VirusTotal - Swiss Intelligence Knife

Hands-on guide to advanced hunting with Yara

Alexey Firsh
@alexey_firsh

22.02.23

01

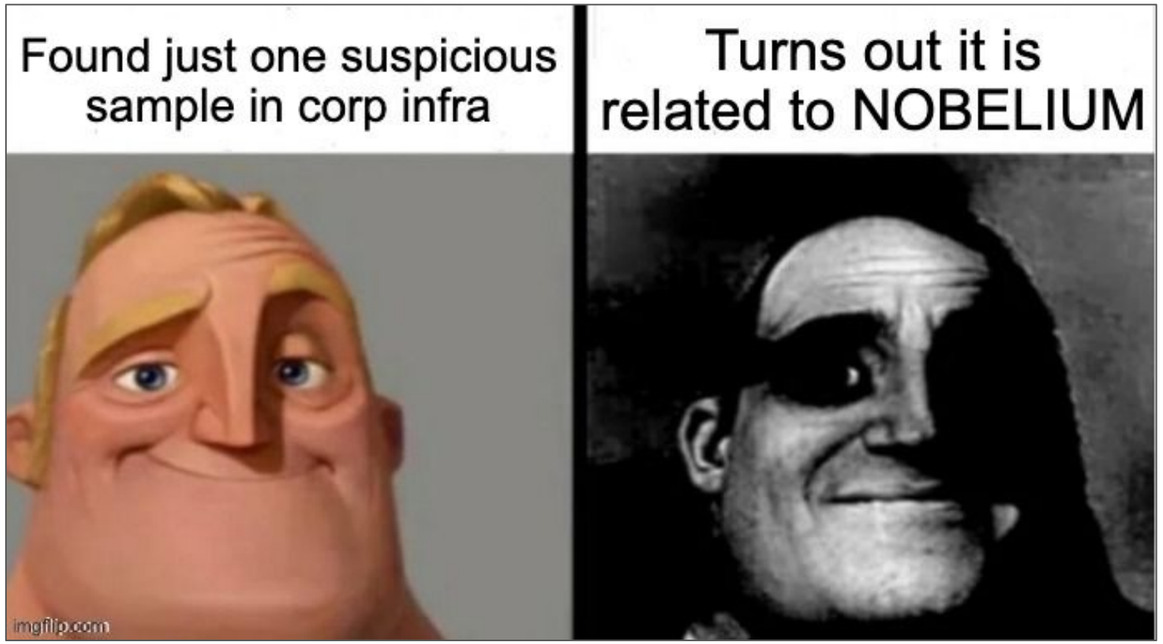
SECTION 1

Threat hunting: brief introduction

Threat hunting introduction - why we need to hunt

Why context matters?

- Cyber threat hunting means focus on undetected threats in your infrastructure
- Finding additional pieces of attack could completely change the vision of ongoing threat
- Understanding the whole picture of attack allows you to pay attention to specific parts of your defending bastion (patch management, checking certain logs, protect mobile, etc)
- Learning the actor TTPs and malware attribution lead to improvement of your threat model



Threat hunting introduction - Yara in a nutshell

- “Superb version” of grep tool
- Industry standard for sharing knowledge
- Main purpose:
  - Malware detection and classification
  - Finding suspicious activity
  - Searching for intellectual property
  - Forensic analysis
- Lots of useful documentation here

```
rule ExampleRule
{
    strings:
        $my_text_string = "text here"
        $my_hex_string = { E2 34 A1 C8 23 FB }

    condition:
        $my_text_string or $my_hex_string
}
```

Threat hunting introduction - Yara in a nutshell

- AV-like detection to detect specific IOCs
- To directly rise an alert and pay max attention
- Very few false positives

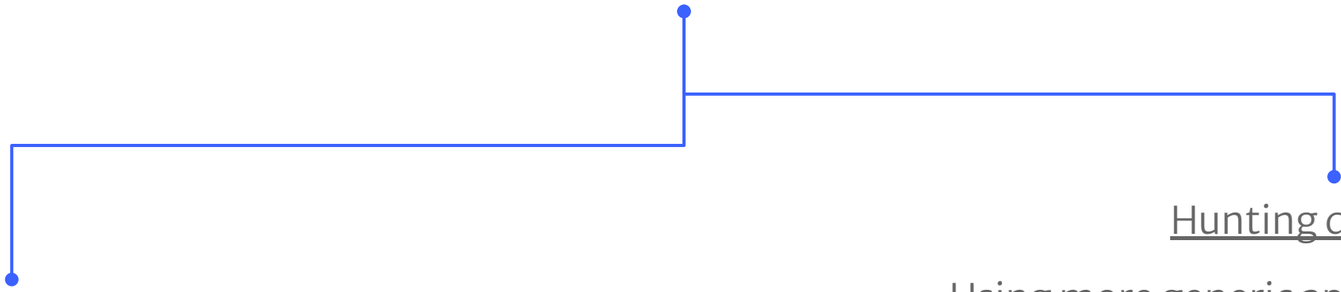
Threat hunting introduction - Yara in a nutshell

