

# NurisBot

---

**Category:** Threat Hunting

**Difficulty:** Easy

**Date Completed:** 2025-04-25

---

## Summary

This lab involved analyzing Suricata and Zeek logs within Splunk to detect and investigate a malware infection originating from an external attacker. The exercise focused on tracking down the attacker's IP, identifying the compromised host, uncovering malicious file downloads, and correlating indicators across HTTP and DNS traffic.

---

## Timeline of Events

I will Upload an updated version later today I want to sleep man

---

## Technical Walkthrough




- **Tools Used:** Splunk, Zeek, Suricata
  - **Artifacts Found:**
    - Download of suspicious executable: `/temp/3425[.]exe`
    - Domain associated: `nocomcom[.]com`
    - Multiple malicious files including disguised `kv4[.]txt` file
  - **Indicators of Compromise (IOCs):**
    - Attacker IP: `195[.]88[.]191[.]59`
    - Victim IP: `147[.]32[.]84[.]165`
    - Malicious Domain: `nocomcom[.]com`
    - Malicious File SHA256:  
`6fbc4d506f4d4e0a64ca09fd826408d3103c1a258c370553583a07a4cb9a6530`
- 

## Detection Logic

- **Data Summary Sourcetypes:** *(found from Data Summary menu)*  
Zeek security monitor and Suricata IDS generated all logs.
- **Key Logs:**
  - Zeek: `zeek:files`, `zeek:conn`, `zeek:dns`, `zeek:http`

- Suricata: `event_type=alert`, `event_type=fileinfo`, `event_type=http`

- **Suricata Event Types** (extracted via `index=* sourcetype=suricata | stats count by event_type`):

Event Type	Count	Description
alert	2872	 Detection of attacks or suspicious activity
fileinfo	630	 File metadata during transfer
http	1,405	 Web traffic monitoring

- **Important Fields in Alerts:**

Field	Purpose
event_type	Confirmed security events
alert.signature	Attack/malware identification
src_ip, dest_ip	Tracing attacker/victim
flow_id	Correlation between events
app_proto	Application used (HTTP, TLS, etc.)
bytes_in, bytes_out	Potential exfiltration detection

- **Finding our IPs:**

```
index=* sourcetype="suricata"
| fields src_ip, dest_ip
| stats count by src_ip, dest_ip
| sort -count
| head 1000
```

---

## Lessons Learned

- **What surprised me?**

No internal IPs made context more confusing; hard to visually map the environment.

- **What would I do differently?**

Use more cross-correlation between Zeek and Suricata earlier instead of trying HTTP filtering only.

- **Which new tool or concept did I master?**

- Zeek: how to leverage `zeek:files` for extracting hashes
- Splunk Query: Advanced `join` to correlate `bytes` between Suricata and Zeek.

---

## Thought Process for Each Question

---

## Q1: What is the IP address from which the initial unauthorized access originated?

During the investigation of network traffic, unusual patterns of activity were observed in Suricata logs, suggesting potential unauthorized access. One external IP address initiated access attempts and was later seen downloading a suspicious executable file. This activity strongly indicates the origin of the attack.

First, I was thinking of going through HTTP and finding GET requests but then decided to go to Suricata event type `fileinfo` and HTTP method GET, and table the `src_ip + fileinfo name + hash`. But I had to do this query first:

```
index=* sourcetype=suricata event_type=alert dest_ip=* src_ip=*
| stats count by dest_ip dest_port
| sort -count
| head 50
```

It turned out the dest IP `147.32.84.165` communicated a lot using random dest ports, so it was most likely used as a C2 server.

There was also `147.32.84.171`.

We could see that this IP used two protocols — HTTP and DCERPC — which is dangerous as it can be used for remote control, and if exposed to the internet it would be very dangerous.

