Co ukázal případ Hacking Team?

Honza Šípek

Nebezpečná kniha

Hacking Team hacknut

- 6. 7. 2015 zveřejněny data
- *Phineas Fisher* – hackerská etika?
- https://www.youtube.com/watch?v=R63CRBNLE2o
- 400 GB dat – šíření dat přes torrent
- spolupráce s nedemokratickými režimy
- jedním z klientů byla PČR (ÚZČ)

Malware

počítačový:

- záznam komunikace
- šifrovaná data
- stahování souborů
- nahrávání souborů
- focení přes webkameru, záznam zvuku

- při fyzické instalaci přežije i přeinstalaci systému

mobilní:

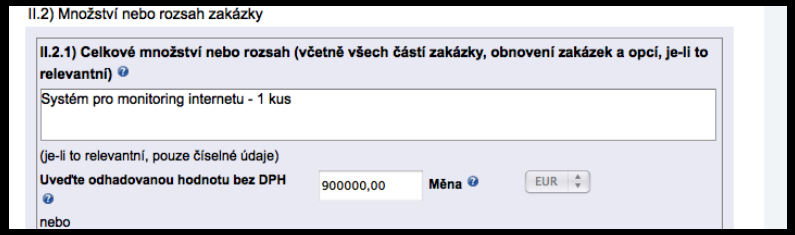
- odposlech
- pozice
- fotky

metoda infekce:

sociální inženýrství, Word, PDF, Flash, síťová infekce, konfigurační SMS

Bull s. r. o. – Dnes Atos IT Solutions and Services

známá firma:



II.2) Množství nebo rozsah zakázky

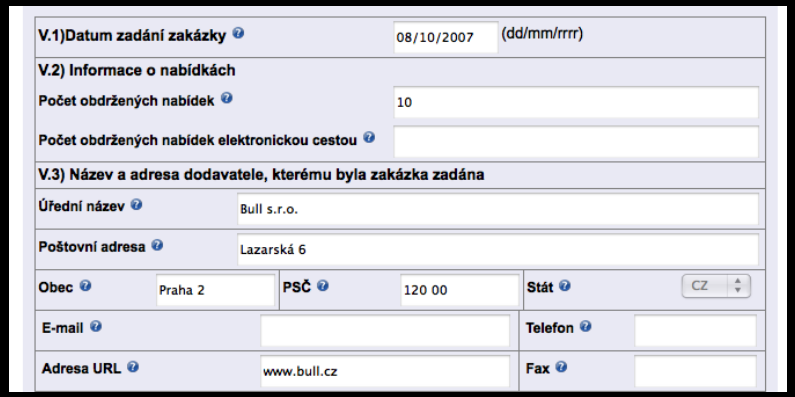
II.2.1) Celkové množství nebo rozsah (včetně všech částí zakázky, obnovení zakázek a opcí, je-li to relevantní)

Systém pro monitoring internetu - 1 kus

(je-li to relevantní, pouze číselné údaje)

