

Stav informační bezpečnosti dnes v 07:00 SEČ ráno

Jakub Urbanec

Radoslav Bodó

Miloš Frýba



Stav informační bezpečnosti

Agenda



Dan Kaminsky

- Velmi nebezpečná chyba
- Obrovský dopad
- Moudré dočasné řešení
- Společná práce aka Císařův pekař



Dan Kaminsky

- DNS cache poisoning
- Záplava podvržených DNS odpovědí

```
Radek do práce:  
900117117
```

```
Kuba 2840
```

```
RADEK 15
```

```
eros.zcu.cz  
147.228.1.10
```

```
ns.t1.cz  
194.108.44.22
```


Dan Kaminsky

- DNS je jako telefonní seznam. Překládá jména na čísla. (umí to ale i naopak)
- Umí toho víc, ale není z papíru

Radek do práce:
900117117

Kuba 2840

RADEK 15

eros.zcu.cz
147.228.1.10

ns.t1.cz
194.108.44.22

Dan Kaminsky

- Cache – dočasně uložená čísla
- Papírek na ledničce

hmmms
ale co když se číslo
změní?

- Vyhledáme v tel.seznamu, napíšeme na papírek
- Vyhledáme v DNS, počítače si to pamatují sami

Dan Kaminsky

- Platnost čísel se mění
- Telefonní seznam se publikuje jednou ročně
- DNS se nepublikuje
- Záznamy v DNS mají platnost – cache si čísla pamatují dobu platnosti TTL

- **ns.tl.cz**
194.108.44.22
TTL 1den

Radek: 15
TTL 1rok

Dan Kaminsky

- Jak se číslo zjistí?
- Seznam prohledám.
- DNS – křičím do sítě

Já: ns.t1.cz?

NS: 194.108.44.22

Já: Radek?

Seznam: 15

Dan Kaminsky

- Ale ale! Co když bude odpovídat falešný NS/Seznam.
- Dostanu dvě odpovědi, беру první.
- Ajaj!

Já: ns.t1.cz?

NS: 147.228.1.48

NS: 194.108.44.22

Já: Radek?

Seznam: 20

Seznam: 15

Dan Kaminsky

- DNS se brání
- Do žádosti vkládám náhodné číslo

64k should be good enough for anyone

Já: ns.t1.cz:6?

NS: 147.228.1.48

NS: 194.108.44.22:6

Já: Radek:6?

Seznam: 20

Seznam: 15:6

Dan Kaminsky

- DNS se brání špatně
- Do žádosti vkládám náhodné číslo, ale málo náhodné.
- Hmmms

Já : radek : 6?

NS : 20 : 1

NS : 20 : 3

NS : 20 : 6

NS : 15 : 6

Dan Kaminsky

- Skutečný útok je složitější, zahrnuje práci s TTL, ale jako základ to stačí
- (útok proti mezilehlému NS, podvržené NS záznamy po záplavě neexistujících dotazů...)

Já : radek : 6?

NS : 20 : 1

NS : 20 : 3

NS : 20 : 6

NS : 15 : 6

Dan Kaminsky

- Dan Kaminsky: přidat náhodu. (Source port randomization)
- Já to říkal!
Dan Bernstein
DJBDNS

Já z místa 4534:
radek:6759?

NS: **radek 20:1**

NS: **radek 20:6**

NS: 4534:**15**:6759

Dan Kaminsky

- Je to dobré řešení?
- 64k x 64k
- V dnešní době rychlých sítí...
- Co vy na to?



Dan Kaminsky

- Je to dobré řešení?
- DNS potřebuje generálku
- DNSSec je složité pro nasazení (NIC.CZ)



Dan Kaminsky

- Jak se chyba řešila

Ten umí to a ten zas tohle a všichni dohromady udělají moc

- Dan a Paul Vixie
- Schůzka v březnu v centrále MS (MS = hell?)
- Dohoda o vydání společné opravy



Dan Kaminsky

- 8. července byla uveřejněna oprava této chyby
- Největší synchronizovaná oprava v dějinách Internetu

Když všichni všechněm všechno dáme, tak budem všichni všechno mít dohromady.



Dan Kaminsky

- 8. července oprava ...
- Oprava byla zvláštní – nebylo z ní patrné, co vlastně opravuje
- 51 hodin po vydání opravy – první pokus o útok
- 6. srpen konference ~~European~~ BlackHat

