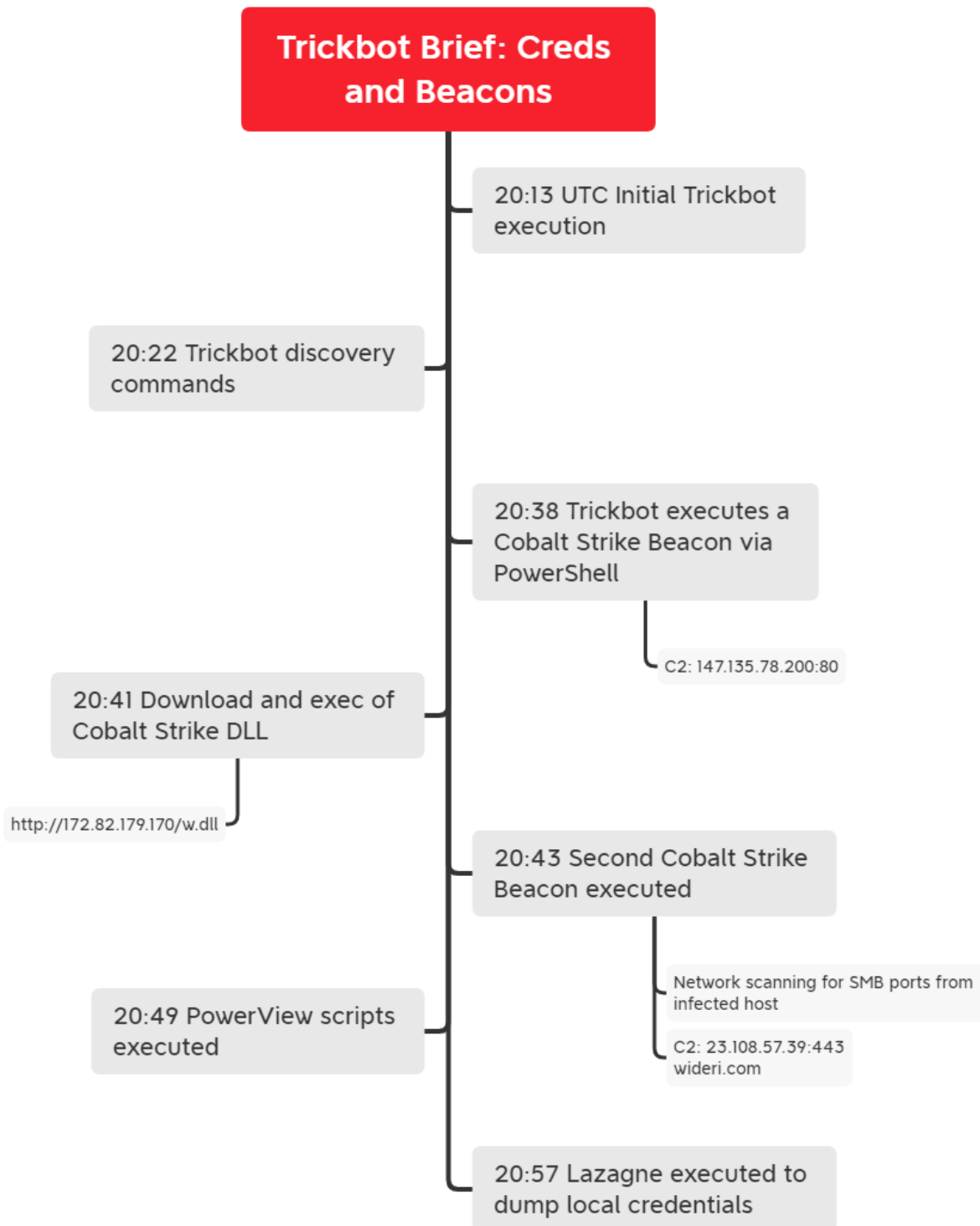


Trickbot Brief: Creds and Beacons



Intro

“TrickBot malware—first identified in 2016—is a Trojan developed and operated by a sophisticated group of cybercrime actors. The cybercrime group initially designed TrickBot as a banking trojan to steal financial data. Through continued development and new functionality, TrickBot has become a highly modular, multi-stage malware that provides its operators a full suite of tools to conduct a myriad of illegal cyber activities. Since TrickBot’s inception, the cybercrime group has used the malware to attack individuals and businesses globally across a wide range of sectors.”

