F6 зафиксировала вредоносные рассылки кибергруппы CapFIX / Хабр

habr.com/ru/companies/F6/articles/966072

EditorF6 November 13, 2025

Мины, тренинги, криптография: F6 зафиксировала вредоносные рассылки кибергруппы CapFIX

6 мин

356
Блог компании F6Информационная безопасность *
Аналитика

Аналитики **Центра кибербезопасности** и **Threat Intelligence** компании **F6** обнаружили новую кампанию вредоносных рассылок. Злоумышленники направляют письма под видом инструкций по действиям при минной угрозе и требования предоставить отчетность по противодействию информационным атакам. Кампания по распространению бэкдора CapDoor нацелена на ритейлеров, коллекторские агентства, микрофинансовые учреждения, страховые компании. Специалисты F6 присвоили группе имя **CapFIX**. Техники злоумышленников из **CapFIX** и индикаторы компрометации приведены в статье далее.

11.11.2025 системой F6 MXDR была заблокирована вредоносная рассылка, целями которой стали минимум следующие организации:

- коллекторское агентство;
- финансовое учреждение;
- страховая компания.

Злоумышленники рассылали письмо, используя спуфинг почты российского турагентства. Характеристики письма:

Тема: СРОЧНО: Ознакомление с инструкцией по действиям при минной угрозе.

Рис. 1 – Скриншот письма

Вложение: Инструкция_минная_угроза_ВСУ_10.11.2025.pdf. При открытии вложение выглядит таким образом, что побуждает жертву скачать программный комплекс КриптоПро для корректного отображения. Содержимое PDF-файла представлено на Рис. 2 ниже.

Рис. 2 – Содержимое PDF-файла

Но ссылка на самом деле ведет не на легитимный ресурс, а на домен, зарегистрированный злоумышленниками. При переходе по ссылке (hxxps://sed-documents[.]com/DpoxjDMaJdmnUVUBMexTyTqBcVBiUOIz/iJOoTzsPbgIooVzxYHbfcMEvtcrQprho/%D0%9F%D0%B0%D0%BA%D0%B5%
на устройство жертвы будет загружаться защищенный паролем архив с именем «Пакет установки КриптоПРО.rar». Пароль представлен в начальном файле-вложении письма: «криптопро2025».

Рис. 3 – Загрузка вредоносного архива «Пакет установки КриптоПРО.rar»

Архив, в свою очередь, содержит вредоносный MSI-файл «Пакет установки КриптоПРО.msi». Этот MSI-файл распаковывает CAB-файл, устанавливает приложение VB Decompiler Lite. Из распакованного содержимого CAB-архива запускает файл architect-stats.exe — это легитимный файл, подписанный цифровой подписью, который используется для загрузки ВПО с помощью техники DLL Side-Loading.

Во время выполнения создает файл-маркер запуска C:\ProgramData\lockfile, чтобы предотвратить повторный запуск — такой файл ранее использовался в бэкдоре CapDoor.

> CapDoor — бэкдор, обнаруженный в 2025 году в ходе исследования атаки с использованием вредоносной капчи (ClickFIX). В ходе взаимодействия с C2 бэкдор получает указание на исполнение следующих команд:
>
> - запуск PowerShell-команды — запускает команду *%WINDIR%\System32\WindowsPowerShell\v1.0\powershell.exe -NoLogo -NoProfile* с перенаправлением ввода и вывода для получения возможности управления интерпретатором команд, отправляет в поток ввода указанную сервером команду, завершает процесс отправкой команды \r\nexit\r\n;
> - загрузка и запуск EXE — загружает с указанного сервером узла EXE-файл, сохраняет в каталоге %Temp% под случайным именем, исполняет файл функцией ShellExecuteW;
> - загрузка и запуск DLL — загружает с указанного сервером узла DLL-файл, сохраняет в каталоге %Temp% под случайным именем, исполняет файл командой *%WINDIR%\System32\rundll32.exe %Temp%\%FNAME%,%ARGNAME%*. C2 указывает, с каким аргументом запускать файл;
> - загрузка и запуск DLL COM-объекта — загружает с указанного сервером узла DLL-файл, сохраняет в каталоге %Temp% под случайным именем, исполняет файл командой *%WINDIR%\System32\regsvr32.exe %Temp%\%FNAME%*.