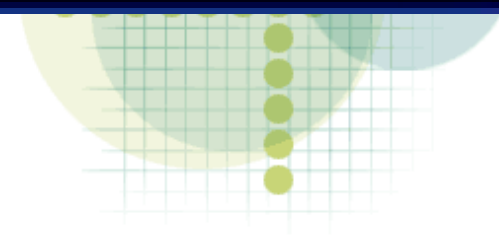


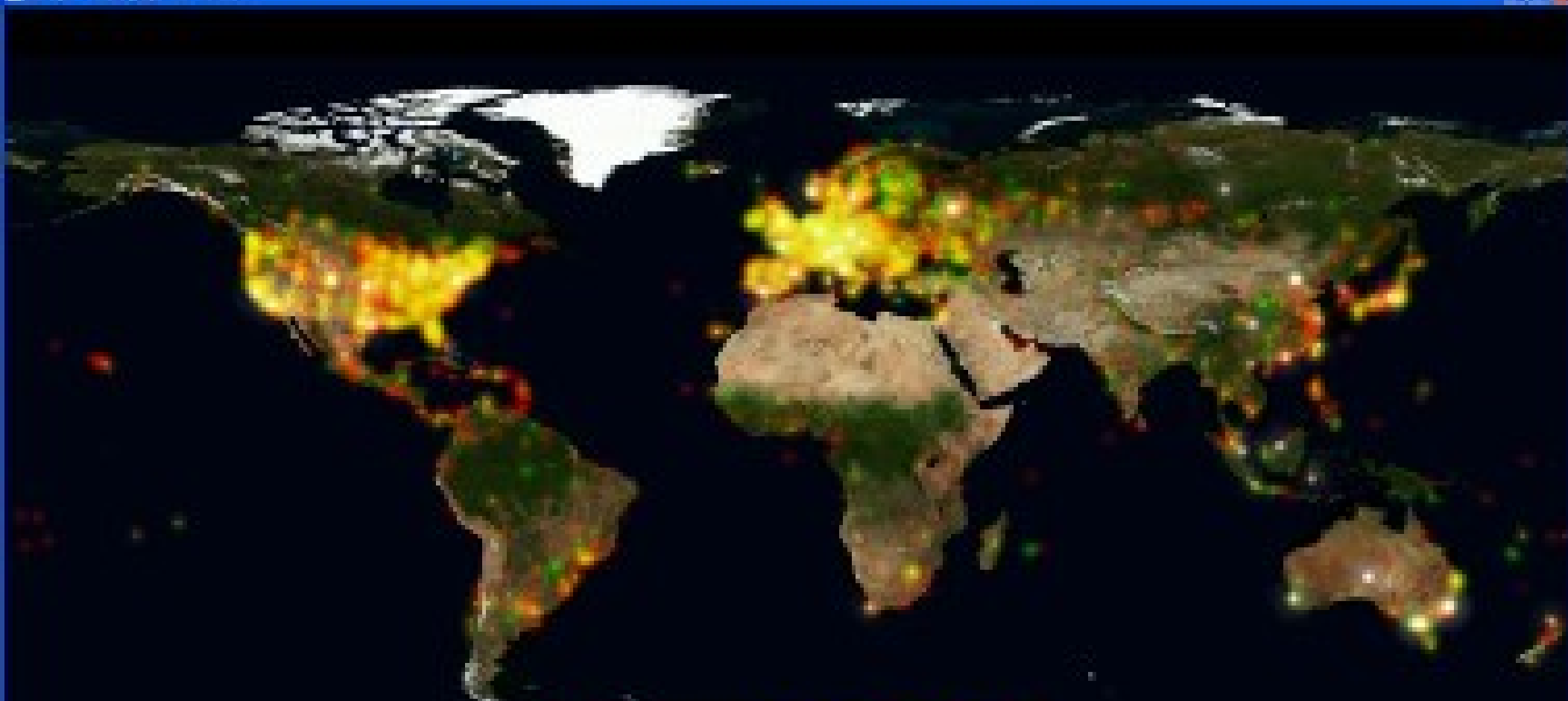


82.13% 2.67% 15.20%

Analysis of Worldwide DNS Register
from Doxpara.Com Data

2008-07-09 13:27:20

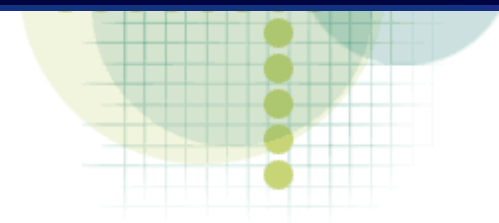


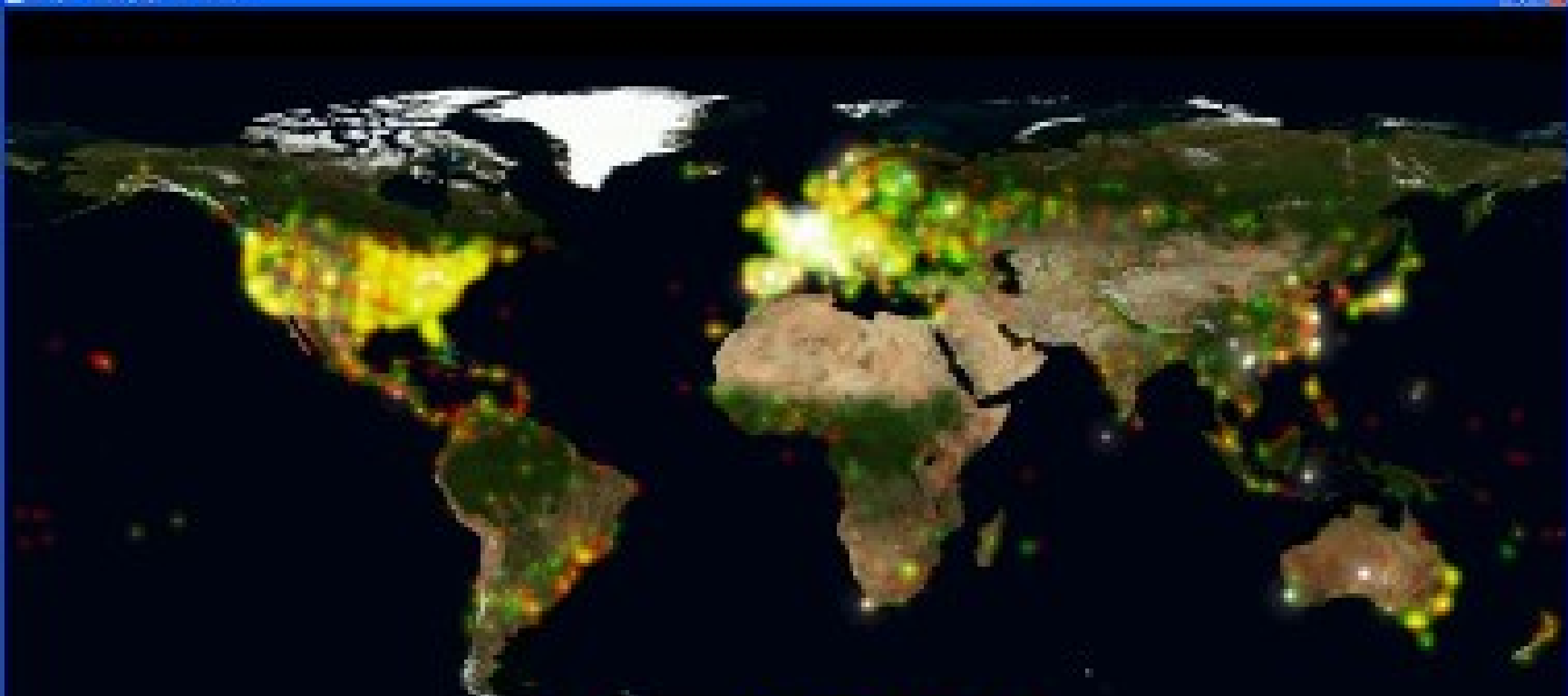


70.98% 4.18% 24.84%

Analysis of Kaminsky DNS Register
from Doxpara.Com Data

2008-07-16 06:40:02

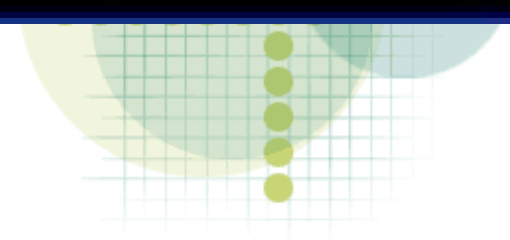


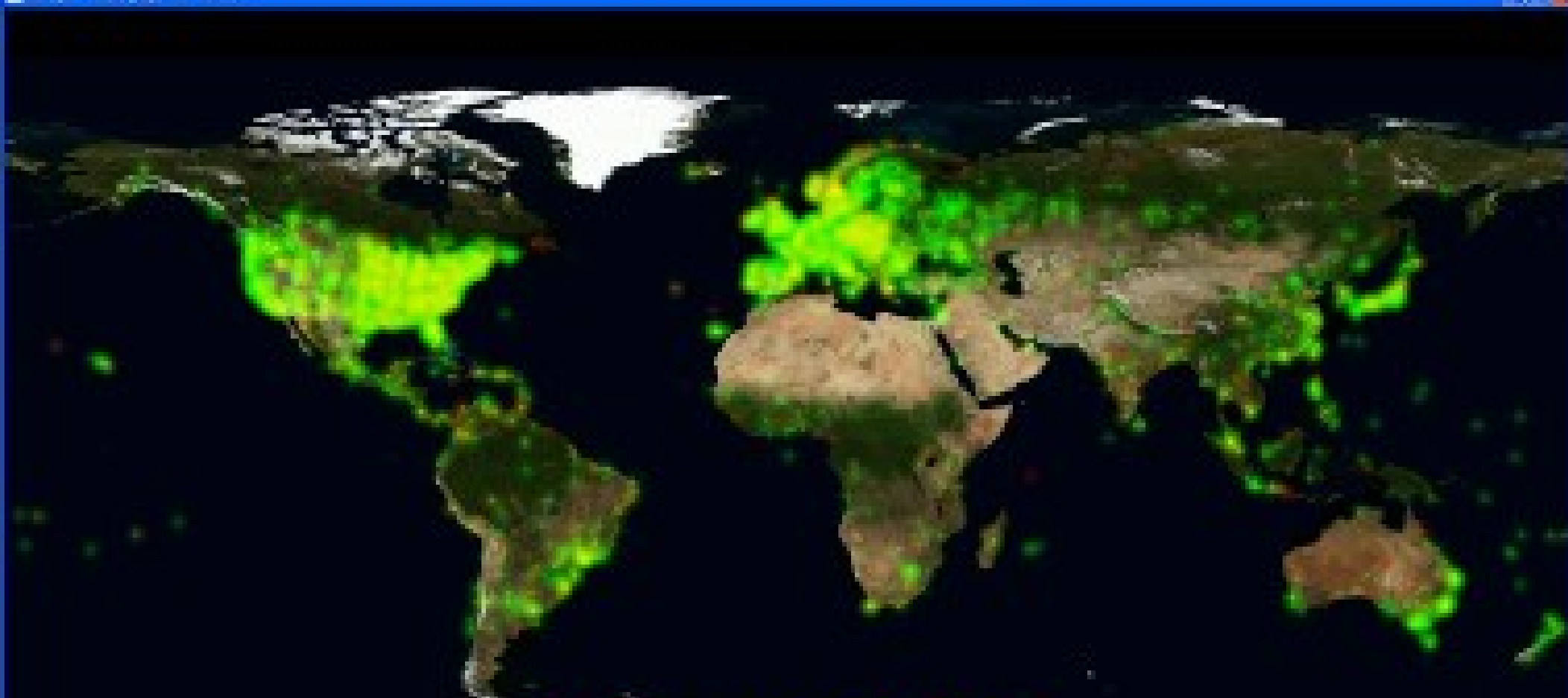


49.82% 7.76% 42.43%

Analysis of Kaminsky DNS Register
from Doxpara.Com Data

2008-07-23 10:32:35

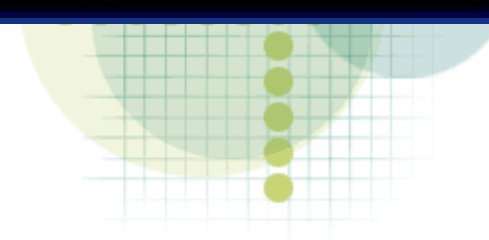




21.22% 13.91% 64.87%

Analysis of Randomly DNS Register
from Doxpara.Com Data

2008-08-03 20:04:15



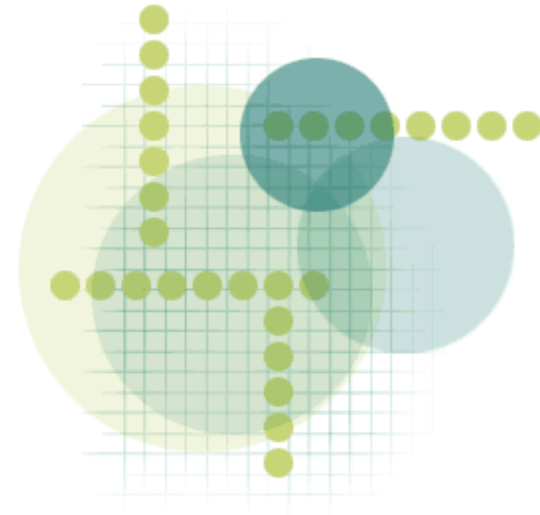
Dan Kaminsky

- No a co? Tak byla chyba v DNS
- www.yahoo.com To je toho
- Možná je toho víc...



Dan Kaminsky

- Mail:
 - Stažení MX záznamu – malá domů
 - Potvrzení o změně hesla, jiná potvrzení
 - AntiSPAM
 - Dopady další viz ...



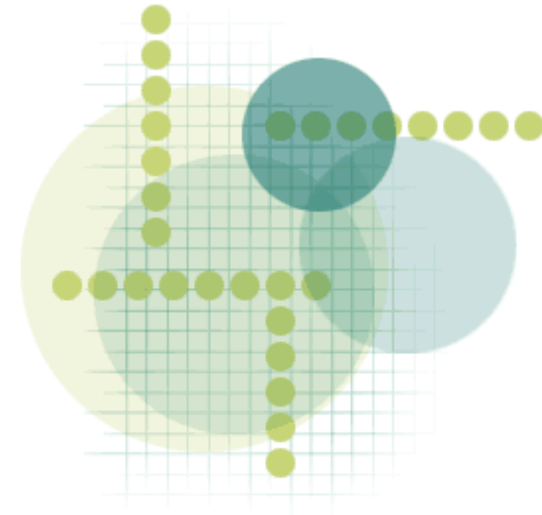
Dan Kaminsky

- SSL:
 - SSL je bezpečné
 - SSL je bezpečné
 - SSL je bezpečné
 - SSL je bezpečné
 - A pro zvlášť nechápavé novináře



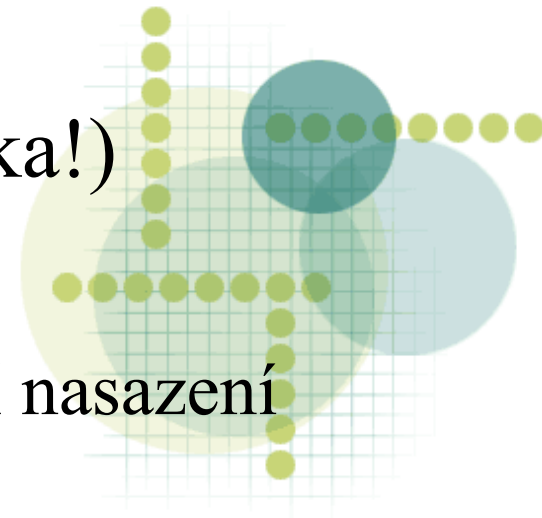
Dan Kaminsky

- SSL: si můžu koupit. Jak se validují domény?
 - Whois lookup aha DNS
 - Ověřovací mail ... aha MX DNS
 - Mrknu se na web ... ehm, zase DNS
- Jeden certifikát pro server www.microsoft.com prosím ...



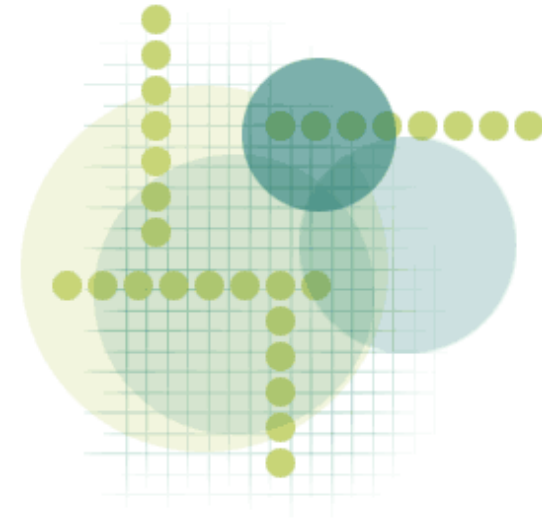
Dan Kaminsky

- 9.12.2008: VeriSign, NeuStar and others team on DNS security – Coalition of top-level domain operators seeks protection against the Kaminsky bug – to deploy DNSSec
- DJ Bernstein: DNSCurve (curve = křivka!)
 - DNSSEC sucks! Go for DNSCurve
 - Nepoužívá RSA, ale E.křivky, snazší nasazení



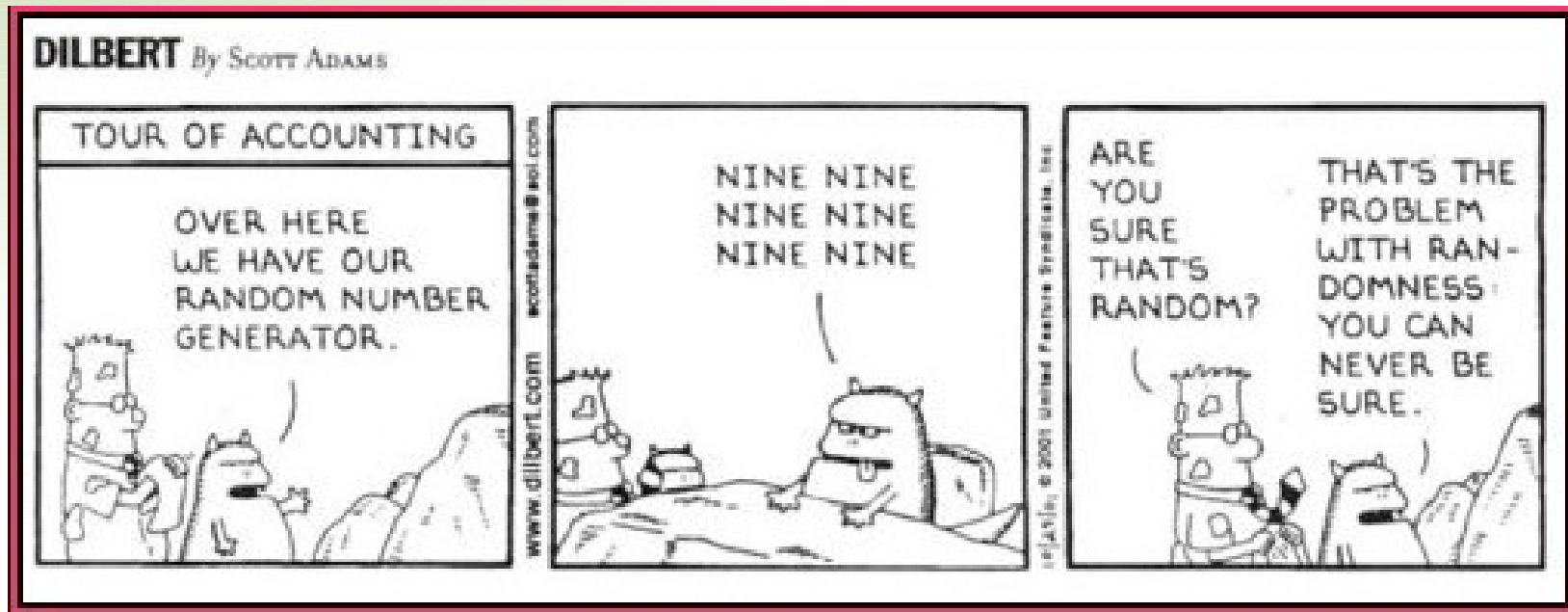
Dan Kaminsky

- **Ohrožení je velké**
 - ale málo pravděpodobné
- **Řešením je:**
 - **Důsledné a včasné aplikování oprav**
- **Možnosti obrany:**
 - Žádné (jako klient)
 - Používat DNSSec, DJBDNS
....a hlavu!



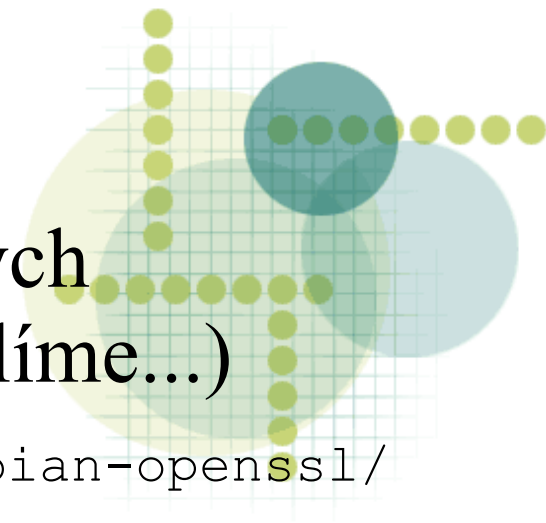
Debian OpenSSL

- 13. května 2008
- V OS Debian/GNU Linuxu a z něj odvozených distribucí byla nalezena chyba v balíčku OpenSSL.
- Vývojáři balíčků odstranili část kódu z náhodného generátoru, protože jim nástroje na kontrolu kódů generovaly varovná hlášení.
- Zbyla pouze entropie založená na PID procesu.



Debian OpenSSL

- Jakékoli klíče vygenerované na systémech s vadnou verzí openssl spadaly do velmi omezené množiny, která se dá předem spočítat.
... musí se vyměnit!
- Tajná část párového klíče se dá zjistit ze znalosti veřejné části.
To bychom od asymetrické kryptoografie nečekali...
- Chyba byla zanesena jako součást opravy jiného problému v roce 2006
- Rozsáhlé útoky pomocí těchto prozrazených klíčů se však nekonalý (alespoň si to myslíme...)
- <http://www.metasploit.com/users/hdm/tools/debian-openssl/>



Clickjacking

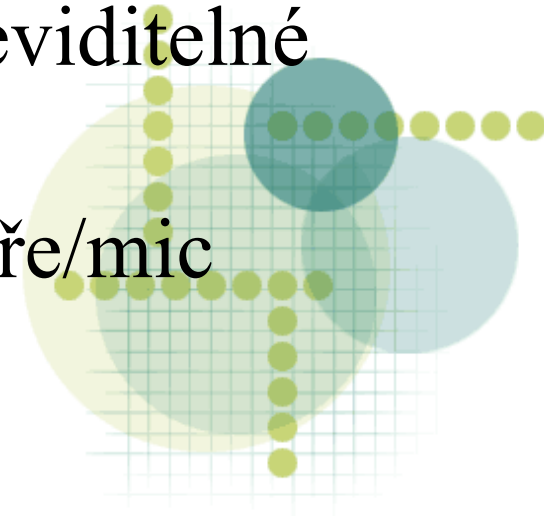
- **Hijack – únos**
- **Clickjack – únos kliku ;-)**
- **Je to typ XSS útoku viz minulá přednáška
Europen, podzim 2008**