Getting back to the search for the file:

```
index=* sourcetype=suricata event_type=fileinfo
| search http.http_method=GET
| table _time src_ip http.hostname http.url fileinfo.filename
| sort _time
```

Among all the files:

2011-08-10 09:01:40.475	195.88.191.59	nocomcom.com	/temp/3425.exe? t=0.3419458	/temp/3425.exe

This is the most suspicious.

New Search

Save As

Create Table View

Close

```

1 index=* source=suricata event_type=fileinfo
2 | search http.http_method=GET
3 | table _time src_ip http.hostname http.url | fileinfo.filename
4 | sort _time

```

✓ 493 events (Before 4/25/25 9:43:02.000 PM)

No Event Sampling

Job

Smart Mode

Events

Patterns

Statistics (493)

Visualization

20 Per Page

Format

Preview

< Prev

1

2

3

4

5

6

7

8

...

Next >

_time *	src_ip ✓	http.hostname ✓	http.url ✓
2011-08-10 09:01:40.475	174.133.57.141	1.95622.com	/p6.asp?MAC=08-00-27-05-07-19&Publicer=dc99
2011-08-10 09:01:40.475	174.133.57.141	a.95622.com	/p6.asp?MAC=08-00-27-05-07-19&Publicer=dc99
2011-08-10 09:01:40.475	98.126.71.122	www.generalamuse.com	/gen.php
2011-08-10 09:01:40.475	74.125.232.217	googleads.g.doubleclick.net	/apps/domainpark/domainpark.cgi?callback=_google_json_callback&output=json&client=ca-dp-oversee32_hph_val&domain_name=riskslot.com&hl=eng&channel=010643&s=riskslot.com&kw_type=broad&num_ads=0&dt=1312968624183&u_tz=1880&hi=0&u
2011-08-10 09:01:40.475	195.113.232.83	ads.pro-market.net	/ads/scripts/site-128535.js
2011-08-10 09:01:40.475	94.63.149.152	ii.ebataoyhuy.com	/rus.php
2011-08-10 09:01:40.475	195.88.191.59	nocomcom.com	/temp/3425.exe?t=0.3419458
2011-08-10 09:06:52.586	60.190.223.75	w.nucleardiscover.com	/sn.php?c=ACB245A1AE3E4595C12B7C54EAS26058B41122488AA75E36F0B2C6525FE1C32430E8736954F6C08360B12B545F0DC7C06843C0BCEAE0F0C431978924A1D1ABD493EBFED20A3350D8360F68A45195C7B0582719537D0BEC29E7918797E6F9288F350AA19E9
2011-08-10 09:06:53.774	195.88.191.59	nocomcom.com	/kx4.txt
2011-08-10 09:06:53.978	60.190.223.75	w.nucleardiscover.com	/sn.php?c=190722C611B115C5C42EF80D450C36039730A3CF809EE72F490B5FCAB700B2551A19076F9C44E7E4520F16BE7C821BEC470484A24F8DCE2AD0B874D7790974080F774E9505CF3A001B6148A64699E71876330C72B0DAE8022254E17E292EA63029889A0B744E2499E7713EA59

So the IP is most likely 195.88.191.59 and it's correct.

So we now know the attacker IP is 195.88.191.59.

But tbh the way [SwordFischer](#) did it was way better:

```
| metadata type=sourcetypes index=*
```

New Search

Save As ▾

Create Table View

Close

1 | metadata type=sourcetypes index=\*

All time ▾

🔍

✓ 25 results (before 4/25/25 10:14:29.000 PM)

No Event Sampling ▾

Job ▾

⏏

🔄

📄

📁

🔖 Smart Mode ▾

Events

Patterns

Statistics (25)

