




VALHALLA Updates - May 2020

Changes and New Features

VALHALLA

- YARA Rule Feed
- Hand-crafted, curated high quality rules
- Five Subscribable Categories:
 - APT
 - Malware
 - Hack Tools
 - Web Shells
 - Exploits
- 10,000 Rules (+1,500 each year)
- Rich API and Python API Client
 - e.g. allows to retrieve rules usable with a YARA version that your product supports
- Comprehensive meta data and tagging (including MITRE ATT&CK tags)



The image shows a YARA rule snippet for detecting ZombieBoy malware. The rule is named `MAL_ZombieBoy_Malware_Gen_Feb19_1_RIDDC6` and is categorized as `EXE FILE MAL GEN`. The rule includes several meta fields: `description` (Detects ZombieBoy malware), `author` (Florian Roth), `reference` (a URL to an AlienVault blog), `date` (2019-02-05 15:47:31), `score` (70), `customer` (x23), `required_modules` (pe), and `minimum_yara` (3.0.0). The rule also includes a `strings` section with three strings: `$x1` (C:\Users\ZombieBoy\), `$s1` (C:\Windows\System32\sys.exe), and `$s2` (RookIE/1.0). The `condition` section is marked as `Performance Optimized` and contains a complex condition involving `uint16`, `filesize`, `pe.imphash`, and `1 of ($x*) or 2 of them`.

```

rule MAL_ZombieBoy_Malware_Gen_Feb19_1_RIDDC6 : EXE FILE MAL GEN {
  meta:
    description = "Detects ZombieBoy malware"
    author = "Florian Roth"
    reference = "https://www.alienvault.com/blogs/labs-research/zombieboy"
    date = "2019-02-05 15:47:31"
    score = 70
    customer = "x23"
    required_modules = "pe"
    minimum_yara = "3.0.0"

  strings:
    $x1 = "C:\\Users\\ZombieBoy\\" ascii
    $s1 = "C:\\Windows\\System32\\sys.exe" fullword ascii
    $s2 = "RookIE/1.0" fullword ascii

  condition:
    uint16 ( 0 ) == 0x5a4d and filesize < 200KB and (
      pe.imphash ( ) == "6a79728a09f4edda13797e5ae0ffa0f3" or
      1 of ( $x* ) or
      2 of them
    )
}
  
```

VALHALLA – Rule Info Pages

- Rule Info Pages
- Publicly Accessible
- Simple URL Scheme

https://valhalla.nextron-systems.com/info/rule/HKTL_Gen_Reflective_Loader

https://valhalla.nextron-systems.com/info/rule/HKTL_Gen_Reflective_Loader



HKTL_Gen_Reflective_Loader

Info

Statistics

Report False Positive

Rule Info

Description	Detects a reflective loader keyword
Score	60
Reference	Internal Research
Minimum Yara	1.7
Av Ratio	71.53
Rule Hash	2ebca185e5d90314bb0bd8e8076c6040
Required Modules	[]
Tags	['FILE', 'GEN', 'HKTL', 'EXE']
Name	HKTL_Gen_Reflective_Loader

VALHALLA – Rule Info Pages

- Rule Meta Data and Specifications
- References as Hyper Links
- Antivirus Verdicts (so far)

Rule Info

Description	Detects a reflective loader keyword
Score	60
Reference	Internal Research
Minimum Yara	1.7
Av Ratio	71.53
Rule Hash	2ebca185e5d90314bb0bd8e8076c6040
Required Modules	[]
Tags	['FILE', 'GEN', 'HKTL', 'EXE']
Name	HKTL_Gen_Reflective_Loader
Date	2018-11-28
Author	Florian Roth
Virustotal Matches	https://www.virustotal.com/gui/search/hkctl_gen_reflective_loader/comments

Antivirus Verdicts

Rating	Number of Samples
Malicious (>= 10 engines)	91781
Suspicious (< 10 engines)	753
Clean (0 engines)	95

VALHALLA – Rule Info Pages

- Rule Matches
- Positives (how many Antivirus engines considered that sample as malicious)
- Total (how many AV engines scanned that sample)
- Timestamp (time + date of detection)
- VT Link is a direct link to the sample on Virustotal