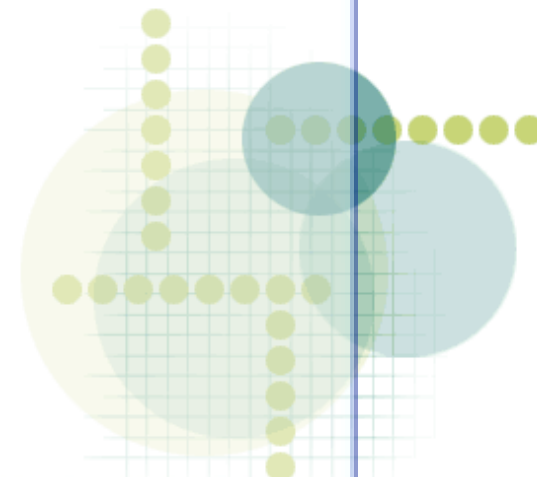
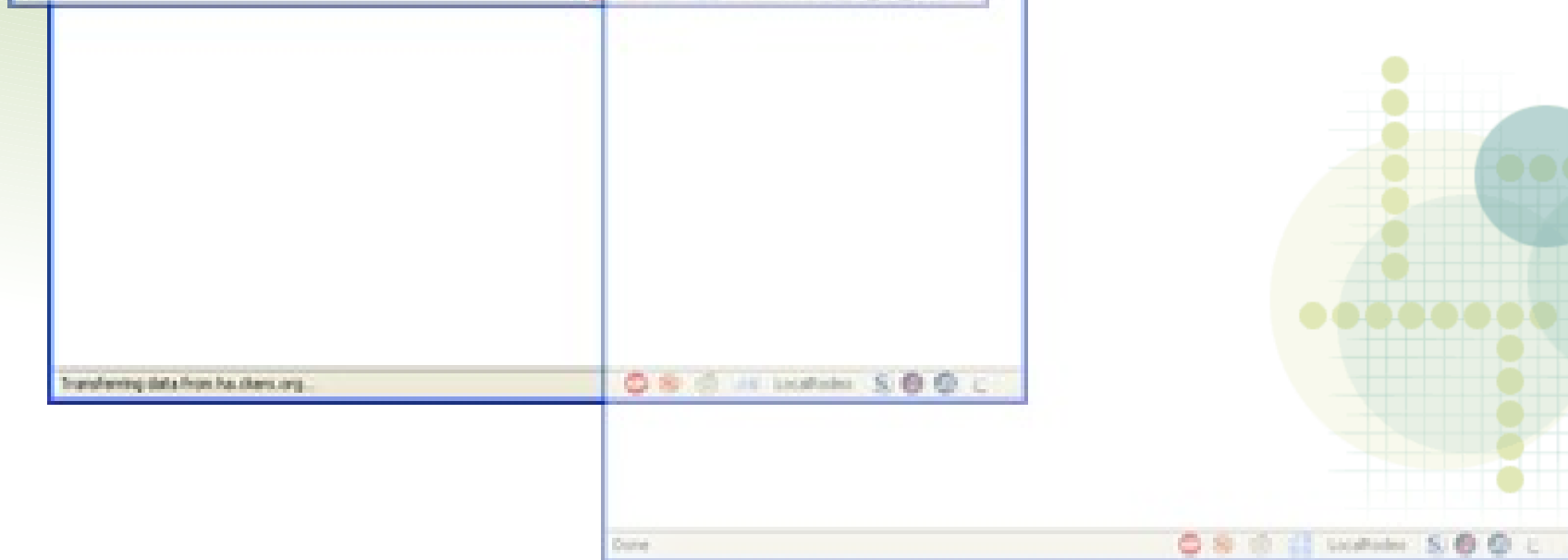
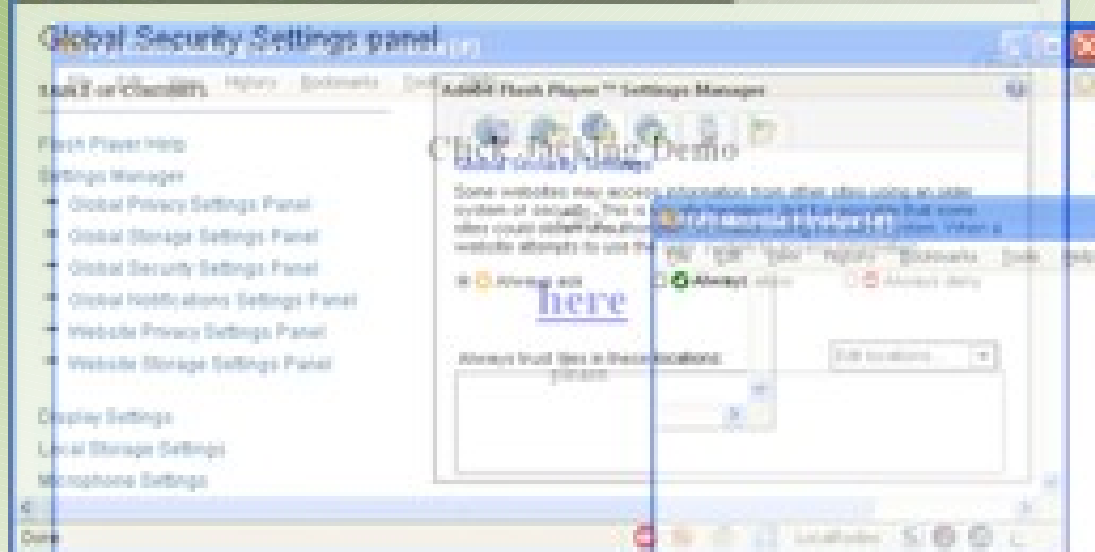
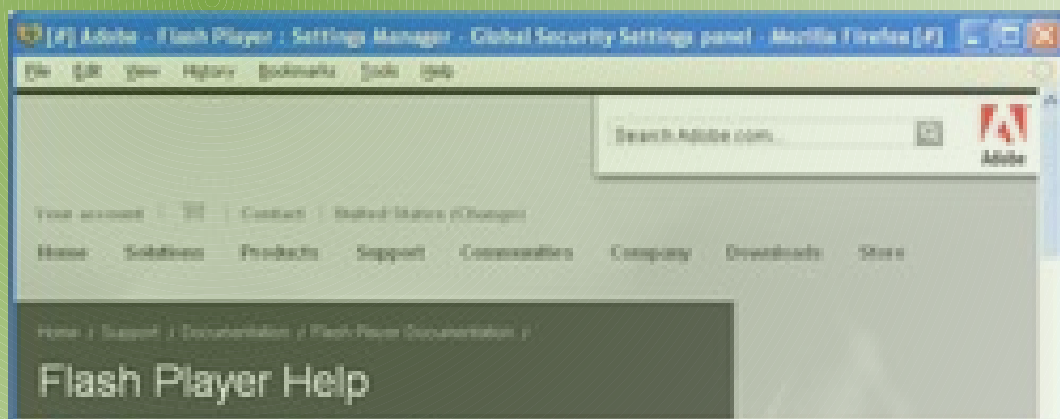


Clickjacking

- **První předvedení:**

- Společně s Flash aplikací (hra) útočník získá přístup k mikrofonu a kameře
- Metoda tupý pták (nevidí sklo)
 - Neviditelné okno (iframe) přes prohlížeč – kamkoliv kliknete, kliknete na neviditelné okno...
 - ... a tím povolíte přístup ke kameře/mic





Clickjacking

- **Možnosti:**
 - Iframe před přihlašovacím oknem:
 - Hotmail, seznam, gmail...
 - Internet banking
 - ... kde všude se přihlašujete z webu?



Clickjacking

- **Ohrožení je malé**
 - ale možné
- **Řešením je: (někdy)**
 - **Důsledné a včasné aplikování oprav**
- **Možnosti obrany:**
 - Vypnutý JS, Flash
 - Links, w3m, NCSA Mosaic
 - NoScript



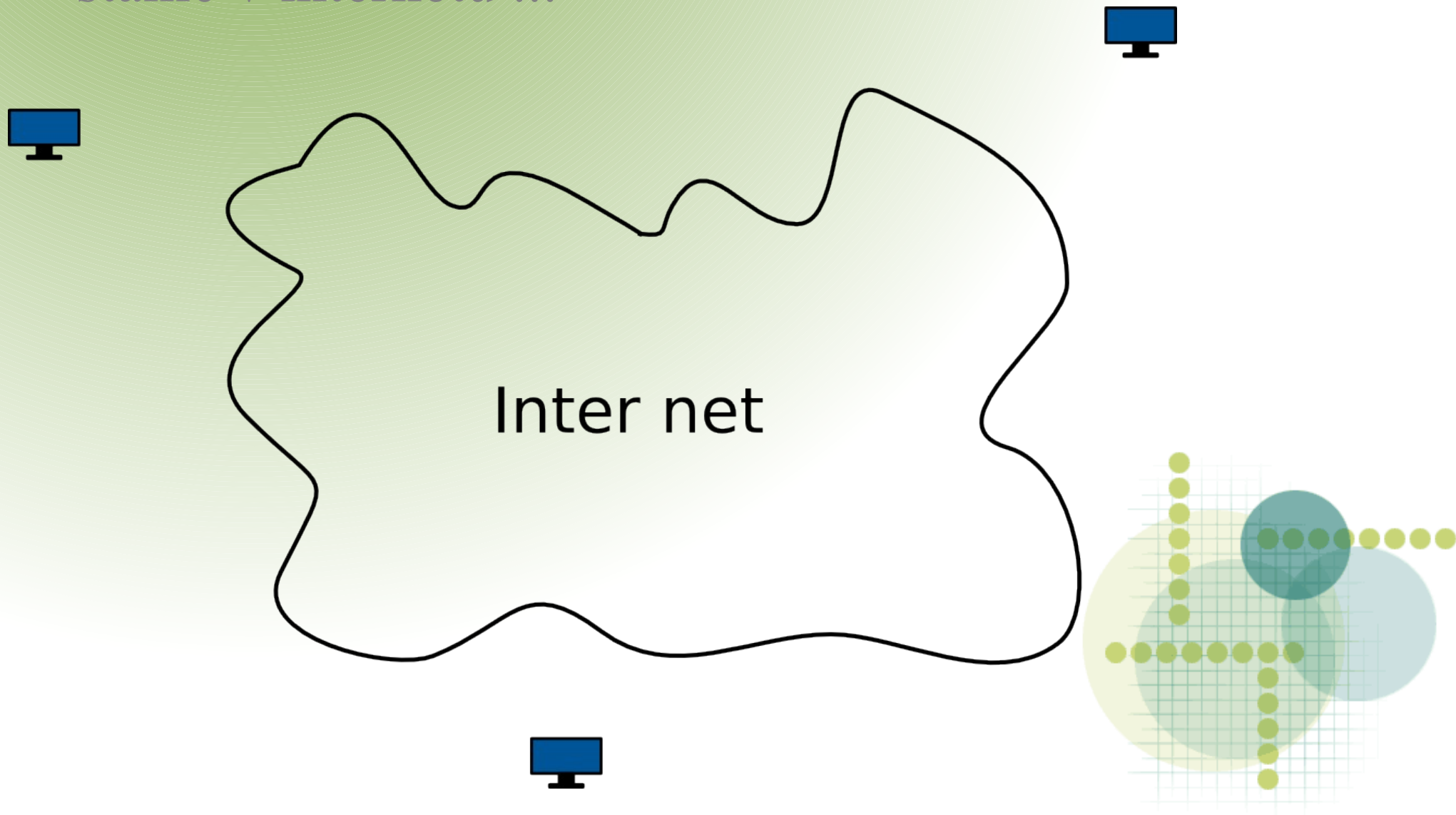
Vývoj C&C v kostce

- *David Dittrich, Sven Dietrich*
Command and Control structures in malware
- *Sam Stover, Dave Dittrich, Joe Hernandez, Sven Dietrich*
Analysis Storm and Nugache trojan: P2P is here
- *Joe Steward*
Inside the Storm: Protocols and Encryption of the Sorm Botnet
- *Brandon Enright*
Exposing Stormworm
- Wikipedia: Kademlia



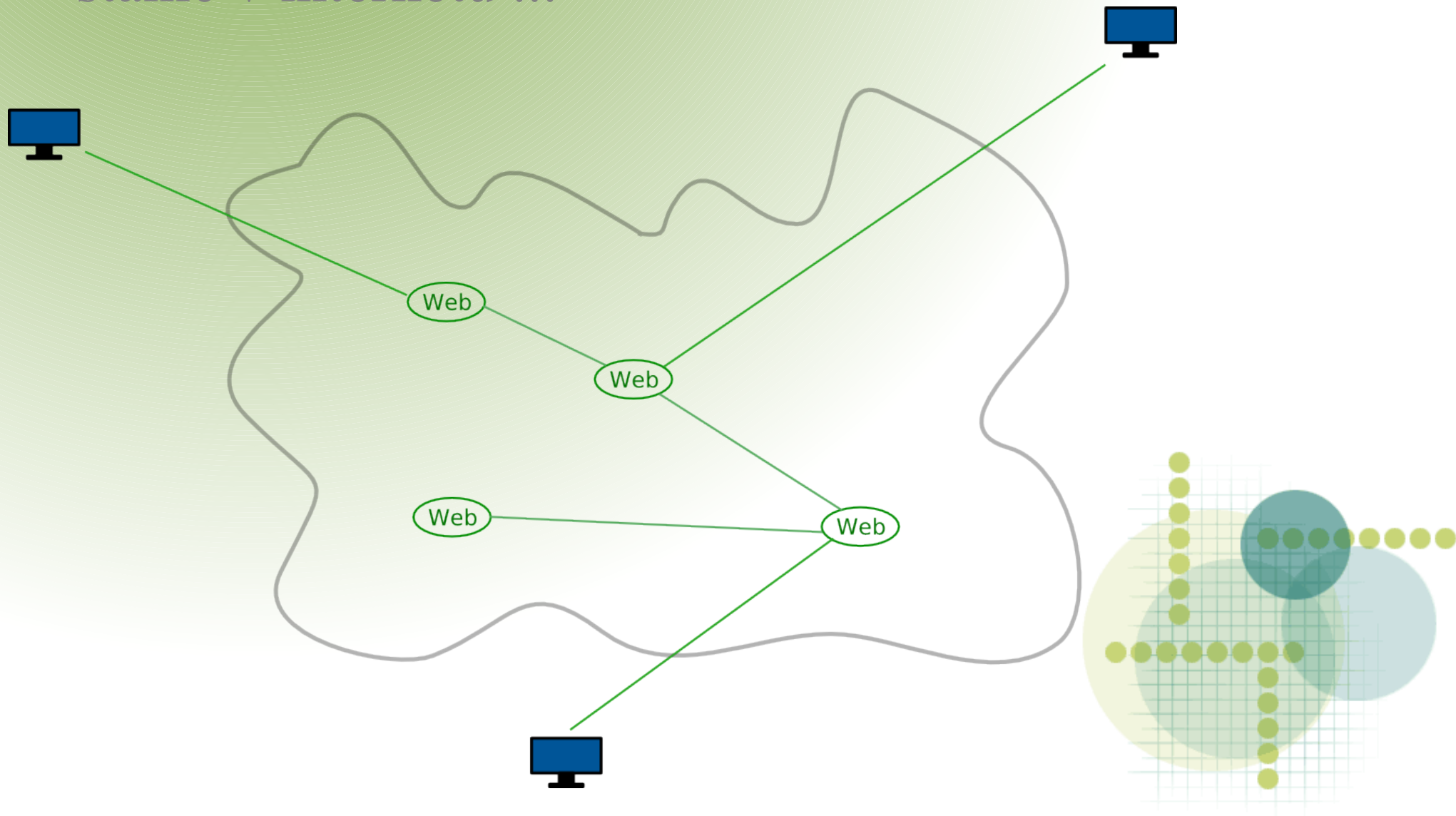
Vývoj C&C v kostce

- botnet - systém jak ovládat velký počet napadených stanic v internetu ...