Visualization

50 Per Page ▾

✓ Format

Preview ▾

firstTime ▾ ✓	lastTime ▾ ✓	recentTime ▾ ✓	sourcetype ▾ ✓	totalCount ▾ ✓	type ▾
1312966900	13176382598	1716560581	suricata	107263	sourcetypes
1312963313	1312984447	1716560559	zeek:app_stats	25	sourcetypes
1312962413	1312984447	1716561893	zeek:conn	4870899	sourcetypes
1312963719	1312984396	1716560562	zeek:dhcp	66	sourcetypes
1312962413	1312984447	1716561163	zeek:dns	1000913	sourcetypes
1312962414	1312984446	1716560572	zeek:dpd	5847	sourcetypes
1312962413	1312984447	1716561179	zeek:files	267856	sourcetypes
1312962953	1312984323	1716560561	zeek:ftp	275	sourcetypes
1312962413	1312984447	1716561215	zeek:http	509601	sourcetypes
1716554806	1716554806	1716560572	zeek:loaded_scripts	301	sourcetypes
1312962616	1312984443	1716560559	zeek:mysql	2748	sourcetypes
1312962416	1312984390	1716560574	zeek:notice	497	sourcetypes
1492191987	1492191987	1716560559	zeek:packet_filter	1	sourcetypes
1312964320	1312984064	1716560573	zeek:pe	21	sourcetypes
1312964950	1312983188	1716560563	zeek:rdp	10	sourcetypes
1312962419	1312984443	1716560559	zeek:sip	1623	sourcetypes
1312962512	1312967588	1716560562	zeek:smtp	253	sourcetypes
1312962414	1312984443	1716560563	zeek:snmp	3896	sourcetypes
1312983810	1312983810	1716560572	zeek:socks	1	sourcetypes
1312964077	1312984442	1716560561	zeek:ssh	10865	sourcetypes
1312962413	1312984446	1716560572	zeek:ssl	59904	sourcetypes
1312962413	1312984446	1716561244	zeek:syslog	96337	sourcetypes
1312962413	1312984447	1716560572	zeek:tunnel	435	sourcetypes
1312962413	1312984447	1716560573	zeek:weird	18732	sourcetypes
1312962416	1312984444	1716560564	zeek:x509	11186	sourcetypes

This lists all sourcetypes and their counts.

We saw Suricata in there, then:

```
index=* sourcetype=suricata
| stats count by eventtype
| sort -count
```

<pre>1 index=* sourcetype=suricata 2   stats count by eventtype 3   sort --count</pre>		All time	
✓ 107,263 events (before 4/25/25 10:19:54.000 PM) No Event Sampling		Job     Smart Mode	
Events	Patterns	Statistics (6)	Visualization
50 Per Page	Format	Preview	
eventtype	count		
suricata_eve_dns	84578		
suricata_eve_flow	17346		
suricata_eve_ids_attack	2872		
suricata_eve_http	1485		
error	841		
suricata_eve_tls	52		

We can see `suricata_eve_ids_attack`.

Then he did:

```
index=* sourcetype=suricata eventtype=suricata_eve_ids_attack
| stats values(dest_ip) values(http.http_user_agent)
values(http.http_content_type) values(http.http_protocol)
values(http.status) values(http.hostname) values(http.url) by src_ip
```

1 index= sourcetype=suricata eventtype=suricata\_eve\_ids\_attack

2 | stats values(dest\_ip) values(http.http\_user\_agent) values(http.http\_content\_type) values(http.http\_protocol) values(http.status) values(http.hostname) values(http.url) by src\_ip

All time

✓ 2,872 events (before 4/25/25 10:21:42.000 PM)

No Event Sampling

Job

Smart Mode

Events

Patterns

Statistics (47)

