



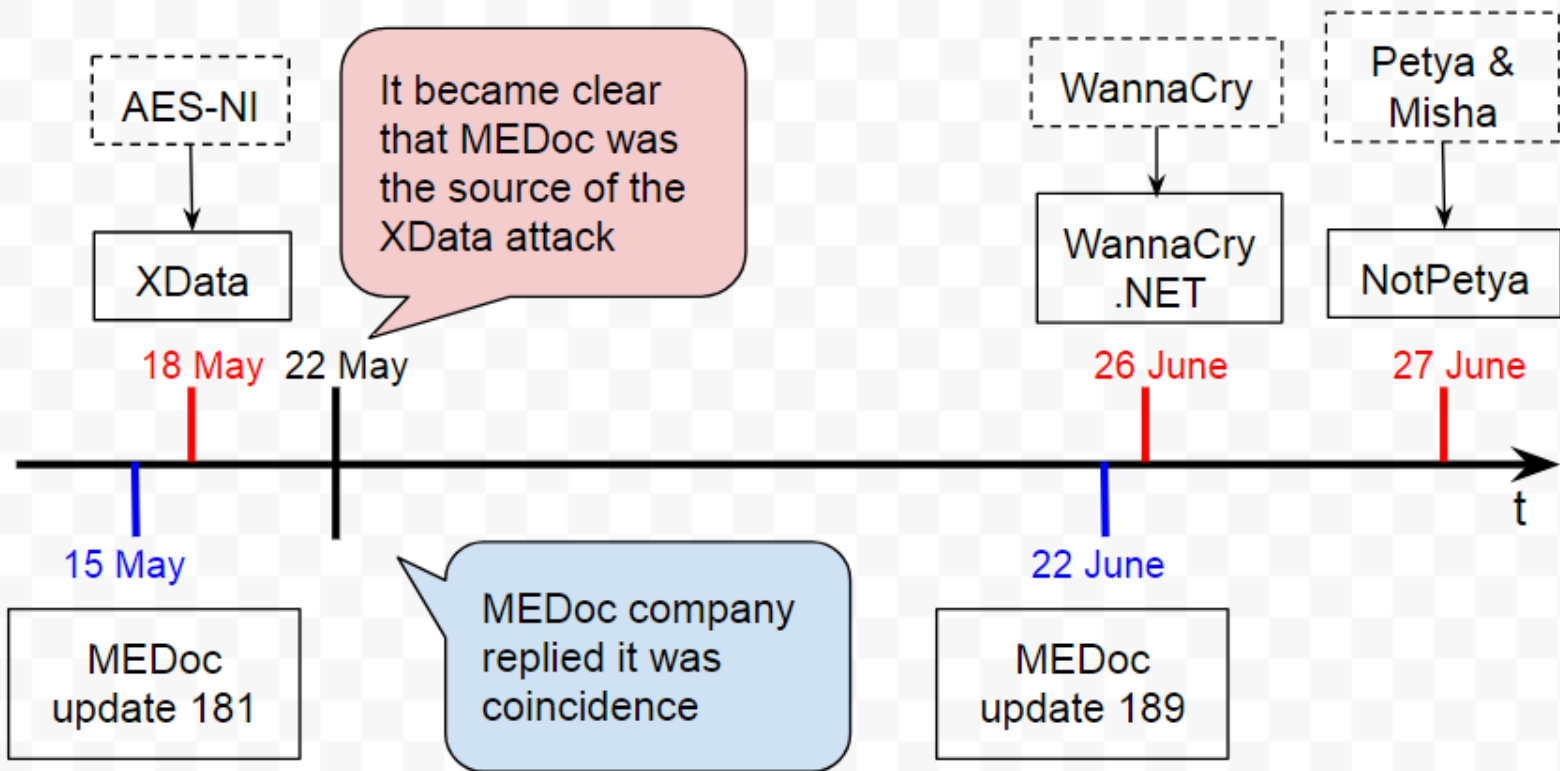
# Как я провел это лето с Petya и его друзьями

Александр Адамов  
NioGuard Security Lab

[ada@nioguard.com](mailto:ada@nioguard.com)

@Alex\_Ad

# Атаки через M.E.Doc



# XData



# Комментарии жертв



Waldemar Müller

🕒 17:46 22.05.2017

Очень странно, но пользователи из двух совсем разных конторы, которые эту дрянь подцепили, тоже утверждают, что это говно случилось именно после обновления M.E.Doc. Может, конечно, это совпадение, но какое-то странное.



