

Почерк LLM: аналитики F6 изучили атаку с использованием PureCrypter и DarkTrack RAT

f6.ru/blog/purecrypter-darktrack-rat

December 8, 2025



С каждым днем искусственный интеллект всё больше интегрируется в нашу жизнь и облегчает многие задачи. Но, к сожалению, он также используется и в арсенале киберпреступников.

Так, в ходе ежедневного мониторинга угроз, 21.11.2025 специалисты [F6 Threat Intelligence](#) обнаружили вредоносный архив с именем Изделие-44 ДСП.rar (MD5: d3b6c14b4bbad6fd72881ff6b88a0de4), загруженный на одну из публичных онлайн-песочниц.

Архив содержит в себе файл Изделие-44 ДСП.hta (MD5: e6846e5074ef5e583df74d989a32833f), запуск которого инициирует цепочку заражения: HTA-загрузчик -> EXE загрузчик\инжектор -> полезная нагрузка DarkTrack RAT.

В ходе анализа содержимого указанного файла прослеживается простота кода, подробное его комментирование, форматирование и отсутствие грамматических ошибок. Эти признаки позволяют предположить, что злоумышленники использовали при разработке своего ВПО LLM.

```
1 <html>
2 <HTA:APPLICATION icon="#" WINDOWSTATE="minimize" SHOWINTASKBAR="no" SYSMENU="no" CAPTION="no" />
3 <body>
4   <script language="VBScript">
5     ' Обфусцированные имена переменных
```

Рис. 1. – Содержимое файла Изделие-44 ДСП.hta

В ходе выполнения .hta-файл осуществляет загрузку исполняемого файла 1.exe с удаленного хоста hXXps://store3.gofile.io/download/direct/590939a1-31ec-476b-b451-40d809d91bde/1.exe, сохраняет его с именем %AppData%\tcpview.exe (MD5: 06d5fdfabf8ef1f61c1182318652509b), после чего запускает.

С целью закрепления в системе ВПО создает ярлык данного файла в папке автозагрузки по пути: %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\tcpview.lnk

Файл tcpview.exe является исполняемым файлом .NET, который мимикрирует под установщик браузера Opera_GX.

Metadata	
Compile date:	2025-11-17 15:50:00
Certificate:	
Issuer:	DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1 (Organization=DigiCert, Inc. / Unit=?..
Subject:	Opera Norway AS
Org Details:	Opera Norway AS / Unit=?? / State=?? / Locality=Oslo / Country=NO / Email=??

Рис. 2 – Метаданные файла tcpview.exe

Исполняемый файл подписан недействительной подписью с именем Opera Norway AS.

Рис. 3. – Информация о цифровой подписи файла
tcpview.exe

Специалисты F6 классифицировали данный файл как загрузчик/инжектор PureCrypter, который содержит в ресурсах изображение Zsiik.jpg.

Размер изображения составляет 32 Мб, практически весь размер картинки занимает оверлей, который, предположительно, используется лишь в целях обхода средств защиты за счет увеличения размера файла.

В ходе выполнения файл дешифрует и запускает в памяти сохраненный в ресурсах файл с именем Efrhk путем использования алгоритма дешифрования RC2.

Рис. 4. – Функция дешифровки полезной нагрузки

Далее создает новый процесс с именем tcpview.exe, внедряет в него и запускает полезную нагрузку (MD5: 50838f9ce351053f1f8707d5aeb11528) с помощью техники process hollowing.

Полезная нагрузка была нами классифицирована как DarkTrack RAT, использующий в качестве управляющего сервера домен wwwuandex[.]org. Конфигурация ВПО:

```
{ "Port": 443, "Password": "112233", "ID": "DT-Victim", "Installation Flag": 192, "Startup Flag": 103,
"Filename": "DtServ32.exe", "HKCU Startup Name": "DtServ32sm.exe", "Mutex":
"I_AM_DTgqWtgzlf", "C2": [ "wwwyandex[.]org" ] }
```

Домен был зарегистрирован 14 ноября 2025 года.

Рис. 5. – Графовый анализ в системе F6 Threat Intelligence

Полезная нагрузка запускает дочерний процесс notepad.exe и может внедрять в него собственный код.

Также в ходе анализа была извлечена версия RAT — 4.1 Alien+.

В ходе дополнительного анализа специалисты F6 обнаружили вредоносный VBA-скрипт (MD5: a7c286cc3ef3e5d3a07b99d53e3be032), выполнение которого приводит к выполнению цепочки атаки, полностью идентичной описанной выше. В результате устанавливается DarkTrack RAT с тем же адресом C2.

Рис. 6. – Содержимое VBA скрипта (MD5: a7c286cc3ef3e5d3a07b99d53e3be032)

Данный случай описывает возможность использования атакующими ИИ как для написания вредоносного кода, способного работать самостоятельно, так и в комбинации с ранее известными угрозами. Это, в свою очередь, позволяет предположить как дальнейшее развитие атак с применением ИИ, так и увеличение частоты его использования в реальных киберинцидентах.

Анализ ВПО на Malware Detonation Platform от компании F6 доступен по ссылке:

<https://detonation.f6.security/ru/Gxxb1ppJrarMGTMsurX6YI3V9>

Индикаторы компрометации

hXXps://store3.gofile.io/download/direct/590939a1-31ec-476b-b451-40d809d91bde/1.exe

wwwyandex[.]org

212.11.64[.]185

Изделие-44 ДСП.rar

MD5: d3b6c14b4bbad6fd72881ff6b88a0de4

SHA1: 83458906E6888B0B20B091CE1250CFC7E0E81CA6

SHA256: D1C9951D5E219981F9FD21D465491728C2005718BE2D96C9814A50C88ACCD1E7

Изделие-44 ДСП.hta

MD5: e6846e5074ef5e583df74d989a32833f

SHA1: 65442d77207892d7668e0899a32a3cae2285b3ab

SHA256: d6a8e2dfc28abcf9b63ec1827d6568b09d76310d1db1794683ea6ded30dc532e

tcpview.exe

MD5: 06d5fdfabf8ef1f61c1182318652509b

SHA1: 5e0cd038f6db10329b65af40790a491fc1d2ed7b

SHA256: bbbc2a56ba69aefa567dbffe1982e21c7317e305741f7027cd0975c4bf79f8df

345cph8xf.exe

MD5: 265dfa924da79d74b1bbaebe348aaf0d

SHA-1: d561018ff9ca536b121ac2ca211ae394d75ac373

SHA-256: dc54a080caeea8f57a7dacfc519d8c17d28ce416a012c37030bfedfb27945a6f

x1dzhb3.exe (DarkTrack RAT)

MD5: 50838f9ce351053f1f8707d5aeb11528

SHA1: 9b61246c955cfad81187930dea280173fae2a04d

SHA256: b1161a07be6ae2742ea5bc397ff173aea9d9e9e6e0440f6bd263ec8a481a76f0

VBS скрипт

MD5: a7c286cc3ef3e5d3a07b99d53e3be032

SHA1: 8bccfb067f0c27b285f3c8586b1d899e69b57565

SHA256: 2f76a3c533e42c18a1734ff872704cfce6463c5e93c0d90045b59e6574f342b5

© 2003 – 2025 F6 — российский разработчик технологий для борьбы с киберпреступлениями.