Threat Hunting with VirusTotal

Keep your enemies closer with state-of-the-art toolset

Alexey Firsh
@alexey_firsh

17.11.22
SECTION 1

VT Intelligence: use search like a true-ninja
The vulnerability was disclosed by nao_sec, a Tokyo-based cybersecurity research group on Twitter.

Tracked as CVE-2022-30190, this zero-day bug (no patch yet) was actively exploited by a number of different actors.

Official statement from MS: “A remote code execution vulnerability exists when MSDT is called using the URL protocol from a calling application such as Word. An attacker who successfully exploits this vulnerability can run arbitrary code with the privileges of the calling application. The attacker can then install programs, view, change, or delete data, or create new accounts in the context allowed by the user’s rights.”

Initial finding - VT link
VT Intelligence: use search like a true-ninja

- Main purpose – made a quick look up
- But also main purpose – construct an advanced queries limited only by your demands or imagination
- You can get recent malicious documents used your org name or urls mimicking your website to phish the victims
- Also could be used to check entity (string) for popularity for further usage in detecting signatures
- Almost unlimited possibilities to operate with existing data
VT Intelligence: use search like a true-ninja - entity magic

Search query: "Supermalware"

- entity:file
  - entity:url
  - entity:ip
  - entity:domain
  - entity:collection

- file-specific keywords
- url-specific keywords
- ip-specific keywords
- domain-specific keywords
- collection-specific keywords
VT Intelligence: use search like a true-ninja - Behaviour search

- 3b99c3bd0a76c23d8d29f3dfc82c66491286cad2 – sample from Kaspersky report on BlueNoroff
- Network activity
- Filesystem operations
- Processes execution
- Combination of other side behaviours not directly related to the malicious activity
VT Intelligence: use search like a true-ninja - Behaviour search

- 3b99c3bd0a76c23d8d29f3dfc82c66491286cad2 - sample from Kaspersky report on BlueNoroff

- Network activity

- Filesystem operations

- Processes execution

- Combination of other side behaviours not directly related to the malicious activity

- Explore hidden cases – Google TAG report on Conti
VT Intelligence: use search like a true-ninja - Behaviour search

- **Sample** from Malwarebytes report on Colibri Loader
- **behaviour_network:"/vpnchecker.php"** – gives us more samples than the original research provides
VT Intelligence: use search like a true-ninja - Behaviour search

- **Sample** from Malwarebytes report on Colibri Loader
- `behaviour_network:"/vpnchecker.php"` - gives us more samples than the original research provides
- FinSpy MacOS installer shared by Amnesty International
- `behaviour_files:"/80C.dat" AND behaviour_files:"/7FC.dat"` - we are able to jump to different platform implants

---

**German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed**

**Summary:**

- FinSpy is a commercial spyware suite produced by the Munich-based company FinFisher GmbH. Since 2011 researchers have documented numerous cases of targeting of Human Rights Defenders (HRDs) – including activists, journalists, and dissidents with the use of FinSpy in many countries, including Bahrain, Ethiopia, UAE, and more. Because of this, Amnesty International’s Security Lab tracks FinSpy usage and development as part of our continuous monitoring of digital threats to Human Rights Defenders.
- Amnesty International published a report in March 2019 describing phishing attacks targeting Egyptian human rights defenders and media and civil society organizations staff carried out by an attacker group known as “NilePhish”. While continuing research into this group’s activity, we discovered it has distributed samples of FinSpy for Microsoft Windows through a fake Adobe Flash Player download website. Amnesty International has not documented human rights violations by NilePhish directly linked to FinFisher products.
- Through additional technical investigations into this most recent variant, Amnesty’s Security Lab also discovered, exposed online by an unknown actor, new samples of FinSpy for Windows, Android, and previously undisclosed versions for Linux and MacOS computers.
- This report provides technical information on these recent FinSpy samples in order to aid the cybersecurity research community in further investigations, enable cybersecurity vendors implement protection mechanisms against these newly discovered variants, and to raise awareness among HRDs of evolving digital attack techniques.

*material*. As it names suggests, it is meant to deliver and manage payloads onto infected computers.
VT Intelligence: use search like a true-ninja

- **Looking for files** signed with what appears to be “trusted” signatures but detected by a number of AVs
- We can also search for URLs with specific **cookie** (MageCart) or even **metadata** (OrigamiElephant)
- **Android files** processed by Androguard
- **Workarounds** to detect brand abuse
- New! Android package **search** – will solve a lot of problems in the future
- Mac/iOS **malware** with known ITW distribution hosts or the **ones** distributed via Discord service.
- **Emails** having attachment that allegedly use an exploit
- There are much more…
SECTION 2

VTI Godmode: APT tracking and API automation
APT tracking and API automation [DEMO]