- For example, this Yara rule is detecting only specific ID, which is not directly related to Rubeus workflow and could be easily changed.
- There is also a magic number filter (0x5A4D) to get only MZ files.

```
rule HackTool_MSIL_Rubeus_1 {
    meta:
        description = "The TypeLibGUID present in a .NET binary maps directly to the ProjectGuid found in the '.csproj' file of a .NET project. This rule looks for .NET PE files that contain the ProjectGuid found in the public Rubeus project."
        md5 = "66e0681a500c726ed52e5ea9423d2654"
        rev = 4
        author = "FireEye"
    strings:
        $typelibguid = "658C8B7F-3664-4A95-9572-A3E5871DFC06" ascii nocase wide
    condition:
        uint16(0) == 0x5A4D and $typelibguid
}
```

Threat hunting introduction - Yara in a nutshell

Yara on malware samples



Exact detection

- AV-like detection to detect specific IOCs
- To directly rise an alert and pay max attention
- Very few false positives

Hunting detection

- Using more generic approach to find not only samples from the initial attack, but also all related IOCs (other campaigns, historical)
- Allows to uncover additional actor's activities
- Perfectly suited for getting a feed of samples to filter manually
- Could get lots of false positives

Threat hunting introduction - Yara in a nutshell

- In this example, we are using “any of them” condition to find files contained at least one of specified entities.
- There is no any additional conditions like file-type filtering.

```
rule hijack_network {
    meta:
        author = "x0r"
        description = "Hijack network configuration"
        version = "0.1"
    strings:
        $p1 = "SOFTWARE\\Classes\\PROTOCOLS\\Handler" nocase
        $p2 = "SOFTWARE\\Classes\\PROTOCOLS\\Filter" nocase
        $p3 = "Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ProxyServer" nocase
        $p4 = "software\\microsoft\\windows\\currentversion\\internet settings\\proxyenable" nocase
        $f1 = "drivers\\etc\\hosts" nocase
    condition:
        any of them
}
```

02

SECTION 2

Yara services at VirusTotal

Yara services at VirusTotal

- Searching in the past - Retrohunt
  - Scans the dataset of previously submitted files (up to 1 year) - more than 500M files (~680TB worth of data) in 2-3 hours and reports you the files that matches your rules
  - Perfect tool for attribution, allows you to uncover additional historical activity of the same actor
  - Also could be used to quickly check the rule for false positives before submitting to production (less than 1min)

Yara services at VirusTotal - Retrohunt

Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units

December 22, 2016 Adam Meyers Research & Threat Intel

Update – As of March 2017, the estimated losses of D-30 howitzer platform have been amended. According to an update provided by the International Institute for Strategic Studies (IISS) Research Associate for Defence and Military Analysis, Henry Boyd, their current assessment is as follows: “excluding the Naval Infantry battalion in the Crimea which was effectively captured wholesale, the Ukrainian Armed Forces lost between 15% and 20% of their pre-war D–30 inventory in combat operations.”

Unknown Android spyware sample

```
private byte[] cryptRc4(byte[] DataCrypt, byte[] Salt) {
    byte[] session_key = new byte[256];
    byte[] KERNEL_CRYPTO_MAIN_KEY = {59, -58, 115, 15, -117, 7, -123, -64, 116,
    byte[] private_key = new byte[KERNEL_CRYPTO_MAIN_KEY.length + Salt.length];
    for (int ind = 0; ind < KERNEL_CRYPTO_MAIN_KEY.length; ind++) {
        private_key[ind] = KERNEL_CRYPTO_MAIN_KEY[ind];
    }
    for (int ind2 = 0; ind2 < Salt.length; ind2++) {
        private_key[KERNEL_CRYPTO_MAIN_KEY.length + ind2] = Salt[ind2];
```