Source – [Fact Sheet: TrickBot Malware Source](#)

In an intrusion this past month, threat actors were seen enumerating and collecting information related to the domain as well as dumping passwords before leaving the network. Multiple Cobalt Strike Beacons were deployed and remained connected despite the lack of activity from the threat actors.

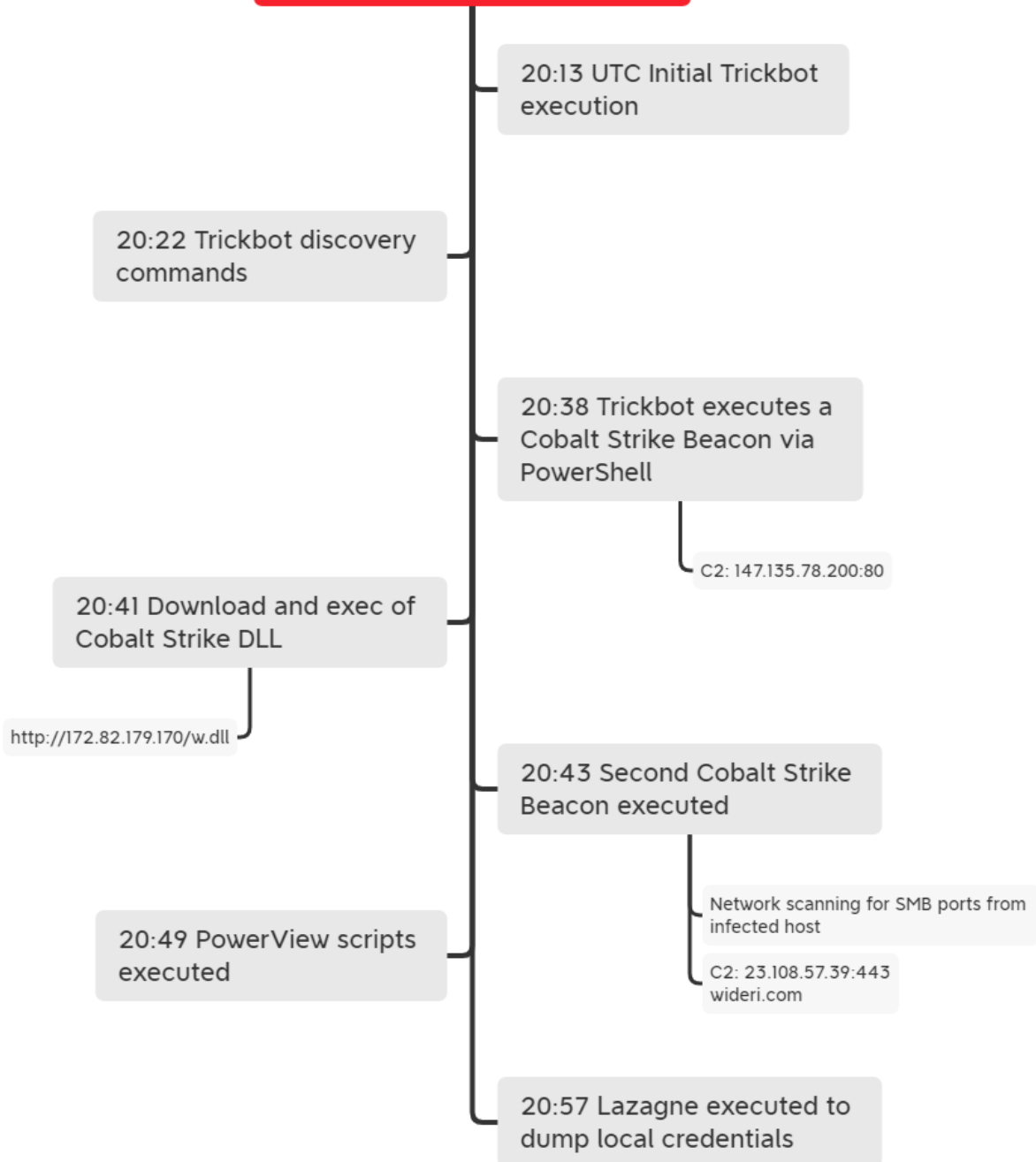
Case Summary

We assess, with moderate confidence, the Trickbot DLL that we executed was originally delivered via a malicious Office document. The threat actors were observed leveraging Trickbot and Cobalt Strike for C2 communication. They began their discovery by running net and nltest commands as well as PowerView domain discovery modules. Minutes later, [Lazagne](#) (“retrieve lots of passwords”) was executed using the “all” switch. A registry value was set to enable storing logon credentials in plaintext in memory (WDigest), likely to facilitate future activity as the host was not restarted for this change to take effect.

Before the threat actors departed the network, they successfully accessed the LSASS process and retrieved credentials from memory. No lateral movement or execution on mission was observed.

Timeline

Trickbot Brief: Creds and Beacons



Analysis and reporting completed by [@kostastsale](#), [@ICSNick](#), and [@RoxpinTeddy](#).

Reviewed by [@TheDFIRReport](#)

MITRE ATT&CK

Getting the IP and port using `sctdbg`.

```
C:\Users\user
λ sctdbg.exe /f C:\Users\user\Desktop\trick-cs.bin
Loaded 31f bytes from file C:\Users\user\Desktop\trick-cs.bin
Initialization Complete..
Max Steps: 2000000
Using base offset: 0x401000

4010a2 LoadLibraryA(wininet)
4010b0 InternetOpenA()
4010cc InternetConnectA(server: 147.135.78.200, port: 80, )