Uveďte odhadovanou hodnotu bez DPH 900000,00 **Měna** EUR

nebo

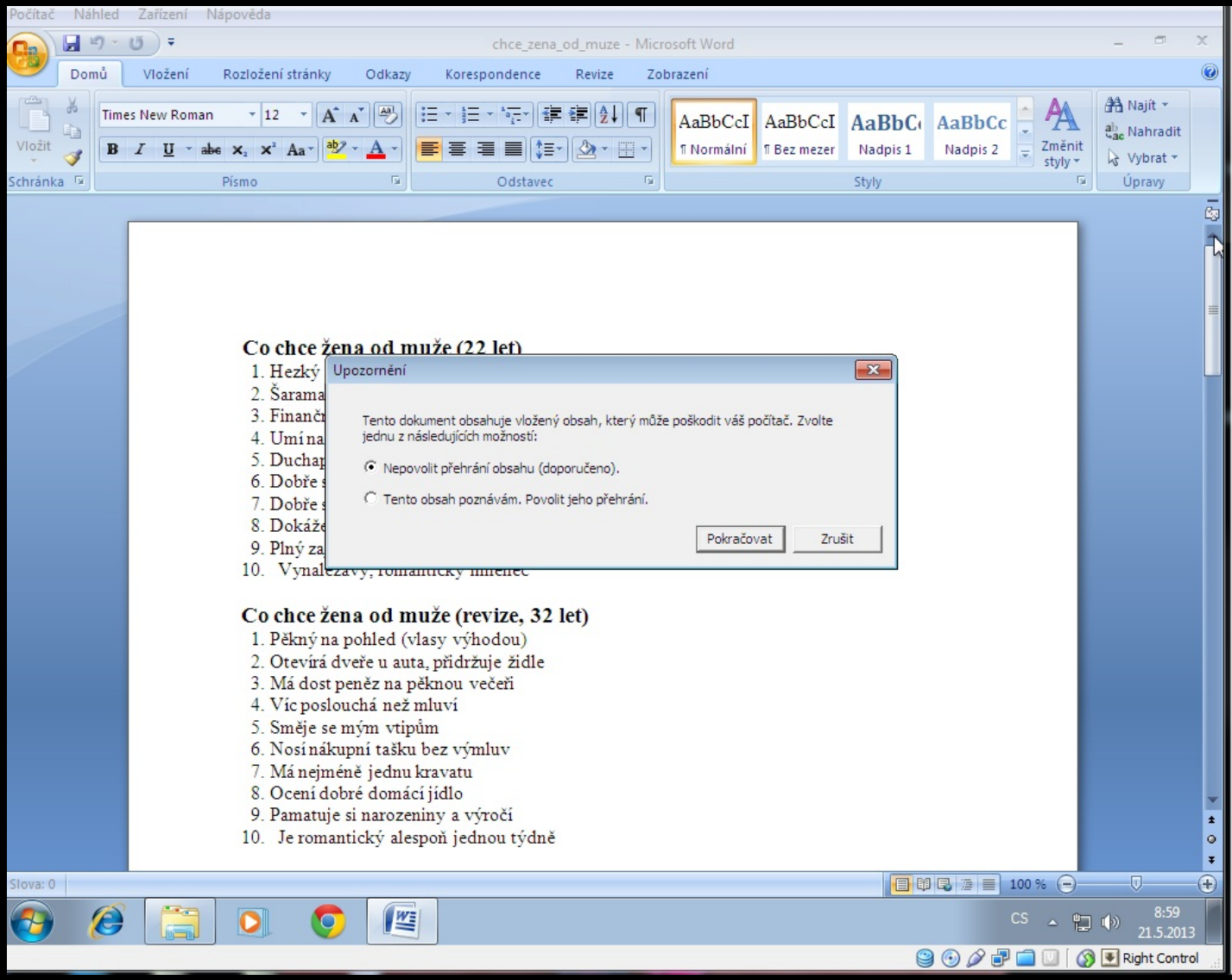


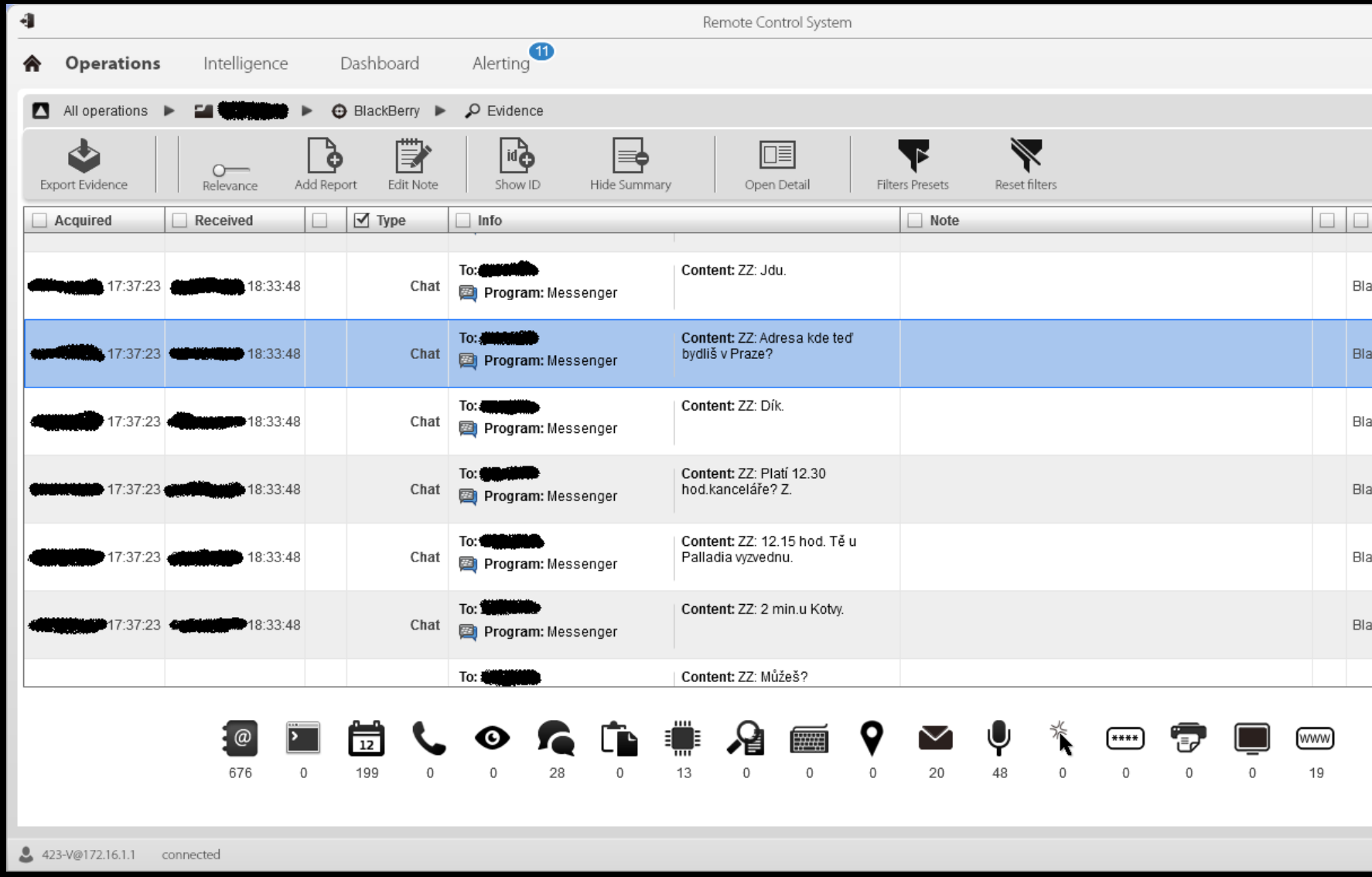
V.1)Datum zadání zakázky	08/10/2007 (dd/mm/rrrr)				
V.2) Informace o nabídkách					
Počet obdržených nabídek	10				
Počet obdržených nabídek elektronickou cestou					
V.3) Název a adresa dodavatele, kterému byla zakázka zadána					
Úřední název	Bull s.r.o.				
Poštovní adresa	Lazarská 6				
Obec	Praha 2	**PSČ**	120 00	**Stát**	CZ
E-mail				**Telefon**	
Adresa URL	www.bull.cz			**Fax**	

