Téma čísla

Ochrana počítačových sítí na bázi stacionárních a událostních IP kanálů

Victor Oppleman 

stupeň obtížnosti

Tento článek popisuje momentálně málo známou techniku zabezpečení počítačové sítě, jenž se ukazuje jako jeden z nejúčinnějších nástrojů pro boj s útoky typ DoS.

Tato podpora buduje základní mechanismus ochrany individuálních klientů, používaný ISP (anglicky *Internet Service Providers*). V tomto článku je ukázána technika, jak využít IP kanály s cílem získání informací o možných nebezpečích, kterým je vystavena každá počítačová síť. Implementací kanálů je možno se účinně bránit před zmiňovanými útoky a současně sbírat informace o nich a detekovat případné problémy v nastavení sítě.

Článek je určen ve většině případů čtenářům obeznámeným se síťovými technologiemi a ukazuje následující řešení:

- Základní pojednání a příklady použití – Vyjasnění koncepce IP kanálů a příklady použití této technologie v kontextu existujících organizací.
- Vytváření sítě vábniček (anglicky. *Decoy Network*) – Analýza možností použití sítě *darknet* a *honeynet*, pro nalezení a analýzu škodlivého skenování, infiltračních pokusů a jiných útoků – také v kontextu monitorovacích mechanismů síťových systémů a detekování průniků.
- Obrana před útoky typu DoS – Ukázka toho jak organizace a její zprostředkovatel Internetu vytvořili metodu obrany před DoS útoky s použitím intenzivního, na událostech založeném, rozprostírání IP kanálů.
- Zpětný rozptyl (anglicky *Backscatter*) a metoda *IP Traceback* – Vyjasnění pojmu *Zpětné rozptyl* a vysvětlení, v čem spočívají metody zpětného sledování IP paketů (anglicky *IP Traceback*), sloužící k identifikaci vstupního bodu DoS útoku ve velké síti.

Z tohoto článku se naučíte...

- Přečtením tohoto článku se naučíte jak používat IP kanály a dozvíte se jak se s jejich použitím bránit před útoky spočívajícími v blokování služeb – známých jako DoS (anglicky *Denial of Service*).

Měl byste vědět...

- Měli byste mít základní znalosti problematiky specifikace DoS útoků.
- Měli byste se orientovat ve způsobu, jakým zprostředkovatelé internetu pracují s tokem dat v počítačových sítích.

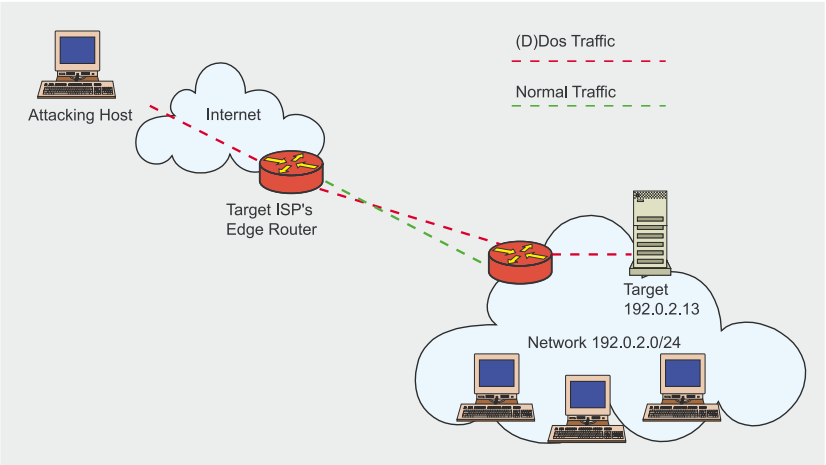
Základní pojednání a příklad využití

V kontextu tohoto textu, může být pojem *„kanál"* definován jako podmíněný způsob přesměrování síťového provozu – pro specifickou IP adresu, s cílem spuštění bezpečnostních mechanismů, takových jako: shromažďování a analýza stop po útoku, provádění rušení útoků nebo detekce neobvyklých činností. Nejlepší zprostředkovatelé Internetu (označováni jako *Tier-1 ISPs*) byli průkopníky v implementaci těchto mechanismů. Jejich hlavní motivací pro přijímání těchto kroků byla ochrana vlastních klientů. V dalším sledu byly zmiňované techniky upraveny pro shromažďování jistých informací s ohledem na bezpečnost informací v objevujících se hrozbách. Abychom si ukázali nejjednodušší formu kanálu podívejme se na následující scénář.