Rule Matches

Positives	Hash	Total	Timestamp	VT Link
30	401735913f8e1c66ae78c75bbf08bb6978531e54d0d637e1c960ce86914fca3b	73	2020-05-26 14:31:03	>
24	45f442421279d3d70be64afddc2fb1b80846c54f93e743ddc9d459bb0aa8e489	71	2020-05-26 14:25:41	>
11	d8a162b9a11d519c128a0c57bcc99310fa69cc9532cce0b790c23f73e3bff85e	73	2020-05-26 14:06:24	>
60	5db04939994cc070123537a07ada1fed9fc3561241eac3eab15c0e69109bbfc7	69	2020-05-26 12:19:06	>
35	959aa5fd274cc6cdc4db58d424e43f1c6a77297ab976586f977496b3a41fd4cb	72	2020-05-26 12:04:53	>
61	cc63a765f8a9da08d92a8e106258e7b935bf7123c8268192163bc03805376c03	73	2020-05-26 12:02:51	>
62	19cc271101549c1115167b58293beac1e2020c6a0dad200ff658a9d008acbcf5	73	2020-05-26 12:01:49	>
32	f397705af7109a2b19cb289703b1b7b3d0efdea242e1801ac1498bd49b98b9eb	71	2020-05-26 11:59:06	>
61	0cbe42f71b3cff71c587463d8f18a4df27388dedb453e06158fd66ac25a07622	72	2020-05-26 11:53:33	>
33	575cfc9dad8119843fdcc2442d4df3b317c0fbcaa9c9b7b21311f3af76229d69	72	2020-05-26 11:48:53	>
58	0188da1b90547712da0871cc9a9805f873b3505cea117434596a48b8a49e4317	70	2020-05-26 11:47:22	>
62	a60f7441781052a23955294eb4828f635fb833a8f72a8f7db133be23ac7919ca	73	2020-05-26 11:45:15	>
62	2402f3afa3036414b13529964416c6c1bb601d16b5b44a888fa8f3a88f763984	73	2020-05-26 11:43:35	>
60	d44a105829e404e244294cf79b7b35c46a0e95d77c4bef7df42b13451a51af92	72	2020-05-26 11:42:29	>
60	840d514528d3555a7c6b46770c29b9663a30e4c7b46448727a54eb1a29c7bd46	72	2020-05-26 11:41:21	>
28	70d502f08f7567601bd60a534b9d31f3bb7653187762af43c3ee5a391a8f351	70	2020-05-26 11:40:03	>

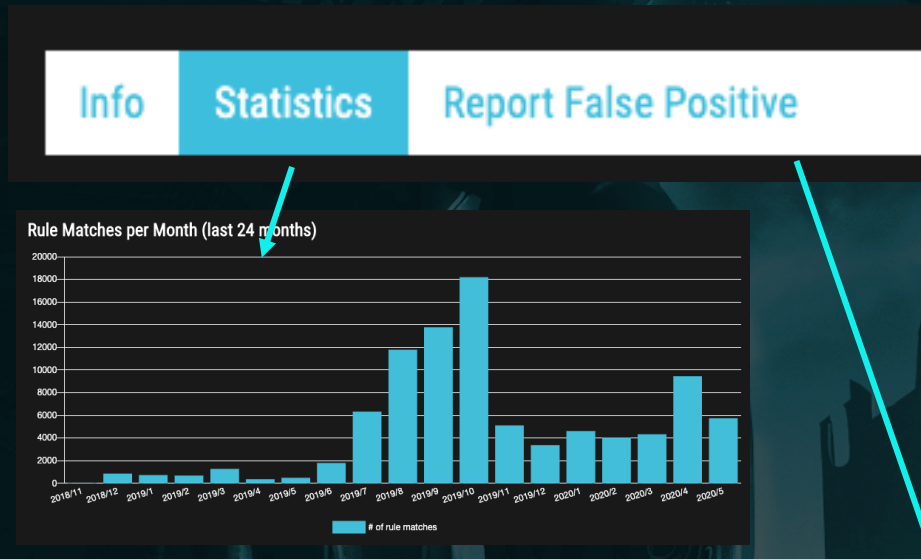
VALHALLA – Rule Info Pages

■ Statistics

- How often did the rule match in the last months?
- How did AV verdicts change over time? (not yet implemented)

■ Report False Positive

- Prefilled Email to rules@nexttron-systems.com



From:

To:

Cc:

Subject:

VALHALLA – Rule Info Pages

- Warning: Access to rule info pages is rate limited
 - Many repetitive requests lead to long-term blocks
 - Limits a rather low to allow user normal user behavior but block automatic harvesting fast
 - Slow harvesting gets also detected ☺
- Why?
 - To avoid data harvesting
 - To avoid system overload
(we have 24,000,000+ entries in our database and complex lookups)

61	08d71530d7e379944b52e1b334edeba49fc117c4d6f1757f19475254bbdc4caa	73	2020-05-09 12:13:03	>
61	015120272993d8e62f4febc2680fb761b800005beeb176707fc85fcce0a11e4f	73	2020-05-09 12:13:03	>
44	9370b594fdc625cccfde643dd160968f39b8c5ee7fb96f160e4acea9c9aa1a09	71	2020-05-09 12:13:01	>

Access to VALHALLA is rate-limited. Once you prove unworthy, access gets denied.