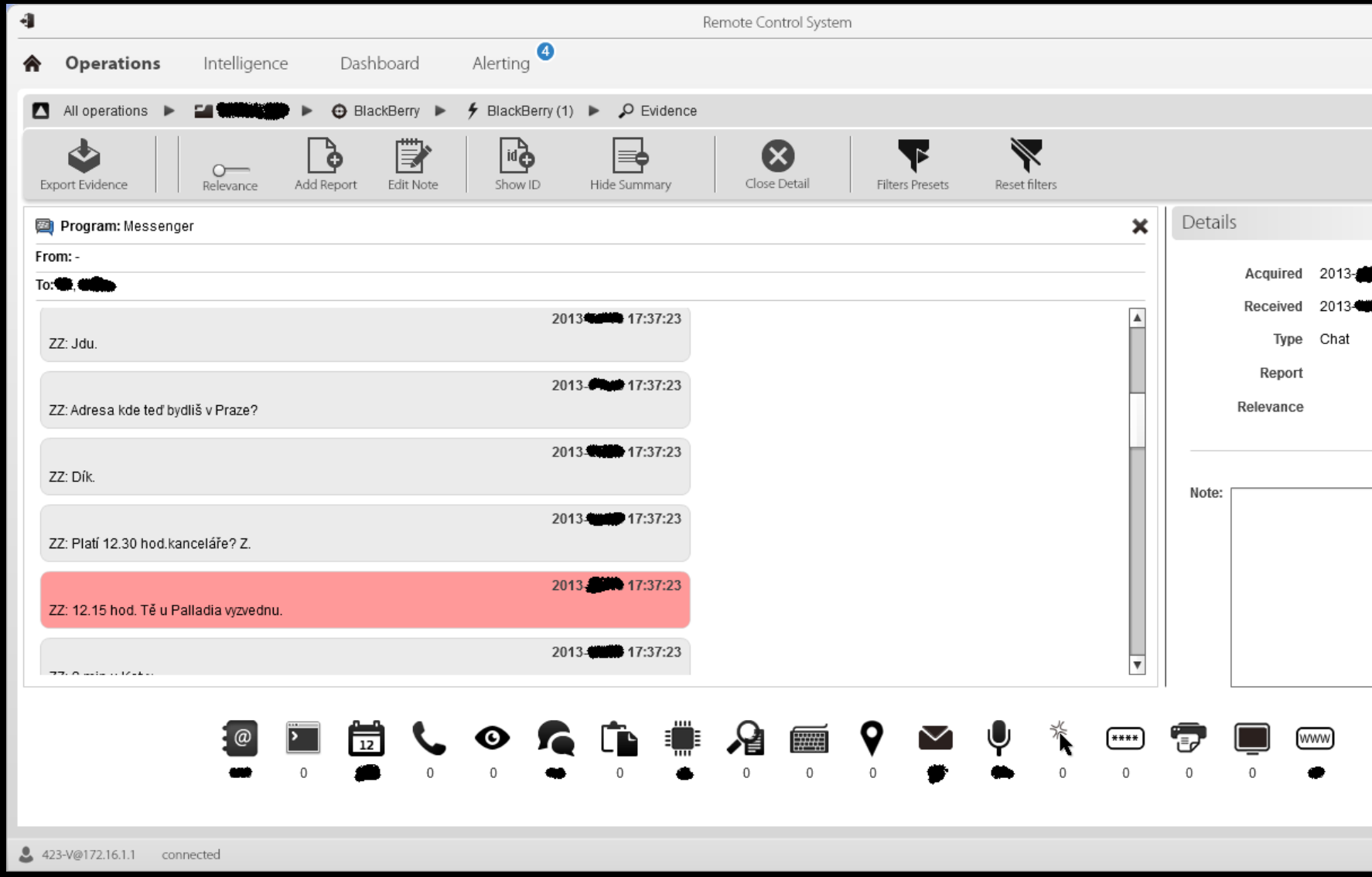
www.vestnikverejnychzakazek.cz (2007)

Analýza dat - Brmlab

- https://brmlab.cz/event/hackedteam


Počítač Náhled Zařízení Nápověda
chce_zena_od_muze - Microsoft Word
Domů Vložení Rozložení stránky Odkazy Korespondence Revize Zobrazení
Times New Roman 12
Vložit Schránka Písmo Odstavec Styly Úpravy
AaBbCcI ¶ Normální
AaBbCcI ¶ Bez mezer
AaBbC Nadpis 1
AaBbCc Nadpis 2
Změnit styly
Najít Nahradit Vybrat
Co chce žena od muže (22 let)
1. Hezký
2. Šarama
3. Finanč
4. Umí na
5. Ducha
6. Dobře
7. Dobře
8. Dokáže
9. Plný za
10. Vynalézavý, romantický milenec
Upozornění
Tento dokument obsahuje vložený obsah, který může poškodit váš počítač. Zvolte jednu z následujících možností:
Nepovolit přehrání obsahu (doporučeno).
Tento obsah poznávám. Povolit jeho přehrání.
Pokračovat
Zrušit
Co chce žena od muže (revize, 32 let)
1. Pěkný na pohled (vlasy výhodou)
2. Otevírá dveře u auta, přidržuje židle
3. Má dost peněz na pěknou večeři
4. Víc poslouchá než mluví
5. Směje se mým vtipům
6. Nosí nákupní tašku bez výmluv
7. Má nejméně jednu kravatu
8. Ocení dobré domácí jídlo
9. Pamatuje si narozeniny a výročí
10. Je romantický alespoň jednou týdně
Slova: 0
100 %
CS
8:59
21.5.2013
Right Control