Visualization

50 Per Page

Format

Preview

src_ip	values(dest_ip)	values(http.http_user_agent)	values(http.http_content_type)	values(http.http_protocol)	values(http.status)	values(http.hostname)	values(http.url)
122.224.6.164	147.32.84.165	Mozilla/4.0 (compatible; MSIE 6.0.2900.2188; Windows NT 5.1.2600)				hm.yigeyuming.com	/fn.gif?r=0.9300886 /fn.gif?r=0.9630548
147.32.84.165	147.32.84.171 173.192.170.88 78.129.163.119 78.129.227.128						
173.192.170.88	147.32.84.165	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; waoe) Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.14) Gecko/2009090217 Ubuntu/9.04 (jaunty) Firefox/3.0.14	text/html	200	www.funlad.com www.100kj.com www.netsgames.com www.newcarus.com www.zkao.com		/funng.html /gl.php?u=900&v=5&m=04FCDF6F-063E-4377-A1F3-EE723AEF499 /netgame.html /newcar.html /r.php?a=vdn=401 /r.php?a=vdn=4459

Which lists all these infos based on each `src_ip`.

Since we know there is an agent called "Download," we will filter by that:

```
index=* sourcetype=suricata eventtype=suricata_eve_ids_attack
http.http_user_agent="Download"
| stats values(dest_ip) values(http.http_user_agent)
values(http.http_content_type) values(http.http_protocol)
values(http.status) values(http.hostname) values(http.url) by src_ip
```

New Search

Save As

Create Table View

Close

1 index=\* sourcetype=suricata eventtype=suricata\_eve\_ids\_attack http.http\_user\_agent="Download"

2 | stats values(dest\_ip) values(http.http\_user\_agent) values(http.http\_content\_type) values(http.http\_protocol) values(http.status) values(http.hostname) values(http.url) by src\_ip

All time

✓ 44 events (before 4/25/25 10:24:05.000 PM) No Event Sampling

Job

<

We have three source IPs that downloaded something.

```
index=* sourcetype=suricata dest_ip IN (60.190.223.75, 195.88.191.59,
94.63.149.152) http.url=*
| table _time dest_ip http.http_user_agent http.http_content_type
http.status http.hostname http.url src_ip
| sort +_time
```

New Search

Save AsCreate Table ViewClose

1 index=\* sourcetype=suricata dest\_ip IN (60.190.223.75, 195.88.191.59, 94.63.149.152) http.url=\*  
2 | table \_time values dest\_ip http.http\_user\_agent http.http\_content\_type http.status http.hostname http.url src\_ip  
3 | sort +\_time

All time

✓ 22 events (before 4/25/25 10:26:34.000 PM)No Event SamplingJobSmart Mode

EventsPatternsStatistics (22)Visualization

50 Per PageFormatPreview

_time	values	dest_ip	http.http_user_agent	http.http_content_type	http.status	http.hostname	http.url
2011-08-10 09:01:40.475		94.63.149.152	Download			ii.ebatmoyhuy.com	/rus.php
2011-08-10 09:01:40.475		195.88.191.59	Mozilla/4.0 (compatible; MSIE 6.0.2900.2180; Windows NT 5.1.2600)			nocomcom.com	/temp/3425.exe?t=0.3419458
2011-08-10 09:01:40.475		60.190.223.75	Mozilla/4.0 (compatible; MSIE 6.0.2900.2180; Windows NT 5.1.2600)	text/html	200	w.nucleardiscover.com	/list.php?c=B4AC885F94224AE64DAAC6F60346C27CD049B58C0B2469F2DC9ECA825FF9F6D90FE10E13
2011-08-10 09:06:52.586		60.190.223.75	Mozilla/4.0 (compatible; MSIE 6.0.2900.2180; Windows NT 5.1.2600)	text/html	200	w.nucleardiscover.com	/sn.php?c=ACB245A1AE3E4595C12B7C54ECA526D58B41122488AA75E9F0B2C6525FE1C3240E987369
2011-08-10 09:06:53.232		195.88.191.59	Download	text/plain	200	nocomcom.com	/kx4.txt
2011-08-10 09:06:53.978		60.190.223.75	Mozilla/4.0 (compatible; MSIE 6.0.2900.2180; Windows NT 5.1.2600)	text/html	200	w.nucleardiscover.com	/sn.php?c=190722C6118115C5C42EF8D0450C936039F30A3CFBD9EE72F490B5FCAB700B25571A9D76F9C44E7E45
2011-08-10 09:06:57.918		94.63.149.152	Download			ii.ebatmoyhuy.com	/ff.exe
2011-08-10 09:06:57.921		60.190.223.75	Mozilla/4.0 (compatible; MSIE 6.0.2900.2180; Windows NT 5.1.2600)	text/html	200	w.nucleardiscover.com	/sn.php?c=ABB5F2168D1D5DFA39D232684D06DA1FC969A491CEE815892111CA8316BF4A6793DF779D3E0383DE1A
2011-08-10 09:06:59.281		60.190.223.75	Mozilla/4.0 (compatible; MSIE 6.0.2900.2180; Windows NT 5.1.2600)	text/html	200	w.nucleardiscover.com	/sn.php?c=B2AC8B6F21B1309704EF356F85CE1ADF3E9EDCE9D4F2A33F86B69CD50BA2DFF26C2059B3CAF7025F28
2011-08-10 09:13:31.597		60.190.223.75	Mozilla/4.0 (compatible; MSIE 6.0.2900.2180; Windows NT 5.1.2600)	text/html	200	w.nucleardiscover.com	/sn.php?c=2C3248ACD949E83827CD1D354E07EC1F33F9ED0B41632FB35733F6BF04DF8BA597DA7E95D9E4083868

