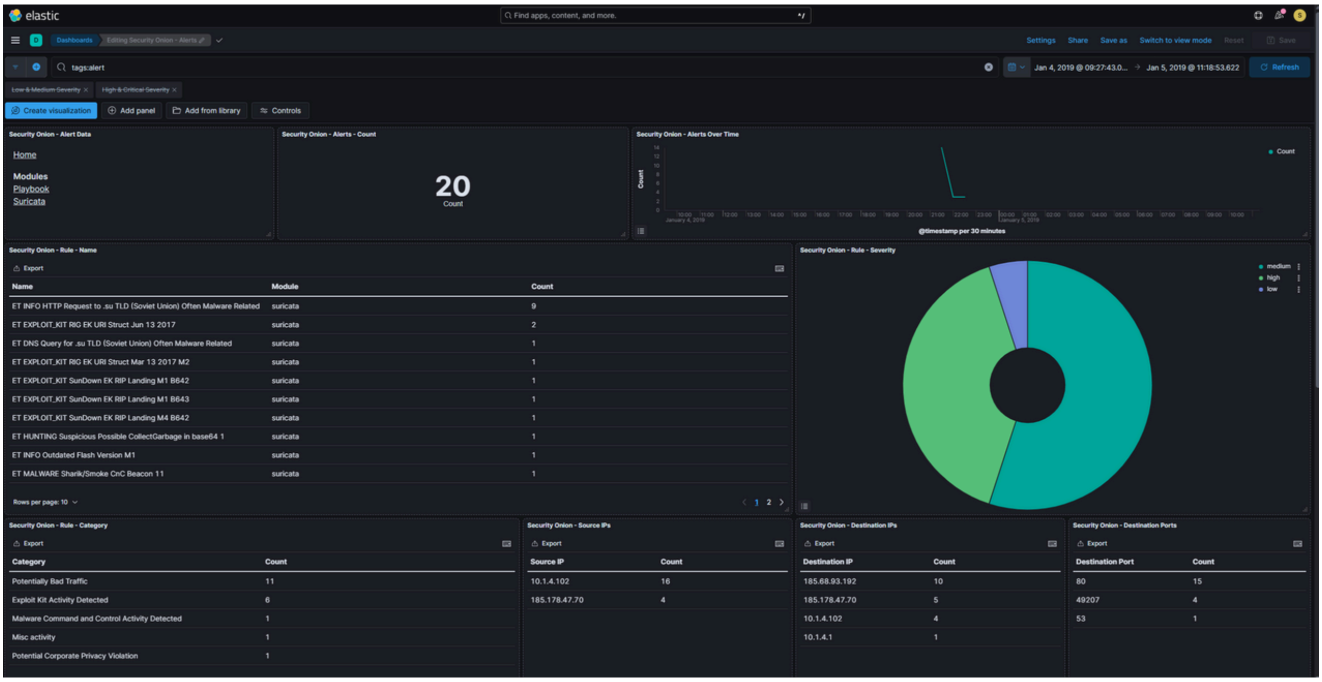
Attack timeline

Phase	Details	Indicator	IP / Domain
User(10.1.41.102) visits a suspicious website	The user makes an HTTP GET request to a suspicious URL address	HTTP GET	http://datitngforllives.info
Malicious page is delivered	The HTML page contains a hidden iframe and javascript that performs a silent redirect	HTTP 200 OK	http://datitngforllives.info
Hidden redirection	A concealed iframe + javascript redirect the user to a new page without their knowledge	HTTP Redirect to exploit kit page	freebitc.pro → 185.56.233.186
Exploitkits activates	RIG EK and SunDown EK activate and start probing the system while attempting exploits. Exploitkits found an outdated flashversion in browser.	GET /POST	185.178.47.70(Russia)
Malicous .exe file is downloaded	The server delivers a malicious .exe file (application/x-msdownload) to the user	HTTP/1.1 200 OK	185.178.47.70(Russia)
Malware activates(Sharik / Smoke C2 beacon)	The malware establishes a connection to its C2-server. The browser performs a DNS query for the *letitbit.su* domain	DNS Query	*letitbit.su* → 185.68.93.192(Bulgaria)
C2 communication continues	The victim communicates with the C2 server over an encrypted channel.	HTTP Encrypted	185.68.93.192(Bulgaria)

Proof of findings

Kibana

Overview of Alerts in Kibana.



tags:alert

Jan 4, 2019 @ 09:27:43.0... → Jan 5, 2019 @ 11:18:53.622

Security Onion - Alert Data

Security Onion - Alerts - Count

20 Count

Security Onion - Alerts Over Time

Security Onion - Rule - Name

Name	Module	Count
ET INFO HTTP Request to .su TLD (Soviet Union) Often Malware Related	suricata	9
ET EXPLOIT_KIT RIG EK URI Struct Jun 13 2017	suricata	2
ET DNS Query for .su TLD (Soviet Union) Often Malware Related	suricata	1
ET EXPLOIT_KIT RIG EK URI Struct Mar 13 2017 M2	suricata	1
ET EXPLOIT_KIT SunDown EK RIP Landing M1 B642	suricata	1
ET EXPLOIT_KIT SunDown EK RIP Landing M1 B643	suricata	1
ET EXPLOIT_KIT SunDown EK RIP Landing M4 B642	suricata	1
ET HUNTING Suspicious Possible CollectGarbage in base64 1	suricata	1
ET INFO Outdated Flash Version M1	suricata	1
ET MALWARE Sharik/Smoke CnC Beacon 11	suricata	1

Security Onion - Rule - Severity

Security Onion - Rule - Category

Category	Count
Potentially Bad Traffic	11
Exploit Kit Activity Detected	6
Malware Command and Control Activity Detected	1
Misc activity	1
Potential Corporate Privacy Violation	1

