Новые целевые атаки RTM

securelist.ru/new-targeted-attacks-rtm/100720/

Исследование

Исследование

03 Мар 2021

мин. на чтение

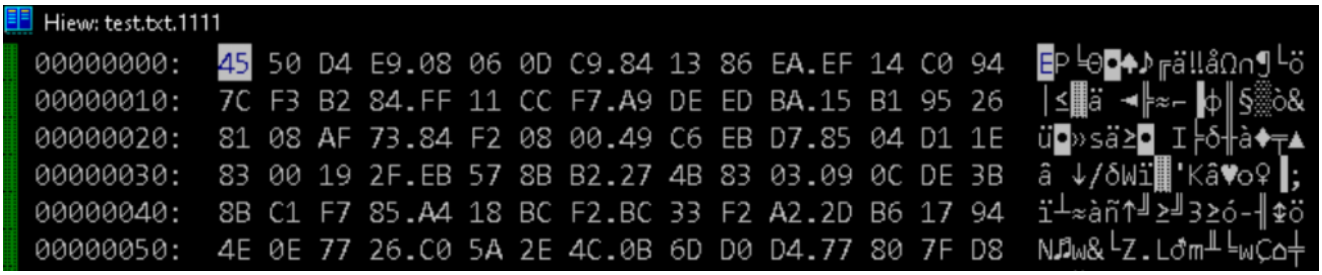
Авторы

Expert Сергей Голованов

Мы обнаружили новую вредоносную кампанию, за которой стоит русскоговорящая группировка RTM. Ее активная фаза началась в декабре 2020 года и продолжается до сих пор. Целью злоумышленников были деньги, однако в этот раз они не ограничились установкой банкера Trojan-Banker.Win32.RTM и подменой банковских реквизитов – в ход также пошли шифровальщик и шантаж. Нам известно о примерно десяти жертвах среди российских организаций из сфер транспорта и финансов.

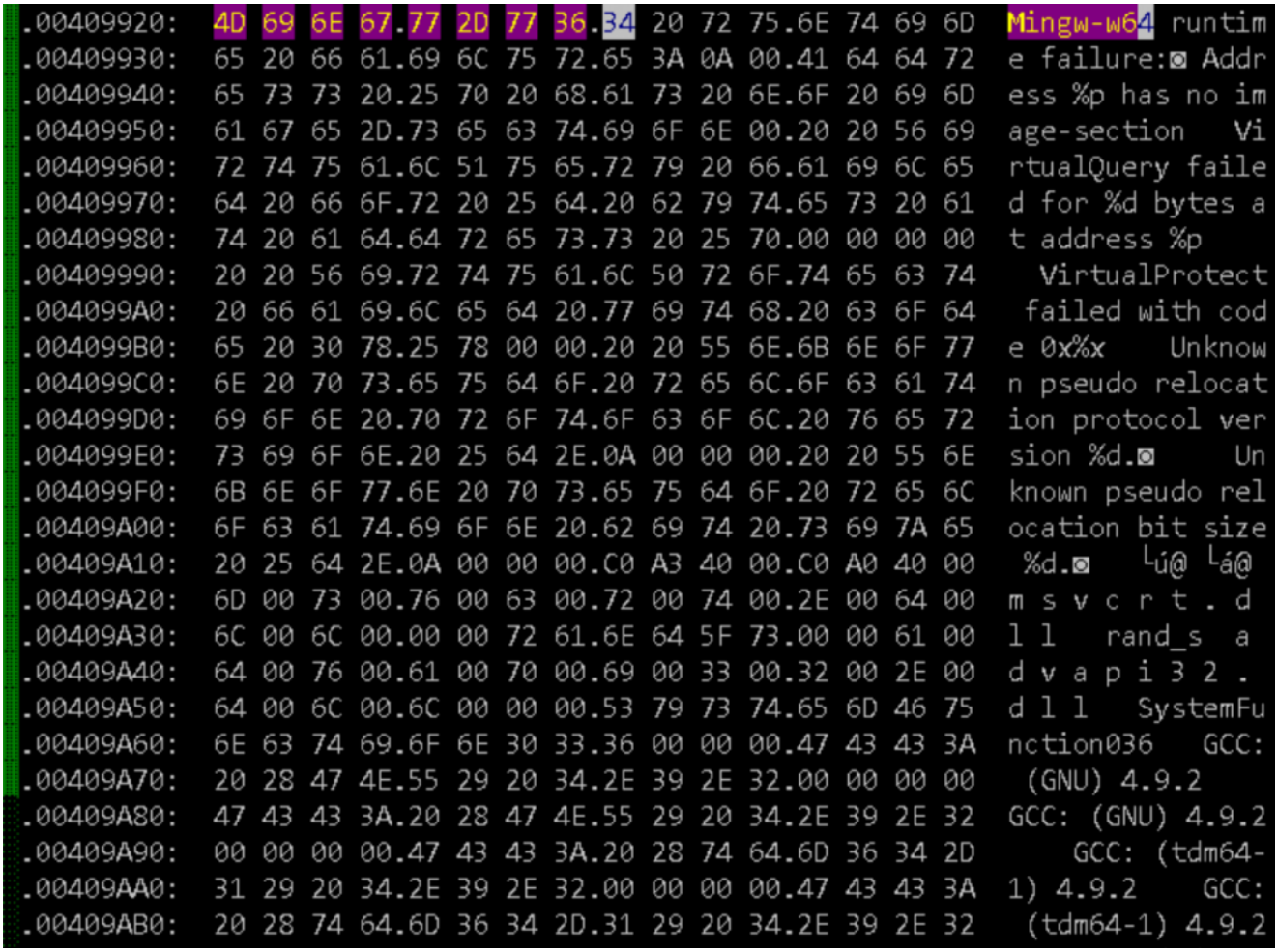
Подготовительная фаза кампании началась еще в середине 2019 года, когда ряд организаций получили фишинговые письма с «корпоративными» заголовками: «Повестка в суд», «Заявка на возврат», «Закрывающие документы» или «Копии документов за прошлый месяц». Текст письма был кратким, и для получения подробной информации требовалось открыть приложенный файл. Если получатель выполнял требование, на его компьютер устанавливалось вредоносное ПО – Trojan-Banker.Win32.RTM. Для последующего закрепления в системе и продвижения внутри локальной сети организации злоумышленники использовали легитимные программы для удаленного доступа, такие как LiteManager и RMS, а также несколько самодельных вредоносных утилит небольшого размера. Основной задачей злоумышленников был поиск компьютеров, принадлежащих сотрудникам бухгалтерии, и вмешательство в работу установленной системы дистанционного банковского обслуживания (ДБО), в частности, подмена реквизитов во время проведения финансовых операций.