Stepcount 2000001
```

The threat actor also executed a second Cobalt Strike Beacon (`wsuC3C.tmp`) using the injected `wermgr.exe` process.

wermgr.exe	rundll32.exe	rundll32.exe C:\Users\redacted\AppData\Local\Temp\wsuC3C.tmp, ControlUnitSpeed
wermgr.exe	rundll32.exe	rundll32.exe C:\Users\redacted\AppData\Local\Temp\wsuC3C.tmp, ControlUnitSpeed

rundll32.exe C:\Users\redacted\AppData\Local\Temp\wsuC3C.tmp, ControlUnitSpeed

Persistence

A scheduled task was created to keep the Trickbot malware persistent on the system.

```

"File created:
RuleName: -
UtcTime:
ProcessGuid: {d095297e-86e2-6074-1f00-000000001700}
ProcessId: 1264
Image: C:\Windows\system32\svchost.exe
TargetFilename: C:\Windows\System32\Tasks\Windows Free Internet Download Manager 5353711913
3

```

```

Event           An unknown process process created a scheduled task 'Windows
                Free Internet Download Manager 5353711913'
Event time      ████████████████████████████████████████████████████████████
Action type     ScheduledTaskCreated
Additional      T1053.005: Scheduled Task
information
Mitre          T1053.005: Scheduled Task
Techniques
Modification    ████████████████████████████████████████████████████████████
time
Subject domain  ████████████████████████████████████████████████████████████
name
Subject logon  4874628
id
Subject user    ████████████████████████████████████████████████████████████
name
Subject user    ████████████████████████████████████████████████████████████
sid
Task name      Windows Free Internet Download Manager 5353711913
Task           C:\Windows\system32\rundll32.exe"
executables    "C:\Users\████████████████████\AppData\Roaming\DownloadMngNet53
                53711913\xxclickdr.dwn",#1