VALHALLA – MITRE ATT&CK Actor Tags

- Auto-Tagging
 - MITRE ATT&CK Techniques
 - NOW: also Actor Group IDs

e.g. “APT41” in rule name causes rule to be tagged with “G0096”

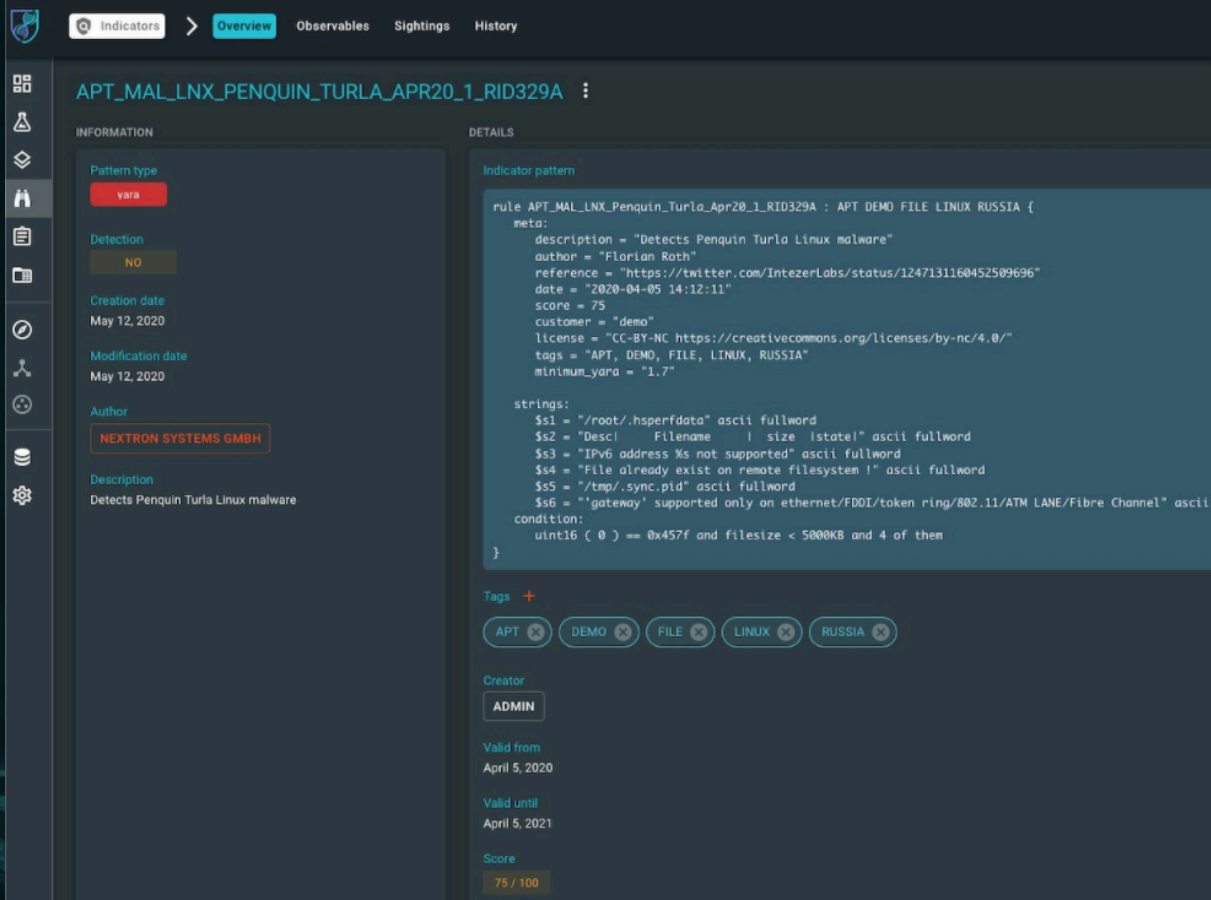
```
rule APT_APT41_CN_ELF_Speculoos_Backdoor_RID3365 : APT DEMO FILE G0096 LINUX MAL {
  meta:
    description = "Detects Speculoos Backdoor used by APT41"
    author = "Florian Roth"
    reference = "https://unit42.paloaltonetworks.com/apt41-using-new-speculoos-backdoor-to-target-organisations/"
    date = "2020-04-14 14:46:01"
    score = 90
    customer = "demo"
    license = "CC-BY-NC https://creativecommons.org/licenses/by-nc/4.0/"
    tags = "APT, DEMO, FILE, G0096, LINUX, MAL"
    minimum_yara = "1.7"

  strings:
    $xc1 = { 2F 70 72 69 76 61 74 65 2F 76 61 72 00 68 77 2E
            70 68 79 73 6D 65 6D 00 68 77 2E 75 73 65 72 6D
            65 6D 00 4E 41 2D 4E 41 2D 4E 41 2D 4E 41 2D 4E
            41 2D 4E 41 00 6C 6F 30 00 00 00 00 25 30 32 78
            2D 25 30 32 78 2D 25 30 32 78 2D 25 30 32 78 2D
            25 30 32 78 2D 25 30 32 78 0A 00 72 00 4E 41 00
            75 6E 61 6D 65 20 2D 76 }
    $s1 = "badshell" ascii fullword
    $s2 = "hw.physmem" ascii fullword
    $s3 = "uname -v" ascii fullword
    $s4 = "uname -s" ascii fullword
    $s5 = "machdep.tsc_freq" ascii fullword
    $s6 = "/usr/sbin/config.bak" ascii fullword
    $s7 = "enter MessageLoop..." ascii fullword
    $s8 = "exit StartCBProcess..." ascii fullword
    $xc1 = { 72 6D 20 2D 72 66 20 22 25 73 22 00 2F 70 72 6F
            63 2F }

  condition:
    uint16 ( 0 ) == 0x457f and filesize < 600KB and 1 of ( $x* ) or 4 of them
}
```