Но если раньше неудачное вмешательство в работу ДБО останавливало злоумышленников (или вынуждало предпринимать новые и новые попытки), то в рамках обнаруженной кампании они подготовили запасной план, и не один. Если банкер RTM не справлялся с работой, в дело вступала другая вредоносная программа – ранее неизвестный нам троянец, получивший впоследствии вердикт Trojan-Ransom.Win32.Quoter. Он шифровал содержимое всех компьютеров, до которых киберпреступники успели дотянуться, и оставлял сообщение с требованием выкупа. К этому времени с момента закрепления RTM в сети организации проходило несколько месяцев.



Пример зашифрованного файла, новое расширение — .1111

Шифровальщик мы назвали Quoter, т.к. в код зашифрованных файлов он добавлял цитаты из популярных кинофильмов. Для работы зловред использует алгоритм AES-256 CBC.



```
.00409920:  4D 69 6E 67.77 2D 77 36.34 20 72 75.6E 74 69 6D  Mingw-w64 runtim
.00409930:  65 20 66 61.69 6C 75 72.65 3A 0A 00.41 64 64 72  e failure:◙ Addr
.00409940:  65 73 73 20.25 70 20 68.61 73 20 6E.6F 20 69 6D  ess %p has no im
.00409950:  61 67 65 2D.73 65 63 74.69 6F 6E 00.20 20 56 69  age-section   Vi
.00409960:  72 74 75 61.6C 51 75 65.72 79 20 66.61 69 6C 65  rtualQuery faile
.00409970:  64 20 66 6F.72 20 25 64.20 62 79 74.65 73 20 61  d for %d bytes a
.00409980:  74 20 61 64.64 72 65 73.73 20 25 70.00 00 00 00  t address %p
.00409990:  20 20 56 69.72 74 75 61.6C 50 72 6F.74 65 63 74    VirtualProtect
.004099A0:  20 66 61 69.6C 65 64 20.77 69 74 68.20 63 6F 64   failed with cod
.004099B0:  65 20 30 78.25 78 00 00.20 20 55 6E.6B 6E 6F 77  e 0x%x    Unknow
.004099C0:  6E 20 70 73.65 75 64 6F.20 72 65 6C.6F 63 61 74  n pseudo relocat
.004099D0:  69 6F 6E 20.70 72 6F 74.6F 63 6F 6C.20 76 65 72  ion protocol ver
.004099E0:  73 69 6F 6E.20 25 64 2E.0A 00 00 00.20 20 55 6E  sion %d.◙     Un
.004099F0:  6B 6E 6F 77.6E 20 70 73.65 75 64 6F.20 72 65 6C  known pseudo rel
.00409A00:  6F 63 61 74.69 6F 6E 20.62 69 74 20.73 69 7A 65  ocation bit size
.00409A10:  20 25 64 2E.0A 00 00 00.C0 A3 40 00.C0 A0 40 00   %d.◙   └ú@ └á@
.00409A20:  6D 00 73 00.76 00 63 00.72 00 74 00.2E 00 64 00  m s v c r t . d
.00409A30:  6C 00 6C 00.00 00 72 61.6E 64 5F 73.00 00 61 00  l l   rand_s  a
.00409A40:  64 00 76 00.61 00 70 00.69 00 33 00.32 00 2E 00  d v a p i 3 2 .
.00409A50:  64 00 6C 00.6C 00 00 00.53 79 73 74.65 6D 46 75  d l l   SystemFu
.00409A60:  6E 63 74 69.6F 6E 30 33.36 00 00 00.47 43 43 3A  nction036   GCC:
.00409A70:  20 28 47 4E.55 29 20 34.2E 39 2E 32.00 00 00 00   (GNU) 4.9.2
.00409A80:  47 43 43 3A.20 28 47 4E.55 29 20 34.2E 39 2E 32  GCC: (GNU) 4.9.2
.00409A90:  00 00 00 00.47 43 43 3A.20 28 74 64.6D 36 34 2D      GCC: (tdm64-
.00409AA0:  31 29 20 34.2E 39 2E 32.00 00 00 00.47 43 43 3A  1) 4.9.2    GCC:
.00409AB0:  20 28 74 64.6D 36 34 2D.31 29 20 34.2E 39 2E 32   (tdm64-1) 4.9.2
```

