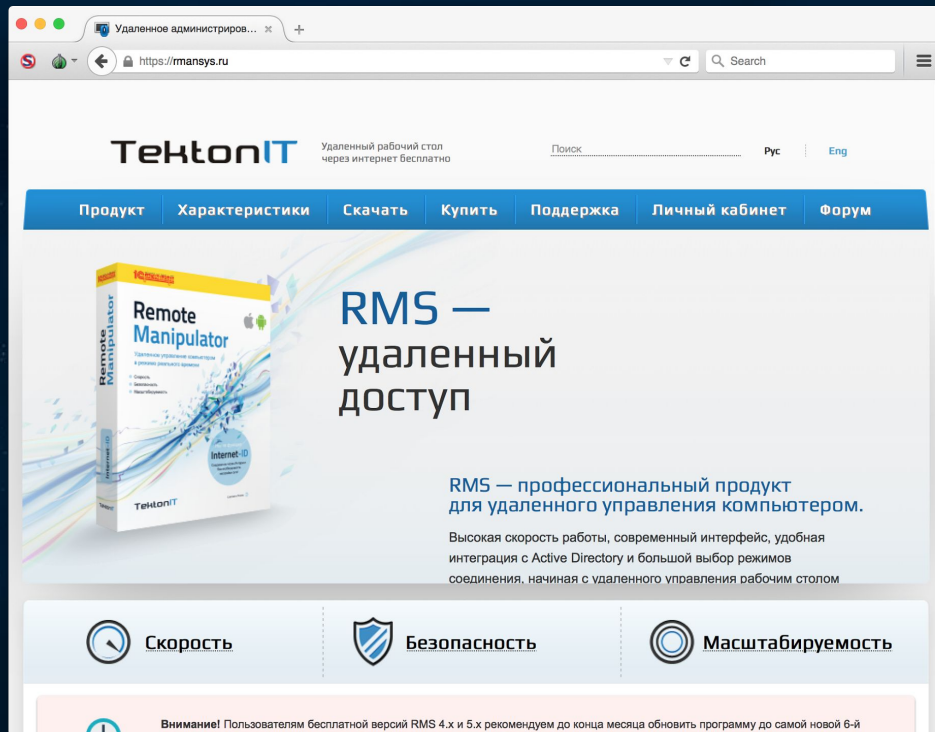
Самые популярные за сутки
Смотреть все »

Арабское такси ★★★★★
02:36

Весы) ★★★★★
01:05

SPASM live at Obscene Extreme Fest ★★★★★
03:24

Новые ↓ Страницы: 1 2 3 4 5 6 ... → Категории ↓



The screenshot shows a web browser window with the URL <https://rmansys.ru>. The page header features the TektonIT logo and the tagline "Удаленный рабочий стол через интернет бесплатно". A navigation menu includes links for "Продукт", "Характеристики", "Скачать", "Купить", "Поддержка", "Личный кабинет", and "Форум". The main content area displays the "Remote Manipulator" software box and the heading "RMS — удаленный доступ". Below this, a sub-heading reads "RMS — профессиональный продукт для удаленного управления компьютером." followed by a descriptive paragraph: "Высокая скорость работы, современный интерфейс, удобная интеграция с Active Directory и большой выбор режимов соединения, начиная с удаленного управления рабочим столом". Three key features are highlighted with icons: "Скорость" (Speed), "Безопасность" (Security), and "Масштабируемость" (Scalability). A footer notice states: "Внимание! Пользователям бесплатной версии RMS 4.x и 5.x рекомендуем до конца месяца обновить программу до самой новой 6-й".

http.log

```
$ cat http.log | bro-cut -u -C id.resp_h method host uri status_code resp_fuids  
resp_mime_types | grep '#fields\|200' | sed -e 's/#fields//g' | column -t
```