```

```

C:\Windows\system32\rundll32.exe"
"C:\Users\redacted\AppData\Roaming\DownloadMngNet5353711913\xxclickdr.dwn",#1

```

Defense Evasion

Trickbot injected into wermgr.exe processes and used this for communication to command and control infrastructure.

wermgr.exe	ConnectionFailed	182.253.184.13 0
wermgr.exe	ConnectionSuccess	81.95.45.234
wermgr.exe	ConnectionSuccess	207.231.106.13 0
wermgr.exe	ConnectionSuccess	116.203.16.95

Credential Access

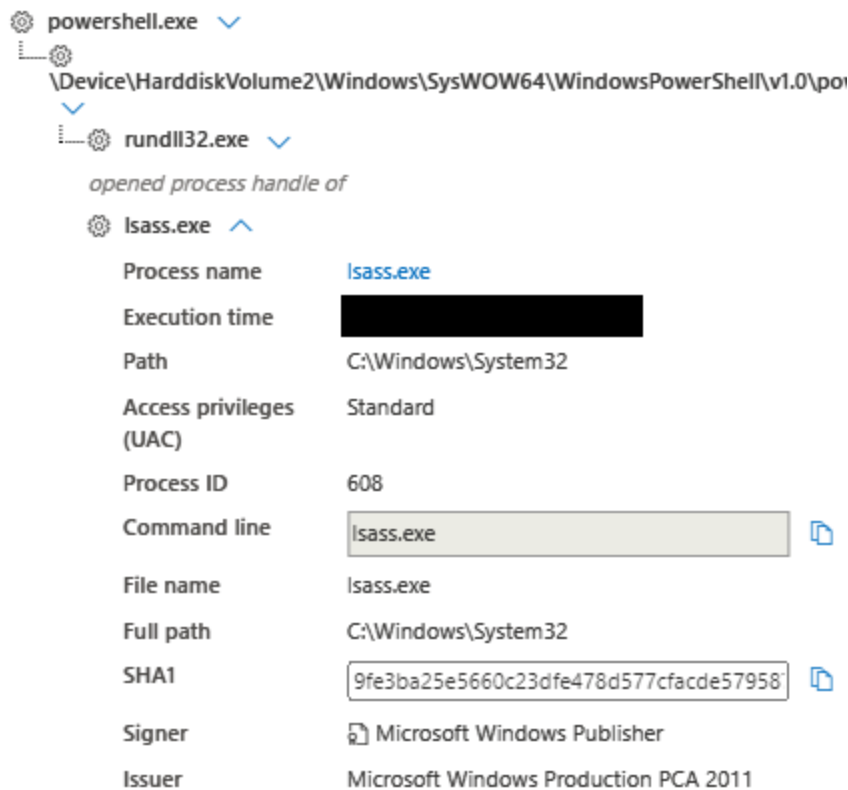
Lazagne was used with the “all” switch, which runs all modules.

Initiating Process File Name	Initiating Process Command Line	Process Command Line
powershell.exe	"powershell.exe" -Version 5.1 -s -NoLogo -NoProfile	cmd.exe /C lazagne.exe all
powershell.exe	"powershell.exe" -Version 5.1 -s -NoLogo -NoProfile	cmd.exe /C lazagne.exe all

Below we can see registry hives being saved to disk.

data.win.eventdata.parentCommandLine	data.win.eventdata.commandLine
lazagne.exe all	cmd.exe /c ^"reg.exe save hk1m\\sam c:\\users\\[REDACTED] \\appdata\\local\\temp\\skeegautwo"
lazagne.exe all	cmd.exe /c ^"reg.exe save hk1m\\system c:\\users\\[REDACTED] \\appdata\\local\\temp\\voyosno"
lazagne.exe all	cmd.exe /c ^"reg.exe save hk1m\\security c:\\users\\[REDACTED] \\appdata\\local\\temp\\oegimudfwa"

