Статья LockBit: программа-вымогатель ставит серверы под прицел

xss.is/threads/71888

LockBit: программа-вымогатель ставит серверы под прицел

Аффилированные лица LockBit используют серверы для распространения программ-вымогателей по сетям.

Symantec, подразделение Broadcom Software, наблюдала, как злоумышленники нацеливались на серверы, чтобы распространять программы-вымогателя LockBit по скомпрометированным сетям.

В одной атаке, наблюдаемой Symantec, LockBit идентифицировал информацию, относящуюся к домену, создавал групповую политику для горизонтального перемещения и выполнял команду "gpupdate /force" на всех системах в одном домене, что принудительно обновляло групповую политику.

ЛокБит

LockBit — это программа-вымогатель как услуга (RaaS), управляемая злоумышленниками, которых Symantec отслеживает как Syrphid.

Вскоре после первого появления в сентябре 2019 года банда Syrphid расширила свою деятельность, используя сеть аффилированных лиц для развертывания программы-вымогателя LockBit в сетях жертв.

Программа-вымогатель, которая в настоящее время достигла версии 3.0, эволюционировала за последние несколько лет, как и ее операторы, которые недавно запустили программу вознаграждения за обнаружение ошибок, чтобы отсеять слабые места в коде вредоносного ПО и работе RaaS в целом.

Цепочка атак

В одном наблюдаемом случае, прежде чем дропнуть и запустить программу-вымогатель LockBit, злоумышленник имел RDP-доступ к корпоративной сети как минимум на пару недель. Этот доступ мог быть получен через приложения удаленного рабочего стола, такие как AnyDesk или Windows RDP, или путем использования известной уязвимости и т. д.

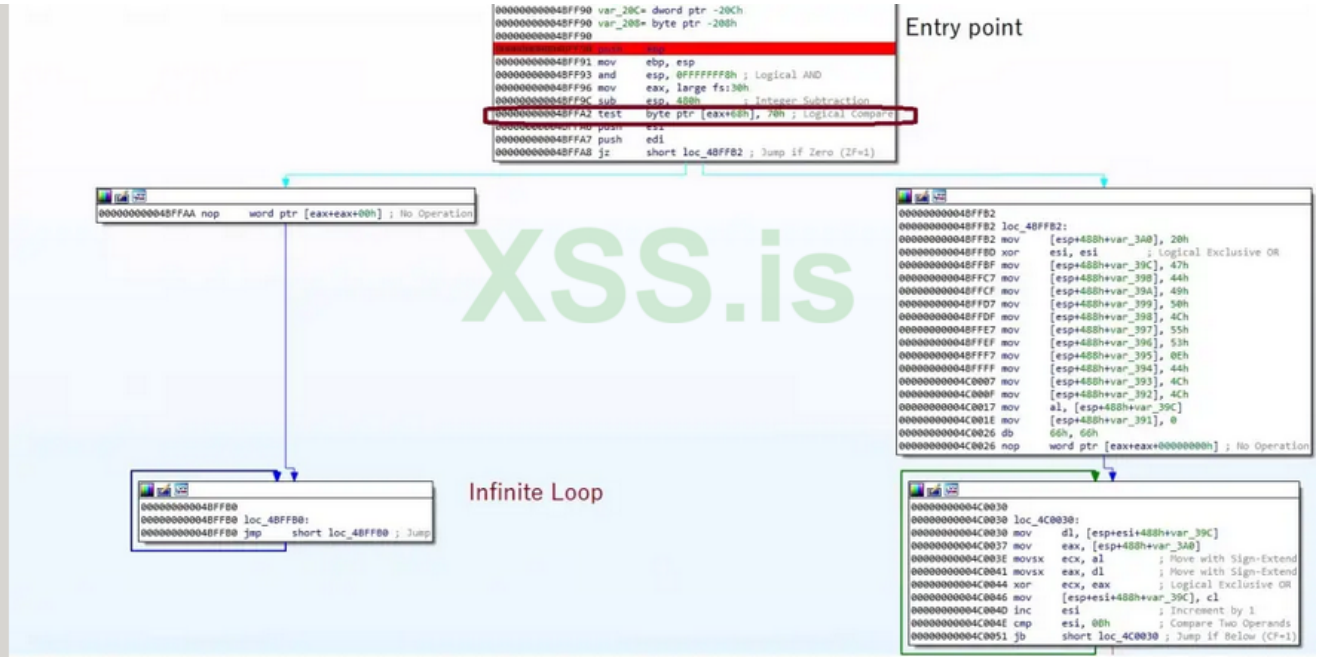
LockBit ведет себя на серверах с контроллерами домена иначе, чем на компьютерах с Windows 10. При выполнении на сервере он может распространяться по сети с помощью групповой политики. На компьютерах с Windows 10 он выполняет обычную

активность программ-вымогателей и шифрует файлы.