Remote Control System
Operations
Intelligence
Dashboard
Alerting
11
All operations
BlackBerry
Evidence
Export Evidence
Relevance
Add Report
Edit Note
Show ID
Hide Summary
Open Detail
Filters Presets
Reset filters
Acquired
Received
Type
Info
Note
17:37:23
18:33:48
Chat
To:
Program: Messenger
Content: ZZ: Jdu.
Content: ZZ: Adresa kde teď bydliš v Praze?
Content: ZZ: Dík.
Content: ZZ: Platí 12.30 hod.kanceláře? Z.
Content: ZZ: 12.15 hod. Tě u Palladia vyzvednu.
Content: ZZ: 2 min.u Kotvy.
Content: ZZ: Můžeš?
676
0
199
0
0
28
0
13
0
0
0
20
48
0
0
0
0
19
423-V@172.16.1.1
connected


Remote Control System
Operations
Intelligence
Dashboard
Alerting
4
All operations
BlackBerry
BlackBerry (1)
Evidence
Export Evidence
Relevance
Add Report
Edit Note
Show ID
Hide Summary
Close Detail
Filters Presets
Reset filters
Program: Messenger
From: -
To:
2013 17:37:23
ZZ: Jdu.
2013 17:37:23
ZZ: Adresa kde teď bydliš v Praze?
2013 17:37:23
ZZ: Dík.
2013 17:37:23
ZZ: Platí 12.30 hod.kanceláře? Z.
2013 17:37:23
ZZ: 12.15 hod. Tě u Palladia vyzvednu.
2013 17:37:23
Details
Acquired
Received
Type
Chat
Report
Relevance
Note:
423-V@172.16.1.1
connected

Tajemný akademický partner

Doc #	Date	Subject	From	To
436716	2012-09-21 10:26:45	Re: R: BULL: exploits detected and described	tomas.hlavsa@bull.cz	m.luppi@hackingteam.it m.bettini@hackingteam.it michal.martinek@bull.cz

Hello Massimilliano
As part of our agreement, we will try
to detect vulnerabilities with our **academic** partner.
These vunerabilities should allow to
be used as exploits in RCS.
Our **academic** partner should be able
to detect vulnerabilities in applications specified by customer.
The question that we need to answer
is, how such detected vulnerability should be described for you
to be able to melt it with your technology
and deliver it to our customer as and exploit.

437116	2013-03-03 20:33:08	Bull: Exploits ready	tomas.hlavsa@bull.cz	m.luppi@hackingteam.it d.milan@hackingteam.it michal.martinek@bull.cz

Hello Massimilliano
Our **academic** partner confirmed that they have some exploits ready.
May we ask you to help us with process of delivery to you and than to the customer please.
S pozdravem / Kind Regards
Tomas Hlavsa
Technical director
Bull s.r.o.
Cell: +420 604 290 196

RIV/68407700:21240/13:00228412 - *Speciální softwarový balíček (2013)

Údaje o výsledku

Identifikační kód	RIV/68407700:21240/13:00228412
Název v původním jazyce	*Speciální softwarový balíček
Druh	R - Software
Jazyk	eng - angličtina
Obor	IN - Informatika
Rok uplatnění	2013
Kód důvěrnosti údajů	C - Předmět podléhá obchodnímu tajemství (§17 až 20 Obchodního zákoníku), ale některé údaje jsou upraveny tak, aby byly zveřejnitelné
Počet výskytů výsledku	1

Tvůrci výsledku

Počet tvůrců celkem	1
Počet domácích tvůrců	1
Tvůrce	Zahradnický Tomáš (státní příslušnost: CZ - Česká republika; A - domácí tvůrce; vedidk: 8192553)

