0)

```
    a)  alert tcp any any -> 100.100.100.100 443 (
 msg: "Possible SYN flood targeting HTTPS server";
 flags: S;
 flow: stateless;
 detection_filter: track by_dst, count 100, seconds 1;
 classtype: attempted-dos;
 priority: 1;
 sid: 1000001;
 rev: 1;
)
```

```
    b)  alert tcp 200.200.200.200 20 -> any any (
          msg: "FTP brute force login failures detected";
          flow: to_client, established;
          content: "Login incorrect"; nocase;
          detection_filter: track by_dst, count 10, seconds 60;
          classtype: attempted-admin;
          priority: 2;
          sid: 1000002;
          rev: 1;
        )
```

```
    c)  alert udp any any -> 192.168.132.1 53 (
 msg: "DNS query for evil.com detected";
 content: "evil.com"; nocase;
 dns_query;
 classtype: misc-activity;
 priority: 3;
 sid: 1000003;
 rev: 1;
)
```

```
    d)  log tcp any any -> 185.210.37.8 666 (
 msg: "Potential EvilDodo C2 backdoor beacon (log)";
 classtype: trojan-activity;
 priority: 3;
 sid: 1000004;
 rev: 1;
)
```

```
    e)  alert tcp any any -> 185.210.37.8 666 (
  msg: "EvilDodo C2 backdoor connection detected";
  flow: to_server, established;
  content: "|45 56 49 4C|";
  offset: 0;
  depth: 10;
  classtype: malware-cnc;
  priority: 1;
  sid: 1000004;
  rev: 2;
)
```

```
    f)  alert tcp any any -> 185.210.37.8 666 (
  msg: "EvilDodo C2 backdoor with DETCEFNI observed";
  flow: to_server, established;
  content: "|45 56 49 4C|";
  offset: 0;
  depth: 10;
  content: "DETCEFNI";
  distance: 6;
  reference: url,www.cybersecuritynews.com/newevilc2malware;
  classtype: malware-cnc;
  priority: 1;
  sid: 1000004;
  rev: 3;
)
```

1)

A)
The first 5–6 alerts are all file-executable detections

119.28.70.207

145.131.10.21

B)
119.28.70.207 is registered in Hong Kong

145.131.10.21 is registered in the Netherlands

C)

[**] [1:28406:1] MALWARE-CNC Win.Trojan.Kazy variant outbound connection [**]

Win.Trojan.Kazy is a signature Snort uses for a family of Trojan downloaders/backdoors

obfuscated JavaScript payload was executed on the host

D)

[**] MALWARE-CNC Win.Trojan.Pushdo variant outbound connection

Both tools begin flagging Win.Trojan.Pushdo

Pushdo is a sophisticated Trojan downloader/backdoor that uses spam and drive by downloads to infect host systems.

213.186.33.16

OVH SAS, based in France.

A network proxy

2)

```
title: Suspicious Outlook Attachment Drop
id: 11111111-1111-1111-1111-111111111111
status: experimental
description: Detect creation of an unsigned .exe in the Temporary Internet Files\Content.Outlook folder.
author: Chase Davis
date: 04/27/2025
logsource:
  product: windows
  category: file_creation
detection:
  attachment_drop:
    TargetFilePath|contains: '\\Temporary Internet Files\\Content.Outlook\\'
    FileExtension: '.exe'
    SignatureStatus: 'Unsigned'
  condition: attachment_drop
```

—---

```
title: PowerShell Reflection Assembly Load by EvilDodo
id: 22222222-2222-2222-2222-222222222222
status: experimental
description: Detect powershell.exe using System.Reflection.Assembly launched by EvilDodo.
author: Chase Davis
date: 04/27/2025
logsource:
  product: windows
  category: process_creation
detection:
  ps_reflection:
    ProcessName: 'powershell.exe'
    CommandLine|contains: 'System.Reflection.Assembly'
    ParentProcessName: 'EvilDodo.exe'
  ps_reflection_renamed:
    ProcessName: 'powershell.exe'
    CommandLine|contains: 'System.Reflection.Assembly'
    ParentProcessOriginalName: 'EvilDodo.exe'
  condition: ps_reflection or ps_reflection_renamed
```

—--

```
title: Process Hollowing of GoogleUpdate.exe by EvilDodo
id: 33333333-3333-3333-3333-333333333333
status: experimental
description: Detect unexpected child cmd/powershell/rundll32/wscript from GoogleUpdate.exe.
author: Chase Davis
date: 04/27/2025
logsource:
  product: windows
  category: process_creation
detection:
  hollowing:
    ParentProcessName: 'GoogleUpdate.exe'
    ProcessName|in:
      - 'cmd.exe'
      - 'powershell.exe'
      - 'rundll32.exe'
      - 'wscript.exe'
  condition: hollowing
```

—--

```
title: Keylogger/Credential Dump Staging File in Music\Tmp
```

```
id: 44444444-4444-4444-4444-444444444444
status: experimental
description: Detect creation of .txt or .log in user’s Music\Tmp directory.
author: Chase Davis
date: 04/27/2025
logsource:
  product: windows
  category: file_creation
detection:
  staging_files:
    TargetFilePath|contains: '\\Music\\Tmp\\'
    FileExtension|in: ['.txt','.log']
  condition: staging_files

—---------------------------------------------------------------------------------------------------------------

title: EvilDodo C2 Heartbeat Outbound Connection
id: 55555555-5555-5555-5555-555555555555
status: experimental
description: Detect outbound connection from EvilDodo.exe to any public IP.
author: Chase Davis
date: 04/27/2025
logsource:
  product: windows
  category: network_connection
detection:
  c2_heartbeat:
    ProcessOriginalName: 'EvilDodo.exe'
    DestinationIp|re: '^((?!10\.|192\.168\.|172\.(1[6-9]|2[0-9]|3[0-1])).*)$'
  condition: c2_heartbeat

—---------------------------------------------------------------------------------------------------------------
title: EvilDodo Backdoor Inbound Shell on Port 6666
id: 66666666-6666-6666-6666-666666666666
status: experimental
description: Detect inbound shell from any public IP to local port 6666 by cmd.exe.
author: Chase Davis
date: 04/27/2025
logsource:
  product: windows
  category: network_connection
detection:
  backdoor_shell:
    ProcessName: 'cmd.exe'
    DestinationPort: 6666
    Direction: 'Inbound'
    SourceIp|re: '^((?!10\.|192\.168\.|172\.(1[6-9]|2[0-9]|3[0-1])).*)$'
  condition: backdoor_shell
```