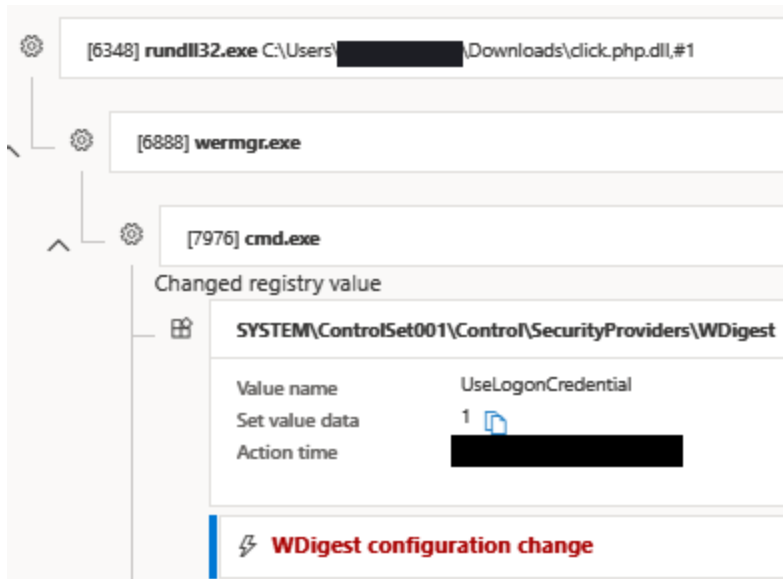
LSASS was accessed by rundll32, but we did not see anything written to disk.



powershell.exe

- \Device\HarddiskVolume2\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
 - rundll32.exe
 - opened process handle of
 - lsass.exe
 - Process name: lsass.exe
 - Execution time: [REDACTED]
 - Path: C:\Windows\System32
 - Access privileges (UAC): Standard
 - Process ID: 608
 - Command line: lsass.exe
 - File name: lsass.exe
 - Full path: C:\Windows\System32
 - SHA1: 9fe3ba25e5660c23dfe478d577cfacde57958
 - Signer: Microsoft Windows Publisher
 - Issuer: Microsoft Windows Production PCA 2011

Trickbot was used to enable the storage of clear text credentials (WDigest) by setting UseLogonCredential to 1.



Key - SYSTEM\ControlSet001\Control\SecurityProviders\WDigest
Value name - UseLogonCredential
Set value data - 1

Discovery

The following net commands were used by the threat actor from the injected Trickbot process.

```
net config workstation  
net view /all  
net view /all /domain  
net group "Domain Computers" /domain
```

The following nltest commands were used by the threat actor from the injected Trickbot process.

```
nltest /domain_trusts  
nltest /domain_trusts /all_trusts
```

PowerView modules were also used by the threat actor executed from the Cobalt Strike beacons.

```
Get-DomainSearcher  
Get-NetComputer  
Get-NetDomain
```

The local network was scanned for port 445/SMB.

Initiating Process File Name	Action Type	Remote IP	Remote Port
cmd.exe	ConnectionFailed	10.	445
cmd.exe	ConnectionSuccess	10.	445
cmd.exe	ConnectionSuccess	10.	445
cmd.exe	ConnectionSuccess	10.	445
cmd.exe	ConnectionSuccess	10.	445
cmd.exe	ConnectionSuccess	10.	445
cmd.exe	ConnectionSuccess	10.	445
cmd.exe	ConnectionSuccess	10.	445
cmd.exe	ConnectionSuccess	10.	445
cmd.exe	ConnectionSuccess	10.	445
cmd.exe	ConnectionSuccess	10.	445
cmd.exe	ConnectionSuccess	10.	445

ipconfig was used to show all IP info.