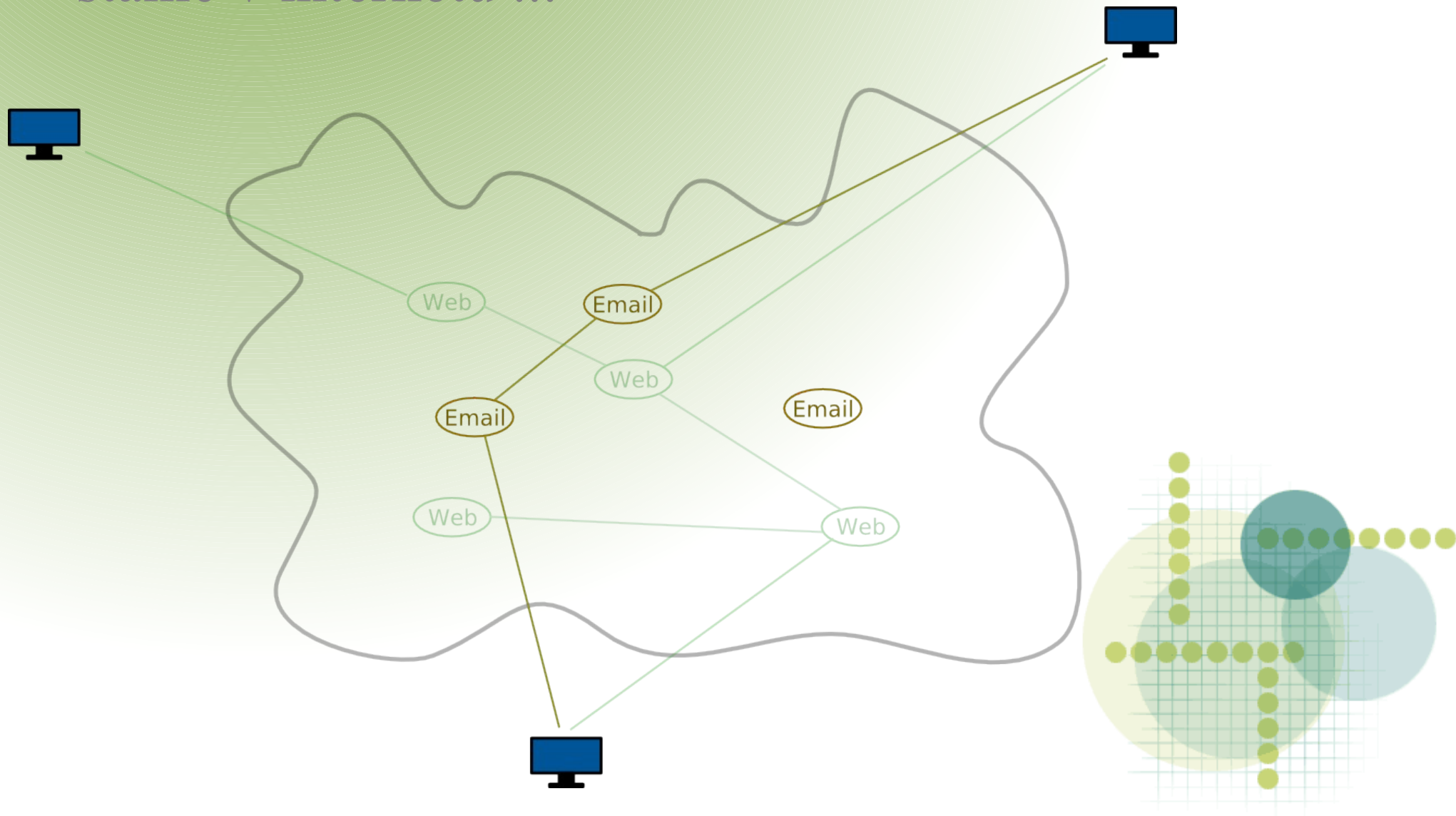
Vývoj C&C v kostce

- botnet - systém jak ovládat velký počet napadených stanic v internetu ...



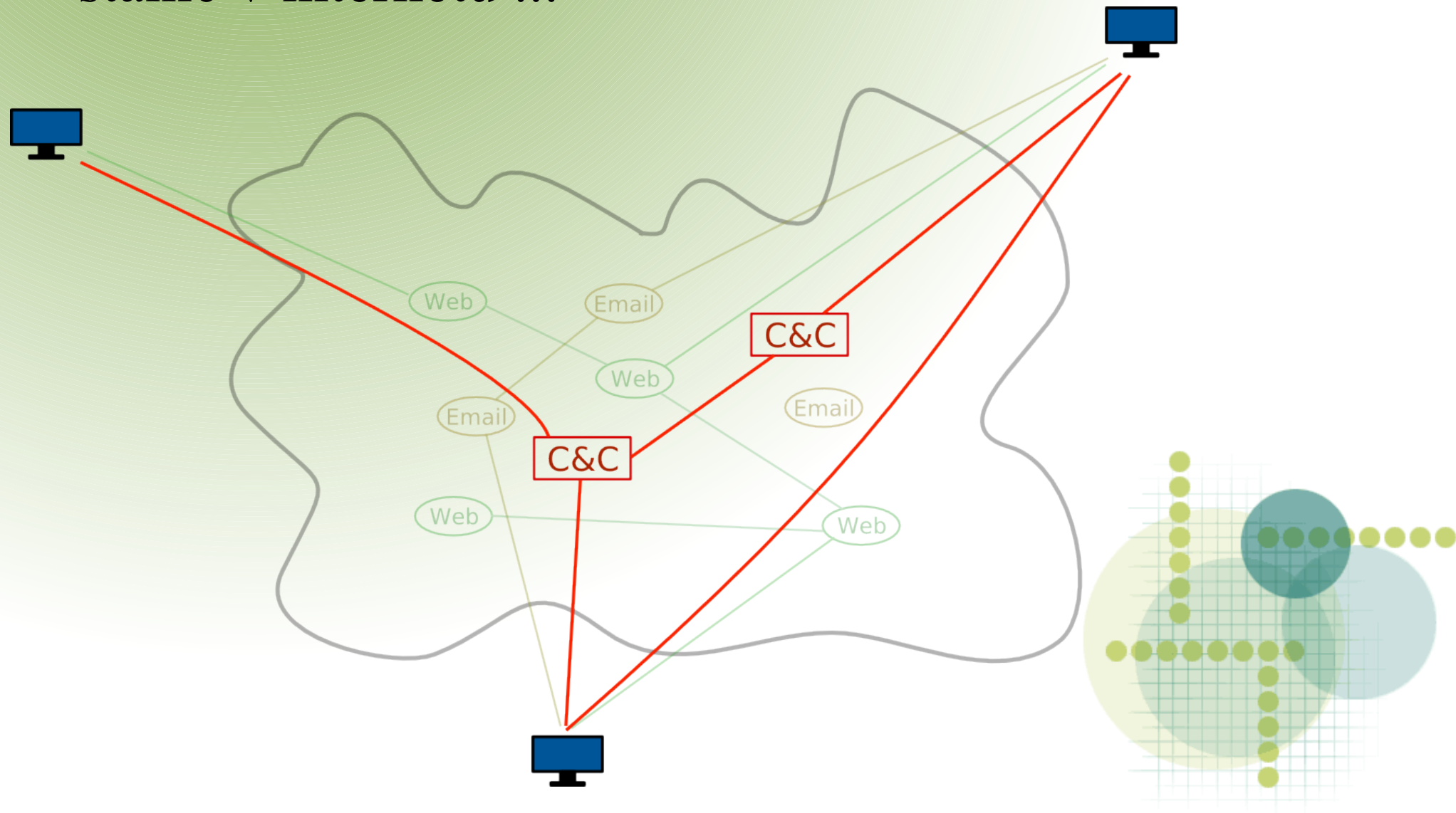
Vývoj C&C v kostce

- botnet - systém jak ovládat velký počet napadených stanic v internetu ...



Vývoj C&C v kostce

- botnet - systém jak ovládat velký počet napadených stanic v internetu ...



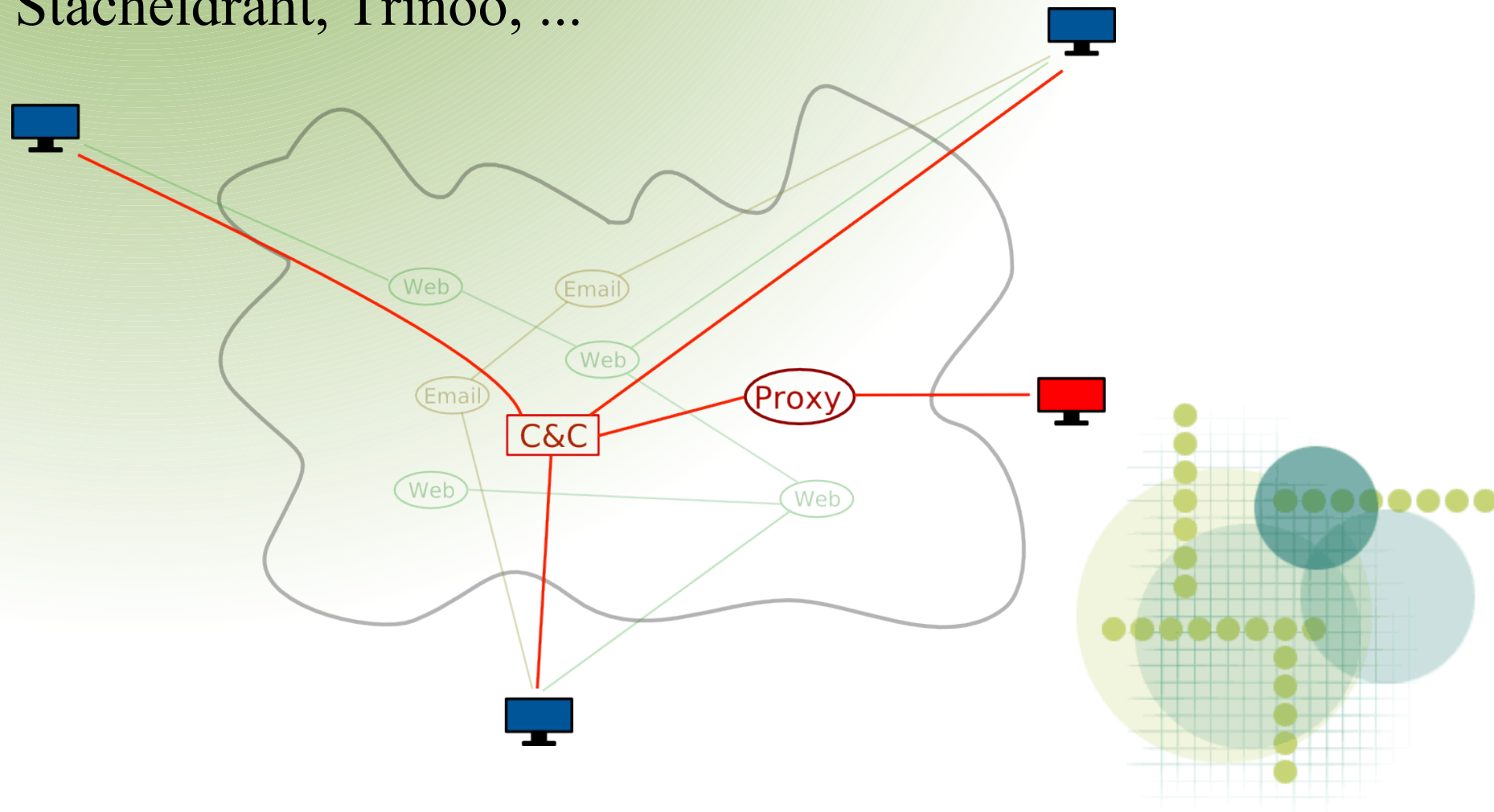
Vývoj C&C v kostce

- *DDoS*
- *Spam, Phishing/Scam*
- *Pump & Dump* - ovlivňování cen menších akciových pomocí falešných zpráv (spamu, IM, ...)
- *Click Fraud* - falešné imprese na reklamních banerech
- Vykrádání hesel, osobních údajů
- Vykrádání sériových čísel legálně zakoupených produktů
- Lámání hashů, šifer, hesel :(, ...
- ...



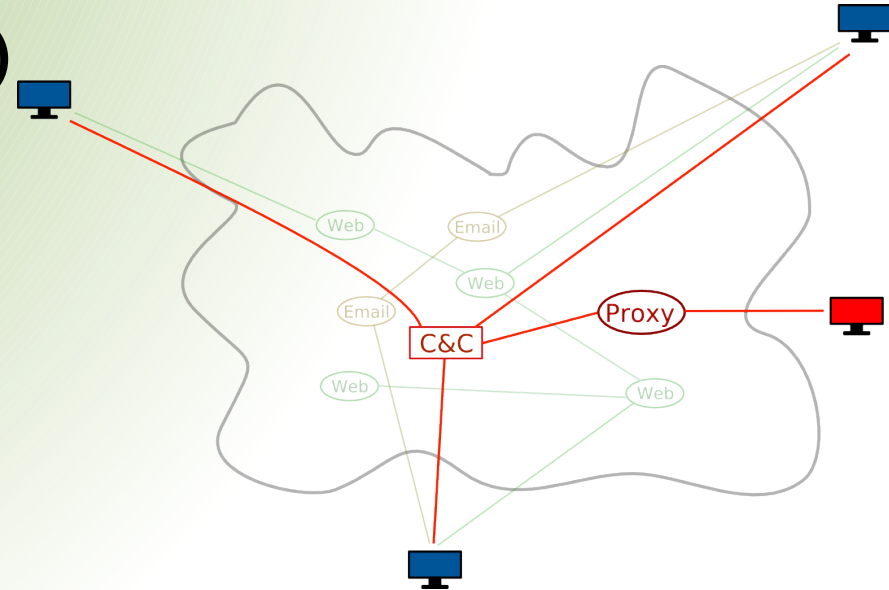
Vývoj C&C v kostce

- < 1998
- Handler/Agent (Master/Slave)
 - Stacheldraht, Trinoo, ...