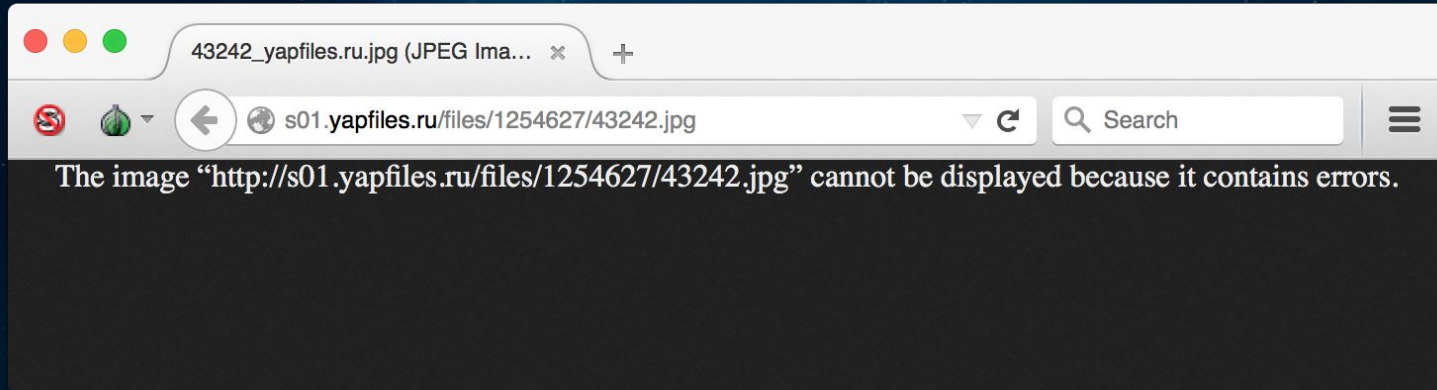
id.resp_h	method	host	uri	status_code	resp_fuids	resp_mime_types
185.26.97.121	GET	s01.yapfiles.ru	/files/1254627/43242.jpg	200	FsFaXR1tyQ8MUJ24wk	application/x-dosexec
90.156.241.111	POST	rmansys.ru	/utils/inet_id_notify.php	200	-	-

http.log

```
$ cat http.log | bro-cut -u -C id.resp_h method host uri status_code resp_fuids  
resp_mime_types | grep '#fields\|200' | sed -e 's/#fields//g' | column -t
```

id.resp_h	method	host	uri	status_code	resp_fuids	resp_mime_types
185.26.97.121	GET	s01.yapfiles.ru	/files/1254627/43242.jpg	200	FsFaXR1tyQ8MUJ24wk	application/x-dosexec
90.156.241.111	POST	rmansys.ru	/utils/inet_id_notify.php	200	-	-

EXE Hidden as JPEG



http.log

```
$ cat http.log | bro-cut -u -C id.resp_h method host uri status_code resp_fuids  
resp_mime_types | grep '#fields\|200' | sed -e 's/#fields//g' | column -t
```

id.resp_h	method	host	uri	status_code	resp_fuids	resp_mime_types
185.26.97.121	GET	s01.yapfiles.ru	/files/1254627/43242.jpg	200	FsFaXR1tyQ8MUJ24wk	application/x-dosexec
90.156.241.111	POST	rmansys.ru	/utils/inet_id_notify.php	200	-	-

http.log

```
$ cat http.log | bro-cut -u -C id.resp_h method host uri status_code resp_fuids  
resp_mime_types | grep '#fields\|200' | sed -e 's/#fields//g' | column -t
```

id.resp_h	method	host	uri	status_code	resp_fuids	resp_mime_types
185.26.97.121	GET	s01.yapfiles.ru	/files/1254627/43242.jpg	200	FsFaXR1tyQ8MUJ24wk	application/x-dosexec
90.156.241.111	POST	rmansys.ru	/utils/inet_id_notify.php	200	-	-

Extracted Files

```
$ find extract_files -type f | grep FsFaXR1tyQ8MUY24wk | xargs file -b
```