- APT dashboard – project based on VirusTotal API only
- Designed to track actor’s recent activities
- Demonstrates powerful capabilities of VirusTotal API
- Apart from infographic, provides the following IOCs:
  - Files (AVs, collections, rules detections)
  - IP/Domains/URLs (collections)
  - Graphs
  - Collections
  - Comments
APT tracking and API automation [DEMO]

- APT dashboard – project based on VirusTotal API only
- Designed to track actor’s recent activities
- Demonstrates powerful capabilities of VirusTotal API
- Apart from infographic, provides the following IOCs:
  - Files (AVs, collections, rules detections)
  - IP/Domains/URLs (collections)
  - Graphs
  - Collections
  - Comments
APT tracking and API automation [DEMO]

- APT dashboard – project based on VirusTotal API only
- Designed to track actor’s recent activities
- Demonstrates powerful capabilities of VirusTotal API
- Apart from infographic, provides the following IOCs:
  - Files (AVs, collections, rules detections)
  - IP/Domains/URLs (collections)
  - Graphs
  - Collections
  - Comments
APT tracking and API automation - Python client for VirusTotal

**Vt-py** – official Python client library for VirusTotal

- Get information about any VirusTotal objects: files, URLs, domains, graphs, collections, etc
- Perform VT Intelligence searches and operate with results found as Python objects
- Manage all the VT services: Livehunt rulesets and notifications, Retrohunt jobs, Graphs, Collections
- We have detailed documentation with 1-click live examples on VT API
- As well as how-to manual on vt-py Python client

```python
import vt
import nest_asyncio

nested_asyncio.apply()

API_KEY = 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX'
COMMENTS_URL = '/comments'

client = vt.Client(API_KEY)

comments = client.iterate(COMMENTS_URL,
                          params={'filter': 'tags:sofacy'},
                          limit=10)
print('
'.join('ID: {}\n{}\n'.format(c.id, c.text) for c in comments))

client.close()
```

**RULE:** Sofacy Jan18.1_PE_Info Anomaly
**RULE SET:** Livehunt - Russia Indicators 🚨
**RULE TYPE:** VALBLLA rule feed only 🔄
**RULE LINK:** https://valbllla.nexten-systems.com/info/rule/Sofacy_Jan18.1_PE_Info Anomaly
**DESCRIPTION:** Detects a PE header anomaly as found in malware from Sofacy campaign in January
**REFERENCE:** MISP Event 9961
**RULE_AUTHOR:** Florian Roth

Detection Timestamp: 2022-05-14 14:31
AV Detection Ratio: 🟢 43 / 68

Use these tags to search for similar matches: #sofacy #info #sofacy_jan18.1_pe_info_anomaly

```
```
import requests
url = "https://www.virustotal.com/api/v3/comments/?" + "limit=10&filter=tag%253Asofacy"
headers = {
    "Accept": "application/json",
    "x-apikey": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
}
response = requests.get(url, headers=headers)
print(response.text)

### OUTPUT: ###
{
    "meta": {
        "cursor": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
    },
    "data": [
        {
            "attributes": {
                "date": 1652389338,
                "text": "YARA Signature Match - THOR APT Scanner"
            }
        }
    ],
    "type": "comments"
}
APT tracking and API automation

VT Intelligence search query – 99% of use cases
- **entity:collection** (name:apt28 OR tag:apt28 OR name:Sofacy OR tag:Sofacy)

VT Graph search (not related to VT Intelligence search)
- **name:**Sofacy OR **actor:**Sofacy OR **label:**Sofacy

```python
collections = client.iterator('/intelligence/search', params={'query': 'entity:collection ( name:apt28 OR tag:apt28 OR name:Sofacy OR tag:Sofacy )', 'order': 'last_modification_date-'}, limit=10)
```

```python
graphs = client.iterator('/graphs', params={'filter': 'name:Sofacy OR actor:Sofacy OR label:Sofacy', 'order': 'last_modified_date-'}, limit=10)
```
APT tracking and API automation

- **Wellmess** – suspected APT29 malware used to target COVID-19 vaccine developing entities
  - engines:wellmess – 60 results
  - kaspersky:wellmess OR eset:wellmess – 35 results

- entity:domain (comment:APT29 OR comment:CozyBear OR comment:NobleBaron OR comment:UNC2452 OR comment:YTTRIUM)

- crowdsourced_yara_rule:APT29 OR crowdsourced_ids:APT29 OR sigma_rule:976e* OR crowdsourced_yara_rule:CozyBear OR crowdsourced_ids:CozyBear OR sigma_rule:34f4*
  - To get Sigma rules detections you should use a hash of specific rule (full list here)

- We can list Collections in which we are interested in and then extract specific entities from them
  - entity:collection (name:APT29 OR tag:APT29 OR name:CozyBear OR tag:CozyBear) creation_date:2021-01-01+
  - entity:file collection:alienvault_60afece345be6dfd2a66ea3c fs:2021-01-01+
Thank you

Alexey Firsh
@alexey_firsh

brighttalk.com/webcast/18282/561655