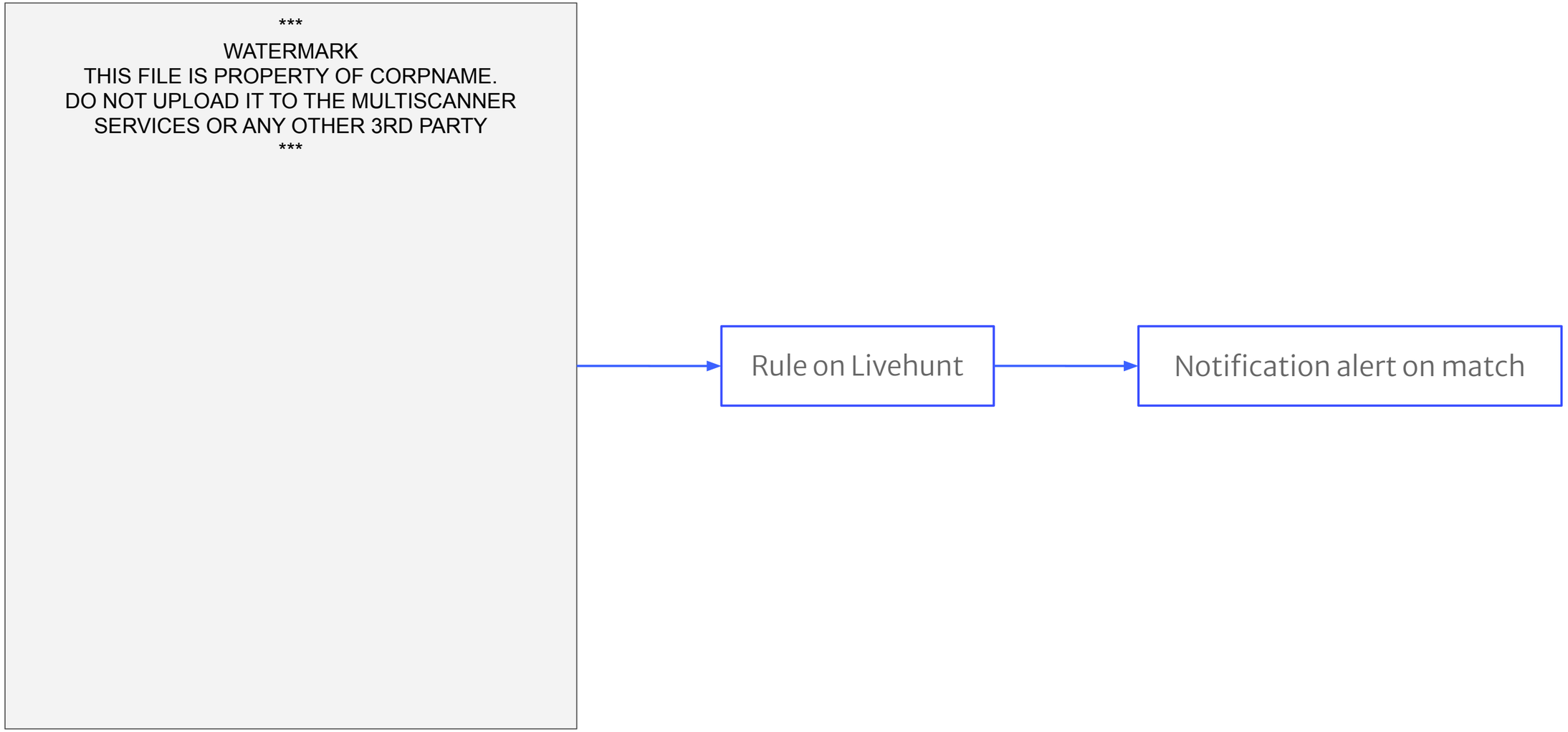
Retrohunt

Historical X-Agent Windows samples used by Sofacy

Yara services at VirusTotal

- Searching in the past – Retrohunt
  - Scans the dataset of previously submitted files (up to 1 year) – more than 500M files (~680TB worth of data) in 2-3 hours and reports you the files that matches your rules
  - Perfect tool for attribution, allows you to uncover additional historical activity of the same actor
  - Also could be used to quickly check the rule for false positives before submitting to production (less than 1min)
- Searching in the future – Livehunt
  - Daily scans of all incoming samples
  - Suitable for tracking ongoing campaigns/further activities
  - Could be also used to track leaked data, brand protection, etc

Yara services at VirusTotal - Livehunt



03

SECTION 3

Yara VirusTotal module

Yara VirusTotal module

- This Yara module created specially for Livehunt service to operate with all available VT context data
- Yara is a static analyzer by default, however with this module you can avoid static obfuscation making signatures on a malware behaviour executed in our sandboxes
- We have a number of third-parties SB (Vmray, Lastline, Tencent, C2AE, etc), as well as our own Jujubox
- Provides features in different categories:
  - Metadata (AVs rate, ExifTool, submissions, type, signature, VT tags, etc)
  - Behaviour (network, file system, SB verdict, Android/Windows specific)
- Our documentation is here

Yara VirusTotal module - Sofacy behaviour

Check out Sofacy's sample from 2017

Synchronization Mechanisms & Signals

Mutexes Created

Local\ZonesCacheCounterMutex

Local\ZonesLockedCacheCounterMutex

OEyZrUgaebnWBiSFZBZreuicRMbbcqHAXkqzLMAJlitMO

RasPbFile

```
import "vt"


rule Sofacy_2018 {
condition:
   for any mutex in vt.behaviour.mutexes_created : (
       mutex == "OEyZrUgaebnWBiSFZBZreuicRMbbcqHAXkqzLMAJIitMO"
    )
}
```

A Slice of 2017 Sofacy Activity

APT REPORTS 20 FEB 2018 9 minute read

// AUTHORS

Expert GREAT

Sofacy, also known as APT28, Fancy Bear, and Tsar Team, is a highly active and prolific APT. From their high volume 0day deployment to their innovative and broad malware set, Sofacy is one of the top groups that we monitor, report, and protect against. 2017 was not any different in this regard.

