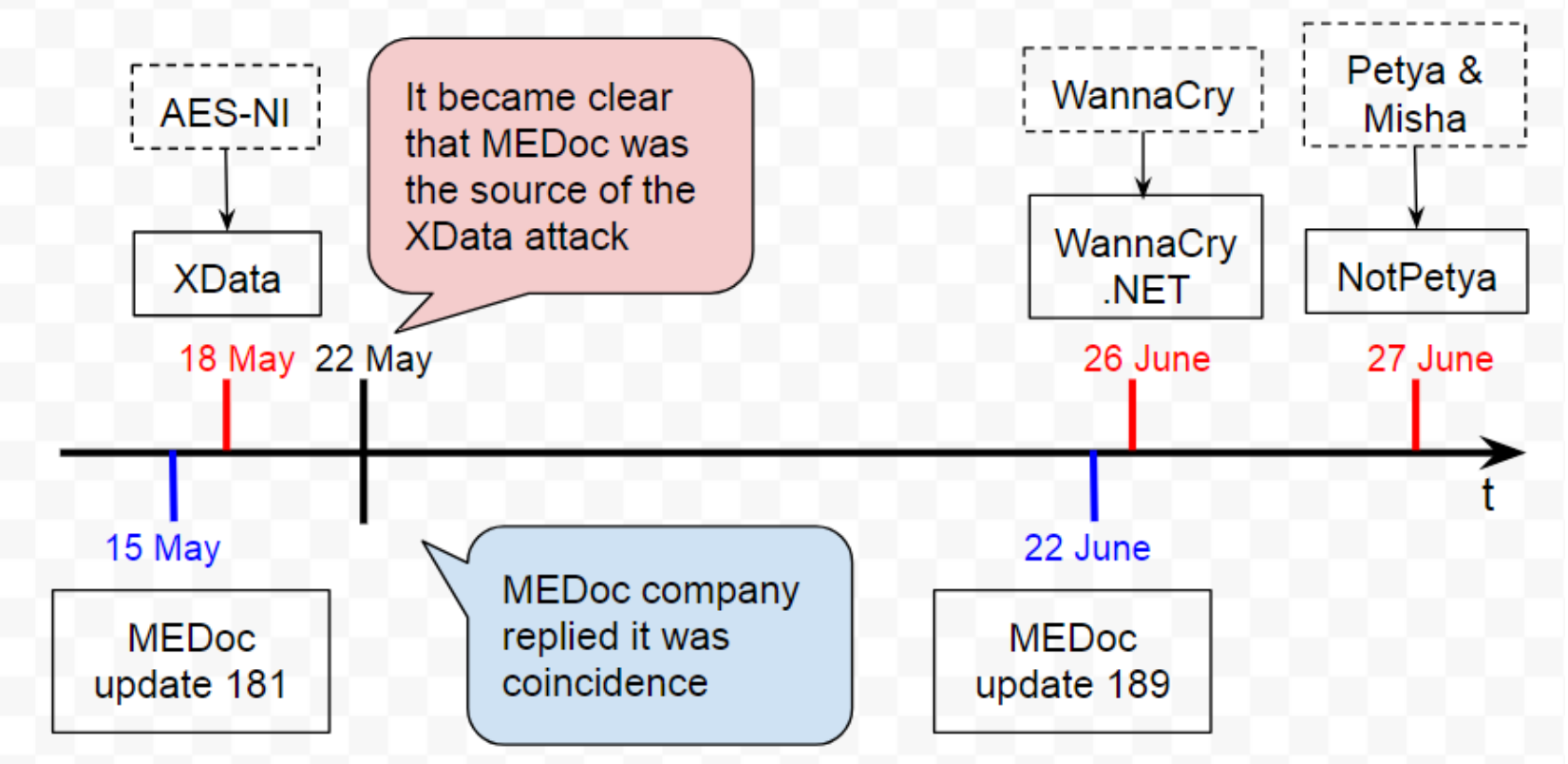
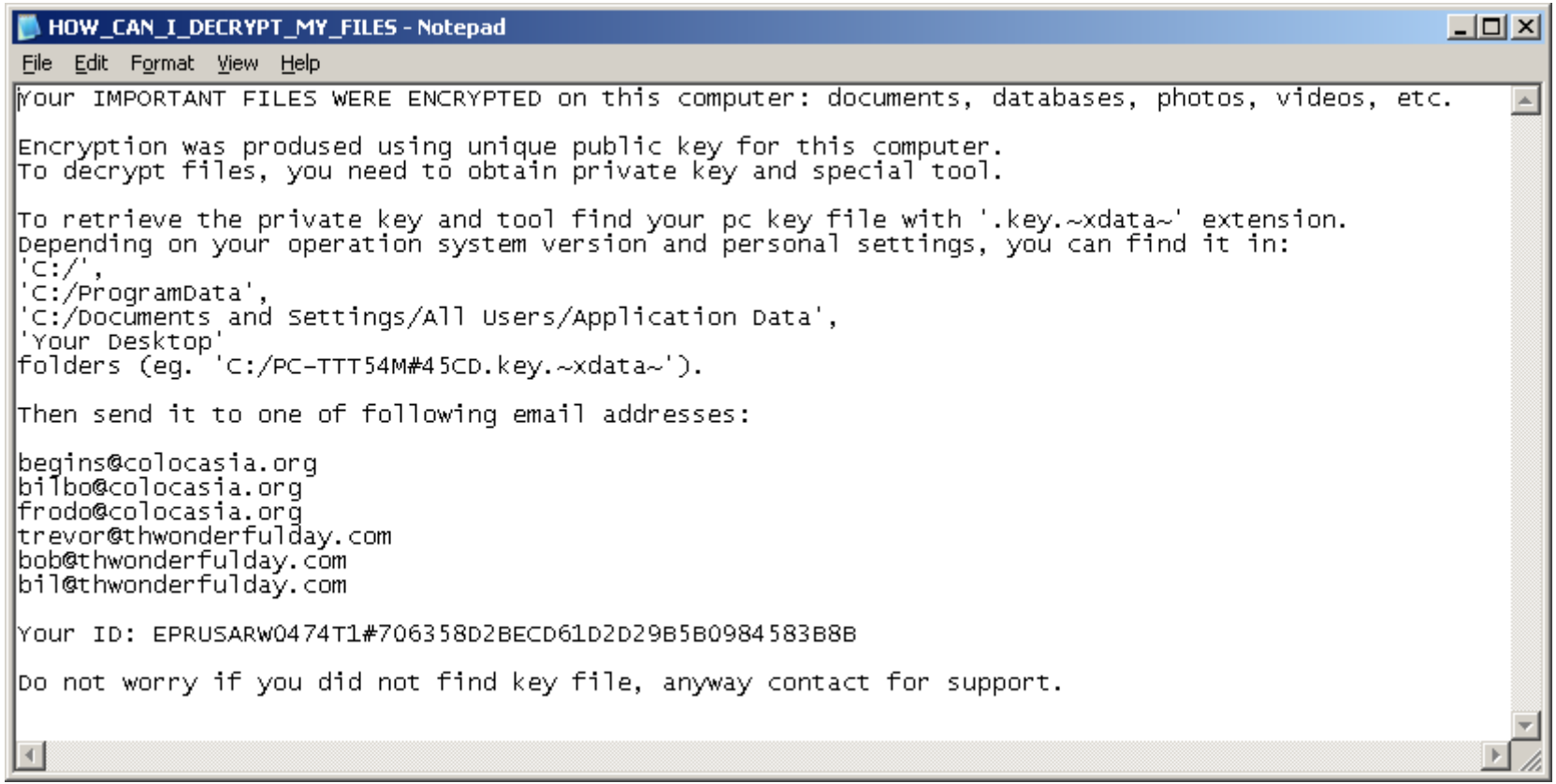
Как я провел это лето с Petya и его друзьями