PE32 executable for MS Windows (GUI) Intel 80386 32-bit

Extracted Files

```
cat files.log | bro-cut -c kuid filename total_bytes md5 sha1 sha256 |  
grep 'FsFaXRltyQ8MUY24wk\|#fields' | sed -e 's/#fields//g' | column -t  
| cut -d " " -f 2- | column -t
```

filename	total_bytes	md5	sha1	sha256
43242_yapfiles.ru.jpg	2421760	d56f4e1839f35b481b5ac8605d1d97fc	367a2c09a691c584f8ff69261e40741e29926b71	c851d93770cfcc1d2

conn.log

```
$ cat conn.log | bro-cut -c uid id.orig_h id.resp_h id.resp_p proto service |
sed -e 's/#fields//g' | grep -v '#' | column -t
```

uid	id.orig_h	id.resp_h	id.resp_p	proto	service
CeJmNF34xN03NtSGnj	fe80::e1f1:a1d3:450a:e764	ff02::16	0	icmp	-
CNlSS928ab78QnKSL3	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CBmkph31212thohefd	192.168.56.18	224.0.0.252	5355	udp	dns
C0LkngQTWe8rv01j	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CdtvgM2r45S8DlASng	192.168.56.18	224.0.0.252	5355	udp	dns
CinmLMpcwJQtXFcja	192.168.56.18	8.8.8.8	53	udp	dns
C0Rpek4S51GPbs1CWg	192.168.56.18	185.26.97.121	80	tcp	http
C0KY1k4E1knNFN5ZWg	fe80::e1f1:a1d3:450a:e764	ff02::1:3	5355	udp	dns
CPu2nu12Xvles4NUj	192.168.56.18	224.0.0.252	5355	udp	dns
C54Xtu1NVmeI4cEZja	192.168.56.18	89.108.101.61	5651	tcp	-
CL6bhh3vEUaIF6sVfd	192.168.56.18	90.156.241.111	80	tcp	http
CI7bFMWiKtPXjkkm3	192.168.56.18	8.8.8.8	53	udp	dns
Cdc37M2hosjXx7dwog	192.168.56.18	80.234.32.33	5651	tcp	-
CyHRbg2kJVuoL9X7	fe80::e1f1:a1d3:450a:e764	ff02::1:2	547	udp	-

Malware Command and Control Traffic

```

.....U.....
.<?.x.m.l .v.e.r.s.i.o.n.="1...0". .e.n.c.o.d.i.n.g.="U.T.F.-.1.6."?>.
.
.<r.o.m._s.e.v.e.r._c.l.i.e.n.t._s.e.t.t.i.n.g.s .v.e.r.s.i.o.n.="4.6.2.3."><i.d.>
5.8.1.4.0.9.</i.d.><i.n.t.e.r.n.a.l._i.d.>4.6.8.8.2.4.5.</i.n.t.e.r.n.a.l._i.d.><n.o.i.p._n.u.m.b.e.r.>-
1.</n.o.i.p._n.u.m.b.e.r.><l.i.c.e.n.s.e.>f.a.l.s.e.</l.i.c.e.n.s.e.><h.o.s.t.></h.o.s.t.><p.o.r.t.>
5.6.5.0.</p.o.r.t.><r.e.d.i.r.e.c.t.e.d.>f.a.l.s.e.</r.e.d.i.r.e.c.t.e.d.><s.e.r.v.e.r._v.e.r.>
4.6.2.3.</s.e.r.v.e.r._v.e.r.><r.e.m.o.t.e.h.i.d.e.s.e.r.v.e.r.r.e.s.u.b.>f.a.l.s.e.</r.e.m.o.t.e.h.i.d.e.s.e.r.v.e.r.
r.e.s.u.b.><c.o.n.n.e.c.t.i.d.>
4.7.4.9.1.7.2.2.0.</c.o.n.n.e.c.t.i.d.></r.o.m._s.e.v.e.r._c.l.i.e.n.t._s.e.t.t.i.n.g.s.>
.
....<?.x.m.l .v.e.r.s.i.o.n.="1...0". .e.n.c.o.d.i.n.g.="U.T.F.-.1.6."?>.
.
.<r.o.m._n.o.i.p._c.l.i.e.n.t._s.e.t.t.i.n.g.s .v.e.r.s.i.o.n.="4.7.2.5."><h.o.s.t.>
8.0...2.3.4...3.2...3.3.</h.o.s.t.><p.o.r.t.>5.6.5.1.</p.o.r.t.><m.a.x._c.o.n.n.e.c.t.i.o.n.s.>
5.0.</m.a.x._c.o.n.n.e.c.t.i.o.n.s.><c.u.r._c.o.n.n.e.c.t.i.o.n.s.>
2.</c.u.r._c.o.n.n.e.c.t.i.o.n.s.><i.p._f.i.l.t.e.r.>f.a.l.s.e.</i.p._f.i.l.t.e.r.><i.d._f.i.l.t.e.r.>f.a.l.s.e.
</i.d._f.i.l.t.e.r.><m.a.c._f.i.l.t.e.r.>f.a.l.s.e.</m.a.c._f.i.l.t.e.r.><c.a.p.t.i.o.n.></c.a.p.t.i.o.n.><d.
e.s.c.r.i.p.t.i.o.n.></d.e.s.c.r.i.p.t.i.o.n.><n.o._i.p._t.y.p.e.>1.</n.o._i.p._t.y.p.e.><l.i.c.e.n.s.e.>
1.</l.i.c.e.n.s.e.><n.u.m.b.e.r.>9.1.6.</n.u.m.b.e.r.><i.n.t.e.r.n.a.l.I.D.>
6.2.5.4.5.8.4.</i.n.t.e.r.n.a.l.I.D.><N.o.I.P.S.e.l.f.>f.a.l.s.e.</N.o.I.P.S.e.l.f.><v.e.r.>
4.6.2.3.</v.e.r.></r.o.m._n.o.i.p._c.l.i.e.n.t._s.e.t.t.i.n.g.s.>
.
.