Security Onion - Source IPs

Source IP	Count
10.1.4.102	16
185.178.47.70	4

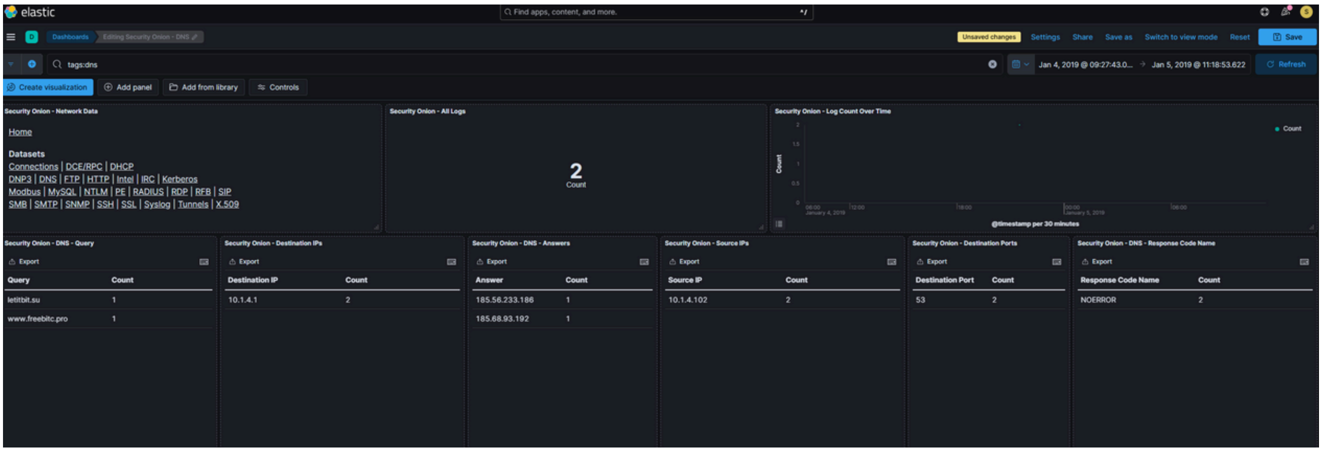
Security Onion - Destination IPs

Destination IP	Count
185.68.93.192	10
185.178.47.70	5
10.1.4.102	4
10.1.4.1	1

Security Onion - Destination Ports

Destination Port	Count
80	15
49207	4
53	1

Kibana's DNS-traffic.


elastic
Find apps, content, and more.
Dashboards
Editing Security Onion - DNS
Unsaved changes
Settings
Share
Save as
Switch to view mode
Reset
Save
Refresh
Create visualization
Add panel
Add from library
Controls
Home
Datasets
Connections | DCE/RPC | DHCP
DNP3 | DNS | FTP | HTTP | Intel | IRC | Kerberos
Modbus | MySQL | NTLM | PE | RADIUS | RDP | RFB | SIP
SMB | SMTP | SNMP | SSH | SSL | Syslog | Tunnels | X.509
Count
2
1.5
1
0.5
0
06:00
12:00
18:00
00:00
06:00
January 4, 2019
January 5, 2019
@timestamp per 30 minutes
Count
Export