Yara VirusTotal module - Metadata exploring

- **vt.metadata.analysis_stats.malicious** – number of antivirus engines that detected the file as malicious.
- **vt.metadata.analysis_stats.failure** – number of antivirus engines that failed scanning the file.
- **vt.metadata.analysis_stats.type_unsupported** – number of antivirus engines that don't support the file's type.
- **vt.metadata.submitter.country** – country from where the file was submitted. Two-letter ISO 3166, in uppercase.
- **vt.metadata.unique_sources** – number of unique sources that have submitted this file.
- **vt.metadata.times_submitted** – number of times the file has been submitted to VirusTotal.
- **vt.metadata.new_file** – True if the file has been submitted to the VirusTotal for the first time.

```
import "vt"


rule Anomalies_test {
   condition:
        vt.metadata.analysis_stats.malicious > 5 and
        vt.metadata.submitter.country == “CN” and
        vt.metadata.unique_sources == 1 and
        vt.metadata.times_submitted == 1 and
        vt.metadata.new_file and
        (vt.metadata.analysis_stats.failure > 10 or vt.metadata.analysis_stats.type_unsupported > 20)

}
```

Yara VirusTotal module

```
import "vt"

rule Colibri_Loader {
    meta:
          author = "Virustotal"
          created = "2022.04.26"
          refer =
       "https://blog.malwarebytes.com/threat-intelligence/2022/04/colibri-loader-combines-task-scheduler-and-powershell-in-clever-persistence-technique/"
          hash = "7c011de51c6d2a058d82101d314bc55b2299d89e"
          hash = "1e1af9c4475419b5c73e57a8a9938ef840e2652c"

    condition:
         for any c in vt.behaviour.http_conversations: (
               c.url contains "/securetunnel.co:" or c.url contains "/securetunnel.co/" or
            c.url contains "/trkal0.dot" or c.url contains "/vpnchecker.php"
               )

         or

         for any file_dropped in vt.behaviour.files_dropped: (
               file_dropped.path contains "\\vpnchecker[1].htm"
               )

         or
         (
               for any file_dropped in vt.behaviour.files_dropped: (
                     file_dropped.path contains "\\WIKWAFRE\\install[1].exe"
               )
               and
               vt.metadata.analysis_stats.malicious > 10
         )
}
```

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 it names suggests, it is meant to deliver and manage payloads onto infected computers.

Yara VirusTotal module

```
.method public c()V
    .registers 37

    move-object/from16 v7, p0

    const-string v8, "VVBMT0FE"

    const-string v9, "Og=="

    const-string v1, "trendsjoy.biz"

    const-string v10, "cmVzb2x2ZSBob3N0"

    const-string v11, "ZmFpbGVkIHRvIGNvbm5lY3Q="
```

Studying Donot Team

Published on 28 May 2020

APT group called Donot Team (aka APT-C-35, SectorE02) has been active since at least 2012. The attackers hunt for confidential information and intellectual property. The hackers' targets include countries in South Asia, in particular, state sector of Pakistan. In 2019, we noticed their activity in Bangladesh, Thailand, India, Sri Lanka, the Philippines, and outside of Asia, in places like Argentina, the United Arab Emirates, and Great Britain.

Yara VirusTotal module

```
.method public c()V
    .registers 37

    move-object/from16 v7, p0

    const-string v8, "VVBMT0FE"

    const-string v9, "Og=="

    const-string v1, "trendsjoy.bi

    const-string v10, "cmVzb2x2ZSE

    const-string v11, "ZmFpbGVkIHF
```

```
# virtual methods
.method public final run()V
    .registers 35

    move-object/from16 v7, p0

    const-string v8, " "

    const-string v9, "NDIzMw=="

    const-string v10, "Y2hhdC56YXF4c3djZGV2ZnJiZ3RuaHltanVraWxvcC5vbmxpbmU="

    const-string v11, "cmVzb2x2ZSBob3N0"

    const-string v12, "ZmFpbGVkIHRvIGNvbm5lY3Q="

    const-string v13, "U2tpcDo="

    const-string v14, "UTF-8"

    const-string v15, "cmNvdW50"
```

chat.zaqxswcdevfrbgtnhymjukilop[.]online

Studying Donot Team

Published on 28 May 2020

APT group called Donot Team (aka APT-C-35, SectorE02) has been active since at least 2012. The attackers hunt for confidential information and intellectual property. The hackers' targets include countries in South Asia, in particular, state sector of Pakistan. In 2019, we noticed their activity in Bangladesh, Thailand, India, Sri Lanka, the Philippines, and outside of Asia, in places like Argentina, the United Arab Emirates, and Great Britain.

Yara VirusTotal module

```
.method public c()V
    .registers 37

    move-object/from16 v7, p0

    const-string v8, "VVBMT0FE"

    const-string v9, "Og=="

    const-string v1, "trendsjoy.bi

    const-string v10, "cmVzb2x2ZSE

    const-string v11, "ZmFpbGVkIHF
```

```
# virtual methods
.method public final run()V
    .registers 35

    move-object/from16 v7, p0

    const-string v8, " "

    const-string v9, "NDIzMw=="

    const-string v10, "Y2hhdC56YXF4c3djZGV2ZnJiZ3RuaHltanVraWxvcC5vbmxpbmU="

    const-string v11, "cmVzb2x2ZSBob3N0"

    const-string v12, "ZmFpbGVkIHRvIGNvbm5lY3Q="

    const-string v13, "U2tpcDo="

    const-string v14, "UTF-8"
```

chat.zaqxswcdevfrbgtnhymjukilop[.]online

```
import "vt"

rule OrigamiElephant_c2 {
    meta:
          author = "Virustotal"
          created = "2022.04.27"
          hash = "949233b8691680db9826b1a9a21926737149f5ae"

    condition:
          for any d in vt.behaviour.dns_lookups: (
               d.hostname contains "chat.zaqxswcdevfrbgtnhymjukilop.online")
          or
          for any t in vt.behaviour.ip_traffic: (
               t.destination_ip contains "131.153.22.218")
          or
          for any text in vt.behaviour.text_decoded: (
               text == "chat.zaqxswcdevfrbgtnhymjukilop.online" or
               text == "this is agdfhgdfh key"
               )
}
```

Studying Donot Team

Published on 28 May 2020

131.153.22.218 (131.153.16.0/21)

AS 60558 (Phoenix Nap, LLC.)