```

Red = Malware, Blue = C2 Server

What Can We Learn From PCAP Only?

- Adversary Likely Russophone
- Office Document generating network traffic
- Payload is “RemoteManupulator”
- Payload is hidden on public image sharing site as JPEG
- C2 server version is 4725
- C2 server license #916, internal ID #6254584
- Trojan version is 4623
- Trojan ID #581409, internal ID #4688245

Collected Lots of Indicators

Type ^	Summary ◇	Rating ◇
Address	185.26.97.121	
Address	89.108.101.61	
Address	90.156.241.111	
Address	80.234.32.33	
File	D56F4E1839F35B481B5AC8605D1D97FC : 367A2C09A691C584F8FF6926..	
File	BCD7C81CBEEFCB25F8FC0D10B57A3B33 : 09229CC895C15DB0C890021..	
Host	s01.yapfiles.ru	
Host	rmansys.ru	
URL	http://s01.yapfiles.ru/files/1254627/43242.jpg	

My local.bro

```
1 @load tuning/defaults
2 @load misc/scan
3 @load misc/app-stats
4 @load misc/detect-traceroute
5 @load frameworks/software/vulnerable
6 @load frameworks/software/version-changes
7 @load-sigs frameworks/signatures/detect-windows-shells
8 @load protocols/ftp/software
9 @load protocols/smtp/software
10 @load protocols/ssh/software
11 @load protocols/http/software
12 @load protocols/http/detect-webapps
13 @load protocols/dns/detect-external-names
14 @load protocols/ftp/detect
15 @load protocols/conn/known-hosts
16 @load protocols/conn/known-services
17 @load protocols/ssl/known-certs
18 @load protocols/ssl/validate-certs
19 @load protocols/ssl/log-hostcerts-only
20 @load protocols/ssl/notary
21 @load protocols/ssh/geo-data
22 @load protocols/ssh/detect-bruteforcing
23 @load protocols/ssh/interesting-hostnames
24 @load protocols/http/detect-sqli
25 @load frameworks/files/hash-all-files
```

```
26 @load frameworks/files/detect-MHR
27 redef HTTP::default_capture_password = T;
28 redef FTP::default_capture_password = T;
29 redef Files::salt = " ";
30 @load frameworks/files/extract-all-files
31 @load frameworks/dpd/detect-protocols
32 @load protocols/dhcp/known-devices-and-hostnames
33 @load protocols/dns/auth-addl
34 @load protocols/http/header-names
35 redef HTTP::log_server_header_names = T;
36 @load protocols/http/software-browser-plugins
37 @load protocols/http/var-extraction-cookies
38 @load protocols/http/var-extraction-uri
39 @load protocols/mysql/software
40 @load protocols/rdp/indicate_ssl
41 @load protocols/smtp/blocklists
42 @load protocols/ssl/expiring-certs
43 @load protocols/ssl/extract-certs-pem
44 redef SSL::extract_certs_pem = ALL_HOSTS;
45 @load protocols/ssl/validate-ocsp
46 @load protocols/ssl/weak-keys
47 event file_new(f: fa_file)
48     {
49         Files::add_analyzer(f, Files::ANALYZER_SHA256);
50     }
```