tags:dns

Jan 4, 2019 @ 09:27:43.0... → Jan 5, 2019 @ 11:18:53.622

Security Onion - Network Data

Security Onion - All Logs

2 Count

Security Onion - Log Count Over Time

Security Onion - DNS - Query

Query	Count
letitbit.su	1
www.freebitc.pro	1

Security Onion - Destination IPs

Destination IP	Count
10.1.4.1	2

Security Onion - DNS - Answers

Answer	Count
185.56.233.186	1
185.68.93.192	1

Security Onion - Source IPs

Source IP	Count
10.1.4.102	2

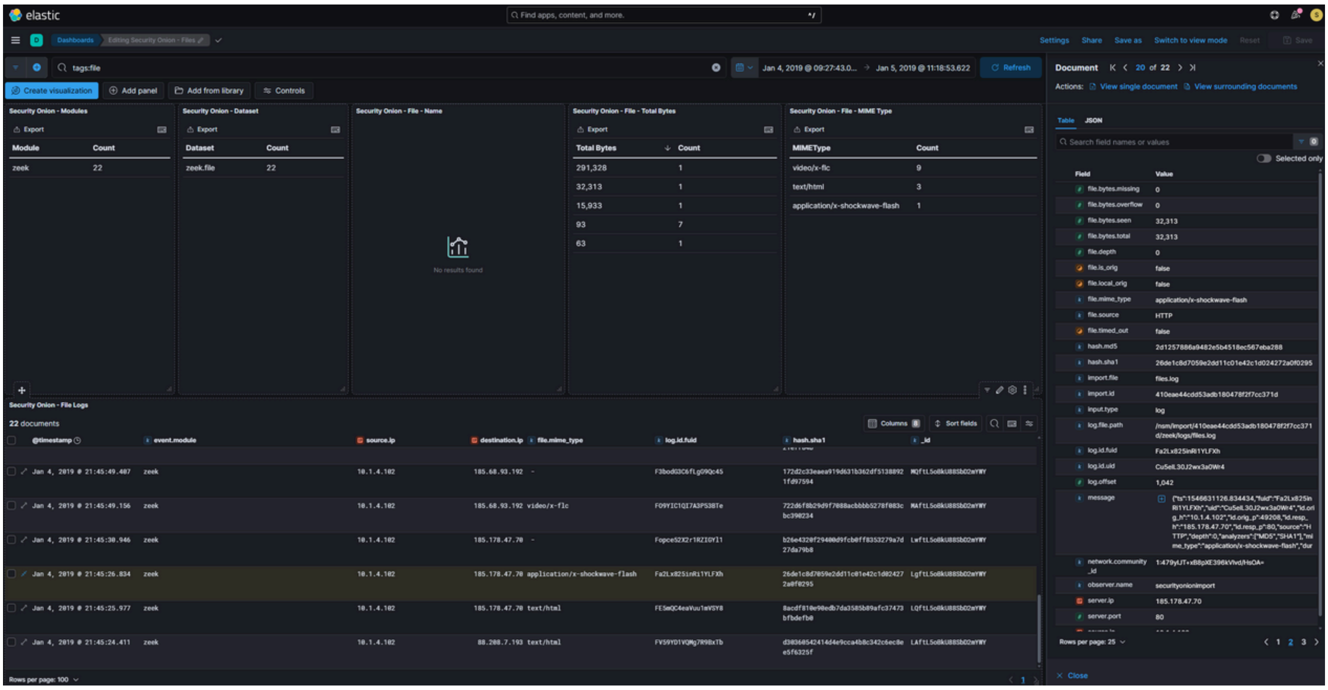
Security Onion - Destination Ports

Destination Port	Count
53	2

Security Onion - DNS - Response Code Name

Response Code Name	Count
NOERROR	2

Highlighted rows shows two files in Kibana that VirusTotal flagged as malicious.



tags:file

Jan 4, 2019 @ 09:27:43.0... → Jan 5, 2019 @ 11:18:53.622

Security Onion - Modules

Module	Count
zeek	22

Security Onion - Dataset

Dataset	Count
zeek.file	22

Security Onion - File - Name

Security Onion - File - Total Bytes

Total Bytes	Count
291,328	1
32,313	1
15,933	1
93	7
63	1

Security Onion - File - MIME Type

MIMEType	Count
video/x-flc	9
text/html	3
application/x-shockwave-flash	1

Security Onion - File Logs

22 documents

@timestamp	event.module	source.ip	destination.ip	file.mime_type	log.id.fuid	hash.sha1	_id
Jan 4, 2019 @ 21:45:49.407	zeek	10.1.4.102	185.68.93.192	-	F3bodG3C6fLg09Qc45	172d2c33eaea919d631b362df5138892 1fd97594	MQftL5o8kU88SbD2mYWY
Jan 4, 2019 @ 21:45:49.156	zeek	10.1.4.102	185.68.93.192	video/x-flc	F09YIC1QI7A3PS38Te	722d6f8b29d9f7088acbbbb5278f083c bc390234	MAftL5o8kU88SbD2mYWY
Jan 4, 2019 @ 21:45:30.946	zeek	10.1.4.102	185.178.47.70	-	Fopce52X2r1RZIGYl1	b26e4320f29400d9fcb0ff8353279a7d 27da79b8	LwftL5o8kU88SbD2mYWY
Jan 4, 2019 @ 21:45:26.834	zeek	10.1.4.102	185.178.47.70	application/x-shockwave-flash	Fa2Lx825inRi1YLFXh	26de1c8d7059e2dd11c01e42c1d02427 2a0f0295	LgftL5o8kU88SbD2mYWY
Jan 4, 2019 @ 21:45:25.977	zeek	10.1.4.102	185.178.47.70	text/html	FESmQC4eaVuu1mVSY8	8acdf810e90edb7da3585b89afc37473 bfbdefb0	LQftL5o8kU88SbD2mYWY
Jan 4, 2019 @ 21:45:24.411	zeek	10.1.4.102	88.208.7.193	text/html	FV59YD1VQMg7R9BxTb	d38360542414d4e9cca4b8c342c6ec8e e5f6325f	LAftL5o8kU88SbD2mYWY