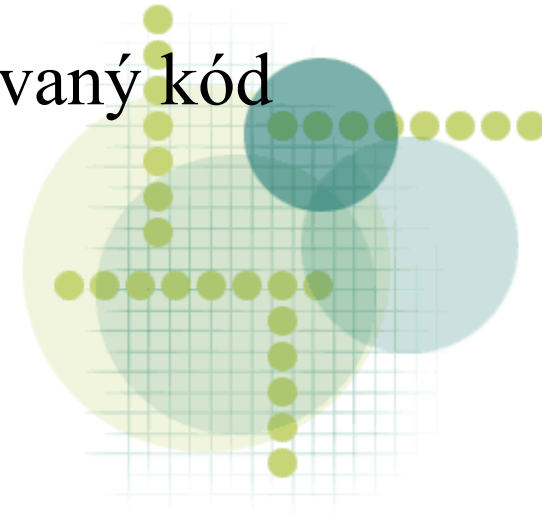


Vývoj C&C v kostce

- < 1998
- Handler/Agent (Master/Slave)
 - Stacheldraht, Trinoo, ...

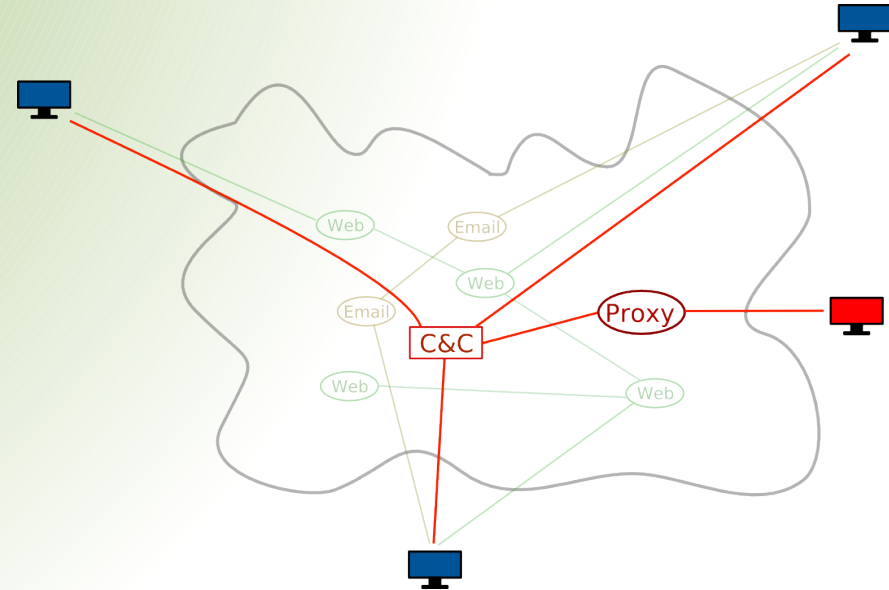


- Statické hodnoty zabudované přímo v malwaru
- Speciální komunikační protokol, specializovaný kód
- Limitovaný nastavením OS (počet otevřených souborů/spojení)
- Sledování: pomocí analýzy TCP



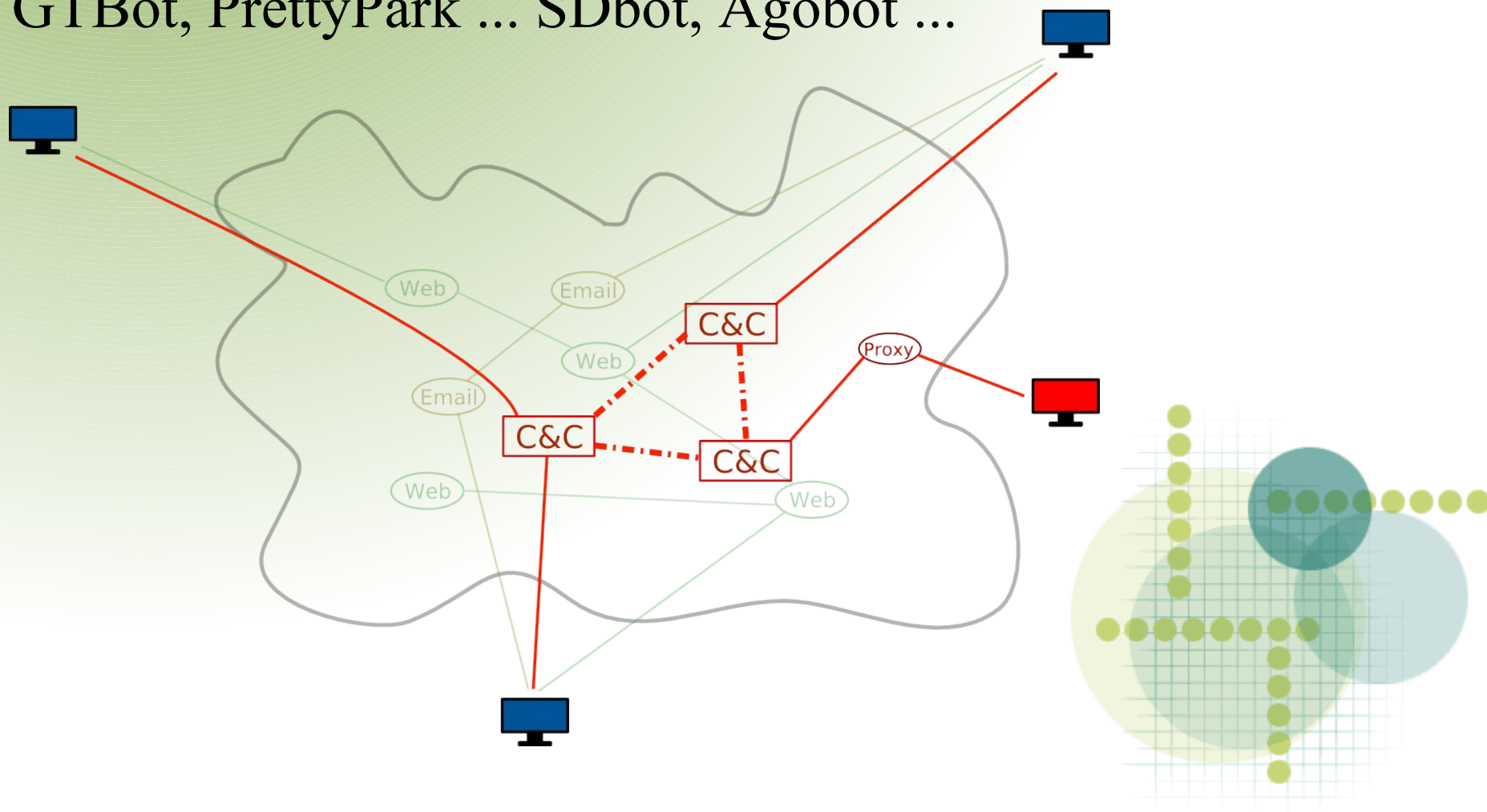
Vývoj C&C v kostce

- ? 1999, 2000 ?
- Web
 - Connect & forget
 - File Data
- FTP, Drop Zones
 - Haxdoor, Dumador
- IM
 - MSN, AIM, ICQ, ... (velmi málo)



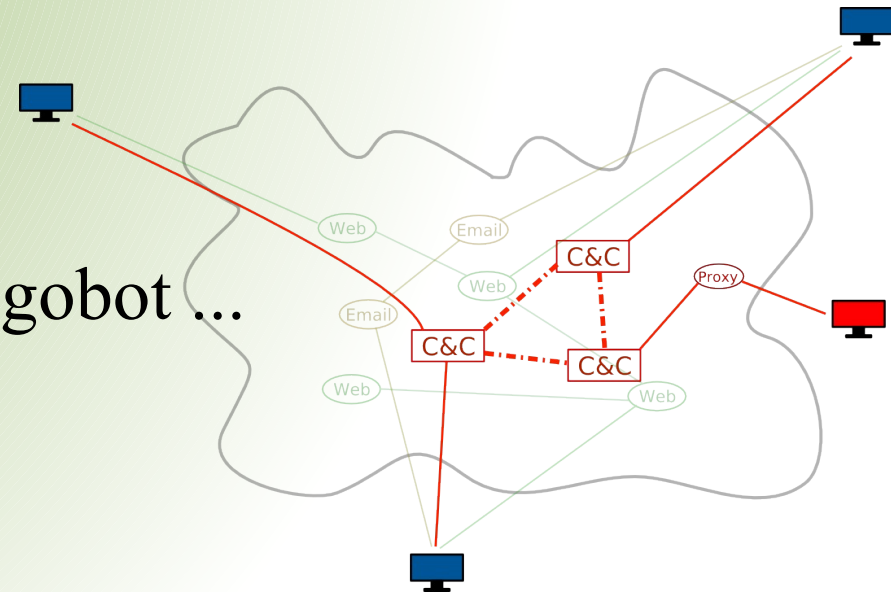
Vývoj C&C v kostce

- 1999, 2000
- IRC (IM podobné ICQ, Jabberu, ...)
 - GTBot, PrettyPark ... SDbot, Agobot ...

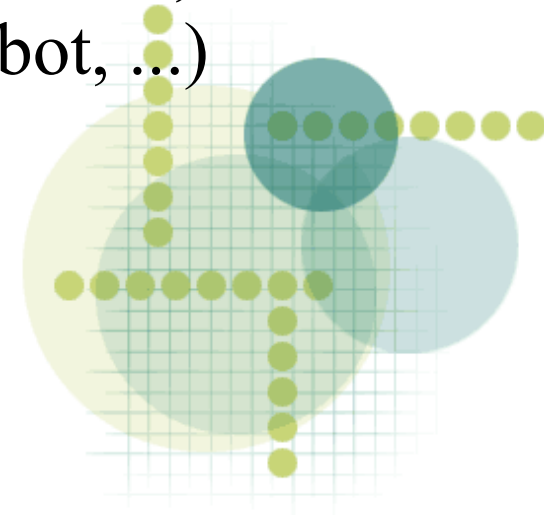


Vývoj C&C v kostce

- 1999, 2000
- IRC
 - GTBot, PrettyPark ... SDbot, Agobot ...

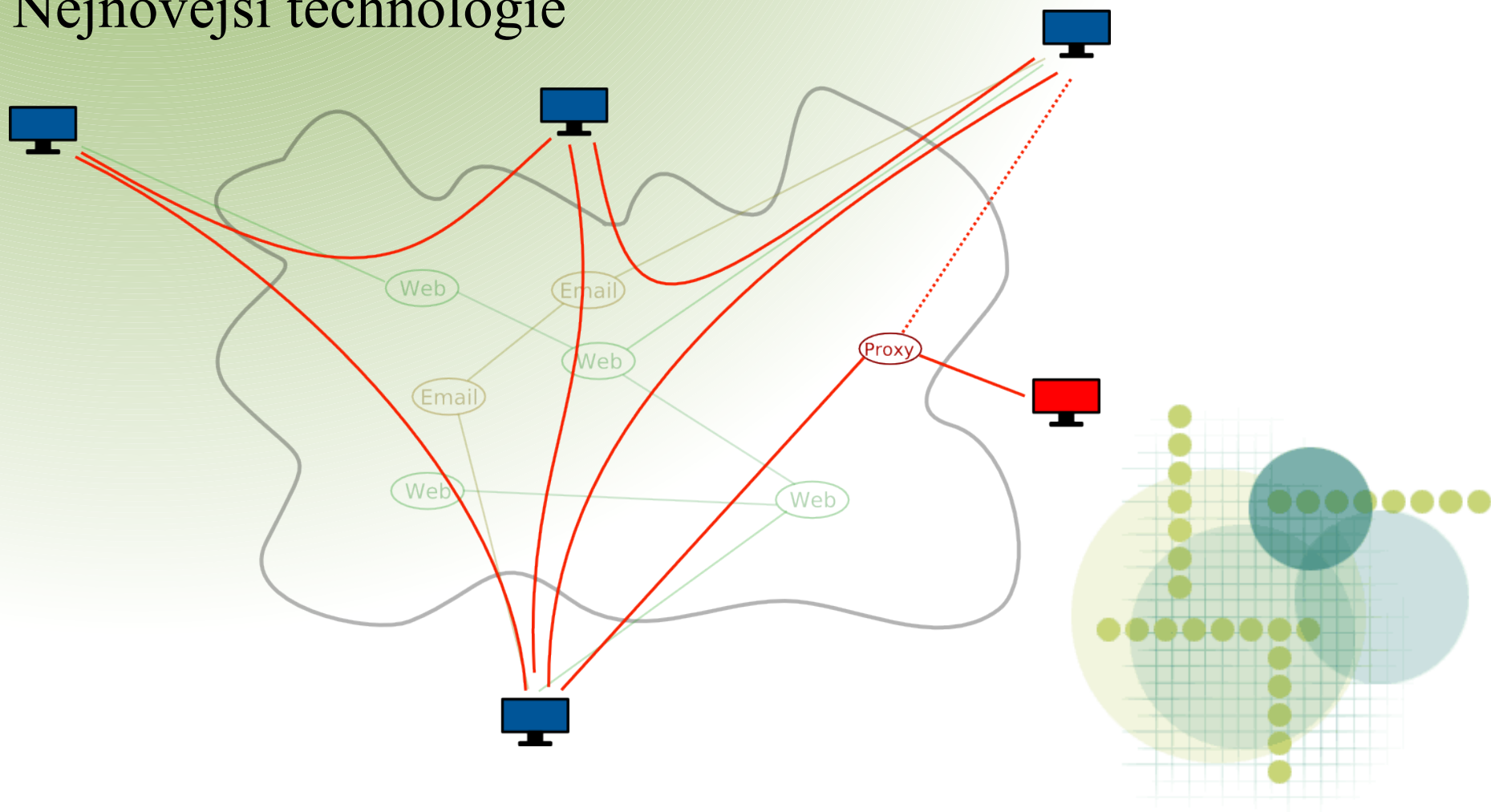


- Lépe škálují, stabilní protokol, distribuovaný C&C
- Realizace: pluginy, standardní boti (EnergyMech, EggDrop), speciální malware (Knight, Agobot, ...)
- Sledování:
 - těžké díky existenci mezilehlé IRC sítě mezi jednotlivými agenty a botmasterem
 - hromadné akce skupin uživatelů/robotů