Q2: What is the domain name of the attacker server?

The query that we had above solved our question.

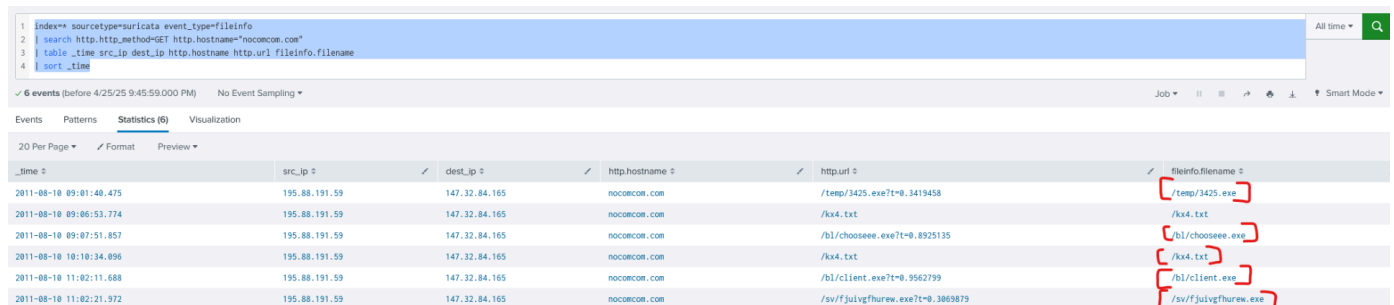


## Q4: Identify all the unique files downloaded to the compromised host. How many of these files could potentially be malicious?

For that, I tweaked the query a bit:

```
index=* sourcetype=suricata event_type=fileinfo
| search http.http_method=GET http.hostname="nocomcom.com"
| table _time src_ip dest_ip http.hostname http.url fileinfo.filename
| sort _time
```

Resulted in:



The screenshot shows the Zeek interface with a search query: `index=* sourcetype=suricata event_type=fileinfo | search http.http_method=GET http.hostname="nocomcom.com" | table _time src_ip dest_ip http.hostname http.url fileinfo.filename | sort _time`. The results table has 6 columns: `_time`, `src_ip`, `dest_ip`, `http.hostname`, `http.url`, and `fileinfo.filename`. There are 6 events listed. Red boxes highlight the `fileinfo.filename` column, showing files like `/temp/3425.exe`, `/xx4.txt`, `/bl/chooseee.exe`, `/xx4.txt`, `/bl/client.exe`, and `/sv/ffjuivgfhurew.exe`.