Rows per page: 100

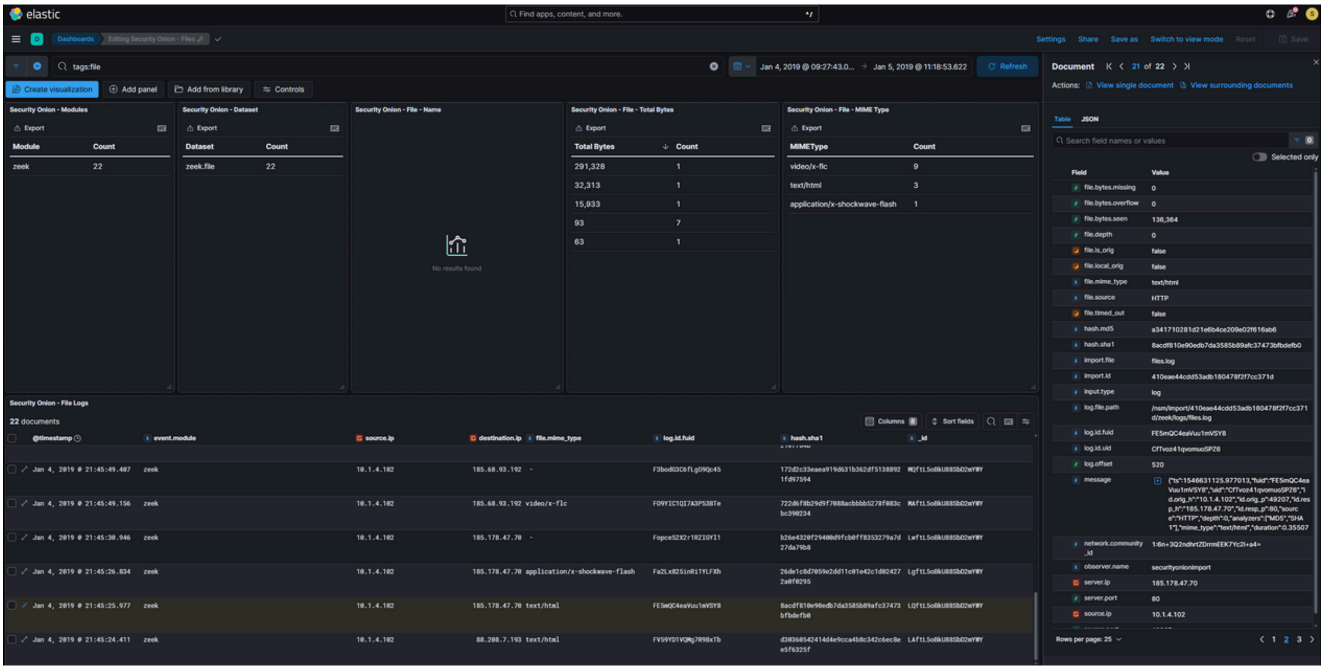
Document 20 of 22

Actions: View single document View surrounding documents

Field	Value
file.bytes.missing	0
file.bytes.overflow	0
file.bytes.seen	32,313
file.bytes.total	32,313
file.depth	0
file.is_orig	false
file.local_orig	false
file.mime_type	application/x-shockwave-flash
file.source	HTTP
file.timed_out	false
hash.md5	2d1257886a9482e5b4518ec567eba288
hash.sha1	26de1c8d7059e2dd11c01e42c1d024272a0f0295
import.file	files.log
import.id	410eae44cdd53adb180478f2f7cc371d
input.type	log
log.file.path	/nsm/import/410eae44cdd53adb180478f2f7cc371d/zeek/logs/files.log
log.id.fuid	Fa2Lx825inRi1YLFXh
log.id.uid	Cu5elL30J2wx3a0Wr4
log.offset	1,042
message	{"ts":1546631126.834434,"fuid":"Fa2Lx825inRi1YLFXh","uid":"Cu5elL30J2wx3a0Wr4","id.orig_h":"10.1.4.102","id.orig_p":49208,"id.resp_h":"185.178.47.70","id.resp_p":80,"source":"HTTP","depth":0,"analyzers":["MD5","SHA1"],"mime_type":"application/x-shockwave-flash","dur
network.community_id	1:479yUT+xB8pXE396kVlvd/HsOA=
observer.name	securityonionimport
server.ip	185.178.47.70
server.port	80

Rows per page: 25

< 1 2 3 >



tags:file

Jan 4, 2019 @ 09:27:43.0... → Jan 5, 2019 @ 11:18:53.622

Security Onion - Modules

Module	Count
zeek	22

Security Onion - Dataset

Dataset	Count
zeek.file	22

Security Onion - File - Name

Security Onion - File - Total Bytes

Total Bytes	Count
291,328	1
32,313	1
15,933	1
93	7
63	1

Security Onion - File - MIME Type

MIMEType	Count
video/x-flc	9
text/html	3
application/x-shockwave-flash	1

Security Onion - File Logs

22 documents

@timestamp	event.module	source.ip	destination.ip	file.mime_type	log.id.fuid	hash.sha1	_id
Jan 4, 2019 @ 21:45:49.407	zeek	10.1.4.102	185.68.93.192	-	F3bodG3C6fLg09Qc45	172d2c33eaea919d631b362df5138892 1fd97594	MQftL5o8kU88SbD2mYWY
Jan 4, 2019 @ 21:45:49.156	zeek	10.1.4.102	185.68.93.192	video/x-flc	F09YIC1QI7A3PS38Te	722d6f8b29d9f7088acbbbb5278f083c bc390234	MAftL5o8kU88SbD2mYWY
Jan 4, 2019 @ 21:45:30.946	zeek	10.1.4.102	185.178.47.70	-	Fopce52X2r1RZIGYl1	b26e4320f29400d9fcb0ff8353279a7d 27da79b8	LwftL5o8kU88SbD2mYWY
Jan 4, 2019 @ 21:45:26.834	zeek	10.1.4.102	185.178.47.70	application/x-shockwave-flash	Fa2Lx825inRi1YLFXh	26de1c8d7059e2dd11c01e42c1d02427 2a0f0295	LgftL5o8kU88SbD2mYWY
Jan 4, 2019 @ 21:45:25.977	zeek	10.1.4.102	185.178.47.70	text/html	FESmQC4eaVuu1mVSY8	8acdf810e90edb7da3585b89afc37473 bfbdefb0	LQftL5o8kU88SbD2mYWY
Jan 4, 2019 @ 21:45:24.411	zeek	10.1.4.102	88.208.7.193	text/html	FV59YD1VQMg7R9BxTb	d38360542414d4e9cca4b8c342c6ec8e e5f6325f	LAftL5o8kU88SbD2mYWY