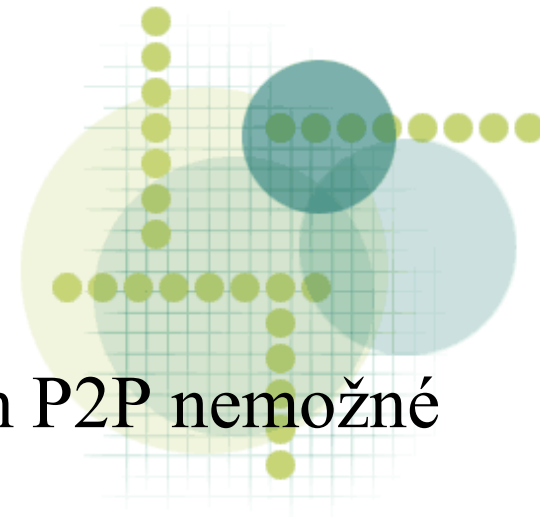
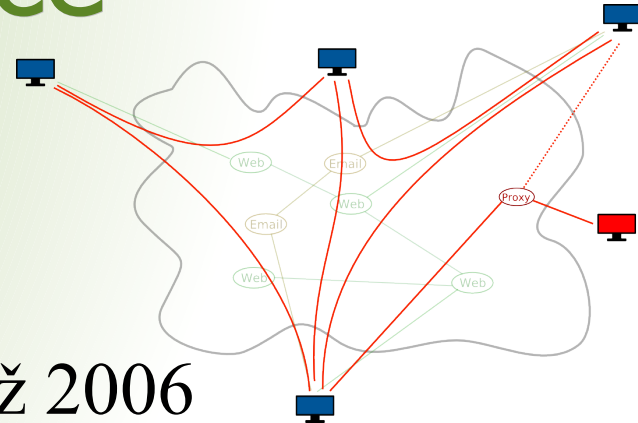
Vývoj C&C v kostce

- 2002 - 2008
- P2P
 - Nejnovější technologie



Vývoj C&C v kostce

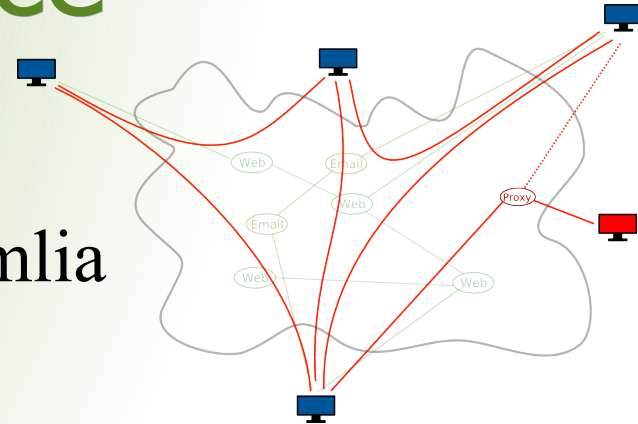
- 2002 - 2008
- P2P
 - Začala se vyvíjet již 2000, ale ujala se až 2006
 - 2002 Linux Slapper – pro vysokou *hlučnost* byl nástup zastaven
 - 2003 Agobot/Phatbot – obsahuje nevyužitý základ P2P
 - 2004 Phatbot – protokol WASTE
 - 2007 Storm, StormWorm, SotrmBotnet – noční můra
 - Detekce je velmi obtížná
 - Snort
 - BotnetHunter
 - Rozebrání díky propracovaným protokolům P2P nemožné



Vývoj C&C v kostce

- Storm

- Objeven 2007, eDonkey/Overnet/Kademlia
- Primárně se šíří pomocí emailu (svátky, olympiáda, elektronické pohlednice, ...)
- Modulární (spam, DdoS, Pump&Dump, proxy, Phishing, ...)
- Složení: Apache C&C, nginx proxy, public nody, private nody
- P2P pouze pro vyhledávání informací k formování botnetu
- Rootkit pro ukrývání na napadeném systému



- Nugache (tcp/8 bot)

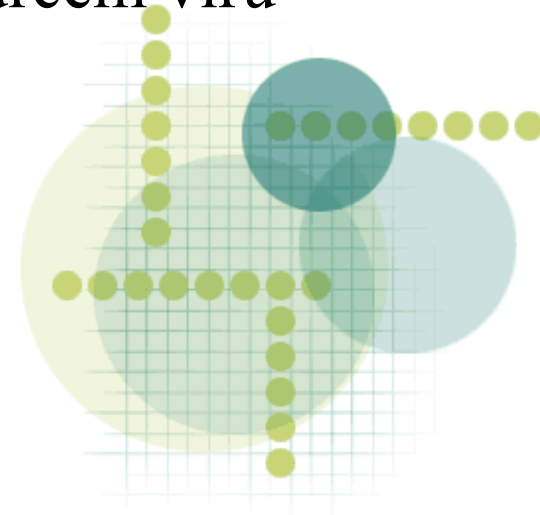
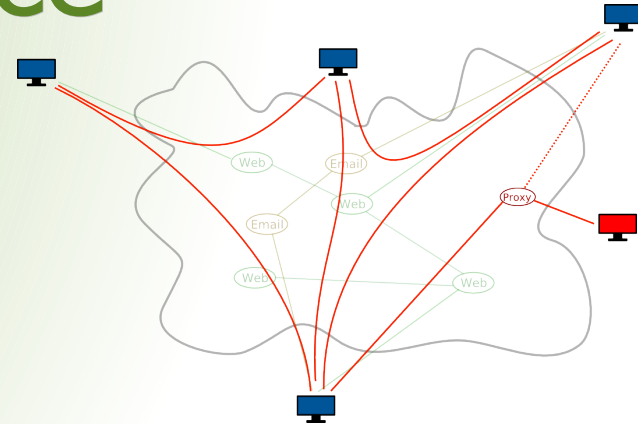
- Jednodušší P2P, ale užívá se pro veškerou komunikaci
- DdoS, proxy, keylogger, ...



	Storm	Nugache
Hlavní C2	Dotazy na C2 server	P2P
Počáteční seznam sousedů	Textový soubor	Natvrdo, Registry
Šifrování C2 komunikace	MD4 hash , 320bit sdílený klíč	512-1024bit RSA Rijndael-256-OFB
Použití DNS pro C2	Žádné/ "Fast Flux" pro ukrytí C2 serverů	Žádné
Udržovaná spojení	Stovky	Jednotky, desítky
Aktualizace	Na příkaz / vůbec ?	Automaticky
Naslouchání sousedům	Náhodný vysoký port	Náhodný vysoký port
Architektura malware	Modulární	Monolitický
Detekce	Antivir hostitele; sledování eDonkey protokolu pomocí signatur	Antivir hostitele; P2P nesledovatelný signaturou

Vývoj C&C v kostce

- Malware se vyvíjí od virů, které jsou
 - Hračkou (Cohen 1983)
 - Ničitelem (Brain 1986; Černobyl 1998; Blaster 2003)
 - Nástrojem organizovaného zločinu (Storm 2007)
- Postupem času adoptují nebo vynalézají nejnovější technologie ... a díky internetu se dají napadené počítače dále tvůrcem viru používat
- Obranou je zdravý rozum, antivir, antispyware, ...



GPU-WPA2crack

- **Metody zabezpečení bezdrátových sítí:**
 - Neustálé problémy
 - WEP jako rozcvička
 - První útoky předpokládaly nasbírání velkého objemu dat
 - Další útoky jsou již rychlejší ;-)



GPU-WPA2crack

- **WPA**
 - Nejprve pokusy stejného charakteru WEP
 - Později útoky jen na autentizační fázi



GPU-WPA2crack

- Útok potřebuje velký výpočetní výkon
- **Kdo má dnes největší výpočetní výkon?**
 - Dual Core?
 - Quad Core?
 - Cluster Quad Core?



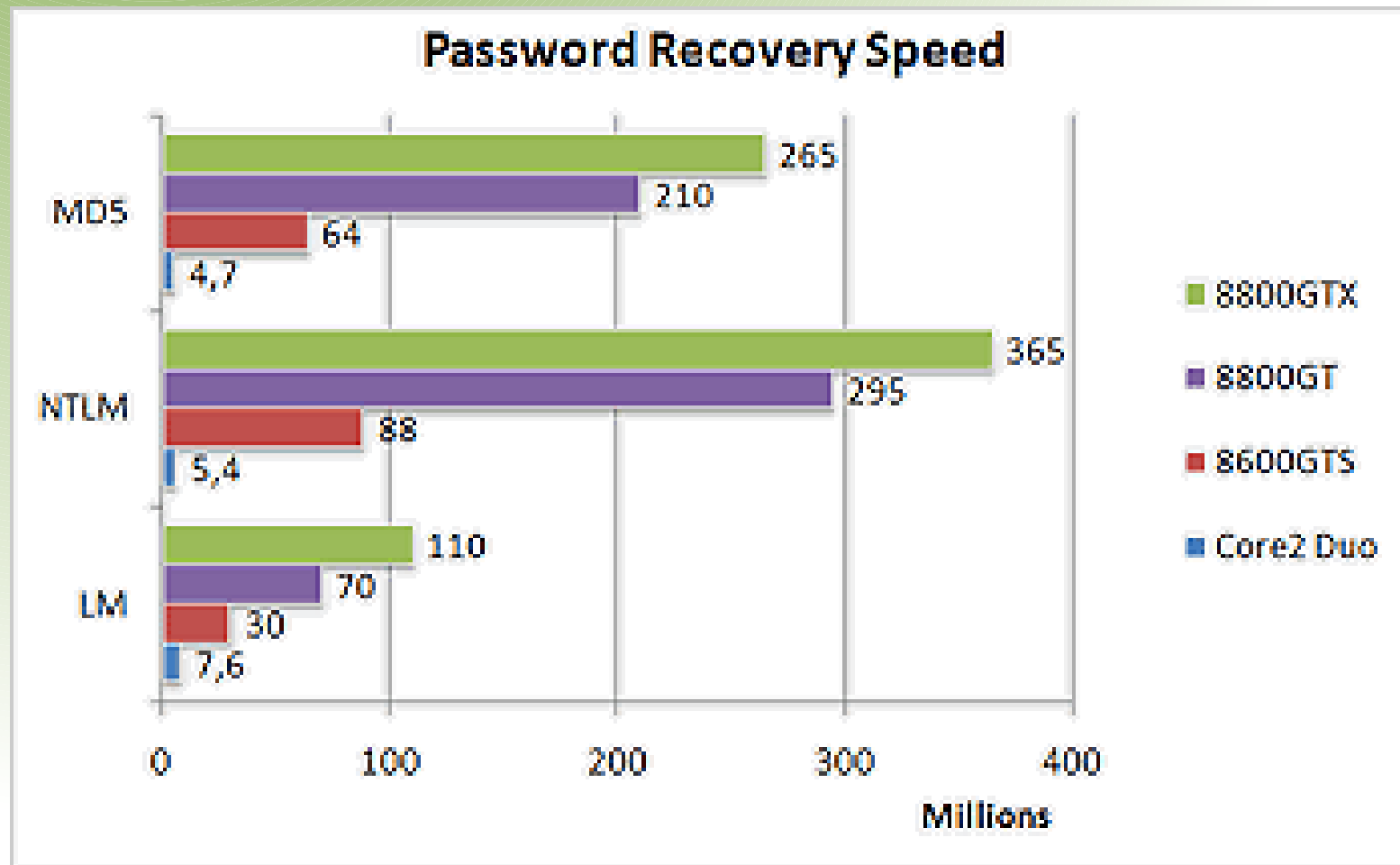
GPU-WPA2crack

- Útok potřebuje velký výpočetní výkon
- **Kdo má dnes největší výpočetní výkon?**

Grafická karta!



GPU-WPA2crack



GPU-WPA2crack

- NVIDIA – CUDA
Compute Unified Device Architecture
- ElcomSoft patent-pending GPU acceleration technology implemented in Elcomsoft Distributed Password **Recovery** allows using laptop, desktop or server computers equipped with supported NVIDIA video cards to break WiFi encryption up to 100 times faster than by using CPU only.



GPU-WPA2crack

- NT LAN Manager (Microsoft authentication protocol)
- Boot password recovery for all NT-based OSes
- Windows Syskey startup passwords
- Windows Domain Cached Credentials (DCC) passwords.
- Unix user passwords
- Oracle user passwords
- Microsoft Office documents
- Various OpenDocument (ODF) filetypes
- A mnoho dalších ...