Community Score

DETECTION | DETAILS | RELATIONS | COMMUNITY

Passive DNS Replication

Date resolved	Detections	Resolver	Domain
2022-04-23	1 / 89	VirusTotal	zaqxswcdevfrbgtnhymjukilop.online
2022-02-04	2 / 89	VirusTotal	chat.zaqxswcdevfrbgtnhymjukilop.online

confidential information and intellectual property. The hackers' targets include countries in South Asia, in particular, state sector of Pakistan. In 2019, we noticed their activity in Bangladesh, Thailand, India, Sri Lanka, the Philippines, and outside of Asia, in places like Argentina, the United Arab Emirates, and Great Britain.

Yara VirusTotal module

04

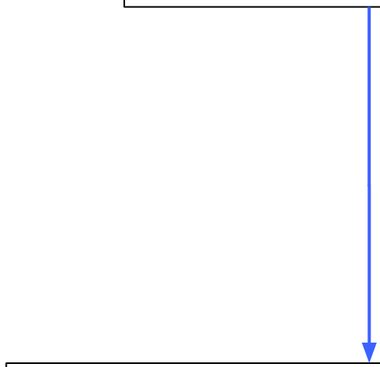
SECTION 4

Other Yara modules

Other Yara modules

- **PE** – operate with attributes and features of PE file format (header fields)
  - pe.timestamp >= 1424563200
- **Dotnet** – similar to PE but for .NET files
  - dotnet.assembly.name == "Keylogger"
- **ELF** – similar to PE but for ELF files
  - elf.number_of_sections == 1
- **Cuckoo** – integrates with Cuckoo sandbox, allows retrieving behavioural info
  - cuckoo.network.host(/192\.168\.1\.1/)
- **Magic** – simplifies magic byte checking (Linux “file” tool)
  - magic.type() contains "PDF"
- **Hash** – allows you to calculate hashes from portions of file/string
  - hash.md5(0, filesize) == "feba6c919e3797e7778e8f2e85fa033d"
- **Math** – allows you to calculate certain values from portions of your file
  - math.entropy(0, filesize) >= 7
- **Time** – epoch time, useful to implement some dynamic time-based condition
  - pe.timestamp > time.now()

```
rule ZIP_Header {
   condition:
         uint16(0) == 0x4b50
}
```



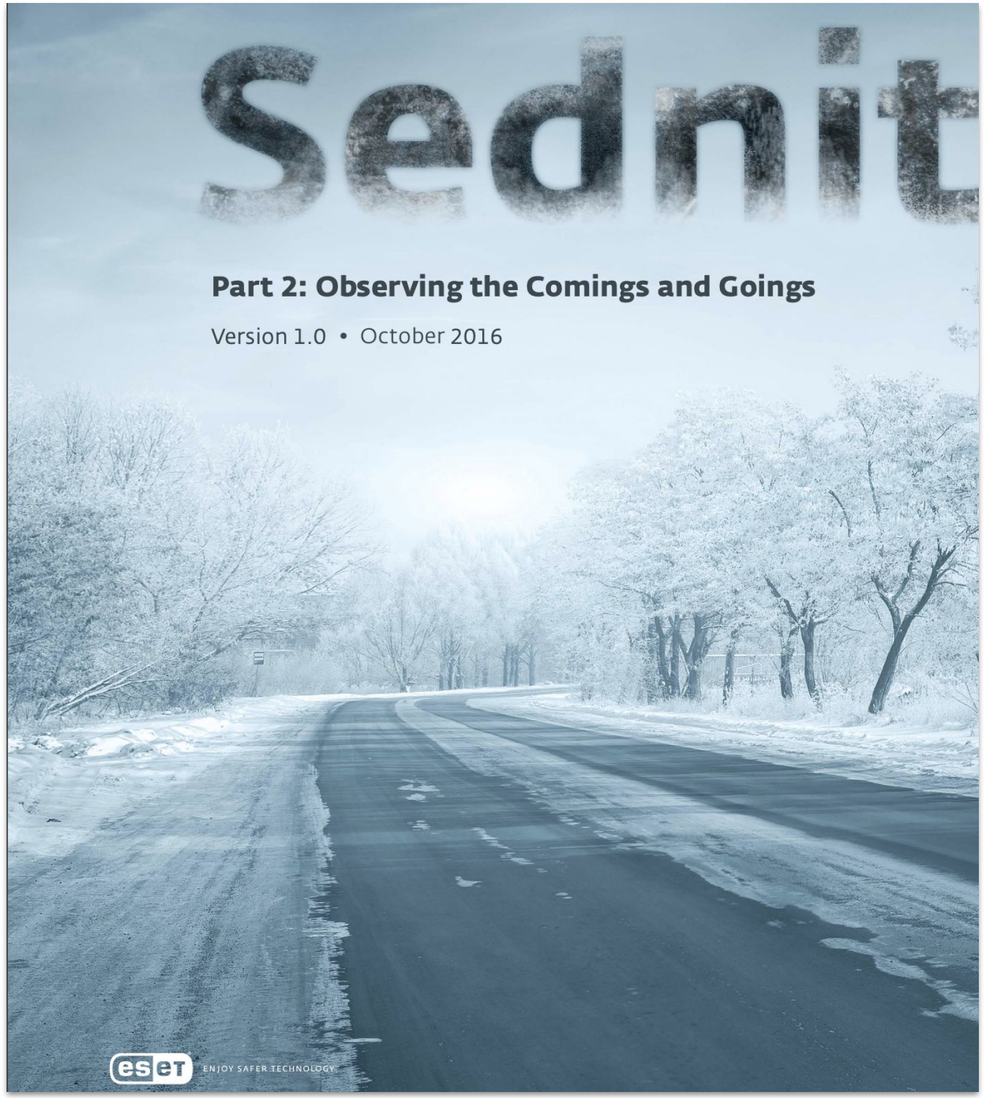
```
import "magic"

rule ZIP_Header {
   condition:
         magic.type() contains "Zip archive"
}
```