Document 21 of 22

Actions: View single document View surrounding documents

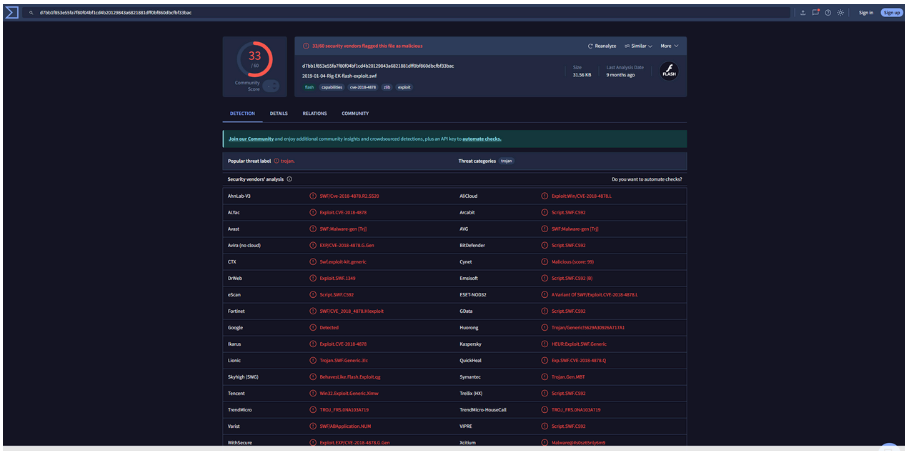
Field	Value
file.bytes.missing	0
file.bytes.overflow	0
file.bytes.seen	136,364
file.depth	0
file.is_orig	false
file.local_orig	false
file.mime_type	text/html
file.source	HTTP
file.timed_out	false
hash.md5	a341710281d21e6b4ce209e02f616ab6
hash.sha1	8acdf810e90edb7da3585b89afc37473bfbdefb0
import.file	files.log
import.id	410eae44cdd53adb180478f2f7cc371d
input.type	log
log.file.path	/nsm/import/410eae44cdd53adb180478f2f7cc371d/zeek/logs/files.log
log.id.fuid	FESmQC4eaVuu1mVSY8
log.id.uid	CfTvoz41qvomuoSPZ6
log.offset	520
message	{"ts":1546631125.977013,"fuid":"FESmQC4eaVuu1mVSY8","uid":"CfTvoz41qvomuoSPZ6","id.orig_h":"10.1.4.102","id.orig_p":49207,"id.resp_h":"185.178.47.70","id.resp_p":80,"source":"HTTP","depth":0,"analyzers":["MD5","SHA1"],"mime_type":"text/html","duration":0.35507
network.community_id	1:6n+3Q2ndhrtZDrmEEK7Yc2I+a4=
observer.name	securityonionimport
server.ip	185.178.47.70
server.port	80
source.ip	10.1.4.102

Rows per page: 25

< 1 2 3 >

Virustotal

Found 2 files flagged as malicious. Both are Trojan-malwares, but the second is categorized as phishing-type threat. The SHA-1 hashes of the above images, when checked on VirusTotal.



d7bb1f853e55fa7f80f04bf1cd4b20129843a6821881dff0bf860dbcfbf33bac
Reanalyze
Similar
More
Sign in
Sign up

33/60 security vendors flagged this file as malicious

33 / 60 Community Score

d7bb1f853e55fa7f80f04bf1cd4b20129843a6821881dff0bf860dbcfbf33bac
2019-01-04-Rig-EK-flash-exploit.swf
flash capabilities cve-2018-4878 zlib exploit

Size 31.56 KB | Last Analysis Date 9 months ago | FLASH

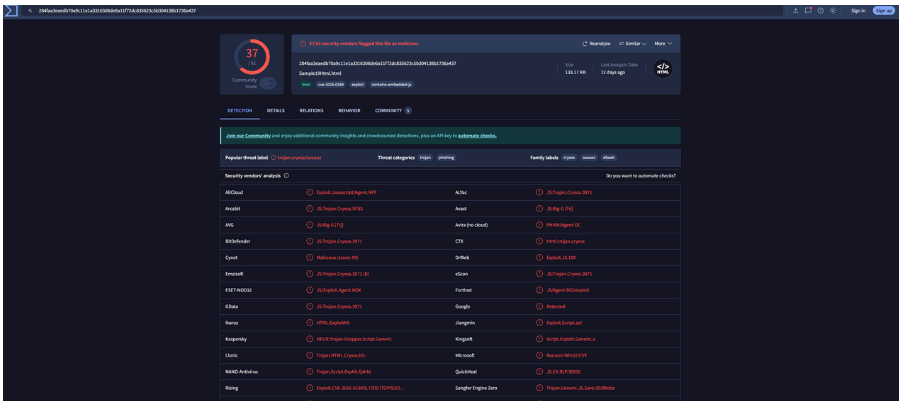
DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan. Threat categories trojan

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	SWF/Cve-2018-4878.R2.S520	AliCloud	Exploit:Win/CVE-2018-4878.L
ALYac	Exploit.CVE-2018-4878	Arcabit	Script.SWF.C592
Avast	SWF:Malware-gen [Trj]	AVG	SWF:Malware-gen [Trj]
Avira (no cloud)	EXP/CVE-2018-4878.G.Gen	BitDefender	Script.SWF.C592
CTX	Swf.exploit-kit.generic	Cynet	Malicious (score: 99)
DrWeb	Exploit.SWF.1349	Emsisoft	Script.SWF.C592 (B)
eScan	Script.SWF.C592	ESET-NOD32	A Variant Of SWF/Exploit.CVE-2018-4878.L
Fortinet	SWF/CVE_2018_4878.H!exploit	GData	Script.SWF.C592
Google	Detected	Huorong	Trojan/Generic!5629A30926A717A1
Ikarus	Exploit.CVE-2018-4878	Kaspersky	HEUR:Exploit.SWF.Generic
Lionic	Trojan.SWF.Generic.3!c	QuickHeal	Exp.SWF.CVE-2018-4878.Q
Skyhigh (SWG)	BehavesLike.Flash.Exploit.qg	Symantec	Trojan.Gen.MBT
Tencent	Win32.Exploit.Generic.Ximw	Trellix (HX)	Script.SWF.C592
TrendMicro	TROJ_FRS.0NA103A719	TrendMicro-HouseCall	TROJ_FRS.0NA103A719
Varist	SWF/ABApplication.NUM	VIPRE	Script.SWF.C592
WithSecure	Exploit.EXP/CVE-2018-4878.G.Gen	Xcitium	Malware@#s0sz65nly6m9



284faa3eaedb70a9c11e1a3316308de6a11f72dc835623c5b304138b1736a437
Sign in
Sign up

37/61 security vendors flagged this file as malicious

37 / 61 Community Score

284faa3eaedb70a9c11e1a3316308de6a11f72dc835623c5b304138b1736a437
Sample19Html.html
html cve-2016-0189 exploit contains-embedded-js