GPU-WPA2crack

- **Ohrožení je malé**
 - ale možné
- **Řešením je: (někdy)**
 - **Návazná ochrana WiFi sítě**
- **Možnosti obrany:**
 - WPA2 + dlouhé WiFi klíče



MS08-67

- 14. října 2008
- Microsoft vydává opravu kritické chyby mimo plánovanou dávku záplat (MS08-067, CVE-2008-4250)
- overflow v kódu RPC
 - netapi32.dll:NetPathCanonicalize()
 - zabývá se "čištěním cest" (path canonicalization), např. odstraněním přebytečných znaků
.. . / \
 - stack overflow ve smyčce, která zpracovává cestu
- nález byl učiněn MS pomocí honeypotu, chyba je červitelná (aka Blaster)



MS08-67

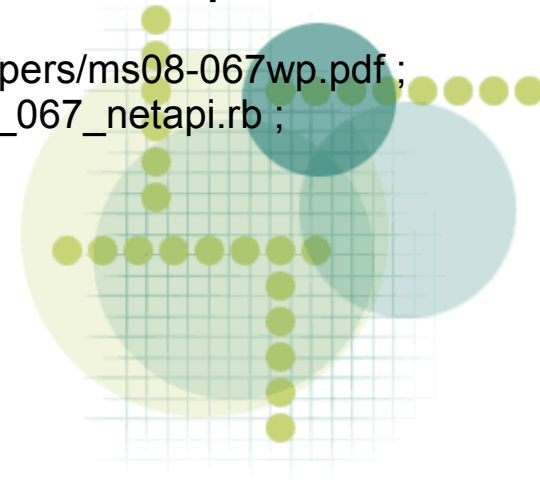
- Postižené systémy:
 - **kriticky:** Win2000, WinXP, Win2003 Server, Win 7 Pre-Beta
 - **závažně:** WinVista, Win2008 Sever (nutná autentizace; UAC+MIC)
- Obrany:
 - **patch**
 - Firewall (139, 445), vypnout síťové služby NetBIOS
 - /GS nepomáhá, zneužití je možné dříve, než dojde ke kontrole kanárka
 - ASLR velmi ztěžuje exploitaci (pouze na Vista a 2008 Server)



MS08-67

- Záplata vydána: 14. října 2008
- PoC by uveřejněn: 24. října 2008
- Aktivní červ byl detekován: 3. listopadu 2008
(SourceFire)

- Odkazy: <http://isc.sans.org/diary.html?storyid=5227> ;
<http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp> ;
<http://blogs.securiteam.com/index.php/archives/1150> ; <http://blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx> ; **<http://blogs.msdn.com/sdl/archive/2008/10/22/ms08-067.aspx>** ;
[http://isc.sans.org/diary.html?storyid=\(5227|5240|5275|5288|5401\)](http://isc.sans.org/diary.html?storyid=(5227|5240|5275|5288|5401)) ;
<http://honeytrap.mwcollect.org/msexploit> ; http://www.snort.org/vrt/docs/white_papers/ms08-067wp.pdf ;
http://metasploit.com/svn/framework3/trunk/modules/exploits/windows/smb/ms08_067_netapi.rb ;
<http://doc.emergingthreats.net/bin/view/Main/WebSearch?search=MS08-067>



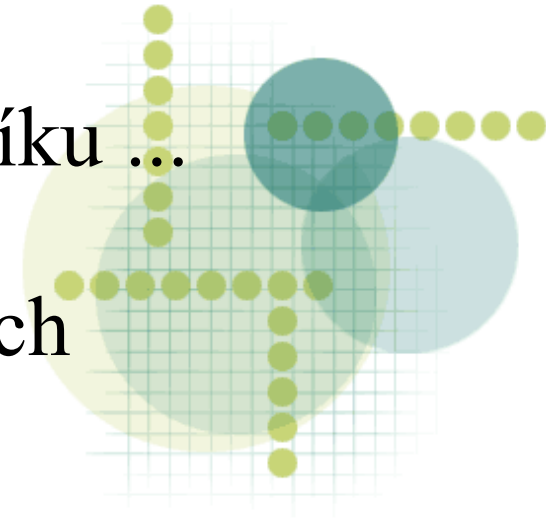
Odposlech bezdrátových klávesnic

- *Max Moser, Philip Schrödel*
27Mhz Wireless Keyboard Analysis Report aka
"We know what you typed last summer"
- Dreamlab Technologies se podařilo prolomit
zabezpečení klávesnic Microsoft Wireless Optical
Desktop 1000 a 2000, zřejmě i 3000 a 4000
- Analýza komunikačního protokolu:
Data, Management, Synch
- Pouze keycode je v datovém paketu šifrován,
zbylá metadata jsou v plainu (CTRL, SHIFT, ...)



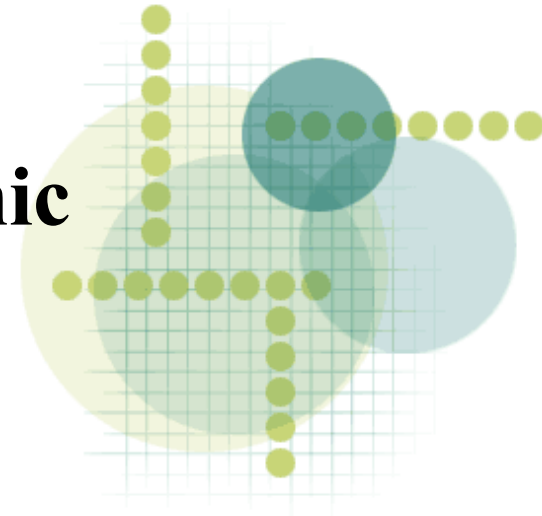
Odposlech bezdrátových klávesnic

- Šifrování je realizováno XORem s jedním bytem (klíčem)
existuje pouze 256 možných hodnot
- Žádná automatická regenerace klíče, pouze při párování zařízení
- Útok na šifrovací klíč je založen na slovníku ...
uživatel píše, *pokud* se útočnému nástroji *podaří sestavit několik slov* ze zachycených dat, *klíč je na světě*



Odposlech bezdrátových klávesnic

- Kód nebyl zveřejnen, protože proti této chybě neexistuje žádná možnost záplatování (klávesnice nemají možnost upgradu firmware)
- **Ohrožení je nízké**, útočník musí:
 - Být blízko
 - Prolomeny jsou pouze 2 konkrétní typy klávesnic
- **Řešením je:**
 - **použití klasických drátových klávesnic**
 - Použití Bluetooth zařízení (které mají vlastní chyby ;)



/GS, SafeSEH, DEP, ASLR ...

- Alexander Sotirov, Mark Dowd:
Bypassing Browser Memory Protections: Setting back browser security by 10 years
- ochrany proti chybám buffer overflow ...
 - WinXP SP2 - /GS, SafeSEH, DEP
 - Vista, 2008 Server – ASLR
- ... stejně nestačí
 - /GS – chrání pouze některé fce (ANI bo, MS08-067)
 - SafeSEH, DEP – dají se vypnout případně nejsou použité (java, flash, activeX, IE7, FF2, ...)
 - ASLR – (javascript) heap spraying ;))



Zprávy

A nyní následují krátké zprávy



Z Domova



- 5. března 2008

- Phishingové útoky na Českou spořitelnu

- `hxxp://www.servis-internetbanking.info`
- `hxxp://arrakis.is.net.pl/~lee/csas.cz/banka/security.htm`
- ...

Drahoušek Zákazník,

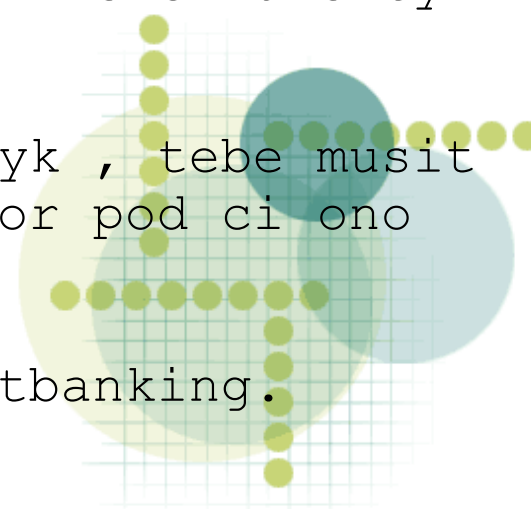
Tato is tvuj funkcionár oznámení dle Česká
Sporitelna aby clen urcity služba dát pozor pod vule
být deactivated a odstranit kdyby nedošlo k obnovit
se bezprostřední.

Predešlý oznámení mít been poslaný až k clen urcity
Žaloba Dotyk prideli až k tato účet.

Ackoliv clen urcity Bezprostřední Dotyk , tebe musít
obnovit se clen urcity služba dát pozor pod ci ono
vule být deactivated a odstranit.

Obnovit se Ted tvuj SERVIS 24 Internetbanking.

...



- 22. října 2008
- Ze seznamovacího webu unikly „ukryté“ intimní fotografie
- Celkem
 - 1 138 slečen
 - 11 587 fotografií
- Některé z nich vyhledaly odbornou lékařskou péči



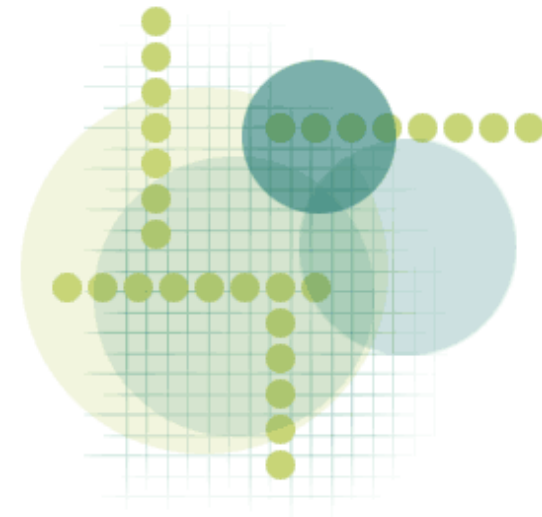
Ze zahraničí



- 19. března 2008
- Microsoft vydává Service Pack 1 pro Windows Vista
- 5. května 2008
- Microsoft vydává Service Pack 3 pro Windows XP



- *Jon Oberheide, Evan Cooke, Farnan Jahainan*
Empirical exploitation of Live Virtual Machine Migration
University of Michigan
- Xenspoit – nástroj pro útok na migraci (Xen, VMware/VMotion)
 - Man-in-the-middle, fragroute
 - HelloWorld – změna stringu v běžícím procesu
 - sshd – změnit proces tak, aby umožnil přihlášení bez autentizace
- V průběhu vývoje našly 2 chyby na úrovni VMM



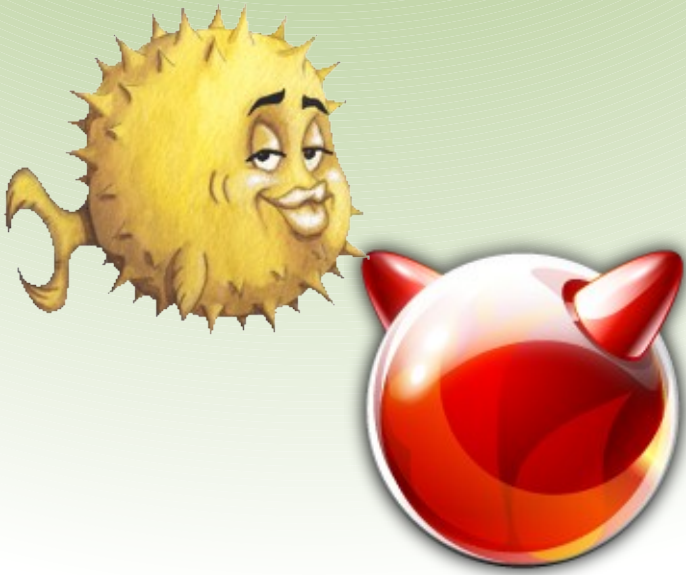
- 8. srpen 2008
- Vojenskou intervencí v Gruzii provázely i internetové útoky na gruzínské vládní servery



- 22. srpna 2008
- Některé z oficiálních serverů společnosti RedHat napadl neznámý útočník.
- Některé z nich sloužily k digitálnímu podepisování vytvářených balíčků pro distribuci Fedora, RHEL 4 , RHEL 5.
- Průnik se podařilo odhalit velmi rychle a napáchané škody odstranit. Podpisové klíče Fedory byly změněny.
- <https://www.redhat.com/archives/fedora-announce-list/2008-August/msg00012.html>
- <http://rhn.redhat.com/errata/RHSA-2008-0855.html>



- 12. května 2008
- V operačních systémech rodiny BSD byla nalezena chyba v knihovně libc (volání seekdir()), která zde byla *ukryta* 25 let ...



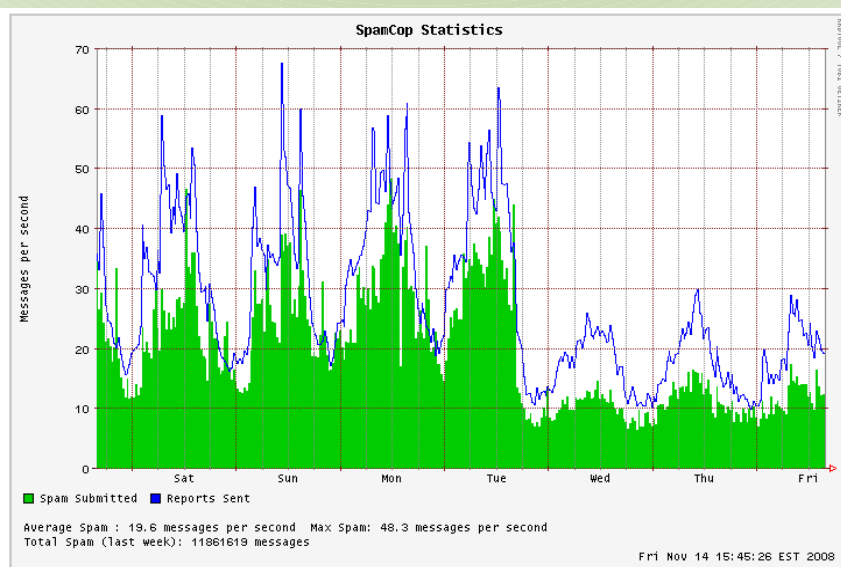
- 16. října 2008
- Emailový účet kandidátky na viceprezidenta USA Sarah Palin byl hacknut
- K prolomení byl použit postup pro změnu zapomenutého hesla pomocí kontrolních otázek:
 - Datum narození
 - Poštovní směrovací číslo
 - Místo seznámení s jejím manželem
- Všechny potřebné údaje jsou veřejně známé