Bro Output

- Multiple Bro Logs
- Important Logs
 - conn.log
 - dns.log
 - http.log
 - file.log
- Extracted Files
- Extracted SSL Certs
- Alternative JSON Output
 - Good for direct import into Elasticsearch



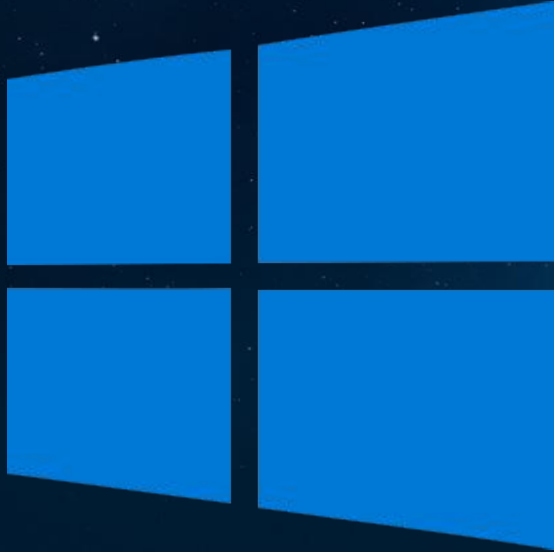
Volatility

Memory Analysis Framework

What is the Volatility Framework?

- Extracts artifacts from samples of volatile memory
- An amazing view into what is happening in memory while a malware sample is running

Operating System Support



Volatility in Action

- Analysis Target: b.exe
- Sample Source: <https://www.hybrid-analysis.com/>
- SHA1: 5149b40858c575238f1cbfcd32dd78a30bc87742
- What can we learn from memory analysis?

Preparing Your Memory Image

- Dump a memory image from running VirtualBox VM
 - `VBoxManage debugvm "Win7x64" dumpvmcore --filename=vbox.img`
- Convert ELF64 image into raw dd-style memory dump
 - `vol.py -f vbox.img --profile=Win7SP1x64 imagecopy -O copy.raw`

pslist & psscan

- psscan shows hidden and terminated processes
- pslist shows running processes
- pslist before and after running malware sample

```
27,29c27
< 0xffffffffa8000996240 SearchProtocol
< 0xffffffffa8000a321f0 SearchFilterHo
< 0xffffffffa8000874330 svchost.exe
---
> 0xffffffffa8000910060 explorer.exe
```

malfind

```
$ vol.py -f copy.raw --profile=Win7SP1x64 malfind -D
```

```
Process: explorer.exe Pid: 1548 Address: 0x80000  
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE  
Flags: Protection: 6
```

```
0x00080000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....  
0x00080010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
```

```
Process: explorer.exe Pid: 1548 Address: 0xa0000  
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE  
Flags: Protection: 6
```

```
0x000a0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....  
0x000a0010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
```

malfind

```
$ vol.py -f copy.raw --profile=Win7SP1x64 malfind -D
```

```
Process: explorer.exe Pid: 1548 Address: 0x80000  
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE  
Flags: Protection: 6
```

```
0x00080000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ... ..  
0x00080010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 @.....
```

```
Process: explorer.exe Pid: 1548 Address: 0xa0000  
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE  
Flags: Protection: 6
```

```
0x000a0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ... ..  
0x000a0010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 @.....
```

Malware Found?

