notebook.community

EDIT AND RUN

Ursnif Malware Download URL Pattern

Detects download of Ursnif malware done by dropper documents.

Rule Content

```
- title: Ursnif Malware Download URL Pattern id: a36ce77e-30db-4ea0-8795-644d7af5dfb4 status: stable de
```

Querying Elasticsearch

Import Libraries

```
In [ ]:

from elasticsearch import Elasticsearch
from elasticsearch_dsl import Search
import pandas as pd
```

Initialize Elasticsearch client

```
In [ ]:

es = Elasticsearch(['http://helk-elasticsearch:9200'])
searchContext = Search(using=es, index='logs-*', doc_type='doc')
```

Run Elasticsearch Query

```
In [ ]:

s = searchContext.query('query_string', query='(c-uri.keyword:*\/*.php?l\=*.cab AND sc-status:"200")'
response = s.execute()
if response.success():
    df = pd.DataFrame((d.to_dict() for d in s.scan()))
```

```
In [ ]:

s = searchContext.query('query_string', query='(c-uri.keyword:(*_2f* OR *_2b*) AND c-uri.keyword:*.av
response = s.execute()
if response.success():
    df = pd.DataFrame((d.to_dict() for d in s.scan()))
```

Show Results

```
In [ ]:

df.head()
```

Content source: Cyb3rWard0g/HELK

Similar notebooks:

- proxy_ursnif_malware
- proxy_chafer_malware
- proxy_ios_implant
- win_mal_ryuk
- proxy_ua_cryptominer
- win_malware_ryuk
- proxy_ua_hacktool
- powershell_shellcode_b64
- sysmon_quarkspw_filedump
- sysmon_susp_lsass_dll_load

notebook.community | gallery | about