PE module

PDB Paths

```
H:\last version 23.04\UNvisible crypt version XAPS select - копия\XAPS_OBJECTIVE\
Release\XAPS_OBJECTIVE.pdb
C:\Users\User\Desktop\xaps_through_squid_default_proxy\Release\XAPS_OBJECTIVE.pdb
C:\Users\John\Documents\Новая папк\XAPS_OBJECTIVE\Release\XAPS_OBJECTIVE.pdb
E:\PROJECT\XAPS_OBJECTIVE_DLL\Release\XAPS_OBJECTIVE.pdb
```

```
import "pe"

rule Sednit_XTunnel {
   meta:
         author = "Virustotal"
         description = "Sednit attack on Bundestag in 2015"
         refer =
     "https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf"

   condition:
         pe.pdb_path contains "XAPS_OBJECTIVE"
}
```



PE module

```
import "pe"

rule SUSP_NVIDIA_LAPSUS_Leak_Compromised_Cert_Mar22_1 {
   meta:
      description = "Detects a binary signed with the leaked NVIDIA certifcate and
compiled after March 1st 2022"
      author = "Florian Roth"
      date = "2022-03-03"
      modified = "2022-03-04"
      score = 70
      reference = "https://twitter.com/cyb3rops/status/1499514240008437762"
   condition:

      uint16(0) == 0x5a4d and filesize < 100MB and

      pe.timestamp > 1646092800 and  // 2022-03-01, comment out to find all files signed
with that certificate

      for any i in (0 .. pe.number_of_signatures) : (
         pe.signatures[i].issuer contains "VeriSign Class 3 Code Signing 2010 CA" and
         (
         pe.signatures[i].serial == "43:bb:43:7d:60:98:66:28:6d:d8:39:e1:d0:03:09:f5"
         or
         pe.signatures[i].serial == "14:78:1b:c8:62:e8:dc:50:3a:55:93:46:f5:dc:c5:18"
         )
      )

}
```

NVIDIA

AWARENESS

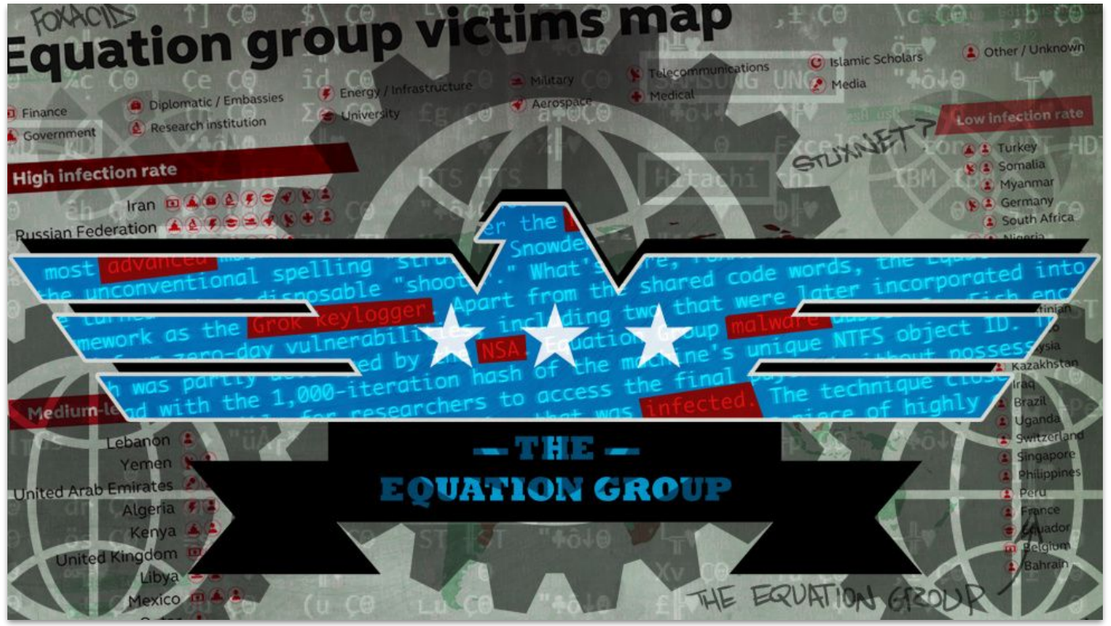
Stolen Nvidia certificates used to sign malware—here's what to do