Когда LockBit выполняется на сервере, он выполняет следующие действия:

1. Проверка отладчика

LockBit сначала проверяет, отлаживается ли вредоносный процесс. Если это так, то он входит в бесконечный цикл.



2. Проверка языка

- Он вызывает GetSystemDefaultUILanguage и GetUserDefaultUILanguage для проверки языка.
- Если язык совпадает с языком в списке вредоносных программ, то он немедленно завершается.
- LockBit не нацелен на Россию и некоторые близлежащие страны.

3. Завершение запущенных процессов и отключение служб

- LockBit завершает список запущенных процессов, связанных с анализом вредоносных программ и других процессов, таких как Process Explorer, Process Monitor, Wireshark, Dumpcap, Process Hacker, cmd.exe, TeamViewer, Notepad, Notepad++, WordPad и т. д.

- Отключает список служб, связанных с SQL, резервным копированием, MSExchange и т. д.

4. Повышение привилегий

- Дублирует токен, вызывая DuplicateTokenEx, и создает новый процесс, используя CreateProcessAsUserW.

- После повышения привилегий LockBit перезапускается под DLLHost.exe. Как только новый процесс создан, процесс LockBit завершается.

5. Обход UAC

- LockBit внедряет код в dllhost.exe с CLSID COM-объектов, который запускает следующую команду для обхода UAC:

A. Использование USERENV.dll для обхода UAC

C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}

B. Метод обхода в UACME hfirefox

C:\Windows\SysWOW64\DllHost.exe /Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}

Эксплуатация COM-интерфейса с повышенными привилегиями ICMLuaUtil

C:\Windows\SysWOW64\DllHost.exe /Processid:{D2E7041B-2927-42FB-8E9F-7CE93B6DC937}

7. Создание групповой политики:

- Как только вредоносная программа определяет, что она работает от имени администратора и в системе установлен контроллер домена, она создает групповую политику для остановки служб, завершения процессов и копирования LockBit и т. д.

- В папке C:\Windows\SYSVOL\domain\Policies\<policy GUID> LockBit создает XML-файлы, необходимые для групповой политики.

Конфигурации компьютера:

- Сначала создается политика для отключения Защитника Windows, подавления всех уведомлений, отключения отправки файлов, отключения защиты в реальном времени и т. д.

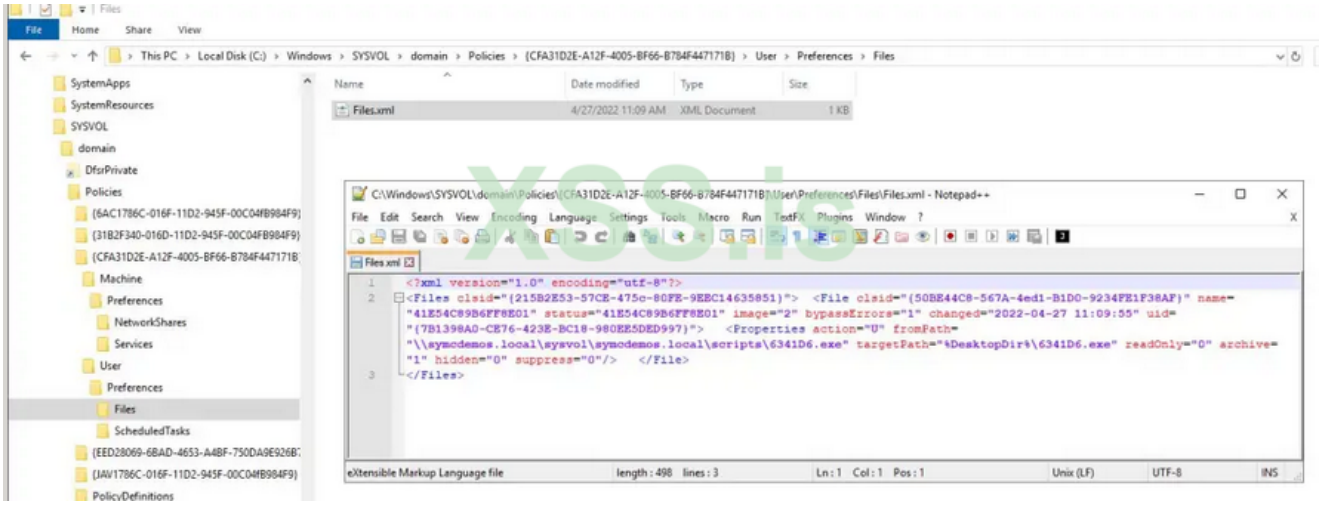
- Затем она сопоставляет сетевой диск через групповую политику.