Zlomyslný, destruktivní tok dat je nasměrován z různých zdrojů na síť 192.0.2.13, jak je vidět na Obrázku 1. Organizace, která bude zdrojem útoku, používá rozsah 192.0.2.0/24 jako svůj blok adres, který je podporován příslušným ISP. Útok snižuje kvalitu komerčních služeb nabízených cílovou organizací a současně způsobuje potenciální zvýšení nákladů této organizace, spojené se zvýšeným využíváním připojení a nutností provedení akcí na straně zprostředkovatele Internetu. ISP subjekt je v tomto případě také ohrožen, protože zvýšený provoz na síti jako vedlejší efekt útoku, může mít vliv na jiné klienty, používající stejné připojení.

Zprostředkovatel Internetu v rámci reakce iniciuje dočasně kanál typu *černá díra* (anglicky *blackhole)*, přesměrovávající provoz na novou adresu (192.0.2.13/32), na jehož výstupu se nachází odmítací rozhraní (známý jako *null0* nebo *bit bucket*) – tato situace je vidět na Obrázku 2.

Tato taktika způsobí přesměrování ofenzivního toku dat na kanál ISP subjektu, odstavující zbylé klienty zprostředkovatele od negativních, vedlejších efektů útoku. Bohužel, napadená IP adresa a ve výsledku zařízení nabízející na této adrese nějaké služby, je zablokovaná a nemůže komunikovat s vnějším světem. Tato situace přetrvává až do chvíle, kdy bude komunikační kanál navrácen do původního stavu (což samozřejmě nastane až po zmírnění aktivity útoku). Samozřejmě, služba poskytovaná na napadené adrese může být přenesena na alternativní zařízení s jinou IP adresou. Bohužel, tento záměr může být z mnoha příčin velmi obtížně realizovatelný vzhledem na vypršení doby DNS záznamu (anglicky *DNS Time To Live*)



Obrázek 1. *Útok na IP adresu 192.0.2.13 (před použitím kanálu)*

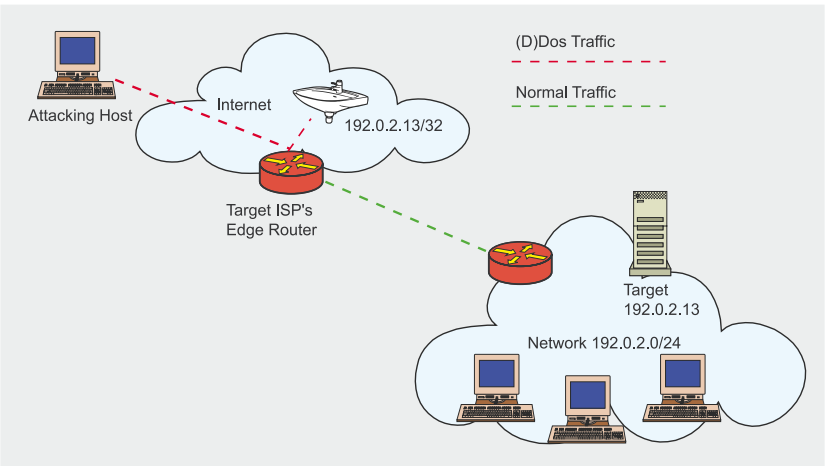
Ukázaný příklad je pouze jedním ze základních způsobů využití kanálu: tzv. *cesta k černé díře připravené zprostředkovatelem* (anglicky *ISP-induced blackhole route*) – by však měl být dostatečný pro seznámení se s obecnou koncepcí využití kanálů při blokování DoS útoků.