Údaje blíže specifikující výsledek

Popis v původním jazyce	*Tento software představuje specializovaný na zakázku vytvořený počítačový software podle požadavků objednatele. Software je předmětem obchodního tajemství a zhotovitel má povinnost mlčenlivosti.
Klíčová slova	specialized custom made software
Interní identifikační kód produktu přidělený tvůrcem	JANUS
Technické parametry	Software byl předán objednateli BULL s.r.o. dne 5.4.2013 na základě předávacího protokolu. Ke smlouvě o dílo a smlouvě licenční ze dne 27.2.2013.
Ekonomické parametry	Předmětem smlouvy bylo vytvoření softwarových balíčků. Cena balíčku byla smlouvou stanovena na 50000,- Kč bez DPH. Byl vytvořen, předán a proplacen celkem 1 ks balíčku.
IČO vlastníka výsledku	68407700
Název vlastníka	ČVUT FIT
Stát vlastníka	CZ - Česká republika
Druh možnosti využití	A - Nabytí licence je nutné vždy
Požadavek na licenční poplatek	A - Poskytovatel licence na výsledek požaduje licenční poplatek
Adresa www stránky s výsledkem	http://www.bull.cz

Údaje o tomto záznamu o výsledku

Předkladatel	České vysoké učení technické v Praze / Fakulta informačních technologií
Dodavatel	MSM - Ministerstvo školství, mládeže a tělovýchovy (MŠMT)

http://www.isvav.cz/

Vyjádření FIT ČVUT v Praze k e-mailové komunikaci zveřejněné na serveru WikiLeaks.org

V reakci na zcizenou emailovou korespondenci společnosti HackingTeam, která byla umístěna na serveru WikiLeaks.org, v níž se objevuje jméno a emailová adresa pracovníka fakulty, uvádíme následující.

Kompletní tisková zpráva ve formátu Microsoft Word Document (.docx), Adobe PDF (.pdf).

Fakulta informačních technologií Českého vysokého učení technického v Praze **(FIT) obecně spolupracuje s orgány činnými v trestním řízení a dalšími státními institucemi v dobré víře a úmyslu napomoci těmto orgánům svými znalostmi a odbornou expertízou.** FIT vstoupila v roce 2013 do smluvního vztahu se společností Bull s.r.o. a zavázala se poskytnout expertízu svých pracovníků v oblasti vývoje softwarových řešení s ohledem na výše uvedené. Při podpisu smlouvy nebyly FIT známy informace o charakteru celého projektu a konečném příjemci. Společnost Bull s.r.o., toho času disponující certifikací na stupeň utajení Tajné podle zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, se FIT zaručila, že takovéto plnění bude poskytnuto toliko státním institucím. V rámci smlouvy mezi FIT a Bull s.r.o. bylo vyvinuto a poskytnuto společnosti Bull s.r.o. při podpisu smlouvy jedno plnění, které však nebylo společností Bull s.r.o. ani jinou společností použito. Firma Bull s.r.o. i FIT v této věci postupovaly striktně v souladu s platnými zákony a toto poskytnuté plnění nemá žádnou souvislost s tzv. „exploity“ ani zranitelnostmi popisovanými v posledních dnech v médiích.

www.isvav.cz – bezpečnostní výzkum ČR

VF20142015037 - Dekódování šifrovaných datových komunikací (2014-2015, MV0/VF)

Údaje o projektu

Identifikační kód	VF20142015037
Důvěrnost údajů	U - Předmět řešení projektu je utajovanou skutečností podle zvláštních právních předpisů nebo je skutečností, jejíž zveřejnění by mohlo ohrozit činnost zpravodajské služby. Dodané daje jsou upraveny tak, aby byly zveřejnitelné
Název v původním jazyce	Dekódování šifrovaných datových komunikací
Poskytovatel	MV0 - Ministerstvo vnitra (MV)
Program	VF - Bezpečnostní výzkum pro potřeby státu v letech 2010 až 2015 (2010-2016)
Kategorie VaV	AP - Aplikovaný výzkum
Hlavní obor	IN - Informatika
Zahájení řešení	2.9.2014
Ukončení řešení	31.12.2015
Datum posledního uvolnění účelové podpory	28.11.2014
Číslo smlouvy	VF20142015037
Poslední stav řešení	K - Končící víceletý projekt, tj. projekt, který byl řešen již v předcházejícím roce, příslušný rok sběru dat je posledním rokem účinnosti smlouvy resp. vykonatelnosti rozhodnutí o poskytnutí podpory

