

## How to stop MortAgent Malware using the snort rule ?

Published: 2020-05-07 · Archived: 2026-04-05 20:42:41 UTC

I want to stop the MortAgent malware by applying /using snort rule & also using yara rule?

How to configure this in Palo alto ?

Below are snort & Yara Rules:

1. The below SNORT rule can be used to detect the MoriAgent Beacon.

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:" MoriAgent Beacon
HTTP Request"; content:"/Index.php?i="; depth:200; content:"&t="; within:64;
content:"HTTP/1.1"; within:64; content:"Content-Type: application/json"; within:32;
content:"Content-Length: 0"; within:90; threshold:type limit,track by_src,count
1,seconds 120; sid:1000001; rev:001;)
```

2. Below are YARA rules to detect POWERSTATS.

YARA rule to detect the substitution table used in PowerShell code.

```
rule SubstitutionTable_in_PowerShell {
meta:
description = "Detect the substitution table used in PowerShell code (2019-2020)"
hash = "A18016AF1E9ACDA5963112EE8BEEB28B"
strings:
$a1 = "Replace('(', 'a'"
$a2 = "Replace(')', 'b'"
$a3 = "Replace('{', 'c'"
$a4 = "Replace('}', 'd'"
$a5 = "Replace('[', 'e'"
$a6 = "Replace(']', 'f'"
condition:
$a1 and
$a2 in (@a1..@a1+200) and
$a3 in (@a1..@a1+200) and
$a4 in (@a1..@a1+200) and
$a5 in (@a1..@a1+200) and
$a6 in (@a1..@a1+200) and
filesize < 100000
}
```

YARA rule to detect PowerStats backdoor.

```
rule POWERSTATS_JscriptLauncher {
meta:
```

```
description = "POWERSTATS Jscript Launcher"  
hash = "6C97A39A7FFC292BAF8BE1391FCE7DA0"  
strings:  
$a1 = "$s=(get-content"  
$a2 = "Get('Win32_Process').Create(cm"  
$a3 = "var cm="  
condition:  
all of them and filesize < 600  
}
```

```
YARA rule to detect PowerStats de-obfuscated  
rule POWERSTATSLite {  
meta:  
hash = "A18016AF1E9ACDA5963112EE8BEEB28B"  
strings:  
$a1 = "$global:key"  
$a2 = "$global:time"  
$a3 = "webreq = [System.Net.WebRequest]::Create($url)"  
condition:  
all of them and filesize < 3000  
}
```

```
YARA rule to detect MoriAgent implant  
rule MoriAgent {  
meta:  
description = "C++ MuddyWater implant"  
hash = "12755B210EC1171045144480ACD05AA8"  
strings:  
$f1 = "|x7d873iqq" ascii fullword  
$f2 = "ljyfiiwnskt" ascii fullword  
$f3 = "htssjhy" ascii fullword  
$f4 = "kwjffiiwnskt" ascii fullword  
$f5 = "hqtjxthpjy" ascii fullword  
$f6 = "\\XFXYfwyzu" ascii fullword  
$f7 = "\\XFHQjfszu" ascii fullword  
$f8 = "ZmilXzwmk{{Umuwz" ascii fullword  
$f9 = "^qz|}itXzw|mk|" ascii fullword  
$f10 = "_zq|mXzwmk{{Umuwz" ascii fullword  
$content = "Content-Type: application/json" ascii fullword  
condition:  
uint16(0) == 0x5A4D and filesize < 2MB and
```

```
$content and 5 of ($f*)  
}
```

YARA rule to detect PowerStats Implants

```
rule POWERSTATS_Implants  
{ meta:  
  description = "Detects all POWERSTATS implants"  
  hash = "A18016AF1E9ACDA5963112EE8BEEB28B"  
  hash = "409558610BE62655FBA0B1F93F2D9596" hash =  
  "DD32B95F865374C31A1377E31FA79E87" strings:  
  $a1 = "if ($resp -ne $null){"  
  $a2 = "out = $_.Exception.Message"  
  $a3 = "IEX $cmd -ErrorAction SilentlyContinue"  
  condition:  
  all of them and filesize < 50000  
}
```

---

Source: <https://live.paloaltonetworks.com/t5/custom-signatures/how-to-stop-mortiagent-malware-using-the-snort-rule/td-p/326590#>