Používání kanálů s cílem umístění návnady

Modernějším způsobem využití kanálů je rozmístění sítí návnad s cílem chycení a odmaskování protivníka a také pro sbírání informací o něm.

Podle slovníku, slovo *návnada* popisuje libovolný předmět jehož cílem je chycení do pasti, pokusný element – jehož cílem je omámit protivníka a vystavit jej nebezpečí, vydat na pospas útočníka. Řečeno krátce, návnada je jistý druh vábničky.

V tomto textu budu popisovat dva druhy sítě návnad: síť typu *darknet* a *honeynet*. Obě technologie je možno využít pro shromáždění informací spojených s výskytem útoků, i když první z jmenovaných typů je užitečný při vytváření bezpečných počítačových sítí.



Obrázek 2. *Útok na adresu IP 192.0.2.13 (použití kanálu)*

Výpis 1. *Ukázková konfigurace BGP*

```
router bgp XXX
redistribute static route-map static-to-bgp
# Používáme mapu přesměrování
# pro určení strategie úpravy
# atributů daného prefixu a politiky
# filtrování
route-map static-to-bgp permit 10
match tag 199
set ip next-hop 192.0.2.1
set local-preference 50
set community no-export
set origin igp
```

Výpis 2. *Ukázková konfigurace BGP na straně ISP*

```
router bgp XXX
# Používáme mapu přesměrování
# pro předávání informací
# o přesměrování
neighbor < customer-ip > route-map customer-in in
# prefix-list je statický seznam klientských prefixů;
# klient by měl mít možnost popsat
# konkrétního hosta pomocí tohoto seznamu
neighbor < customer-ip > prefix-list 10 in
# zápis ebgp-multihop je nutný
# pro předejití neustálému rozesílání a odmítání
# informací o prefixech
neighbor < customer-ip > ebgp-multihop 2
# Definujeme mapu přesměrování a strategii
# rozpoznávání a nastavování černých děr
# při dalším skoku
route-map in-customer permit 5
# Klient nastaví parametr community na své straně,
# zatímco ISP je kontroluje na své straně;
# XXXX  může být ASN klienta,
# zatímco NNNN libovolně zvoleným číslem
# na obou stranách
match ip community XXXX:NNNN
set ip next-hop < blackhole-ip>
set community additive no-export
```

Rozmisťování sítí typu darknet

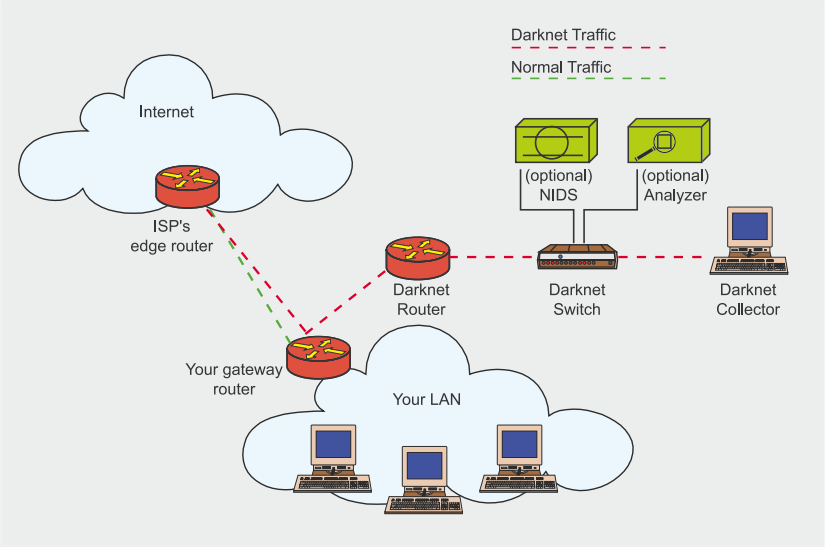
Obecně, sítě typu *darknet* nastavují rozsah IP adresového prostoru, do kterého nejsou připojeny žádné reagující služby. Sítě tohoto typu jsou klasifikovány jako *temné* (anglicky *dark*) vzhledem k tomu, že uvnitř nich není nic, co by je mohlo *osvítit*. Síť typu *darknet* v sobě obsahuje nejméně jeden server, vytvořený jako *nasávač* paketů. Tento server skladuje a organizuje data, která vstupují do prostoru *darknet*, což umožňuje provádění užitečných analýz – buď v reálném čase tak i při pozdějším hledání stop elektronických zločinů v síti.