Финальная нагрузка представляет собой модифицированную версию бэкдора CapDoor для x64-архитектуры. В качестве C2 используется: hxxp://213.165.61.133/search/?text=[a-z]{30}.

12 и 13 ноября злоумышленники провели повторную рассылку — системой F6 MXDR были заблокированы еще несколько писем, направленных в рамках этой же кампании в адрес сетевого ритейлера и фин. организаций. Характеристики писем:

Темы:

- СРОЧНО: Требуется предоставить отчетность по прохождению тренинга по противодействию информационным атакам. Срок — 24 часа.
- ОБЯЗАТЕЛЬНО К ОЗНАКОМЛЕНИЮ: Инструкция ФСБ по действиям при терактах, совершаемых вооружёнными формированиями Украины

Вложения:

- Перечень_документов_для_отчета_по_тренингу_ИБ_ФСБ ([0-9]{1,2}).pdf
- Методические_рекомендации_ФСБ_по_организации_безопасности_при _террористической_угрозе ([0-9]{1,2}).pdf

На этот раз злоумышленники проводили рассылки с адреса российской IT-компании. При открытии вложения пользователю, как и в предыдущей рассылке, отображается кнопка для корректного отображения через «КриптоПро». Ссылка и дальнейшая цепочка файлов идентичны рассылке от 11.11.2025.

Домен sed-documents[.]com, с которого на начальных этапах на машину жертвы загружается архив, был зарегистрирован 24 сентября 2025 года. Этот домен имеет такие же регистрационные данные, как и созвучный домен, зарегистрированный 3 сентября 2025, documents-sed[.]com. Этот домен также использовался злоумышленниками в ходе атак, но, предположительно, в более ранний период.

