

Snort: Multiple signatures 032

By Y M via Snort-sigs

Archived: 2026-04-05 16:30:35 UTC



[Snort mailing list archives](#)

From: Y M via Snort-sigs <snort-sigs () lists snort org>

Date: Fri, 20 Sep 2019 11:12:03 +0000

Hello,

Here are some new rules with Yara/ClamAV signatures as well as PCAPs available for the majority of the

Thank you.

YM

Title: .NET binary AspireCrypt

Reference: Research

Tests: pcap

Detection:

- Yara: INDICATOR_Executable_Packed_AspireCrypt

- ClamAV: INDICATOR_Executable.Packed.AspireCrypt

Hashes:

- 176c6d49d475cfcf0723824e0b401eff33d1e2f55a07bddbdc7a47755f7c9bd1 (AgentTesla)

- 3c094942e47ddfc79c9ffa196ad2537dbce8b97841fb01e1d62fbc803e3317de (Nanocore)

- 4b9fdee9692066142596e6164dfed4ba1d860f34949fcbd2ec78471dbd05cbce (Remcos)

- 9e4035b96ff9dec31125d57a0b845cbe4fbaf057565583637601609c26a62976 (AgentTesla)

Notes: NA

```
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"INDICATOR-OBFUSCATION AspireCrypt ob
binary download attempt"; flow:to_client,established; flowbits:isset,file.exe; file_data; content:"p
AspireCrypt"; fast_pattern:only; metadata:ruleset community, service ftp-data, service http, service
pop3; classtype:misc-activity;; sid:8000694; rev:1;)
```

```
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"INDICATOR-OBFUSCATION AspireCrypt obfuscated .l
attempt"; flow:to_server,established; flowbits:isset,file.exe; file_data; content:"protected by Aspi
fast_pattern:only; metadata:ruleset community, service smtp; classtype:misc-activity; sid:8000695; r
```

```
# -----
# Title: Laturu Stealer
# Reference: Research
# Tests: pcap
# Detection:
# - Yara: MALWARE_Win_Trojan_Laturu
# - ClamAV: MALWARE_Win.Trojan.Laturu
# Hashes: ab9d492b71cb61129034b94296ae0e1bec9d2d12477c236e51ba6be372c33c15
# Notes:
# - Coincides with AveMaria.
# - OS choices also include "unknown" but was not considered in the second signature.
# - First signature maybe ignored since the follow up traffic also contains "Hwid".

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC Win.Trojan.Laturu stealer ini
connection"; flow:to_server,established; content:"Hwid."; fast_pattern:only; http_header; content:".|
content:!"Connection"; http_header; metadata:ruleset community, service http; classtype:trojan-activ
rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC Win.Trojan.Laturu stealer ini
connection"; flow:to_server,established; content:"Os: WIN_"; fast_pattern:only; http_header; content
http_header; content:"Special: "; http_header; content:"Arch: "; http_header; metadata:ruleset communi
classtype:trojan-activity; sid:8000697; rev:1;)

# -----
# Title: AsyncRAT
# Reference: Research
# Tests: pcap
# Detection:
# - Yara:
#   1. MALWARE_Win_Trojan_AsyncRAT
#   2. INDICATOR_Executable_Packed_Spices
# - ClamAV:
#   1. MALWARE_Win.Trojan.AsyncRAT
#   2. INDICATOR_Executable.Packed.Spices
# - SSL/TLS Fingerprints:
# - JA3:
#   1. 769,47-53-5-10-49171-49172-49161-49162-50-56-19-4,65281-10-11,23-24,0 --> 6734f37431670b3a1
#   2. 769,47-53-5-10-49171-49172-49161-49162-50-56-19-4,10-11-65281,23-24,0 --> 4c5c120f2e0b1bc5
# - Joy:
#   1. (0301)(002f00350005000ac013c014c009c00a0032003800130004)((ff01)(000a0006000400170018)(000b
#   2. (0301)(002f00350005000ac013c014c009c00a0032003800130004)((0000)(000a0006000400170018)(000b
# Hashes:
# - Previous Sample: ab9d492b71cb61129034b94296ae0e1bec9d2d12477c236e51ba6be372c33c15
# - Recent Sample: 2c24b6cdb05c0aceb0564f6afbfc8b22e3d6343ed3662578c0b54e01474cec57
# Notes:
# - The rule was submitted on June 04, 2019 (Multiple signatures 029) and modified, triggering on
#   the old and new sample traffic.
```

```
# - The recent sample was dropped from Discord CDN:  
# 1. Tiny executable generates .CS file containing the code responsible for downloading from Disc  
# 2. Tiny executable compiles and executes the compiled .CS code DLL.  
# 3. Compiled .CS code downloads .TXT file from Discord CDN containing a base64-encoded executabl  
#     decodes it, and then injects it.
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"MALWARE-CNC Win.Trojan.AsyncRAT variant SSL certi  
flow:to_client,established; content:"|55 04 03 0C|"; content:"AsyncRAT Server"; distance:1; fast_pat  
metadata:ruleset community, service ssl; classtype:trojan-activity; sid:8000660; rev:2;)
```

```