Александр Адамов
NioGuard Security Lab
ada@nioguard.com
@Alex_Ad

Атаки через M.E.Doc



XData


HOW_CAN_I_DECRYPT_MY_FILES - Notepad
File Edit Format View Help
Your IMPORTANT FILES WERE ENCRYPTED on this computer: documents, databases, photos, videos, etc.
Encryption was produsedusing unique public key for this computer.
To decrypt files, you need to obtain private key and special tool.
To retrieve the private key and tool find your pc key file with '.key.~xdata~' extension.
Depending on your operation system version and personal settings, you can find it in:
'C:/',
'C:/ProgramData',
'C:/Documents and Settings/All Users/Application Data',
'Your Desktop'
folders (eg. 'C:/PC-TTT54M#45CD.key.~xdata~').
Then send it to one of following email addresses:
begins@colocasia.org
bilbo@colocasia.org
frodo@colocasia.org
trevor@thwonderfulday.com
bob@thwonderfulday.com
bil@thwonderfulday.com
Your ID: EPRUSARW0474T1#706358D2BECD61D2D29B5B0984583B8B
Do not worry if you did not find key file, anyway contact for support.

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

Source: https://ain.ua/2017/05/22/ukraincev-atakuet-novyj-virus-xdata

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=d462966166450416d6addd3bfdf48590f8440dd80fc571a389023b7c860ca3ac

Оновлено: Будьте пильні: вірусна атака на корпоративний сектор!

22.05.2017

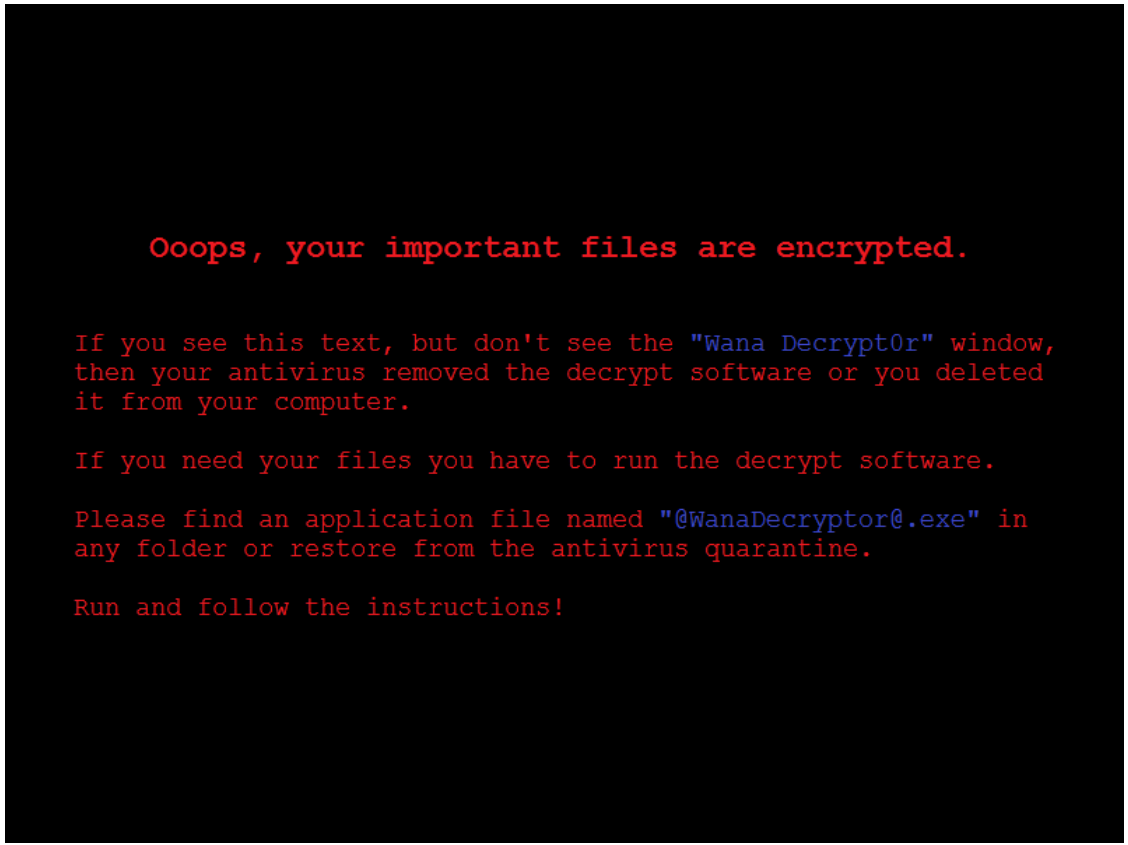
У мережі з'явився вірус XData Ransomware. Вірус спрямований на корпоративний сектор і діє за схемою WannaCry - шифрує файли на комп'ютері з метою отримання викупу за повернення оригінальних файлів.