0x80000

Avira: TR/Patched.Ren.Gen7
Qihoo-360: HEUR/QVM40.1.Malware.Gen

0xa000

Qihoo-360: HEUR/QVM40.1.Malware.Gen


```
$ vol.py -f copy.raw --profile=Win7SP1x64 netscan | grep explorer
```

```
Volatility Foundation Volatility Framework 2.5  
0x1e39e010 TCPv4 -:49280 216.170.126.105:80 CLOSED 1548 explorer.exe  
0x1fc3b430 TCPv4 -:49282 216.170.126.105:80 CLOSED 1548 explorer.exe
```

What Can We Learn From Memory Analysis?

- Sample uses process injection
- Injects explorer.exe
- Command and Control IP Address: 216.170.126.105

More Volatility Tools

- connscan -> looks for network connections (XP only)
- yarascan -> leverages YARA
- handles, w/type Mutant -> helps find suspicious mutexes
- handles, w/type File -> helps find suspicious file handles
- dlllist and ldrmodules -> helps find hidden DLLs
- dlldump -> dump the hidden DLL
- modules and driverscan -> hidden drivers
- moddump -> dump drivers
- iehistory -> dump URLs

Volatility Output

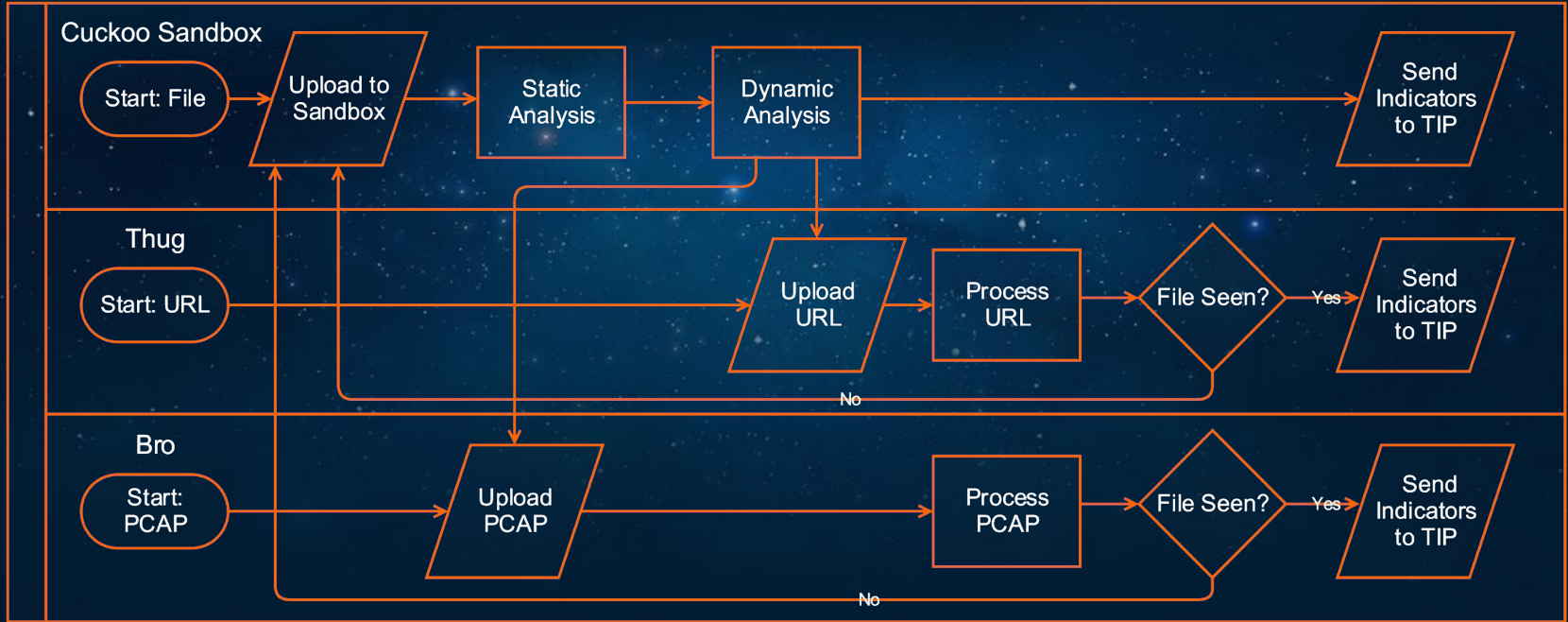
- Files extracted from services
- Files extracted from injection
- DLLs extracted
- IP addresses extracted from network connections
- URLs extracted from IE history
- URLs extracted from malware configuration
- Suspicious mutexes