ipconfig /all

Command and Control

Trickbot

gtag: rob52

Malware Config

Extracted

Family	trickbot
Version	2000028
Botnet	rob52

C2	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>89.250.208.42:449</td><td>182.253.184.130:449</td></tr> <tr><td>31.211.85.110:443</td><td>85.112.74.178:449</td></tr> <tr><td>102.68.17.97:443</td><td>103.76.150.14:443</td></tr> <tr><td>96.9.77.142:443</td><td>91.185.236.170:449</td></tr> <tr><td>87.76.1.81:449</td><td>91.225.231.120:443</td></tr> <tr><td>62.213.14.166:443</td><td>81.95.45.234:449</td></tr> <tr><td>140.216.32.55:443</td><td>109.185.139.90:449</td></tr> <tr><td>202.166.211.197:443</td><td>196.41.57.46:449</td></tr> <tr><td>84.21.206.164:449</td><td>190.122.168.219:443</td></tr> <tr><td>77.95.93.132:449</td><td>41.77.134.250:443</td></tr> <tr><td>87.116.151.237:449</td><td>185.205.250.162:443</td></tr> <tr><td>103.9.188.23:449</td><td>78.138.187.231:443</td></tr> <tr><td>138.185.72.142:443</td><td>173.81.4.147:443</td></tr> <tr><td>31.134.124.90:443</td><td>200.90.11.177:449</td></tr> <tr><td>5.59.205.32:443</td><td></td></tr> </table> <p style="text-align: center; margin-top: 5px;">Copy all</p>	89.250.208.42:449	182.253.184.130:449	31.211.85.110:443	85.112.74.178:449	102.68.17.97:443	103.76.150.14:443	96.9.77.142:443	91.185.236.170:449	87.76.1.81:449	91.225.231.120:443	62.213.14.166:443	81.95.45.234:449	140.216.32.55:443	109.185.139.90:449	202.166.211.197:443	196.41.57.46:449	84.21.206.164:449	190.122.168.219:443	77.95.93.132:449	41.77.134.250:443	87.116.151.237:449	185.205.250.162:443	103.9.188.23:449	78.138.187.231:443	138.185.72.142:443	173.81.4.147:443	31.134.124.90:443	200.90.11.177:449	5.59.205.32:443	
89.250.208.42:449	182.253.184.130:449																														
31.211.85.110:443	85.112.74.178:449																														
102.68.17.97:443	103.76.150.14:443																														
96.9.77.142:443	91.185.236.170:449																														
87.76.1.81:449	91.225.231.120:443																														
62.213.14.166:443	81.95.45.234:449																														
140.216.32.55:443	109.185.139.90:449																														
202.166.211.197:443	196.41.57.46:449																														
84.21.206.164:449	190.122.168.219:443																														
77.95.93.132:449	41.77.134.250:443																														
87.116.151.237:449	185.205.250.162:443																														
103.9.188.23:449	78.138.187.231:443																														
138.185.72.142:443	173.81.4.147:443																														
31.134.124.90:443	200.90.11.177:449																														
5.59.205.32:443																															

Attributes	autorun Name: pwgrab
-------------------	--------------------------------

ecc_pubkey.base64 | RUNTHzAAAAAL/ZqmPBLarFg1hPotFJrZz2Zi2/EC4B3f1X8VnaOUVKndBr+jEqWc7mw4v3ADT1wp64K5Qe1LLZ27jUzXl4bwjxARPo85hv72nuedeZhRQ+ad00/gIsV869MycRzghc=

Cobalt Strike C2 #1

147.135.78[.]200:80 (Our Threat Feed service has known about this Cobalt Strike server since at least 4-4-2021)