Posted: March 15, 2022 by Pieter Arntz

As we wrote on March 3, 2022 Nvidia, was recently attacked by the LAPSUS$ ransomware group. The ensuing data leak included two of NVIDIA's code signing certificates. Those certificates are now being used to sign malware.

PE module

```
import "pe"

rule Suspicious_too_old_x64_PE {
    meta:
        author = "Kaspersky"
        description = "Rule based on TripleFantasy from Equation group"

    condition:
       (uint16(0) == 0x5A4D)
        and (pe.machine == pe.MACHINE_AMD64 or pe.machine == pe.MACHINE_IA64)
        and pe.timestamp > 631155661      // 1990-01-01
        and pe.timestamp < 1072915200     // 2004-01-01
        and filesize < 2000000
}
```



05

SECTION 5

VirusTotal Diff - Yara generator

VirusTotal Diff - what are Yara generators?

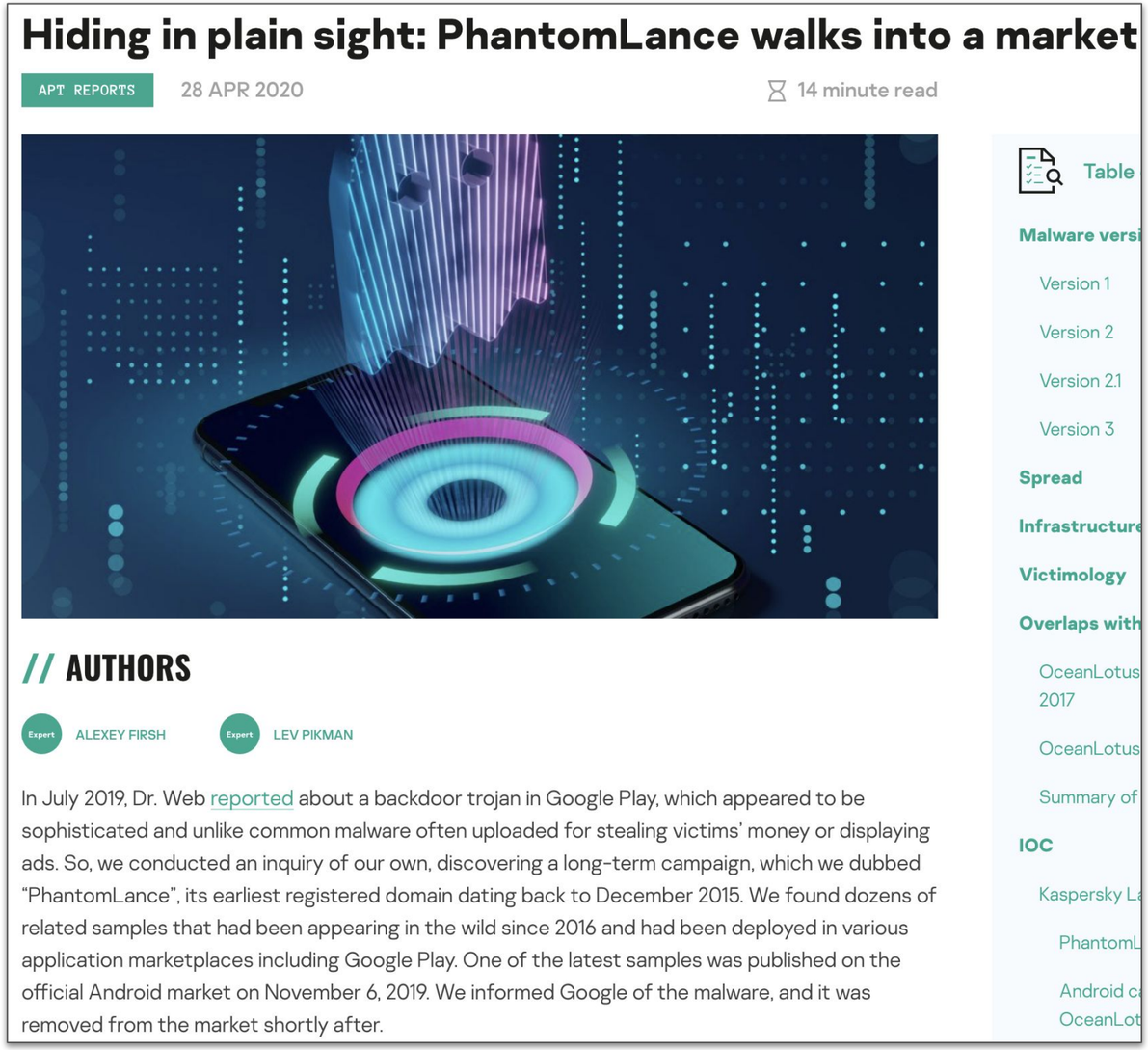
One-click tool to make Yara ruleset

- Pros:
  - Fast!
  - Quite useful to make exact detections
- Cons:
  - Need to deploy and maintain ‘clean’ collection
  - Rule quality highly depends on whitelisting quality (whitelisting ~ FP number)
  - Could be overfitting with 0 additional detects

```
REPO_URLS = {
    'good-opcodes-part1.db': 'https://www.bsk-consulting.de/yargen/good-opcodes-part1.db',
    'good-opcodes-part2.db': 'https://www.bsk-consulting.de/yargen/good-opcodes-part2.db',
    'good-opcodes-part3.db': 'https://www.bsk-consulting.de/yargen/good-opcodes-part3.db',
    'good-opcodes-part4.db': 'https://www.bsk-consulting.de/yargen/good-opcodes-part4.db',
    'good-opcodes-part5.db': 'https://www.bsk-consulting.de/yargen/good-opcodes-part5.db',
    'good-opcodes-part6.db': 'https://www.bsk-consulting.de/yargen/good-opcodes-part6.db',
    'good-opcodes-part7.db': 'https://www.bsk-consulting.de/yargen/good-opcodes-part7.db',
    'good-opcodes-part8.db': 'https://www.bsk-consulting.de/yargen/good-opcodes-part8.db',
    'good-opcodes-part9.db': 'https://www.bsk-consulting.de/yargen/good-opcodes-part9.db',

    'good-strings-part1.db': 'https://www.bsk-consulting.de/yargen/good-strings-part1.db',
    'good-strings-part2.db': 'https://www.bsk-consulting.de/yargen/good-strings-part2.db',
    'good-strings-part3.db': 'https://www.bsk-consulting.de/yargen/good-strings-part3.db',
    'good-strings-part4.db': 'https://www.bsk-consulting.de/yargen/good-strings-part4.db',
    'good-strings-part5.db': 'https://www.bsk-consulting.de/yargen/good-strings-part5.db',
    'good-strings-part6.db': 'https://www.bsk-consulting.de/yargen/good-strings-part6.db',
    'good-strings-part7.db': 'https://www.bsk-consulting.de/yargen/good-strings-part7.db',