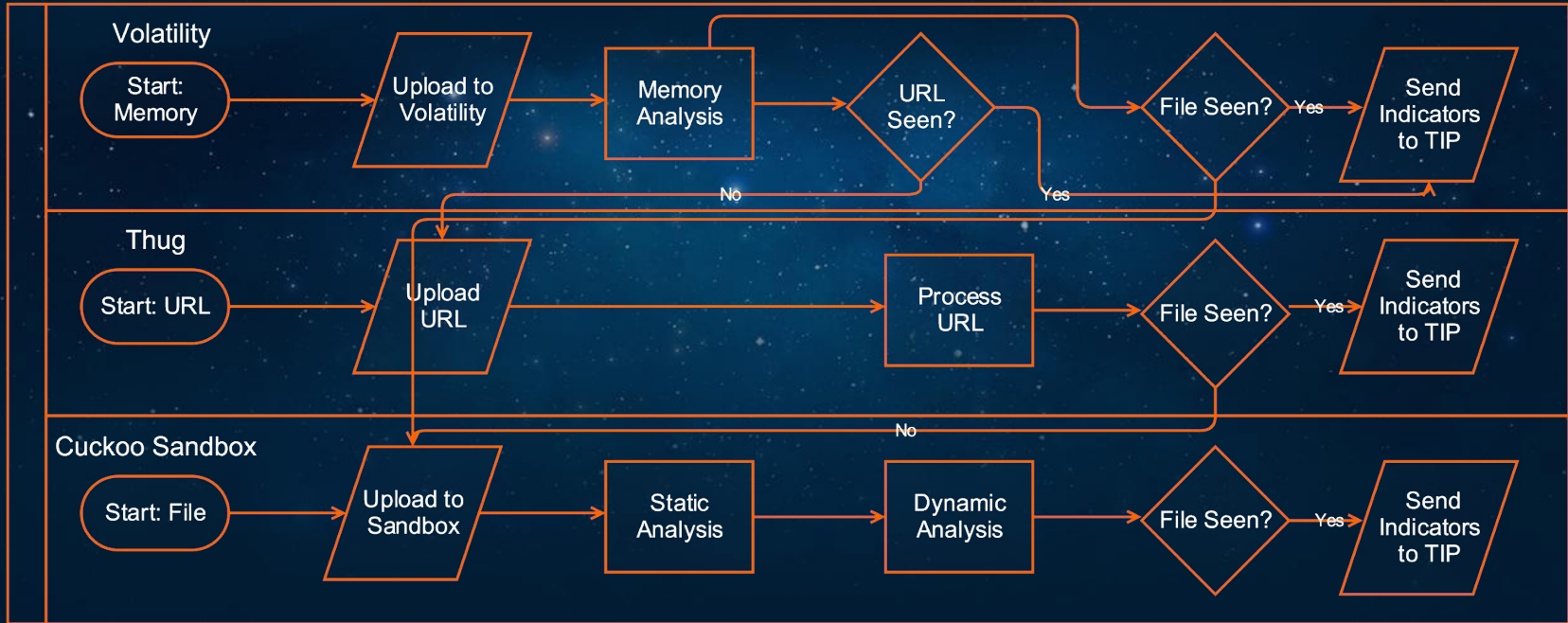
Tying It All Together

Conclusion

Cuckoo, Thug, Bro Process



Volatility, Thug, Cuckoo Process



Orchestration and Automation

- Use a message queue
 - Redis
 - Rabbit MQ
 - ZeroMQ <- Preferred
- Use NGINX for file transfer under message queue
- Keep all output in Elasticsearch
 - Cuckoo needs to be cuckoo-modified or write your own report plugin
 - Thug uses ES natively
 - Bro can export logs in JSON format
 - Volatility needs help
- Glue everything together with Python3

<https://www.threatconnect.com/blog/>

Questions?

@MalwareUtkonos

@ThreatConnect