# Ryuk

Ransomware

## Ryukoм не трогали! Разбираем новую версию шифровальщика Ryuk

Автор: Kaspersky Lab Дата: 8 Фев 2019 Просмотров: 1 Комментариев: 0

Ryuk ransomware, как VB-шифровщик и ЗОЛОТ ограничивал ЖЕРТ начиная. Тот, кто ранее не сталкивался с ним, может подумать, что это очередная версия Ryuk, но дьявол, что называется, в детали. Мы изучили, модифицировали, без ложной скромности, и теперь рассказываем, как Ryuk теперь шифрует файлы, что в нем изменилось и почему, а также как расшифровать файлы, если у вас стоит старая версия.

Ryuk — ransomware-вымогатель, который пишет в любой с целью ясно и цифровые данные, а потом требует за ключ для расшифровки вымогательство в биткоин. Ему нравится шифровать не только отдельные компьютеры, но и целые сети, поэтому он часто используется в атаках на крупные компании. Ранее мы уже писали о Ryuk, а также о его ближайшем родственнике Hermes, который, в отличие от Ryuk, не ограничивается вымогательством, а еще и воровал пароли.

Ryuk — ransomware-вымогатель, который пишет в любой с целью ясно и цифровые данные, а потом требует за ключ для расшифровки вымогательство в биткоин. Ему нравится шифровать не только отдельные компьютеры, но и целые сети, поэтому он часто используется в атаках на крупные компании. Ранее мы уже писали о Ryuk, а также о его ближайшем родственнике Hermes, который, в отличие от Ryuk, не ограничивается вымогательством, а еще и воровал пароли.

Ранее мы уже рассказывали, как Ryuk шифровал файлы, а также как расшифровать файлы, если у вас стоит старая версия. Но с момента последнего обзора в семействе Ryuk произошло немало изменений, поэтому мы решили рассмотреть, что же изменилось в новой версии Ryuk, что осталось прежним и как расшифровать файлы, если у вас стоит старая версия.

### Содержание статьи

1. Общая информация
2. Исполнение
3. Сообщение о выкупе
4. Сообщение о выкупе
5. Конфигурация и ключ шифрования
6. Генерация ключа шифрования и ключей
7. Перебор процессов
8. Перебор сервисов
9. Перебор файлов
10. Расширения шифруемых файлов
11. Остановка сетевых ресурсов, общих ресурсов, сервисов
12. Удаление теневых копий
13. Шифрование
14. Расширение
15. Задание пароля
16. Дистанционная включение RDP
17. Последовательный перебор процессов сетевых папок
18. Рассылка сообщений (WM)
19. Шифрование
20. Заключение

### ОБЩАЯ ИНФОРМАЦИЯ

Ryuk — ransomware, который использовался вымогателями против известных компаний. Как правило, перед тем, как начать атаку, вымогатели собирают учетные данные, а потом уже запускают Ryuk.

| Имя | Ryuk |
|---|---|
| Платформа | Win32 (только 32-битная версия) |
| Язык | Компилируется на Visual Studio 2010 |

Основные признаки шифрования Ryuk: файлы не шифруются, расширения файлов не меняются, в каждом шифруемом файле есть сообщение о выкупе.

### ИСПОЛНЕНИЕ

Ryuk поставлен в виде исходного текста, компилируется вымогателями и запускается на каждом компьютере вручную. Для запуска вымогатели используют Cobalt Strike, Empire, Metasploit и другие инструменты для удаленного управления компьютером.

Для компиляции на каждом компьютере используется msbuild.exe, файлы для компиляции — .sln, .vcxproj, .vcxproj.filters, .vcxproj.user, .bat, .exe, .dll, .tlog, .log, .pdb, .ipch, .obj, .lnk, .exe.

```
C:\Windows\Microsoft.Net\Framework\v4.0.30319\msbuild.exe
```

Ryuk использует для компиляции msbuild.exe из .Net Framework 4.0.