    'good-strings-part8.db': 'https://www.bsk-consulting.de/yargen/good-strings-part8.db',
    'good-strings-part9.db': 'https://www.bsk-consulting.de/yargen/good-strings-part9.db',

    'good-exports-part1.db': 'https://www.bsk-consulting.de/yargen/good-exports-part1.db',
    'good-exports-part2.db': 'https://www.bsk-consulting.de/yargen/good-exports-part2.db',
    'good-exports-part3.db': 'https://www.bsk-consulting.de/yargen/good-exports-part3.db',
    'good-exports-part4.db': 'https://www.bsk-consulting.de/yargen/good-exports-part4.db',
    'good-exports-part5.db': 'https://www.bsk-consulting.de/yargen/good-exports-part5.db',
    'good-exports-part6.db': 'https://www.bsk-consulting.de/yargen/good-exports-part6.db',
    'good-exports-part7.db': 'https://www.bsk-consulting.de/yargen/good-exports-part7.db',
    'good-exports-part8.db': 'https://www.bsk-consulting.de/yargen/good-exports-part8.db',
    'good-exports-part9.db': 'https://www.bsk-consulting.de/yargen/good-exports-part9.db',

    'good-imphashes-part1.db': 'https://www.bsk-consulting.de/yargen/good-imphashes-part1.db',
    'good-imphashes-part2.db': 'https://www.bsk-consulting.de/yargen/good-imphashes-part2.db',
    'good-imphashes-part3.db': 'https://www.bsk-consulting.de/yargen/good-imphashes-part3.db',
    'good-imphashes-part4.db': 'https://www.bsk-consulting.de/yargen/good-imphashes-part4.db',
    'good-imphashes-part5.db': 'https://www.bsk-consulting.de/yargen/good-imphashes-part5.db',
    'good-imphashes-part6.db': 'https://www.bsk-consulting.de/yargen/good-imphashes-part6.db',
    'good-imphashes-part7.db': 'https://www.bsk-consulting.de/yargen/good-imphashes-part7.db',
    'good-imphashes-part8.db': 'https://www.bsk-consulting.de/yargen/good-imphashes-part8.db',
    'good-imphashes-part9.db': 'https://www.bsk-consulting.de/yargen/good-imphashes-part9.db',
}
```

VirusTotal Diff - [DEMO]

- Our own binary diff tool weaponized with signature generator
- Most useful while dealing with a bunch of similar samples (same malware family) to make generic signatures
- Most suitable for widely spreaded malware
- Also could be used as an effective RE tool to highlight common and unique code instead of reversing it manually in decompiler
- Provides one-click rules for Livehunt and Retrohunt
- We can instantly pivot on specific signatures to get more samples or to check for uniqueness
- Let's explore the collection of dex files from PhantomLance campaign conducted by OceanLotus group



Thank you

Alexey Firsh
@alexey_firsh

brighttalk.com/webcast/18282/573479