+4



ОТВЕТИТЬ



Odarchuk Oleksandr

🕒 14:27 22.05.2017

Маю 2 зашифровані ПК. Різні організації/ПК/юзери ( обоє бух-и) але обоє стверджують, що сталося це після оновлення локальної версії МЕДОКа....



+4



ОТВЕТИТЬ

# Комментарии MEDoc



39 / 63

## 39 engines detected this file

SHA-256	d462966166450416d6add
File name	ZvitPublishedObjects.dll
File size	4.93 MB
Last analysis	2017-08-09 09:29:08 UTC
Community score	-27

<https://www.virustotal.com/intelligence/search/?query=d462966166450416d6add3bfdf48590f8440dd80fc571a389023b7c860ca3ac>

Оновлено: Будьте пильні: вірусна атака на корпоративний сектор!

22.05.2017



**Вірусна атака  
на корпоративний сектор  
Будьте пильні!**

У мережі з'явився вірус XData Ransomware. Вірус спрямований на корпоративний сектор і діє за схемою WannaCry - шифрує файли на комп'ютері з метою отримання викупу за повернення оригінальних файлів.

Інформація про вірус почала з'являтися в мережі з 18.05.2017р., наступного дня після виходу оновлення програми «М.Е.Дос» - саме тоді, коли бухгалтери України встановлювали останнє оновлення. Як результат, у користувачів, які заразилися вірусом XData, також була пошкоджена програма «М.Е.Дос». Цей збіг міг послужити приводом для проведення асоціації між вірусом та програмою. Подібні висновки - однозначно помилкові, адже розробник «М.Е.Дос», як відповідальний постачальник програмного продукту, стежить за безпекою і чистотою власного коду. Для цього нами були укладені договори з великими антивірусними компаніями для надання виконуваних бінарних файлів на аналіз та підтвердження їхньої безпеки. Це означає, що **перед випуском кожного оновлення «М.Е.Дос» передає в антивірусні компанії свої файли для аналізу.**

Переконалися в цьому може кожен користувач. За допомогою [www.virustotal.com](https://www.virustotal.com) можна перевірити, як ті чи інші антивірусні програми реагують на оновлення. Хеш-коди всіх оновлень знаходяться в прямому доступі на сайті програми.

# WannaCry .NET



<https://blockchain.info/address/13KBb1G7pkqcJcxpRHg387roBj2NX7Ufyf>

Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

# NotPetya



[https://blockchain.info/  
address/1Mz7153HMu  
xXTuR2R1t78mGSdza  
AtNbBWx](https://blockchain.info/address/1Mz7153HMuXtUR2R1t78mGSdzaAtNbBWx)

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuXtUR2R1t78mGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail [wowsmith123456@posteo.net](mailto:wowsmith123456@posteo.net). Your personal installation key:

c7a5ox-6ReCFR-kcRYfp-6ozqpm-Lr7wkq-eHD3wD-bJ6MB7-3EuQ8m-wx23mK-NHmKap

If you already purchased your key, please enter it below.

Key: \*

# Crystal Finance Millennium

## Crystal Finance Millennium

Логін  Пароль  [Скачати нову версію](#)

### Бухгалтерський облік



- спрямований на повну комп'ютаризацію бухгалтерського, економічного та кадрового відділів. Програма дозволяє вирішити питання повної автоматизації бухгалтерського обліку, починаючи з формування первинних документів, розрахунку заробітної платні, складського обліку, і закінчуючи отриманням "Головної книги" та "Балансу підприємства".

Програмний комплекс повністю враховує специфіку бухгалтерського обліку в бюджетних організаціях. Формування звітів відбувається згідно з типовими формами затвердженими наказами Державного казначейства України, Міністерства фінансів України, Національного банку України та Державного комітету статистики України.

### Служба крові



- це повномасштабне інтегроване рішення автоматизації обліку донорів. Програма дозволяє вирішити всі аспекти роботи: від занесення картки первинного донора та здачі крові до формування вихідних статистичних звітів лише за допомогою однієї програми.

Програмний комплекс "Служба крові" повністю враховує специфіку роботи служби крові: від відділу комплектування донорських кадрів до відділу заготівлі крові та експедиції. Всі необхідні звіти роздруковуються в повній відповідності з типовими формами затвердженими Міністерством охорони здоров'я України.