_time	src_ip	dest_ip	http.hostname	http.url	fileinfo.filename
2011-08-10 09:01:40.475	195.88.191.59	147.32.84.165	nocomcom.com	/temp/3425.exe?t=0.3419458	/temp/3425.exe
2011-08-10 09:06:53.774	195.88.191.59	147.32.84.165	nocomcom.com	/xx4.txt	/xx4.txt
2011-08-10 09:07:51.857	195.88.191.59	147.32.84.165	nocomcom.com	/bl/chooseee.exe?t=0.8925135	/bl/chooseee.exe
2011-08-10 10:10:34.896	195.88.191.59	147.32.84.165	nocomcom.com	/xx4.txt	/xx4.txt
2011-08-10 11:02:11.688	195.88.191.59	147.32.84.165	nocomcom.com	/bl/client.exe?t=0.9562799	/bl/client.exe
2011-08-10 11:02:21.972	195.88.191.59	147.32.84.165	nocomcom.com	/sv/ffjuivgfhurew.exe?t=0.3669879	/sv/ffjuivgfhurew.exe

I got the answer wrong — it was actually 5.

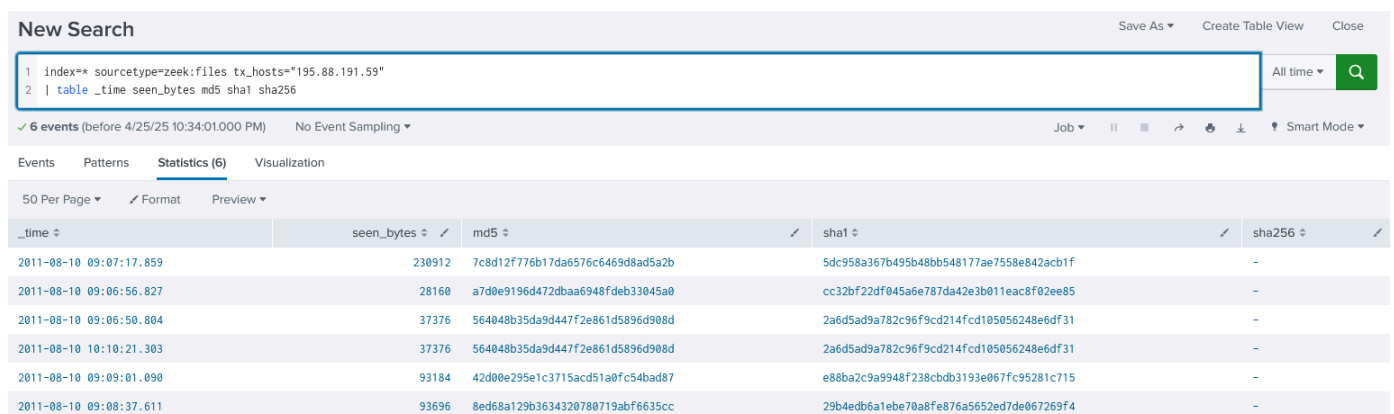
They included the `.txt` file as potentially malicious.

I thought it would be 4, but turns out it's 5 — we learn from that.

Damn, for this one I missed up hard.

I didn't know Zeek has `zeek:file` which contains hashes.

```
index=* sourcetype=zeek:files tx_hosts="195.88.191.59"
| table _time seen_bytes md5 sha1 sha256
```



The screenshot shows the Zeek interface with a search query: `index=* sourcetype=zeek:files tx_hosts="195.88.191.59" | table _time seen_bytes md5 sha1 sha256`. The results table has 6 columns: `_time`, `seen_bytes`, `md5`, `sha1`, and `sha256`. There are 6 events listed. The `md5` and `sha1` columns contain hash values, while the `sha256` column contains dashes.