Velmi důležitý je fakt, že žádný paket mířící do sítě *darknet* není očekávaný. Nějak to vyplývá ze samotné podstaty této sítě. Souhrnně, protože žádný legální paket by se nikdy neměl objevit uvnitř sítě *darknet*, proto je výsledkem, že jakýkoliv provoz objevující se v této síti musí být nevyžádaným jevem – vyplývajícím z potenciálně špatné konfigurace, mající svůj zdroj ve vnějším útoku ze strany nějakého škodlivého programu.

Právě ten poslední případ znamená nejčastější příčinu objevení se nevyžádaných paketů v *temné síti*. Zmiňovaný zlomyslný program skenuje obvyklý rozsah dostupných IP adres s cílem nalezení nezabezpečených zařízení – i takové pakety přicházejí do sítě *darknet* – vystavující současně zkoušce mechanismy bezpečnosti systému. Použití tohoto mechanismu znamená také nezávislý přístup při hledání síťové havěti a různého druhu samopropagující se škodlivý software. Díky použití sítě *darknet* (i bez použití dalších dodatečných doplňků) může správce systému jednoduše a rychle lokalizovat výskyt skenování (např. pokusy detekce připojených hostů znamenající potencionální cesty další propagace) v síti libovolné velikosti. Je to výkonný nástroj při vytváření systému zabezpečení. Navíc – jak jsem již dříve zmínil – sítě typu *darknet* umožňují zalepit potencionální díry a chyby v konfiguraci sítě, což umožňuje správci přijetí rychlých rozhodnutí s cílem odstranění těchto nedostatků. Tato technika má široké využití v oblasti bezpečnosti sítě – může být využita při kontrole provozu mezi hosty, detekci výskytu aktuálního šíření, prohlížení paketů či při vytváření systémů detekce průniků. Síla a elegance tohoto řešení spočívá v tom, že se sítě *darknet* opírají o analýzu výskytu negativních událostí – zůstávajíc nezávislé na konkrétních technologiích nebo zařízeních.

Implementace sítě *darknet* je velmi jednoduchá. Je možno tu zmínit pět základních kroků, které je nutno provést.

Je nutno vybrat jeden nebo několik nepoužívaných oblastí v IP adresovém prostoru dané sítě, které budou znamenat cestu k *temné síti*. Může to být rozsah adres z prefixem /16 nebo větším a i celý rozsah samostatné adresy (/32). Čím větší je rozsah používaných adres, tím s předčíslím (ve statistickém smyslu) jsou získané informace o nevyžádané aktivitě ve zdrojové síti. Osobně doporučuji využití různých segmentů adres, např. /29 pro každou vnější podsíť a /25 pro veřejný rozsah (dostupných z vnějšku) vstupu do sítě. Nejsou také protiargumenty pro využití vnitřního, privátního adresového prostoru při vytváření sítě *darknet* (může to být například rozsah 10.0.0.0/8 popsaný v dokumentu RFC 1918). Ve skutečnosti je to doporučo-



Obrázek 3. *Referenční fyzická topologie sítě typu darknet*

váno: zapnutím vnitřních, privátních rozsahů své *temné sítě* máme možnost analýzy skenování z vnějšku – což by mohlo ujít naší pozornosti – kdybychom vytvořili *darknet* jenom na základě veřejných adres.

Jinou strategií výběru adres pro síť typu *darknet*, zvláště zajímavou pro organizace využívající specifické způsoby řízení průchodu paketů ve svých vnitřních sítích, spočívá na využití zásady *nejspecifičtější cesta průchodu dat vyhrává.* Vypadá to tak, že pokud používáme adresy 10.1.1.0/24 a 10.2.1.0/24 vnitřně, pak můžeme přesměrovat celou síť 10.0.0.0/8 do své *temné sítě*. Pokud víme, že naše síť je správně nastavena, pak *darknet* odebere celý provoz v síti 10.0.0.0/8 s výjimkou podsítě, kterou používáme specifickým způsobem nebo bezprostředně přesměrovaný (tyto podsítě mají obvykle statické zápisy v registru přesměrování v infrastruktuře sítě).