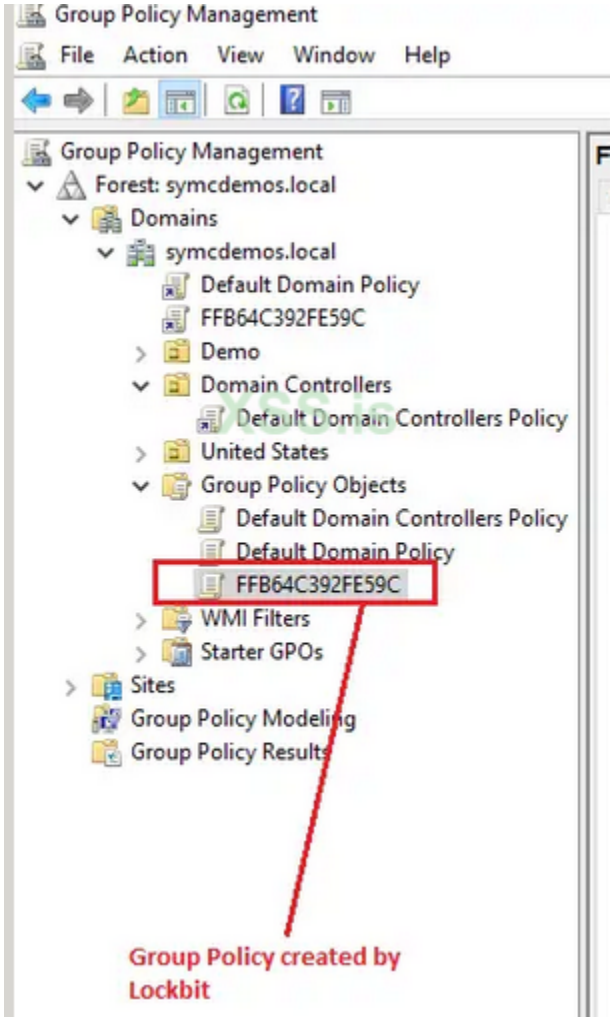
- Отключает службы, связанные с SQL-сервером при запуске.

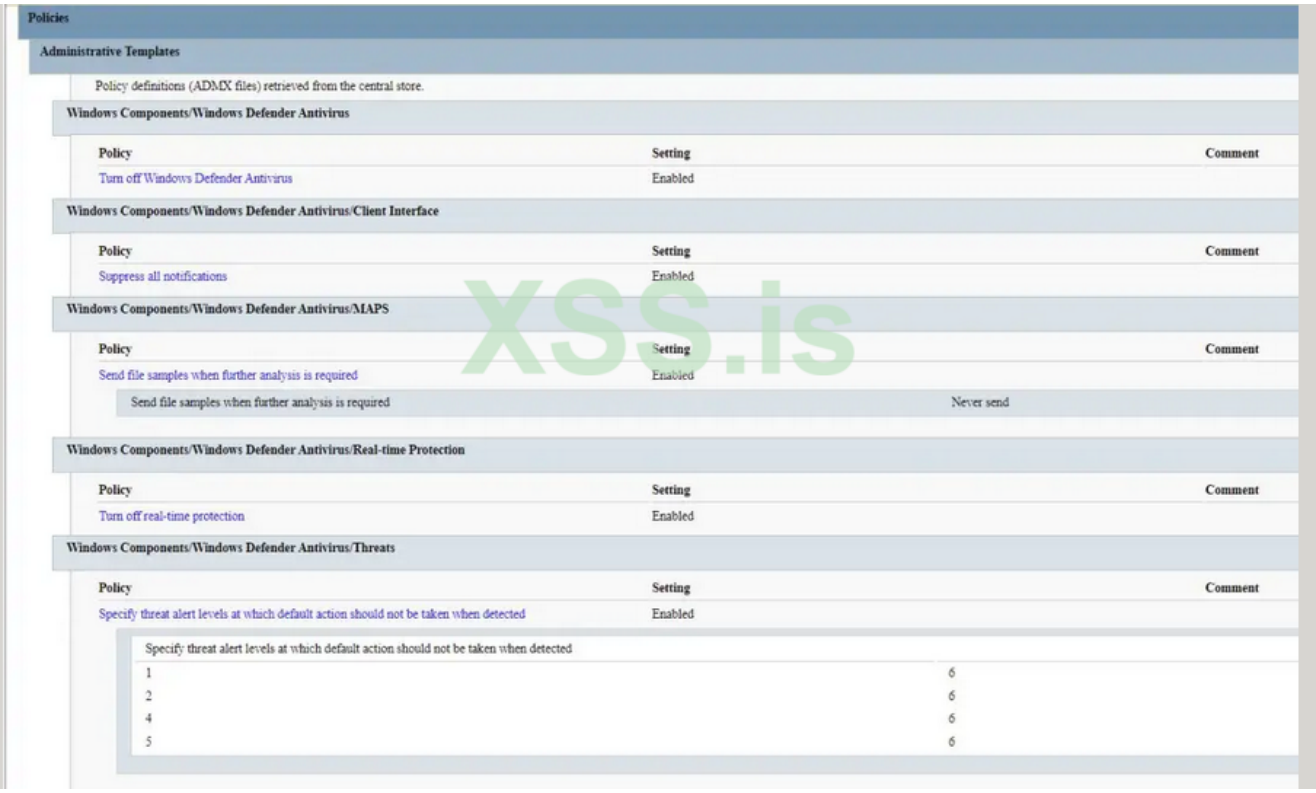
Конфигурации пользователя:

- Вредоносная программа копирует программу-вымогатель из SYSVOL в каталог Desktop.

- Затем вымогатель создает запланированную задачу, чтобы завершить список процессов, упомянутых ранее.


This PC > Local Disk (C:) > Windows > SYSVOL > domain > Policies > {CFA31D2E-A12F-4005-BF66-B784F447171B} > User > Preferences > Files
SystemApps
SystemResources
SYSVOL
domain
DfsrPrivate
Policies
Machine
Preferences
NetworkShares
Services
User
Preferences
Files
ScheduledTasks
PolicyDefinitions
Files.xml
4/27/2022 11:09 AM
XML Document
1 KB
C:\Windows\SYSVOL\domain\Policies\{CFA31D2E-A12F-4005-BF66-B784F447171B}\User\Preferences\Files\Files.xml - Notepad++
<?xml version="1.0" encoding="utf-8"?>
<Files clsid="{215B2E53-57CE-475c-80FE-9EEC14635851}"> <File clsid="{50BE44C8-567A-4ed1-B1D0-9234FE1F38AF}" name="
"41E54C89B6FF8E01" status="41E54C89B6FF8E01" image="2" bypassErrors="1" changed="2022-04-27 11:09:55" uid=
"{7B1398A0-CE76-423E-BC18-980EE5DED997}"> <Properties action="U" fromPath=
"\\symcdemos.local\sysvol\symcdemos.local\scripts\6341D6.exe" targetPath="%DesktopDir%\6341D6.exe" readOnly="0" archive=
"1" hidden="0" suppress="0"/> </File>
</Files>
eXtensible Markup Language file
length : 498 lines : 3
Ln : 1 Col : 1 Pos : 1
Unix (LF)
UTF-8
INS


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: symcdemos.local
Domains
symcdemos.local
Default Domain Policy
FFB64C392FE59C
Demo
Domain Controllers
Default Domain Controllers Policy
United States
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
FFB64C392FE59C
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy created by Lockbit



8. Боковое передвижение:

LockBit запускает powershell.exe для выполнения команды, показанной ниже, для поиска по всем компьютерам в Active Directory. Для каждого хоста используется команда GPUpdate force (gpupdate) для применения вновь созданной групповой политики.

powershell.exe. exe -Command "Get-ADComputer -filter * -Searchbase 'DC=symcdemos,DC=local' | foreach{ Invoke-GPUpdate -computer $_.name -force -RandomDelayInMinutes 0}"

9. Выполняет команду gpupdate на контроллере домена, на котором работает LockBit. Также запускает gpupdate для запуска политик из конфигураций компьютеров и пользовательских конфигураций.

gpupdate.exe /target:computer /force
gpupdate.exe /target:user /force

10. Брандмауэр

LockBit считывает правила брандмауэра с помощью брандмауэра Защитника Windows с объектом FwPolicy2 API расширенной безопасности. Вызывается следующий COM-объект CLSID:

C:\Windows\system32\DllHost.exe /Processid:{E2B3C97F-6AE1-41AC-817A-F6F92166D7DD}

11. Воздействие

LockBit пытается удалить теневые копии с помощью VSSADMIN и WMIC. Он также пытается отключить восстановление с помощью команды BCDEdit.