_time	seen_bytes	md5	sha1	sha256
2011-08-10 09:07:17.859	230912	7c8d12f776b17da6576c6469d8ad5a2b	5dc958a367b495b48bb548177ae7558e842acb1f	-
2011-08-10 09:06:56.827	28160	a7d0e9196d472dbaa6948fdeb33045a0	cc32bf22df045a6e787da42e3b011eac8f02ee85	-
2011-08-10 09:06:50.804	37376	564048b35da9d447f2e861d5896d908d	2a6d5ad9a782c96f9cd214fcd105056248e6df31	-
2011-08-10 10:10:21.303	37376	564048b35da9d447f2e861d5896d908d	2a6d5ad9a782c96f9cd214fcd105056248e6df31	-
2011-08-10 09:09:01.090	93184	42d00e295e1c3715acd51a0fc54bad87	e88ba2c9a9948f238cbdb3193e067fc95281c715	-
2011-08-10 09:08:37.611	93696	8ed68a129b3634320780719abf6635cc	29b4edb6a1ebe70a8fe76a5652ed7de067269f4	-

Hashes found:

- Hash 1: `42d00e295e1c3715acd51a0fc54bad87`
- Hash 2: `8ed68a129b3634320780719abf6635cc`



- Hash 3: `7c8d12f776b17da6576c6469d8ad5a2b`
- Hash 4: `a7d0e9196d472dbaa6948fdeb33045a0`
- Hash 5: `b5f3729e5418905ad2b21ce186b1c01d`
- Hash 6: `564048b35da9d447f2e861d5896d908d`

## Q5: What is the SHA256 hash of the malicious file disguised as a `.txt` file?

So I'm out of luck — really, Suricata `fileinfo` doesn't have the hash for `kx4.txt`.

I have to find another way in my environment to get hashes and I don't want to throw random queries.

Tried:

```
index=* kx4.txt
```

and

```
index=* sourcetype="suricata" url="/kx4.txt"
```

11 results but no hash.

So I ended up going to this report:

<https://mcfp.felk.cvut.cz/publicDatasets/CTU-Malware-Capture-Botnet-54/botnet-capture-20110815-fast-flux-2.html>

and found the hash.

6fbc4d506f4d4e0a64ca09fd826408d3103c1a258c370553583a07a4cb9a6530	

64/72 security vendors flagged this file as malicious

6fbc4d506f4d4e0a64ca09fd826408d3103c1a258c370553583a07a4cb9a6530

qtfcyp.exe

Size: 36.50 KB | Last Analysis Date: 23 days ago

peexe checks-user-input runtime-modules malware direct-cpu-clock-access calls-wmi detect-debug-environment hosts-modifier upx checks-network-adapters

long-sleeps spreader nxdomain

Also learned this amazing query:

```
index=* sourcetype=zeek:files tx_hosts="195.88.191.59"
| join left=L right=R where L.seen_bytes=R.bytes
[search index=* sourcetype=suricata src_ip=147.32.84.165
dest_ip=195.88.191.59 url=*]
| table L.md5, L.sha1, R.url
```

1index\*\* sourcetype=zeek:files tx\_hosts="195.88.191.59"

2| join left=L right=R where L.seen\_bytes=R.bytes

3[search index\*\* sourcetype=suricata src\_ip=147.32.84.165 dest\_ip=195.88.191.59 url=\* ]

4| table L.md5, L.sha1, R.url

All time

✓ 2 events (before 4/25/25 10:38:09.000 PM) No Event Sampling

Job || ↗ ⚙ ⬇ ⚡ Smart Mode

Events Patterns **Statistics (2)** Visualization

50 Per Page ✓ Format Preview

L.md5	L.sha1	R.url
564048b35da9d447f2e861d5896d908d	2a6d5ad9a782c96f9cd214fcd105056248e6df31	/kx4.txt
564048b35da9d447f2e861d5896d908d	2a6d5ad9a782c96f9cd214fcd105056248e6df31	/kx4.txt

This query matches the results from suricata bytes field and from zeek seen\_bytes to get one table that have url and hash in it