CS Config:

```
"x64": {
  "md5": "d963ff232b5b519014cbca17e7e9d512",
  "sha256": "0f0cf5e9b35012fc51306179ba4c8cfdaa4f60bf293d8140a77a74db548182e5",
  "sha1": "77430b1da03bf6fee12d12abd810666a7751e3c0",
  "config": {
    "HTTP Method Path 2": "/submit.php",
    "Method 2": "POST",
    "C2 Server": "147.135.78.200,/cx",
    "Method 1": "GET",
    "Polling": 60000,
    "Spawn To x86": "%windir%\syswow64\rundll32.exe",
    "Beacon Type": "0 (HTTP)",
    "Spawn To x64": "%windir%\sysnative\rundll32.exe",
    "Jitter": 0,
    "Port": 80
  }
}

"x86": {
  "md5": "ec2fc2b33d60ddc829c9aeabb6ce0bbe",
  "sha256": "93008b078e8358c948877c7fde261231fc72bcd45143132070761550046701f2",
  "sha1": "91ea27632c363b821d8f84b8320b1d76f1d91899",
  "config": {
    "HTTP Method Path 2": "/submit.php",
    "Method 2": "POST",
    "C2 Server": "147.135.78.200,/push",
    "Method 1": "GET",
    "Polling": 60000,
    "Spawn To x86": "%windir%\syswow64\rundll32.exe",
    "Beacon Type": "0 (HTTP)",
    "Spawn To x64": "%windir%\sysnative\rundll32.exe",
    "Jitter": 0,
    "Port": 80
  }
}
```

Cobalt Strike C2 #2

23.108.57[.]39:443 (Our Threat Feed service has known about this Cobalt Strike server since at least 4-12-2021)

wideri[.]com

```
JA3s:ae4edc6faf64d08308082ad26be60767
JA3:a0e9f5d64349fb13191bc781f81f42e1
Certificate:[10:cd:12:74:dc:9d:3d:15:b5:e9:f1:f1:22:e1:ff:65:77:a3:c9:93]
Not Before: 2021/04/04 00:00:00
Not After: 2022/04/04 23:59:59
Issuer Org: Sectigo Limited
Subject Common: wideri.com
Public Algorithm:rsaEncryption
JARM:07d14d16d21d21d07c42d41d00041d58c7162162b6a603d3d90a2b76865b53
```

CS Config:

```
"x64": {
  "time": 1618262029857.8,
  "config": {
    "Jitter": 46,
    "Spawn To x86": "%windir%\syswow64\wusa.exe",
    "Beacon Type": "8 (HTTPS)",
    "Method 1": "GET",
    "Method 2": "POST",
    "C2 Server": "wideri.com,/tab_shop.css",
    "Spawn To x64": "%windir%\sysnative\wusa.exe",
    "Port": 443,
    "Polling": 5000,
    "HTTP Method Path 2": "/language"
  },
  "md5": "249f38615a76d47892fc530102a8a178",
  "sha256": "91d6230999853424f158fd58bd343c781fd687c71173ee39ed98429181d3cdb4",
  "sha1": "9b1f5d93af2344529b37055af8e3db0d3867c5bc"
}

"x86": {
  "time": 1618262025634.5,
  "config": {
    "Jitter": 46,
    "Spawn To x86": "%windir%\syswow64\wusa.exe",
    "Beacon Type": "8 (HTTPS)",
    "Method 1": "GET",
    "Method 2": "POST",
    "C2 Server": "wideri.com,/language.css",
    "Spawn To x64": "%windir%\sysnative\wusa.exe",
    "Port": 443,
    "Polling": 5000,
    "HTTP Method Path 2": "/sq"
  },
  "md5": "46a3380418ce59563c3adfa8f6624d3f",
  "sha256": "8cf43734e0d187aad93e950646a883820b20ca2837480c1140e1751cf6557b2",
  "sha1": "44e19c7f2534226e6774591713fbd659931d2e10"
}
```

Impact

Aside from the initial compromise on the beachhead host and the stolen credentials, no further impact was observed during this intrusion. No lateral movement or execution on mission was observed.