Size 133.17 KB | Last Analysis Date 12 days ago | HTML

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 5

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

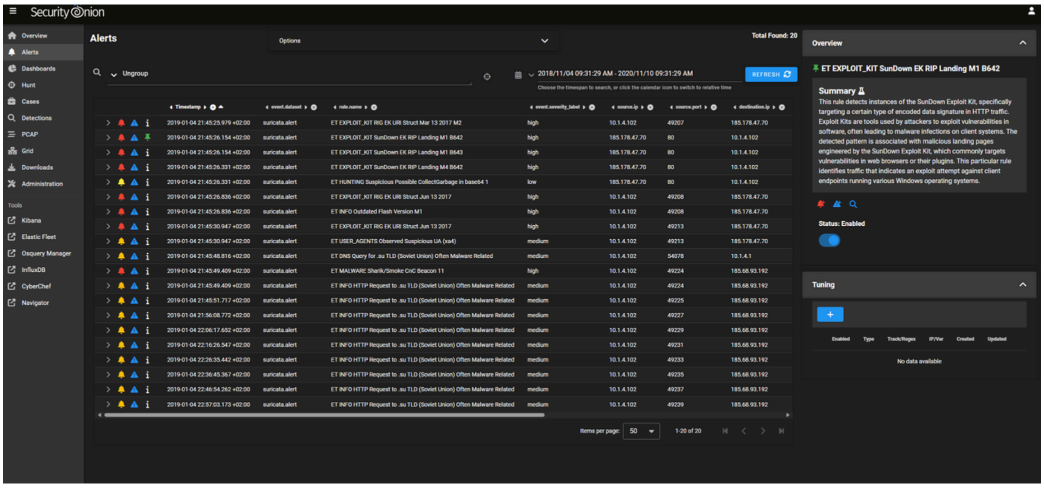
Popular threat label trojan.cryxos/ausuoz Threat categories trojan phishing Family labels cryxos ausuoz dloadr

Security vendors' analysis Do you want to automate checks?

AliCloud	Exploit:Javascript/Agent.NPF	ALYac	JS:Trojan.Cryxos.3971
Arcabit	JS:Trojan.Cryxos.DF83	Avast	JS:Rig-G [Trj]
AVG	JS:Rig-G [Trj]	Avira (no cloud)	PHISH/Agent.OC
BitDefender	JS:Trojan.Cryxos.3971	CTX	Html.trojan.cryxos
Cynet	Malicious (score: 99)	DrWeb	Exploit.JS.109
Emsisoft	JS:Trojan.Cryxos.3971 (B)	eScan	JS:Trojan.Cryxos.3971
ESET-NOD32	JS/Exploit.Agent.NOX	Fortinet	JS/Agent.RIG!exploit
GData	JS:Trojan.Cryxos.3971	Google	Detected
Ikarus	HTML.ExploitKit	Jiangmin	Exploit.Script.act
Kaspersky	HEUR:Trojan-Dropper.Script.Generic	Kingsoft	Script.Exploit.Generic.a
Lionic	Trojan.HTML.Cryxos.b!c	Microsoft	Ransom:Win32/CVE
NANO-Antivirus	Trojan.Script.ExpKit.fjahbl	QuickHeal	JS.EK.RLP.30935
Rising	Exploit.CVE-2016-0189!8.72D0 (TOPIS:E0...	Sangfor Engine Zero	Trojan.Generic-JS.Save.502fbcba

Security Onion

Picture of SO Alert page showing the whole attack.



Alerts

Total Found: 20

Ungroup

2018/11/04 09:31:29 AM - 2020/11/10 09:31:29 AM

Choose the timespan to search, or click the calendar icon to switch to relative time

Timestamp	event.dataset	rule.name	event.severity_label	source.ip	source.port	destination.ip
2019-01-04 21:45:25.979 +02:00	suricata.alert	ET EXPLOIT_KIT RIG EK URI Struct Mar 13 2017 M2	high	10.1.4.102	49207	185.178.47.70
2019-01-04 21:45:26.154 +02:00	suricata.alert	ET EXPLOIT_KIT SunDown EK RIP Landing M1 B642	high	185.178.47.70	80	10.1.4.102
2019-01-04 21:45:26.154 +02:00	suricata.alert	ET EXPLOIT_KIT SunDown EK RIP Landing M1 B643	high	185.178.47.70	80	10.1.4.102
2019-01-04 21:45:26.331 +02:00	suricata.alert	ET EXPLOIT_KIT SunDown EK RIP Landing M4 B642	high	185.178.47.70	80	10.1.4.102
2019-01-04 21:45:26.331 +02:00	suricata.alert	ET HUNTING Suspicious Possible CollectGarbage in base64 1	low	185.178.47.70	80	10.1.4.102
2019-01-04 21:45:26.836 +02:00	suricata.alert	ET EXPLOIT_KIT RIG EK URI Struct Jun 13 2017	high	10.1.4.102	49208	185.178.47.70
2019-01-04 21:45:26.836 +02:00	suricata.alert	ET INFO Outdated Flash Version M1	high	10.1.4.102	49208	185.178.47.70
2019-01-04 21:45:30.947 +02:00	suricata.alert	ET EXPLOIT_KIT RIG EK URI Struct Jun 13 2017	high	10.1.4.102	49213	185.178.47.70
2019-01-04 21:45:30.947 +02:00	suricata.alert	ET USER_AGENTS Observed Suspicious UA (xa4)	medium	10.1.4.102	49213	185.178.47.70
2019-01-04 21:45:48.816 +02:00	suricata.alert	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	medium	10.1.4.102	54078	10.1.4.1
2019-01-04 21:45:49.409 +02:00	suricata.alert	ET MALWARE Sharik/Smoke CnC Beacon 11	high	10.1.4.102	49224	185.68.93.192
2019-01-04 21:45:49.409 +02:00	suricata.alert	ET INFO HTTP Request to .su TLD (Soviet Union) Often Malware Related	medium	10.1.4.102	49224	185.68.93.192
2019-01-04 21:45:51.717 +02:00	suricata.alert	ET INFO HTTP Request to .su TLD (Soviet Union) Often Malware Related	medium	10.1.4.102	49225	185.68.93.192
2019-01-04 21:56:08.772 +02:00	suricata.alert	ET INFO HTTP Request to .su TLD (Soviet Union) Often Malware Related	medium	10.1.4.102	49227	185.68.93.192
2019-01-04 22:06:17.652 +02:00	suricata.alert	ET INFO HTTP Request to .su TLD (Soviet Union) Often Malware Related	medium	10.1.4.102	49229	185.68.93.192
2019-01-04 22:16:26.547 +02:00	suricata.alert	ET INFO HTTP Request to .su TLD (Soviet Union) Often Malware Related	medium	10.1.4.102	49231	185.68.93.192
2019-01-04 22:26:35.442 +02:00	suricata.alert	ET INFO HTTP Request to .su TLD (Soviet Union) Often Malware Related	medium	10.1.4.102	49233	185.68.93.192
2019-01-04 22:36:45.367 +02:00	suricata.alert	ET INFO HTTP Request to .su TLD (Soviet Union) Often Malware Related	medium	10.1.4.102	49235	185.68.93.192
2019-01-04 22:46:54.262 +02:00	suricata.alert	ET INFO HTTP Request to .su TLD (Soviet Union) Often Malware Related	medium	10.1.4.102	49237	185.68.93.192
2019-01-04 22:57:03.173 +02:00	suricata.alert	ET INFO HTTP Request to .su TLD (Soviet Union) Often Malware Related	medium	10.1.4.102	49239	185.68.93.192