VALHALLA – MITRE ATT&CK Actor Tags

Example Use Case: OpenCTI Integration



The screenshot displays the VALHALLA interface for an indicator pattern. The top navigation bar includes tabs for Indicators, Overview, Observables, Sightings, and History. The left sidebar contains various icons for navigation. The main content area is divided into two panels: INFORMATION and DETAILS.

INFORMATION

- Pattern type:** vara
- Detection:** NO
- Creation date:** May 12, 2020
- Modification date:** May 12, 2020
- Author:** NEXTRON SYSTEMS GMBH
- Description:** Detects Penguin Turla Linux malware

DETAILS

Indicator pattern

```
rule APT_MAL_LNX_Penguin_Turla_Apr20_1_RID329A : APT DEMO FILE LINUX RUSSIA {
  meta:
    description = "Detects Penguin Turla Linux malware"
    author = "Florian Roth"
    reference = "https://twitter.com/IntezerLabs/status/1247131160452509696"
    date = "2020-04-05 14:12:11"
    score = 75
    customer = "demo"
    license = "CC-BY-NC https://creativecommons.org/licenses/by-nc/4.0/"
    tags = "APT, DEMO, FILE, LINUX, RUSSIA"
    minimum_yara = "1.7"

  strings:
    $s1 = "/root/.hsperfdata" ascii fullword
    $s2 = "Desc| Filename | size |state|" ascii fullword
    $s3 = "IPv6 address %s not supported" ascii fullword
    $s4 = "File already exist on remote filesystem !" ascii fullword
    $s5 = "/tmp/.sync.pid" ascii fullword
    $s6 = "'gateway' supported only on ethernet/FD0I/token ring/802.11/ATM LANE/Fibre Channel" ascii
  condition:
    uint16 ( 0 ) == 0x457f and filesize < 5000KB and 4 of them
}
```

Tags: APT, DEMO, FILE, LINUX, RUSSIA

Creator: ADMIN

Valid from: April 5, 2020

Valid until: April 5, 2021

Score: 75 / 100

VALHALLA – Status with Version Number

The feed status now contains a version number that can be used in “greater” or “less” comparisons.

It consists of the year+month+day+hour of the last change.

This allows a user to check and retrieve the feed only if a new version is available.

Status Includes Version

The status endpoint now includes a version number.

The version number is an integer value generated from the last update timestamp using a format string “%Y%m%d%H”. This way it is not just a version number that you can compare with you local last change (e.g. “>=”) but also an implicit timestamp.

You can access that endpoint via POST request (/api/v1/status) or Python API’s “`get_status()`” function.

```
Headers  JSON  Raw
1 HTTP/1.0 200 OK
2 Content-Type: application/json
3 Content-Length: 93
4 Server: Werkzeug/0.14.1 Python/3.6.7
5 Date: Tue, 12 May 2020 11:11:37 GMT
6
7 {
8   "error": "none",
9   "num_rules": 10463,
10  "status": "green",
11  "version": 2020051212
12 }
13
```