Інформація про вірус почала з'являтися в мережі з 18.05.2017р., наступного дня після виходу оновлення програми «M.E.Doc» - саме тоді, коли бухгалтери України встановлювали останнє оновлення. Як результат, у користувачів, які заразилися вірусом XData, також була пошкоджена програма «M.E.Doc». Цей збіг міг послужити приводом для проведення асоціації між вірусом та програмою. Подібні висновки - однозначно помилкові, адже розробник «M.E.Doc», 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 «M.E.Doc» передає в антивірусні компанії свої файли для аналізу.**

Переконатися в цьому може кожен користувач. За допомогою 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.

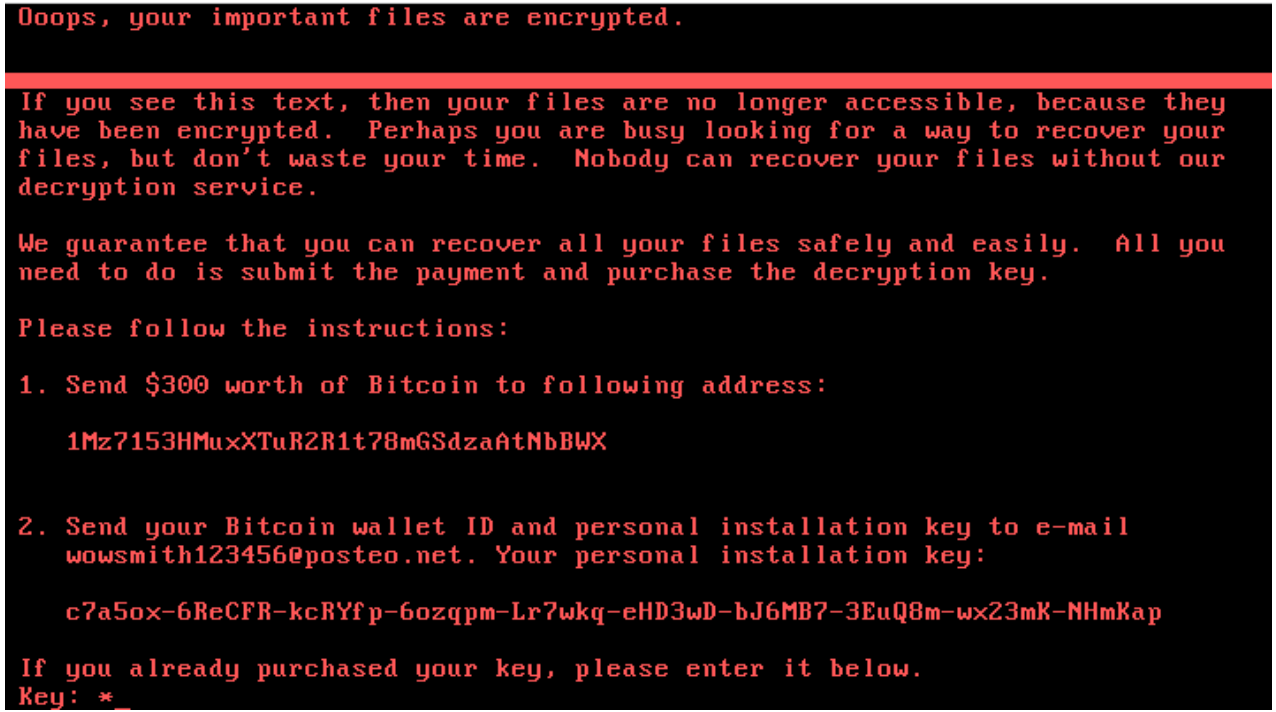
WannaCry .NET

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



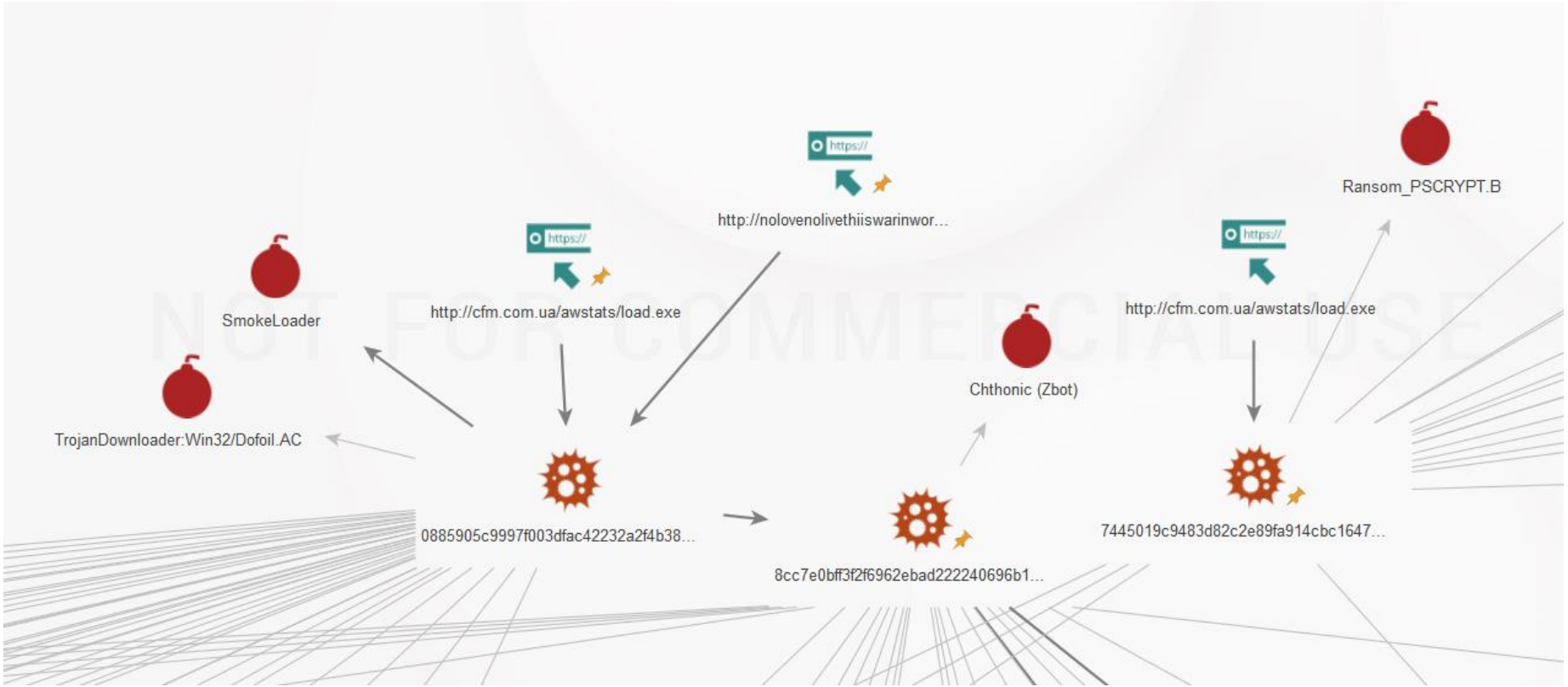
NotPetya

https://blockchain.info/address/1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX



Crystal Finance Millennium

Атаки через cfm.com.ua




CYBERSECURITY
MEETUP #1
T.ME/CYBERSECURITYCLUSTER