Програма ідеальна для автоматизації як обласних станцій переливання крові, так і відділів переливання крові. [Детальніше](#)

### Автоматизація лікарського кабінету



- програмно-технічний комплекс, розроблений для полегшення роботи у лікарському кабінеті. Це автоматизована система ведення графіку прийому пацієнтів та медичних карток з історією хвороби.

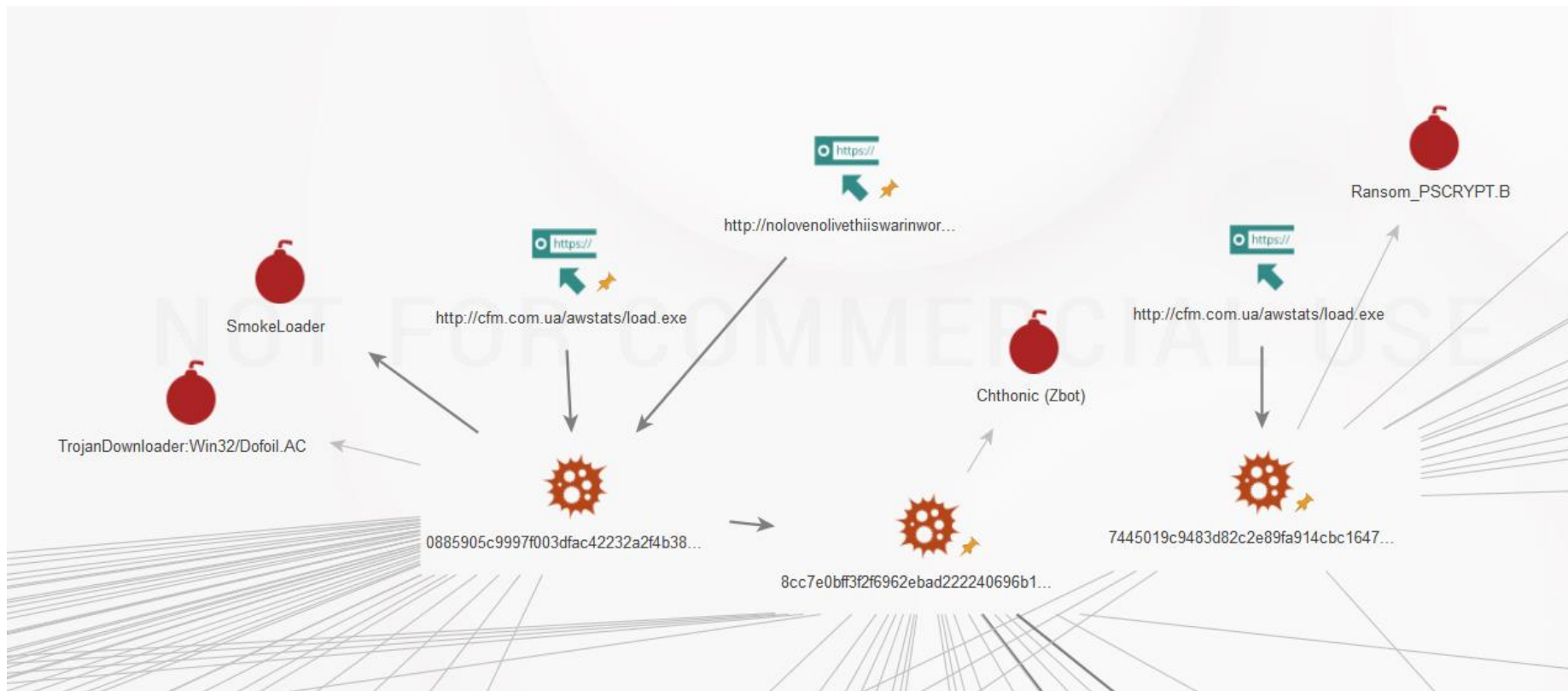
### Персоніфікований облік медичної допомоги



- спрямований на повну комп'ютаризацію усіх медичних установ міста задля повного звіту медичної допомоги.



# Атаки через cfm.com.ua



# CYBERSECURITY



## MEETUP #1

[T.ME/CYBERSECURITYCLUSTER](https://t.me/cybersecuritycluster)