Items per page: 50 1-20 of 20

Overview

ET EXPLOIT_KIT SunDown EK RIP Landing M1 B642

Summary

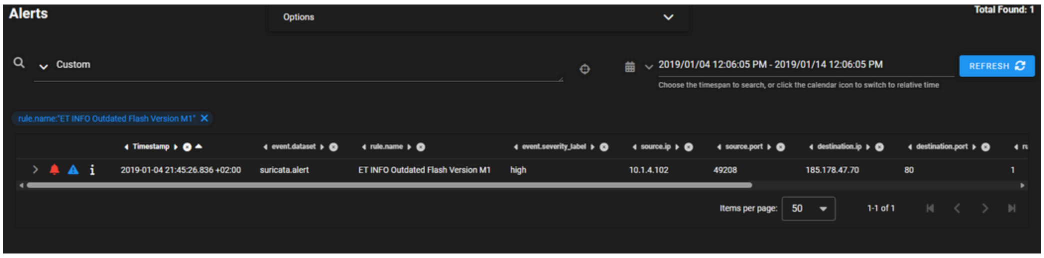
This rule detects instances of the SunDown Exploit Kit, specifically targeting a certain type of encoded data signature in HTTP traffic. Exploit Kits are tools used by attackers to exploit vulnerabilities in software, often leading to malware infections on client systems. The detected pattern is associated with malicious landing pages engineered by the SunDown Exploit Kit, which commonly targets vulnerabilities in web browsers or their plugins. This particular rule identifies traffic that indicates an exploit attempt against client endpoints running various Windows operating systems.

Status: Enabled

Tuning

Enabled	Type	Track/Regex	IP/Var	Created	Updated
No data available					

SO image of found outdated flash version.



Alerts

Total Found: 1

Custom

2019/01/04 12:06:05 PM - 2019/01/14 12:06:05 PM

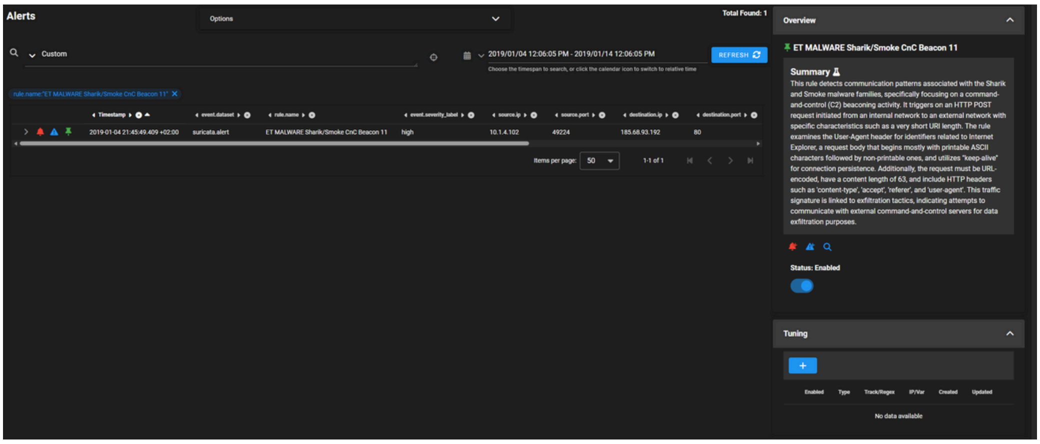
Choose the timespan to search, or click the calendar icon to switch to relative time

rule.name:"ET INFO Outdated Flash Version M1"

Timestamp	event.dataset	rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port	
2019-01-04 21:45:26.836 +02:00	suricata.alert	ET INFO Outdated Flash Version M1	high	10.1.4.102	49208	185.178.47.70	80	1

Items per page: 50 1-1 of 1

SO image of Sharik/Smoke C2-beacon.