IOCs

Network

Cobalt Strike:

147.135.78.200|80
23.108.57.39|443
wideri[.]com
http://172.82.179.170/w.dll

Trickbot:

102.68.17.97|443
103.76.150.14|443
103.9.188.23|449
109.185.139.90|449
138.185.72.142|443
148.216.32.55|443
173.81.4.147|443
182.253.184.130|449
185.205.250.162|443
190.122.168.219|443
196.41.57.46|449
200.90.11.177|449
202.166.211.197|443
31.134.124.90|443
31.211.85.110|443
41.77.134.250|443
5.59.205.32|443
62.213.14.166|443
77.95.93.132|449
78.138.187.231|443
81.95.45.234|449
84.21.206.164|449
85.112.74.178|449
87.116.151.237|449
87.76.1.81|449
89.250.208.42|449
91.185.236.170|449
91.225.231.120|443
96.9.77.142|443

File

click.php.dll
8c0d352934271350cfe6c00b7587e8dc8d062817
0ae86e5abbc09e96f8c1155556ca6598c22aebd73acbba8d59f2ce702d3115f8

xxclickdr.dwn
8c0d352934271350cfe6c00b7587e8dc8d062817
0ae86e5abbc09e96f8c1155556ca6598c22aebd73acbba8d59f2ce702d3115f8

wsuC3C.tmp
b7d9f3e387021bba138dbe3d153fef4e7e2196ad
97dedd5ca85a13ab1a8910416b13ffd088b1c7e3486d6629a71f5c118d56fba

lazagne.exe
75f4115024b5d0818f0696345eef98d92db92118
61deb3a206cc203252418b431f6556e3f7efd9556fc685eeda7281d9baf89851

Detections

Network

ET CNC Feodo Tracker Reported CnC Server group 11
ET MALWARE Trickbot Checkin Response
ET INFO SUSPICIOUS Dotted Quad Host MZ Response

Sigma

https://github.com/SigmaHQ/sigma/blob/084cd39505861188d9d8f2d5c0f2835e4f750a3f/rules/windows/process_creation/win_malware_trickbot_recon_activity.yml

https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/process_creation/win_grabbing_sensitive_hives_via_reg.yml

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_enc_cmd.yml

Yara

```

/*
YARA Rule Set
Author: The DFIR Report
Date: 2021-04-27
Identifier: Case 3521 Trickbot
Reference: https://thedfirreport.com
*/

/* Rule Set ----- */

import "pe"

rule click_php {
meta:
description = "files - file click.php.dll"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-04-27"
hash1 = "0ae86e5abbc09e96f8c1155556ca6598c22aebd73acbba8d59f2ce702d3115f8"
strings:
$s1 = "f_+ (Q" fullword wide
$s2 = "'/l-;2m" fullword wide
$s3 = "y'L])[" fullword wide
$s4 = "1!1I1m1s1" fullword ascii
$s5 = "&+B\"wm" fullword wide
$s6 = ">jWR=C" fullword wide
$s7 = "W!\\R.S" fullword wide
$s8 = "r-`4?b6" fullword wide
$s9 = "]Iip!x" fullword wide
$s10 = "!k{l`<" fullword wide
$s11 = "D-C:RA" fullword wide
$s12 = "]T-as" fullword wide
$s13 = "7%8+8^8" fullword ascii
$s14 = "f]-hKa" fullword wide
$s15 = "StartW" fullword ascii /* Goodware String - occurred 5 times */
condition:
uint16(0) == 0x5a4d and filesize < 1000KB and
( pe.imphash() == "8948fb754b7c37bc4119606e044f204c" and pe.exports("StartW") or 10
of them )
}

```

MITRE

User Execution – T1204
Command and Scripting Interpreter – T1059
PowerShell – T1059.001
Windows Command Shell – T1059.003
Domain Trust Discovery – T1482
Network Service Scanning – T1046
Remote System Discovery – T1018
System Network Configuration Discovery – T1016
System Information Discovery – T1082

Process Injection – T1055
Credentials from Web Browsers – T1555.003
OS Credential Dumping – T1003
LSASS Memory – T1003.001
Exfiltration Over C2 Channel – T1041
Non-Standard Port – T1571

Internal case #3521