Finance projektu

Období	2014	2015	celkem
Výše podpory ze státního rozpočtu	1 179 tis. Kč	2 704 tis. Kč	3 883 tis. Kč
Celkové uznané náklady	1 179 tis. Kč	2 704 tis. Kč	3 883 tis. Kč
Typ	skutečně čerpané	přidělené	

Druh soutěže	VZ - Veřejná zakázka podle zákona č. 199/1994 Sb., resp. podle zákona č. 40/2004 Sb., o veřejných zakázkách
Cíle řešení v původním jazyce	Cílem projektu je výzkum nových metod pro odhalování a vyšetřování případů kybernetické kriminality a ochrany informačních systémů před kybernetickými hrozbami.
Klíčová slova v anglickém jazyce	data; communication; cyber; protection
Rok dodání údajů do CEP	2015
Systémové označení dodávky dat	CEP15-MV0-VF-R/02:2
Datum dodání záznamu	25.3.2015

Účastníci projektu

Počet příjemců	1
Počet dalších účastníků projektu	0
Příjemce / Organizační jednotka garantující řešení	Masarykova univerzita / Ústav výpočetní techniky
Řešitel	doc. Ing. Pavel Čeleda, Ph.D. (státní příslušnost: CZ - Česká republika; vedidk: 6606288)

Co to znamená?

- Policie sama neumí nasazovat malware
- ale dělá to za pomoci externích firem
- vysoké školy pracují na útocích proti našemu soukromí
- nepřiměřeně vysoké náklady na útoky
- zpochybnitelnost důkazů předložených soudům

```ruby
require 'rcs-common/evidence/common'

require 'digest/md5'

module RCS

module FileopenEvidence

  ELEM_DELIMITER = 0xABADC0DE

  def content(*args)
    hash = [args].flatten.first || {}

    process = hash[:process] || ["Explorer.exe\0", "Firefox.exe\0", "Chrome.exe\0"].sample
    process.encode!("US-ASCII")

    path = hash[:path] || ["C:\\Utenti\\pippo\\pedoporno.mpg", "C:\\Utenti\\pluto\\Documenti\\childporn.avi", "C:\\secr
    path = path.to_utf16le_binary_null

    content = StringIO.new
    t = Time.now.getutc
    content.write [t.sec, t.min, t.hour, t.mday, t.mon, t.year, t.wday, t.yday, t.isdst ? 0 : 1].pack('l*')
    content.write process
    content.write [ 0 ].pack('L') # size hi
    content.write [ hash[:size] || 123456789 ].pack('L') # size lo
    content.write [ 0x80000000 ].pack('l') # access mode
    content.write path
    content.write [ ELEM_DELIMITER ].pack('L')
    content.string
  end

```

Rizika

- Hacking Team měl pravděpodobně C&C server v infrastruktuře policie (backdoor?)
- soukromá data uživatelů se dostala ke komerční firmě s pochybnou pověstí (Bull měl údajně bezpečnostní prověrku, ale Hacking Team ne)
- možnost plošného nasazení? (NIA)

❇ „ani soudce o tom nebude vědět“

„Hello Massimiliano

Sure, no problem

14 - This point is in RFP because customer want to keep the information that they have such a system confidential. Even for trial (judge) this information will not be available. The group of persons who know about this technology will be limited. BULL will sign NDA for this project.

15 - This point refers to infection invisibility“

(tomas.hlavsa@bull.cz, 2010-07-23)

https://wikileaks.org/hackingteam/emails/emailid/437403

Obrana

- pozor na to, co instalujete
- nepoužívat Adobe Flash
- updatovat prohlížeč
- opatrně na přílohy
- používat Linux
- pozor na falešný pocit bezpečí

http://eldar.cz/kniha