



Analiza Banker trojanskog konja

INFIGO-TD-2008-02

2008-12-10

Ovaj dokument namijenjen je javnoj objavi, a vlasništvo je INFIGO IS. Svatko ga smije koristiti pozivati se na njega ili ga citirati, ali isključivo u izvornom obliku i uz obvezno navođenje izvora.

Korištenje dokumenata na bilo koji drugi način od gore navedenog, bez dozvole INFIGO IS predstavlja povredu vlasništva i kao takvo podložno je zakonskoj odgovornosti koja je regulirana zakonima Republike Hrvatske ili drugom primjenjivom regulativom.

Infigo IS d.o.o.
Horvatovac 20
10000 Zagreb

tel. +385 1 4662 700
fax. +385 1 4662 701
info@infigo.hr
www.infigo.hr



SADRŽAJ

1. SAŽETAK	4
2. TEHNIČKA ANALIZA	5
2.1. INICIJALNA INFEKCIJA	5
2.2. KRADA PODATAKA	6
2.3. ŠLANJE UKRADENIH PODATAKA NAPADAČU	7
3. ZAŠTITA	8

1. SAŽETAK

Trend porasta kriminalnih aktivnosti na Internetu primjetan je već nekoliko godina, no u posljednje vrijeme posebnu pažnju privlače maliciozne aktivnosti usmjerene prema korisnicima Internet bankarstva. Naime, broj malicioznih programa koji se ciljano razvijaju u svrhu krađe podataka korisnika Internet bankarstva pojedinih banaka u značajnom je porastu i svakako poziva na oprez.

Autori ovakvih trojanskih konja do sada su zaobilazili hrvatske banke, vjerojatno zbog percepcije male isplativosti napada ili više razine zaštite u odnosu na druge banke u svijetu, no posljednji događaji ukazuju da i klijenti hrvatskih banaka imaju razloga za oprez.

U okviru redovitog praćenja i analize malicioznih aktivnosti na Internetu, stručnjaci tvrtke INFIGO IS detektirali su trojanski konj pod nazivom Banker, koji prvi puta, osim inozemnih banaka, napada i hrvatske banke. Kao što se moglo očekivati, riječ je o dvije najveće hrvatske banke, Zagrebačkoj i Privrednoj, koje su napadačima posebno zanimljive s obzirom na broj korisnika, odnosno potencijalnih ciljeva napada.

Analizirani trojanski konj napada isključivo krajnje korisnike i ograničen je na krađu podataka iz formi Internet preglednika, što znači da napadač, zbog korištenja tehnologija tokena i OTP autentikacije, nije u stanju provesti maliciozne transakcije na standardnim sustavima Internet bankarstva u slučaju navedenih banaka, Međutim neke slabije zaštićene usluge kod kojih se ne koristi autentikacija bazirana na tokenima mogu biti iskorištene za čitanje stanja računa i provođenje neovlaštenih transakcija na štetu korisnika.

U nastavku dokumenta dana je tehnička analiza identificiranog trojanskog konja te preporuke za zaštitu korisnika i detekciju inficiranih računala.

Potrebno je napomenuti da, iako pojedine mogućnosti trojanskog konja još nisu u potpunosti funkcionalne (npr. krađa podataka ne radi iz Mozilla Firefox web preglednika), za očekivati je da će napadači u budućnosti proširiti mogućnosti trojanskog konja i ciljeve napada.

U svrhu zaštite korisnika preporučuje se provođenje aktivnosti opisanih u poglavlju 3.

2. TEHNIČKA ANALIZA

2.1. INICIJALNA INFEKCIJA

Trojanski konj nema mogućnosti automatskog širenja, već se nova računala inficiraju putem drugih vektora napada. Vektori napada koje koristi Banker trojanski konj navedeni su u nastavku:

- Kompromitirani web poslužitelji usmjeruju korisnika na poseban poslužitelj putem kojeg se trojanski konj instalira iskorištavanjem sigurnosne ranjivosti u Internet Explorer web pregledniku.
U svrhu instaliranja trojanskog konja iskorištava se starija sigurnosna ranjivost, MS06-014 (*Microsoft Data Access Components*) koja omogućava izvođenje proizvoljnog programa na ranjivom računalu.
- U slučaju neuspjelog pokušaja iskorištavanja sigurnosne ranjivosti korisnika se pokušava navesti tehnikom socijalnog inženjeringa na samostalnu instalaciju trojanskog konja.