"C:\Windows\System32\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no

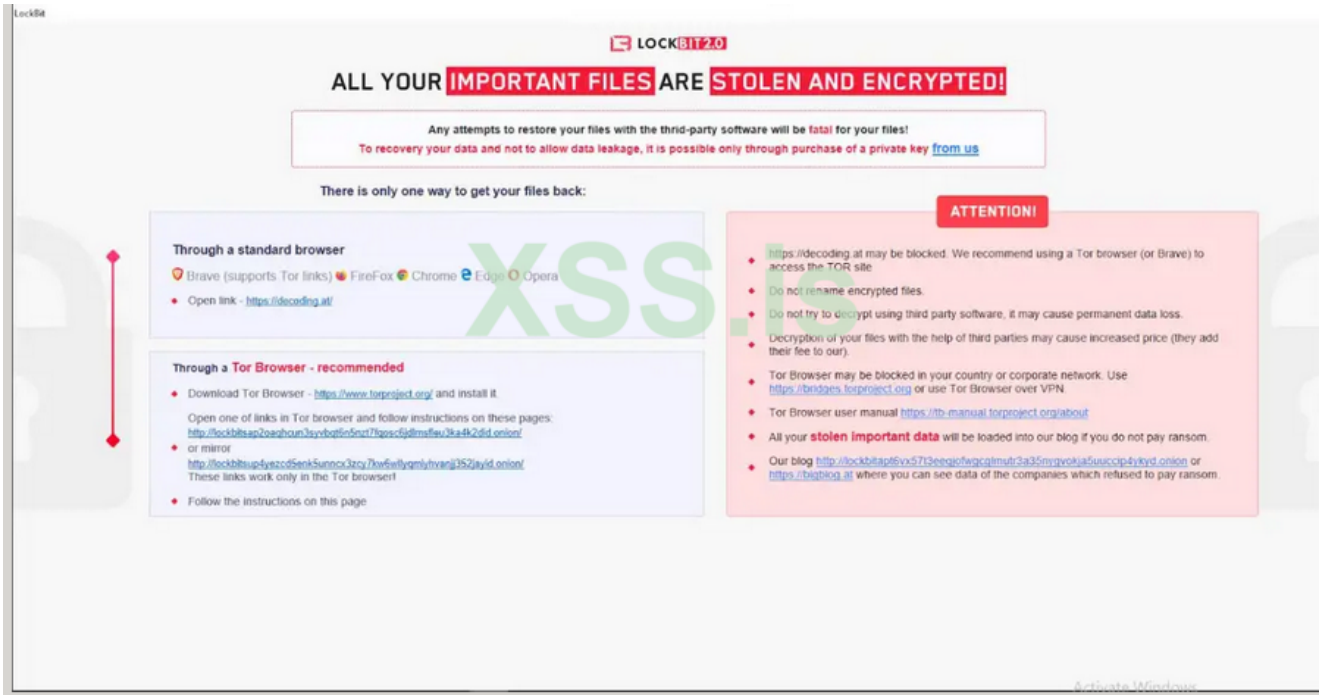
Удаляет журналы событий Windows, используя:

wevtutil cl security
wevtutil cl system
wevtutil cl application

12. Шифрует файлы и добавляет к ним расширение .lockbit.

13. MSHTA.exe

Создает файл lockbit.hta и запускает его для отображения примечания о выкупе.



LockBit была одной из, если не самой активной бандой RaaS в 2022 году. Падение активности Conti в мае помогло LockBit выйти на первое место, при этом в некоторых отчетах говорится, что эта угроза стоит за 40% атак программ-вымогателей.

Успех LockBit также обусловлен тем, что его разработчики и партнеры продолжают развивать функции и тактику, включая высокую скорость шифрования вредоносного ПО, способность нацеливаться как на машины Windows, так и на Linux, его дерзкие кампании по набору персонала и высококлассные цели. Кроме того, как упоминалось ранее, запуск программы вознаграждений за уязвимости в коде LockBit и за предложения по улучшению работы RaaS, несомненно, поможет программам-вымогателям оставаться серьезной угрозой для организаций.