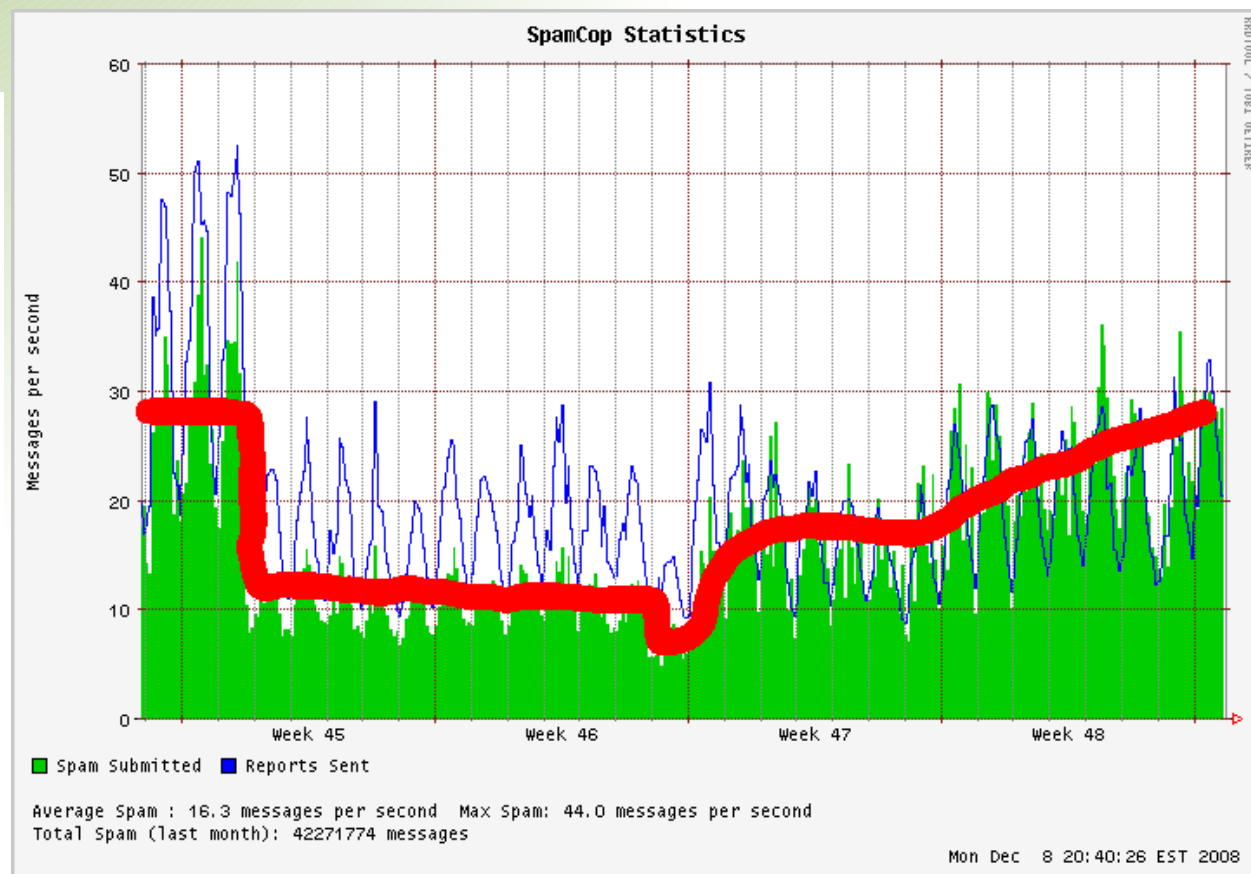
- 3. listopadu 2008
- Sarrah Palin se stala obětí žertovného telefonátu dvou francouzských komiků
- V šesti minutovém rozhovoru hovořila s *Nicholasem Sarkozym* o kráse Carly Bruni a honech na divokou zveř ...
- Rozhovor byl zveřejněn v kanadských rádiích ...



- 12. listopadu 2008
- Odpojením kalifornského poskytovatele hostingových služeb **McColo** poklesl objem světového spamu **na třetinu** !
- Potřebné důkazy shromáždil bezpečnostní expert Brian Krebs a pokles udal i Miloš Wimmer ...
- Kromě spamu byla McColo zodpovědná i za distribuci a provoz mnoha botnetů, hostingu keyloggerů a rootkitů.



[Return to stats menu](#)



- 10. - 12. prosince 2008

GREEN

YELLOW

ORANGE

RED

- Objevila se nová 0-day chyba v prohlížeči: IE5, IE6, IE7, IE8 Beta na všech typech Windows (heap overflow). Chyba je v kódu XML parseru
- Veřejný exploit užívá heapspraying pro obchvat ASLR (DEP je v IE vypnutý)

- isc.sans.org/diary.html?storyid=5458
- milw0rm.com/exploits/7410



- Výsledkem je spuštění libovolného kódu s právy uživatele browseru
- **Aktivně šířena internetem pomocí SQL injection**
- **Ochrana:**
 - do vydání záplaty použít alternativní browser
 - Nechodit na podezřelé stránky

Sport



... No nmap ? No time ? No problem ...

```
C:\> for /L %i in (1,1,255) do ping -n 1 -w 300 "192.168.20.%i" >> b 2>&1
```

```
C:\> type b | findstr Reply
```

```
C:\> type b | findstr Odpov
```

```
C:\> type b | findstr Antwort
```

```
C:\>for /L %i in (1,1,255) do ping -n 1 -w 1000 "10.109.234.%i" >> b 2>&1
```

```
C:\>ping -n 1 -w 1000 "10.109.234.1" 1>>b 2>&1
```

```
C:\>ping -n 1 -w 1000 "10.109.234.2" 1>>b 2>&1
```

```
C:\>ping -n 1 -w 1000 "10.109.234.3" 1>>b 2>&1
```

```
C:\>ping -n 1 -w 1000 "10.109.234.4" 1>>b 2>&1
```

```
C:\>type b | findstr Odpo
```

```
C:\>Odpověď od 10.109.234.32: bajty=32 čas=2ms TTL=64
```

```
C:\>Odpověď od 10.109.234.35: bajty=32 čas=3ms TTL=64
```

```
C:\>Odpověď od 10.109.234.50: bajty=32 čas < 1ms TTL=250
```

```
C:\>Odpověď od 10.109.234.75: bajty=32 čas < 1ms TTL=128
```

```
C:\>Odpověď od 10.109.234.111: bajty=32 čas=1ms TTL=255
```

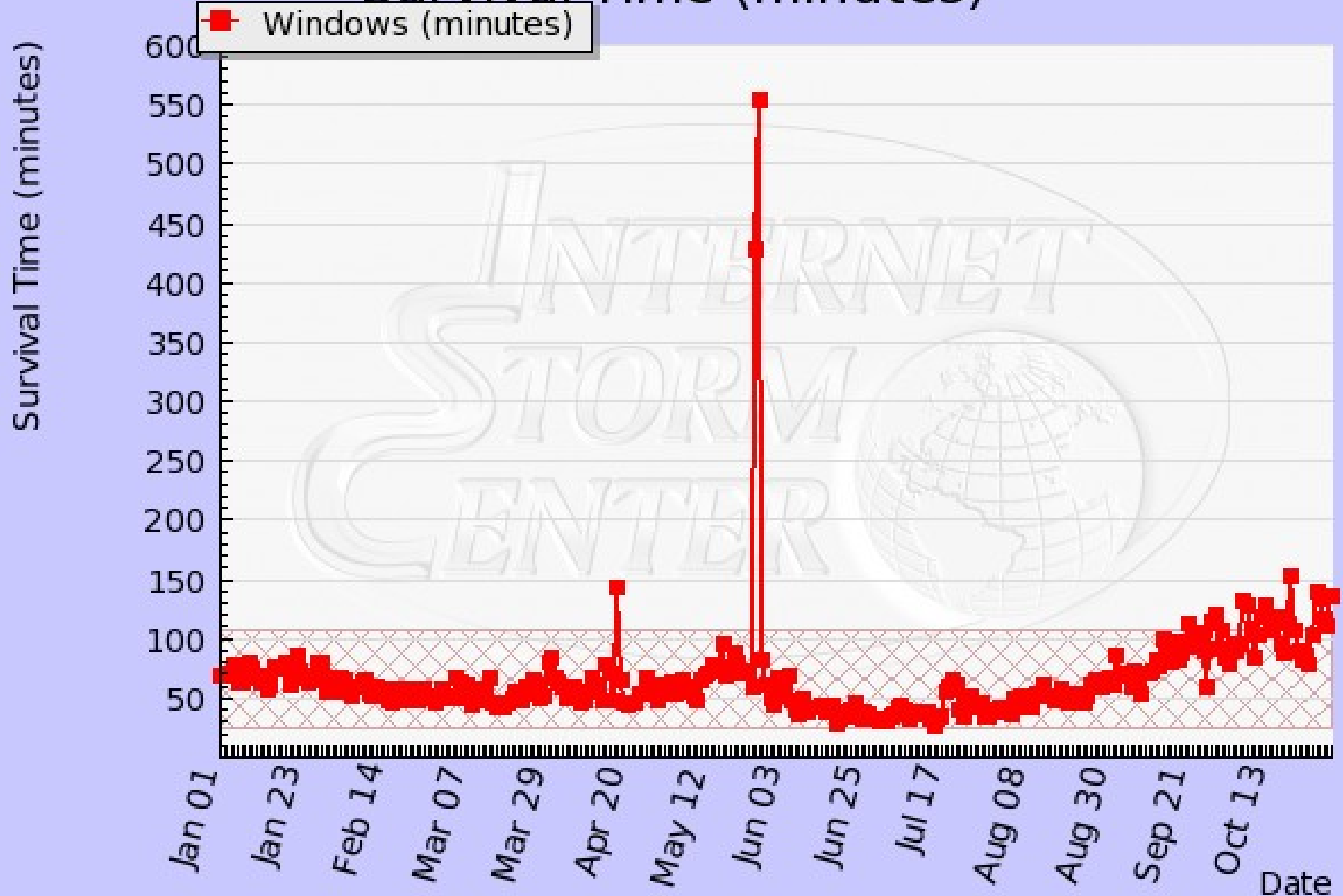
```
C:\>Odpověď od 10.109.234.146: bajty=32 čas < 1ms TTL=128
```

```
C:\>Odpověď od 10.109.234.170: bajty=32 čas=1ms TTL=127
```

```
C:\>Odpověď od 10.109.234.182: bajty=32 čas < 1ms TTL=48
```

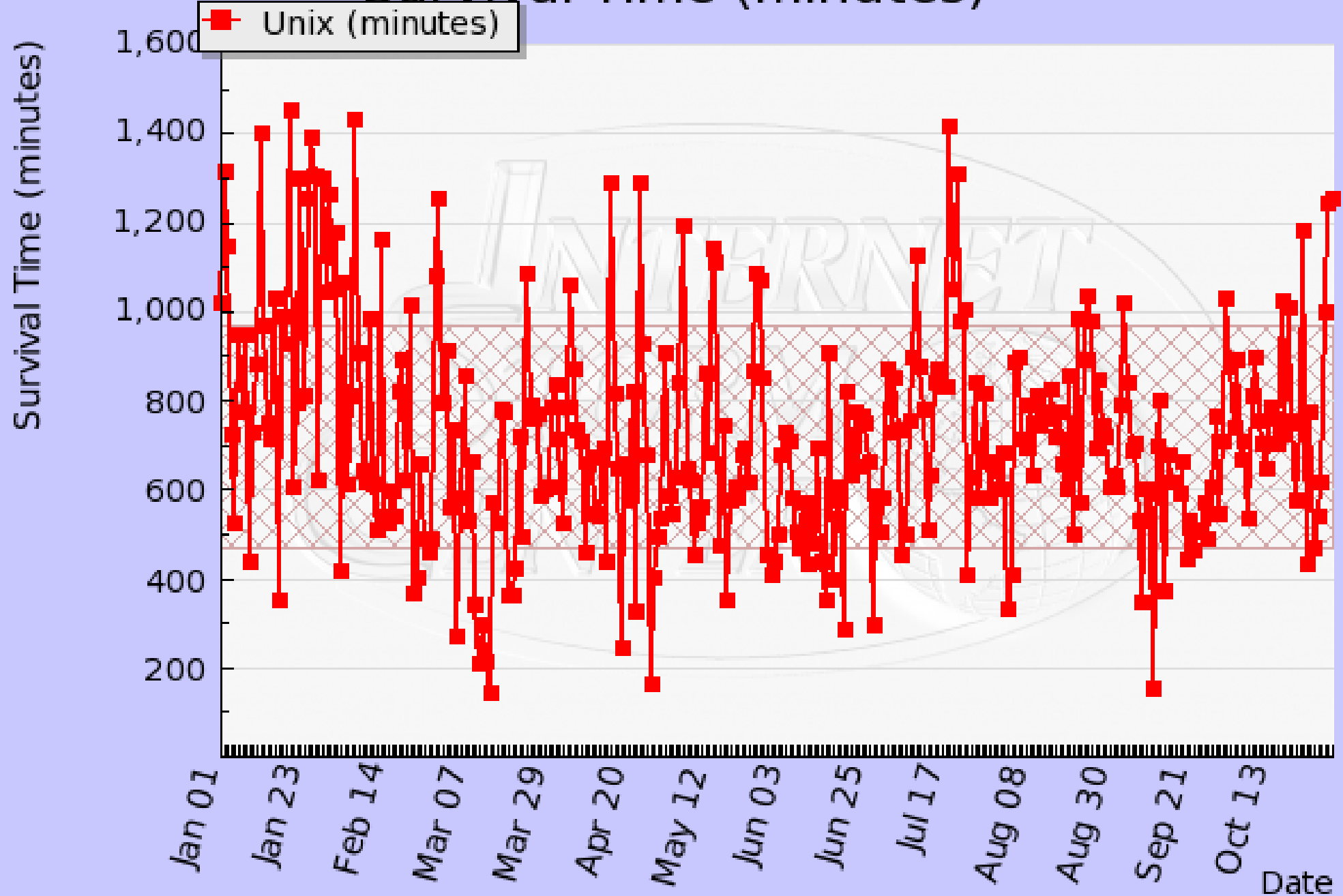
Počasí

Survival Time (minutes)



Počasí

Survival Time (minutes)



Počasi

- Sun Alerts
<http://blogs.sun.com/security/?cat=alerts&date=200811>
- Debian Security Advisories
<http://www.debian.org/security/2008/>
- Microsoft Security Bulletin
<http://www.microsoft.com/technet/security/current.aspx>
- Gentoo Linux Security Advisories
<http://www.gentoo.org/security/en/glsa/index.xml>
- FreeBSD Security Advisories
<http://www.freebsd.org/security/advisories.html>
<http://www.vuxml.org/freebsd/>
- CVE Candidates
<http://cve.mitre.org/data/downloads/allcans.txt>

173



235



69



191



161

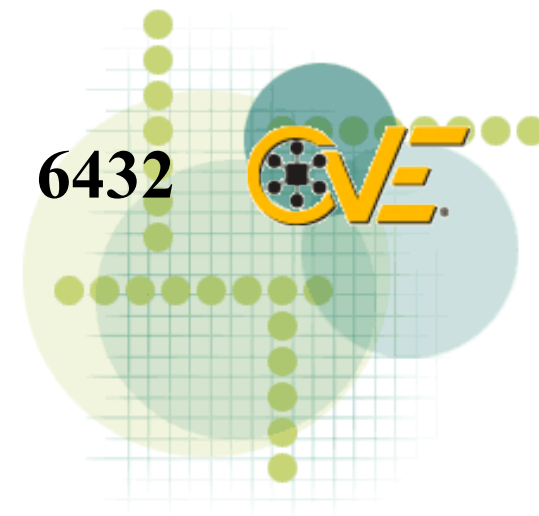


6432



Tlaková tendence: neustálý vzestup

stav ke 3.12.2008 00:42 CET



Krásný zbytek dne přejí

Jakub Urbanec
Radoslav Bodó
a Miloš Frýba