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"INDICATOR-OBFUSCATION Spices.Net obfi  
download attempt"; flow:to_client,established; flowbits:isset,file.exe; file_data; content:"protected  
Spices.Net Obfuscator"; fast_pattern:only; metadata:ruleset community, service ftp-data, service http  
service pop3; classtype:misc-activity;; sid:8000698; rev:1;)
```

```
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"INDICATOR-OBFUSCATION Spices.Net obfuscated .N  
attempt"; flow:to_server,established; flowbits:isset,file.exe; file_data; content:"protected by 9Ray  
Obfuscator"; fast_pattern:only; metadata:ruleset community, service smtp; classtype:misc-activity; s
```

```
# -----
```

```
# Title: HawkEye variant  
# Reference: Research  
# Tests: pcaps  
# Yara: NA  
# ClamAV: NA  
# Hashes: e4b4a93dc889952a88ac8b37561f5160ce341586cd582623abc493978dbd55a0  
# Notes: NA
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET [25,587] (msg:"MALWARE-CNC Win.Trojan.HawkEye variant outbo  
attempt"; flow:to_server,established; content:"Subject: Logger - Server Ran"; fast_pattern:only; met  
community, service smtp; classtype:trojan-activity; sid:8000710; rev:1;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET [25,587] (msg:"MALWARE-CNC Win.Trojan.HawkEye variant outbo  
attempt"; flow:to_server,established; content:"Subject: Logger|7C|"; fast_pattern:only; metadata:rule  
service smtp; classtype:trojan-activity; sid:8000711; rev:1;)
```

```
# -----
```

```
# Title: macOS MaxOfferDeal PUA  
# Reference: Research  
# Tests: pcaps  
# Yara: MALWARE_Osx_Adware_MaxOfferDeal  
# ClamAV: MALWARE_Osx.Adware.MaxOfferDeal  
# Hashes:  
# - 3066e6ea814592462257d4f5a1af431db40e6f06503e6ca2b3ea1d6b4ebff7ae  
# - 4a48fd4d27a559f5c90cc6a3fb814a34a82b8ea4f7a2aca3a2d7220d381c6d83  
# - f73a4de505c1f3689e21ce4d15e83c07ff0acd76c7ca8961bda68604cf4fc39c  
# Notes: VideoPlayer behaves differently when FireFox is installed
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC Osx.Adware.MaxOfferDearl outb  
flow:to_server,established; content:"/lion-update"; fast_pattern:only; http_uri; urilen:12; metadata  
service http; classtype:trojan-activity; sid:8000712; rev:1;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC Osx.Adware.MaxOfferDearl outb  
flow:to_server,established; content:"/squirrel-log"; fast_pattern:only; http_uri; urilen:13; metadata:  
community, service http; classtype:trojan-activity; sid:8000713; rev:1;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC Osx.Adware.MaxOfferDearl outb  
flow:to_server,established; content:"/kitten-update"; fast_pattern:only; http_uri; urilen:14; metadata:  
community, service http; classtype:trojan-activity; sid:8000714; rev:1;)
```

```
# -----
```

```
# Title: Njrat/Bladabindi variant
```

```
# Reference: Research
```

```
# Tests: pcaps
```

```
# Yara: MALWARE_Win_Trojan_Njrat
```

```
# ClamAV: MALWARE_Win.Trojan.Njrat
```

```
# Hashes:
```

```
# - 2be873726dedb8f3a26d8fb61c513c95354d9a9b47f81934670497fcdbe4e0da (AutoIt)
```

```
# - ea262b6675d2a05a8182f7d0cf63e6cb22e76457e01e0a2319086514315e24eb (AutoIt)
```

```
# - bd92dd8a37cfbf1496344e9de97039579192e1dc4b945b11e3ebc6f38587bc1f (.NET dump)
```

```
# Notes: Separator is 20201
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"MALWARE-CNC Win.Trojan.Njrat/Bladabindi variant o  
flow:to_server,established; content:"|00|ll20201"; offset:3; depth:8; fast_pattern; metadata:ruleset  
classtype:trojan-activity; sid:8000715; rev:1;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"MALWARE-CNC Win.Trojan.Njrat/Bladabindi variant o  
flow:to_server,established; content:"|00|inf20201"; offset:3; depth:9; fast_pattern; metadata:ruleset  
classtype:trojan-activity; sid:8000716; rev:1;)
```

```
-----  
Snort-sigs mailing list
```

```
Snort-sigs () lists snort.org
```

```
https://lists.snort.org/mailman/listinfo/snort-sigs
```

```
Please visit http://blog.snort.org for the latest news about Snort!
```

```
Please follow these rules: https://snort.org/faq/what-is-the-mailing-list-etiquette
```

```
Visit the Snort.org to subscribe to the official Snort ruleset, make sure to stay up to date to catch  
href=" https://snort.org/downloads/#rule-downloads";>emerging threats</a>!
```

Current thread:

- **Multiple signatures 032 Y M via Snort-sigs (Sep 20)**

Source: <https://seclists.org/snort/2019/q3/343>