Фрагмент кода троянца Trojan-Ransom.Win32.Quoter

Если же и запасной план не срабатывал по тем или иным причинам, то спустя пару недель злоумышленники переходили к шантажу. Жертва получала сообщение, что ее данные были украдены и их возвращение обойдется буквально в миллион долларов (естественно, в биткоинах). В случае неуплаты вымогатели угрожали выложить конфиденциальную информацию в интернет для свободного скачивания. На размышление отводилось несколько дней.

Примечательным в этой истории является не только переход стоящей за RTM группировки на нетипичные для нее методы «заработка» и инструменты – вымогательство и доксинг вполне укладываются в тренды последних лет. Необычно, что злоумышленники атакуют организации в России, хотя, как правило, шифровальщики используются в целевых атаках на организации из других стран.

IoC

589ab3de15696b51e77b8923d1ed7e40 — Trojan-Ransom.Win32.Quoter

Авторы

Expert Сергей Голованов

Новые целевые атаки RTM

Ваш e-mail не будет опубликован. Обязательные поля помечены *

Подпишитесь на еженедельную рассылку

Самая актуальная аналитика – в вашем почтовом ящике

-
-
-
-

Отчеты

Lazarus распространяет протрояненный DeFi-кошелек

Недавно мы обнаружили протрояненное DeFi-приложение, которое имплантирует в систему полнофункциональный бэкдор. Проанализировав этот бэкдора, мы обнаружили многочисленные совпадения с другими инструментами группы Lazarus.

MoonBounce: скрытая угроза в UEFI

В конце 2021 года мы обнаружили прошивку UEFI, в которую был внедрен вредоносный код, названный нами MoonBounce. В данном отчете мы подробно опишем принцип действия импланта MoonBounce и его связь с APT41.

PuzzleMaker атакует, используя цепочку эксплойтов нулевого дня под Chrome

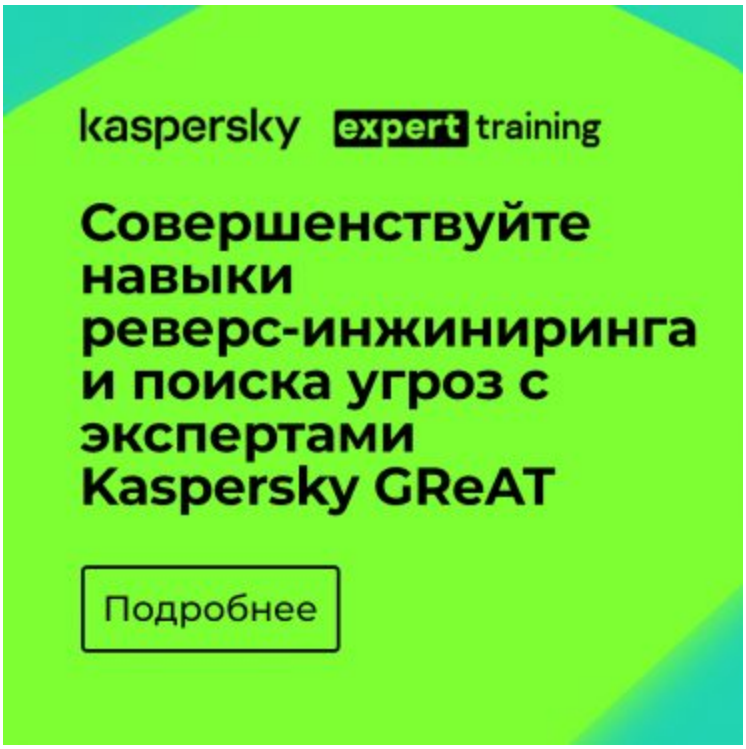
Мы зафиксировали волну целевых атак, для осуществления которых использовалась цепочка эксплойтов нулевого дня для Google Chrome и Microsoft Windows.

Lazarus атакует оборонную промышленность с помощью ThreatNeedle

В 2020 году мы обнаружили, что группировка Lazarus запустила атаки на оборонную промышленность с использованием вредоносных программ ThreatNeedle, относящихся к кластеру вредоносного ПО Manuscrypt (также известен как NukeSped).

Подпишитесь на еженедельную рассылку

Самая актуальная аналитика – в вашем почтовом ящике



Подпишитесь на еженедельную рассылку

Самая актуальная аналитика – в вашем почтовом ящике