2019/01/04 12:06:05 PM - 2019/01/14 12:06:05 PM

Choose the timespan to search, or click the calendar icon to switch to relative time

rule.name:"ET MALWARE Sharik/Smoke CnC Beacon 11"

Timestamp	event.dataset	rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port
2019-01-04 21:45:49.409 +02:00	suricata.alert	ET MALWARE Sharik/Smoke CnC Beacon 11	high	10.1.4.102	49224	185.68.93.192	80

ET MALWARE Sharik/Smoke CnC Beacon 11

Summary

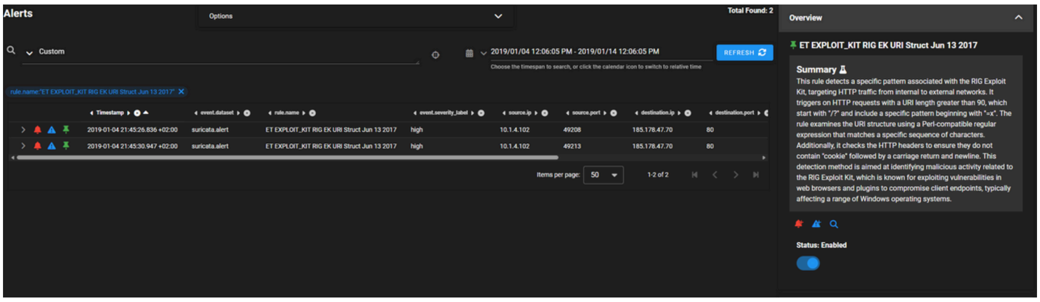
This rule detects communication patterns associated with the Sharik and Smoke malware families, specifically focusing on a command-and-control (C2) beaconing activity. It triggers on an HTTP POST request initiated from an internal network to an external network with specific characteristics such as a very short URI length. The rule examines the User-Agent header for identifiers related to Internet Explorer, a request body that begins mostly with printable ASCII characters followed by non-printable ones, and utilizes "keep-alive" for connection persistence. Additionally, the request must be URL-encoded, have a content length of 63, and include HTTP headers such as 'content-type', 'accept', 'referer', and 'user-agent'. This traffic signature is linked to exfiltration tactics, indicating attempts to communicate with external command-and-control servers for data exfiltration purposes.

Status: Enabled

Enabled	Type	Track/Regex	IP/Var	Created	Updated

No data available

SO image of exploit kit RIG EK.



2019/01/04 12:06:05 PM - 2019/01/14 12:06:05 PM

Choose the timespan to search, or click the calendar icon to switch to relative time

rule.name:"ET EXPLOIT_KIT RIG EK URI Struct Jun 13 2017"

Timestamp	event.dataset	rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port
2019-01-04 21:45:26.836 +02:00	suricata.alert	ET EXPLOIT_KIT RIG EK URI Struct Jun 13 2017	high	10.1.4.102	49208	185.178.47.70	80
2019-01-04 21:45:30.947 +02:00	suricata.alert	ET EXPLOIT_KIT RIG EK URI Struct Jun 13 2017	high	10.1.4.102	49213	185.178.47.70	80

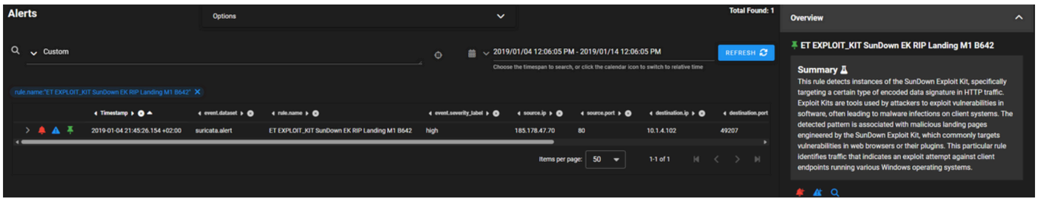
ET EXPLOIT_KIT RIG EK URI Struct Jun 13 2017

Summary

This rule detects a specific pattern associated with the RIG Exploit Kit, targeting HTTP traffic from internal to external networks. It triggers on HTTP requests with a URI length greater than 90, which start with "/?" and include a specific pattern beginning with "=x". The rule examines the URI structure using a Perl-compatible regular expression that matches a specific sequence of characters. Additionally, it checks the HTTP headers to ensure they do not contain "cookie" followed by a carriage return and newline. This detection method is aimed at identifying malicious activity related to the RIG Exploit Kit, which is known for exploiting vulnerabilities in web browsers and plugins to compromise client endpoints, typically affecting a range of Windows operating systems.

Status: Enabled

SO image of exploit kit SunDown EK RIP.



2019/01/04 12:06:05 PM - 2019/01/14 12:06:05 PM

Choose the timespan to search, or click the calendar icon to switch to relative time

rule.name:"ET EXPLOIT_KIT SunDown EK RIP Landing M1 B642"

Timestamp	event.dataset	rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port
2019-01-04 21:45:26.154 +02:00	suricata.alert	ET EXPLOIT_KIT SunDown EK RIP Landing M1 B642	high	185.178.47.70	80	10.1.4.102	49207

ET EXPLOIT_KIT SunDown EK RIP Landing M1 B642

Summary

This rule detects instances of the SunDown Exploit Kit, specifically targeting a certain type of encoded data signature in HTTP traffic. Exploit Kits are tools used by attackers to exploit vulnerabilities in software, often leading to malware infections on client systems. The detected pattern is associated with malicious landing pages engineered by the SunDown Exploit Kit, which commonly targets vulnerabilities in web browsers or their plugins. This particular rule identifies traffic that indicates an exploit attempt against client endpoints running various Windows operating systems.

Document by: JO, JJ