U trenutku analize kôd koji iskorištava ranjivost u Internet Explorer web pregledniku bio je dostupan na URL adresi [http://buskirava.awardspace.com/\[UKLONJENO\].htm](http://buskirava.awardspace.com/[UKLONJENO].htm).

Na navedenom poslužitelju nalazi se i trojanski konj koji se, u slučaju uspješnog iskorištavanja sigurnosne ranjivosti na računalo pohranjuje u datoteci pod imenom `b14ck.exe` te pokreće.

Nakon pokretanja trojanski konj inficira ciljno računalo i pokušava prikriti svoje tragove slijedećim aktivnostima:

- Izvorna datoteka kopira se u direktorij sustava (`C:\WINDOWS\System32`) pod imenom `mshelp.exe`.
- Nakon uspješnog kopiranja izvorni proces se gasi te se pokreće `mshelp.exe` datoteka.
- Trojanski konj provjerava lokaciju i ime datoteke iz koje je pokrenut te nastavlja s radom samo ako su prethodne dvije točke zadovoljene.
- U svrhu ponovnog pokretanja trojanski konj dodaje slijedeće *Registry* ključeve s sadržajem `mshelp.exe`:
 - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run" sadržaja "Generic Host Process for WinXP Services",
 - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices" sadržaja "Generic Host Process for WinXP Services".
- Nakon instalacije trojanski konj dohvaća konfiguracijsku datoteku s URL adrese [http://buskirava.awardspace.com/\[UKLONJENO\].txt](http://buskirava.awardspace.com/[UKLONJENO].txt), koja se pohranjuje u datoteku `C:\WINDOWS\System32\descript.lnk`.
- Ovisno o parametrima u konfiguracijskoj datoteci trojanski konj dohvaća druge datoteke s slijedećih poslužitelja:
 - `bisyeton.netfirms.com`,
 - `festashka.awardspace.com`,
 - `bsakurmeh.awardspace.com`.

2.2. KRAĐA PODATAKA

Nakon uspješne instalacije trojanski konj inicijalizira strukturu s adresama web stranica s kojih će krasti podatke. Između ostalih web stranica, nalaze se i slijedeće adrese hrvatskih web stranica (.hr domena) s kojih se krađu podaci:

- pbz.hr
- zaba.hr
- open.hr
- kaptol.hr

Navedene adrese obuhvaćaju i sve pod-domene koje korisnik inficiranog računala posjećuje, tako da će trojanski konj ukrasti podatke bez obzira na prefiks URL adrese (npr. www.pbz.hr i net.pbz.hr).

Slika u nastavku prikazuje programski kôd trojanskog konja pokrenutog u OllyDbg alatu, gdje su vidljive reference na adrese iz hrvatskog domenskog prostora:

The screenshot shows the OllyDbg interface with the following assembly code and references:

```
00412B63 . AA STOS BYTE PTR ES:[EDI]
00412B64 . 8B0D 74FE4200 MOV ECX,DWORD PTR DS:[42FE74] ref .open.hr
00412B6A . 898D 2899FFF MOV [LOCAL.6582],ECX
00412B70 . 8B15 78FE4200 MOV EDX,DWORD PTR DS:[42FE78]
00412B76 . 8995 2C99FFF MOV [LOCAL.6584],EDX
00412B7C . A0 70FE4200 MOV AL,BYTE PTR DS:[42FE7C]
00412B81 . 8885 3099FFF MOV BYTE PTR SS:[EBP+FFFF9930],AL
00412B87 . B9 0A000000 MOV ECX,0A
00412B8C . 33C0 XOR EAX,EAX
00412B8E . 8D8D 3199FFF LEA EDI,DWORD PTR SS:[EBP+FFFF9931]
00412B94 . F3:AB REP STOS DWORD PTR ES:[EDI]
00412B96 . AA STOS BYTE PTR ES:[EDI]
00412B97 . 8B0D 80FE4200 MOV ECX,DWORD PTR DS:[42FE80] ref .kaptol.hr
00412B9D . 898D 5A99FFF MOV DWORD PTR SS:[EBP+FFFF995A],ECX
00412BA3 . 8B15 84FE4200 MOV EDX,DWORD PTR DS:[42FE84]
00412BA9 . 8995 5E99FFF MOV DWORD PTR SS:[EBP+FFFF995E],EDX
00412BAF . 66:A1 88FE4200 MOV AX,WORD PTR DS:[42FE88]
00412BB5 . 66:8985 6299 MOV WORD PTR SS:[EBP+FFFF9962],AX
00412BBC . 8A0D 8AFE4200 MOV CL,BYTE PTR DS:[42FE8A]
00412BC2 . 888D 6499FFF MOV BYTE PTR SS:[EBP+FFFF9964],CL
00412BC8 . B9 09000000 MOV ECX,9
00412BCD . 33C0 XOR EAX,EAX
00412BCF . 8D8D 6599FFF LEA EDI,DWORD PTR SS:[EBP+FFFF9965]
00412BD5 . F3:AB REP STOS DWORD PTR ES:[EDI]
00412BD7 . 66:AB STOS WORD PTR ES:[EDI]
00412BD9 . AA STOS BYTE PTR ES:[EDI]
00412BDA . 8B15 8CFE4200 MOV EDX,DWORD PTR DS:[42FE8C] ref .pbz.hr
00412BE0 . 8995 8C99FFF MOV [LOCAL.6587],EDX
00412BE6 . A1 90FE4200 MOV EAX,DWORD PTR DS:[42FE90]
00412BEB . 8985 9099FFF MOV [LOCAL.6586],EAX
00412BF1 . B9 0A000000 MOV ECX,0A
00412BF6 . 33C0 XOR EAX,EAX
00412BF8 . 8D8D 9499FFF LEA EDI,[LOCAL.6585]
00412BFE . F3:AB REP STOS DWORD PTR ES:[EDI]
```

The bottom part of the screenshot shows a memory dump with the following data:

Address	Hex dump	ASCII
0042FE8C	2E 70 62 7A 2E 68 72 00 2E 72 7A 62 2E 63 6F 2E	.pbz.hr..rzb.co.
0042FE9C	61 74 00 00 2E 65 6E 74 65 72 70 72 69 73 65 2E	at..enterprise.
0042FEAC	6E 65 74 00 2E 65 62 73 2E 69 65 00 2E 73 64 61	net..ebs.ie..sda
0042FEBC	2E 64 6B 00 2E 65 79 70 2E 65 65 00 2E 64 65 70	.dk..eyp.ee..dep
0042FECC	6F 2E 65 65 00 00 00 00 2E 65 65 00 2E 66 6F 72	o.ee.....ee..for
0042FEDC	65 78 2E 65 65 00 00 00 2E 61 6B 74 69 61 2E 66	ex.ee.....aktia.f
0042FEEC	69 00 00 00 2E 66 75 69 62 2E 63 6F 6D 00 00 00	i....fuib.com...
0042FEFC	2E 75 63 62 2E 63 72 69 6D 65 61 2E 75 61 00 00	.ucb.crimea.ua..
0042FF0C	2E 74 63 6D 62 2E 67 6F 76 2E 74 72 00 00 00 00	.tcmb.gov.tr....
0042FF1C	2E 6E 73 6D 61 6E 6C 63 2E 63 6E 6D 74 72 00 00	csenit.com.tr