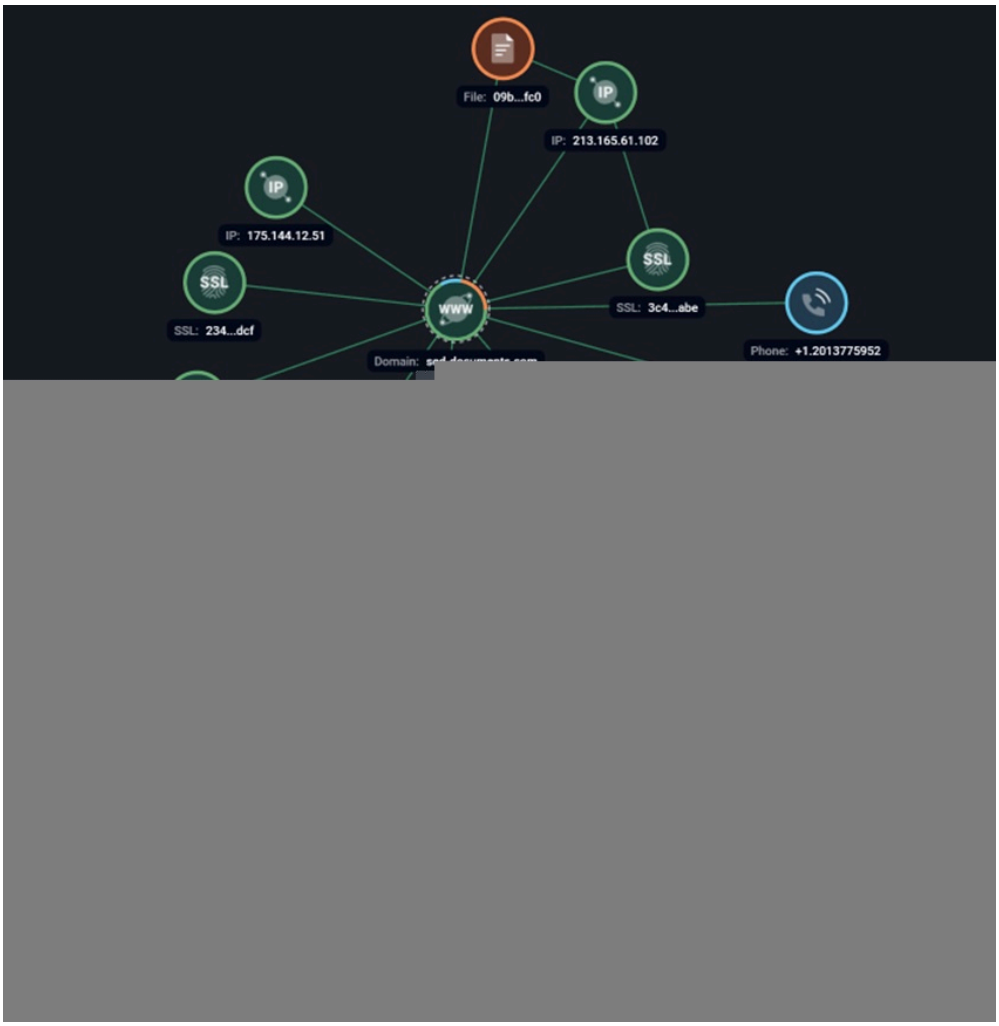

Рис. 4. Графовый анализ доменов злоумышленников

В ходе анализа был обнаружен еще один адрес управляющего сервера CapDoor — hxxp://94[.]156[.]232[.]113/search/?text=[a-z]{30} и связанные с ним экземпляры, они представлены в разделе с индикаторами. Содержимое PDF-файла представлено на рисунке ниже.

Рис. 5 – Содержимое PDF-файла

В PDF-файле содержится ссылка, ведущая на загрузку архива «Установщик КриптоПРО 2025.rar» (hXXps://documents-sed[.]com/downloads/storage/v5.6.3/release/%D0%A3%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D1%89%D0%B8% недоступного на момент анализа.

Анализ одного из вредоносных вложений на Malware Detonation Platform от компании F6.

Злоумышленники продолжают активно атаковать российские компании из разных отраслей, часто используя вредоносные рассылки для доставки вредоносных программ. Киберпреступники используют проверенные «легенды» и изобретают новые методы обмана сотрудников. Необходимо избегать загрузки программного обеспечения из непроверенных источников, в том числе из ссылок в электронных письмах, и использовать передовые решения для защиты электронной почты. Также хотим напомнить, что не существует одного единственного вектора атаки, используемого злоумышленниками. Успешная защита требует комплексного, многослойного подхода, сочетающего технические средства, строгие политики, своевременное обновление ПО и непрерывное обучение пользователей.

Индикаторы компрометации

Сетевые:
documents-sed[.]com
sed-documents[.]com
213[.]165[.]61[.]133
94[.]156[.]232[.]113

Файлы:
Инструкция_минная_угроза_ВСУ_10.11.2025.pdf
Методические_рекомендации_ФСБ_по_организации_безопасности_при_террористической_угрозе ([0-9]{1,2}).pdf
Перечень_документов_для_отчета_по_тренингу_ИБ_ФСБ ([0-9]{1,2}).pdf
Пакет установки КриптоПРО.rar
Пакет установки КриптоПРО.msi
Установщик КриптоПРО.msi
VB Decompiler Lite.cab
payload.bin
[9wdTGE] GoogleUpdate.zip
[9wdTGE] GoogleUpdate.exe
t3dt88paa.exe
Installer.msi

Хэши:
b6bda06568d91ae0c65fabf4332eab2691547482
cffdfc201ace5e8d441b97a5e27a32516deece17
fc39f2ab4dfd7bc890415c20488289e553db856b
f87753bfc75f881d0264c5eb19252cca4456e1e4
1587195bb358a5784ce31b877ee1018125e6feae
eaf7f9206a667d9a5e4ad2f1604471864527cd82
85d3fde12541f890fba37e27dde694acbac30989
1f6df9177de2c5ceaaf861f6c4e92406bbef1182
fe63dc492c9002fe96fc953b5d3654fbc94fb40e
d54d3f0eac9a34e80082d1a092a407142e76f6c9
e4da80af21b1f38658a5ff765cee9e4164f97cfa
2db32b4905f685aa6db4b4f8e0e0bf4e9f26422d

Теги:

- бэкдоры
- кибербезопасности
- центр кибербезопасности
- вредоносные рассылки

Хабы:

- Блог компании F6
- Информационная безопасность