Slika 1: Referenciranje adresa iz hrvatskog domenskog prostora

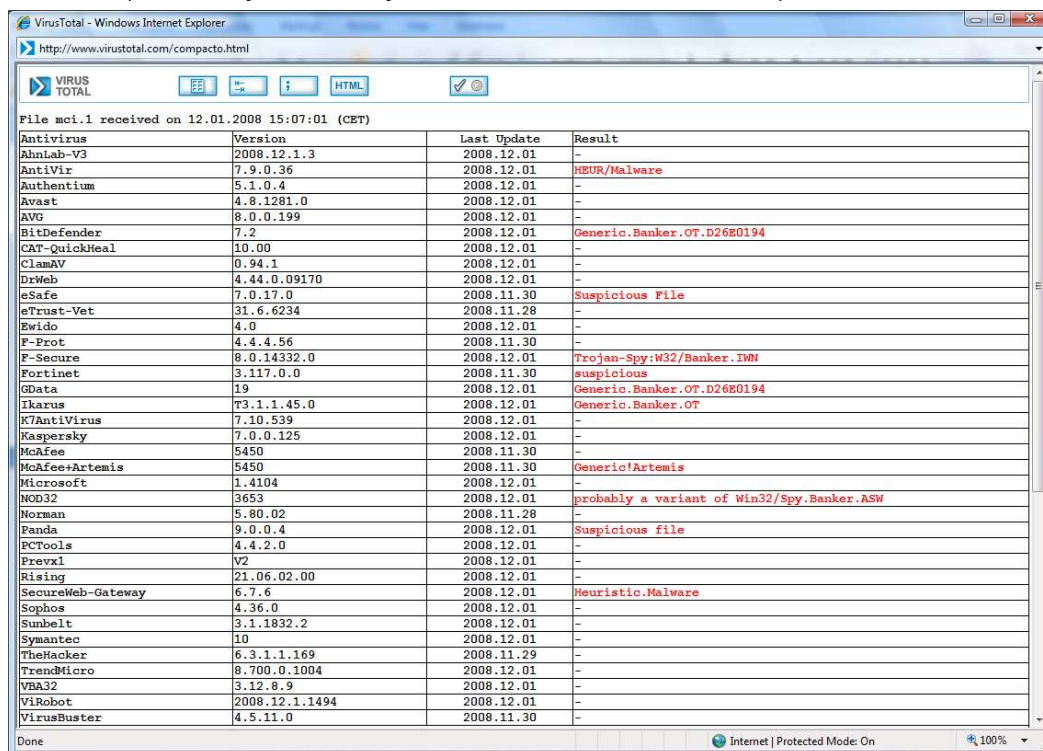
Trojanski konj u stanju je krasti podatke iz Internet Explorer i Mozilla Firefox web preglednika, no detaljnom analizom programskog kôda utvrđeno je da programski dio zadužen za krađu podataka iz Mozilla Firefox web preglednika nije u potpunosti implementiran, tako da će podaci biti uspješno ukradeni samo iz Internet Explorer web preglednika.

U svrhu identifikacije web preglednika trojanski konj koristi EnumWindows() funkciju. Ova funkcija omogućava identifikaciju trenutno otvorenih prozora. U slučaju da je identificiran prozor Internet Explorer preglednika, trojanski konj dohvaća sadržaj adresnog polja (eng. *address bar*) i provjerava da li trenutno posjećena adresa odgovara jednoj iz strukture napravljene u prethodnom koraku.

3. ZAŠTITA

Kao i kod većine trojanskih konja, ne postoji jedinstveno rješenje zaštite korisnika, već ju je potrebno provesti na svim razinama. Da bi se zaštitili korisnici bi trebali provoditi sljedeće:

- Redovito instalirati sigurnosne zakrpe za operacijske sustave i aplikacije. Zakrpe moraju biti redovito instalirane na sva računala kako bi se izbjegla mogućnost iskorištavanja poznatih sigurnosnih ranjivosti. Konkretno u ovom slučaju, analizirani trojanski konj za napad na korisnike iskorištava ranije spomenutu ranjivost unutar Internet Explorer web preglednika. Pritom, posebnu pozornost valja obratiti na aplikacije čije osvježavanje nije moguće putem Windows Update servisa.
- Instalirati i redovito osvježavati anti-virusne programe. Iako anti-virusni programi ne mogu u potpunosti zaštititi korisnika, oni mogu podići razinu zaštite računala. U konkretnom primjeru, prilikom inicijalne analize otkriveno je da samo manji broj anti-virusnih proizvođača ispravno detektira analizirani trojanski konj, kao što je prikazano u nastavku (test obavljen korištenjem VirusTotal servisa 1.12.2008):



Antivirus	Version	Last Update	Result
AhnLab-V3	2008.12.1.3	2008.12.01	-
AntiVir	7.9.0.36	2008.12.01	HEUR/Malware
Authentium	5.1.0.4	2008.12.01	-
Avast	4.8.1281.0	2008.12.01	-
AVG	8.0.0.199	2008.12.01	-
BitDefender	7.2	2008.12.01	Generic.Banker.OT.D26E0194
CAT-QuickHeal	10.00	2008.12.01	-
ClamAV	0.94.1	2008.12.01	-
DrWeb	4.44.0.09170	2008.12.01	-
eSafe	7.0.17.0	2008.11.30	Suspicious File
eTrust-Vet	31.6.6234	2008.11.28	-
Ewido	4.0	2008.12.01	-
F-Prot	4.4.4.56	2008.11.30	-
F-Secure	8.0.14332.0	2008.12.01	Trojan-Spy:W32/Banker.IWN
Fortinet	3.117.0.0	2008.11.30	suspicious
GData	19	2008.12.01	Generic.Banker.OT.D26E0194
Ikarus	T3.1.1.45.0	2008.12.01	Generic.Banker.OT
K7AntiVirus	7.10.539	2008.12.01	-
Kaspersky	7.0.0.125	2008.12.01	-
McAfee	5450	2008.11.30	-
McAfee+Artemis	5450	2008.11.30	Generic!Artemis
Microsoft	1.4104	2008.12.01	-
NOD32	3653	2008.12.01	probably a variant of Win32/Spy.Banker.ASW
Norman	5.80.02	2008.11.28	-
Panda	9.0.0.4	2008.12.01	Suspicious file
ECTools	4.4.2.0	2008.12.01	-
Prevx1	V2	2008.12.01	-
Rising	21.06.02.00	2008.12.01	-
SecureWeb-Gateway	6.7.6	2008.12.01	Heuristic.Malware
Sophos	4.36.0	2008.12.01	-
Sunbelt	3.1.1832.2	2008.12.01	-
Symantec	10	2008.12.01	-
TheHacker	6.3.1.1.169	2008.11.29	-
TrendMicro	8.700.0.1004	2008.12.01	-
VBA32	3.12.8.9	2008.12.01	-
ViRobot	2008.12.1.1494	2008.12.01	-
VirusBuster	4.5.11.0	2008.11.30	-

Slika 3: Inicijalni test detekcije korištenjem VirusTotal servisa

- Koristiti osobne vatrozide i na taj način maksimalno ograničiti izloženost svojih računala prilikom povezivanja na Internet.

S druge strane, u cilju zaštite svojih klijenata banke bi trebale osigurati sljedeće:

- Kako se za distribuciju malicioznih programa danas uglavnom koriste kompromitirani web poslužitelji, preporučuje se redovito provođenje penetracijskih testova web poslužitelja, ali i drugih dijelova informacijskog sustava kako bi se potvrdila i održala visoka razina sigurnosti sustava njihovih sustava.
- Kontinuirano provođenje edukacije svojih korisnika u svrhu podizanja razine sigurnosne osviještenosti.
- Redovito praćenje sigurnosnih grupa od strane sigurnosnih timova banaka i preventivno djelovanje u slučaju otkrivanja informacija o malicioznim programima koji mogu imati utjecaj na njihove klijente.