Dalším krokem je konfigurace fyzické topologie. Proto potřebujeme router nebo switch (*layer-3*) přepojující provoz do sítě *darknet*, server s velkou zásobou diskového prostoru – sloužící jako úložiště dat a ethernetový switch, používaný pro propojení těchto komponent (a v budoucnosti také k připojení dalších mechanismů – například IDS senzor nebo analyzátor protokolů). Pokud jde o router, je možno vybrat interní nebo externí zařízení (a i obě naráz – i když toto

pojetí není doporučováno). Sítě typu *darknet* více komerčního charakteru jsou obvykle umístěny uvnitř DMZ dané organizace a odděleny od zbylé části síťové infrastruktury.

Je možno zvážit použití firewallu, který bude provádět požadované činnosti místo routeru. Já osobně doporučuji použití routeru řídící příchozí provoz – v případě implementace vnitřních sítí *darknet*. Při vytváření neveřejné *temné sítě* doporučuji využití vnitřního switche. Nezávisle na zvolené topologii, je základní otázkou ke zvážení nastavení zařízení odpovědného za přesměrování paketů, které mají nakonec dojít do sítě *darknet* s cílem obsloužení dedikovaným serverem. Server přechovávající data musí být vybaven rozhraním umožňujícím zachytávání příchozích paketů. Hodí se také alespoň jedno Ethernet rozhraní. Toto rozhraní značně ulehčuje práci se sítí typu *darknet*. Celý podsystém obsluhující *temnou síť* musí být navržen velmi promyšleně – zvláště v bezpečnostním kontextu – a to zvláště proto, že do této sítě budou přicházet různí škůdci. Je dobré také věnovat trochu času na využití existujícího DMZ switche, s cílem správného propojení popisovaných komponent. Abyste dosáhli požadovaného výsledku, musíte se pokusit o příslušnou konfiguraci VLAN, tak aby přicházející tok nepřicházel do sítě *darknet*. Je nutno pamatovat, že *temná síť* je určena pouze a výlučně pro podporu nelegálních a neočekávaných paketů. Na Obrázku 3 je vidět referenční konfigurace pracující se sítí typu *darknet*. V tomto konkrétním případě je použit router nebo switch podporovaného softwarem Cisco IOS se softwarovou třetí vrstvou (layer-3) a serverem založeným na systému FreeBSD. Pro spojení zařízení byl použit switch druhé vrstvy (layer-2).

Protože server skladující data nemusí podporovat ARP (anglicky *address resolution protocol*), musíme pro každou adresu v rozsahu sítě *darknet* nakonfigurovat router, aby automaticky přesměrovával provoz patřící do *temné sítě* na unikátní IP adresu, nacházející se na ethernetovém rozhraní zmiňovaného serveru. Pro získání tohoto výsledku doporučuji využití dedikované sítě (/30) sloužící jako bezprostřední spojení mezi routerem a rozhraním sítě *darknet* – může to být např. síť 192.0.2.0/30. V tom případě by bylo ethernetové rozhraní routeru umístěno na adrese 192.0.2.1/30, zatímco přístup k serveru skladujícího data by bylo možno získat odvoláním se na 192.0.2.2/30. Konfigurace rozhraní je silně závislá na cílové platformě a obecně se musí každý správce poprat s tímto problémem samostatně. V kontextu již dříve ukázaného příkladu (software Cisco IOS s licencí layer-3) stačí nastavit switch tak, aby přesměroval provoz určený do sítě *darknet* na adresu 192.0.2.2 – na dedikovaný server:

```
router#conf t
router(config)# ip route 10.0.0.0 ←┘
255.0.0.0 192.0.2.2
router(config)# ^Z
router# wr
```

Ukázka logické topologie systému je vidět na Obrázku 4.

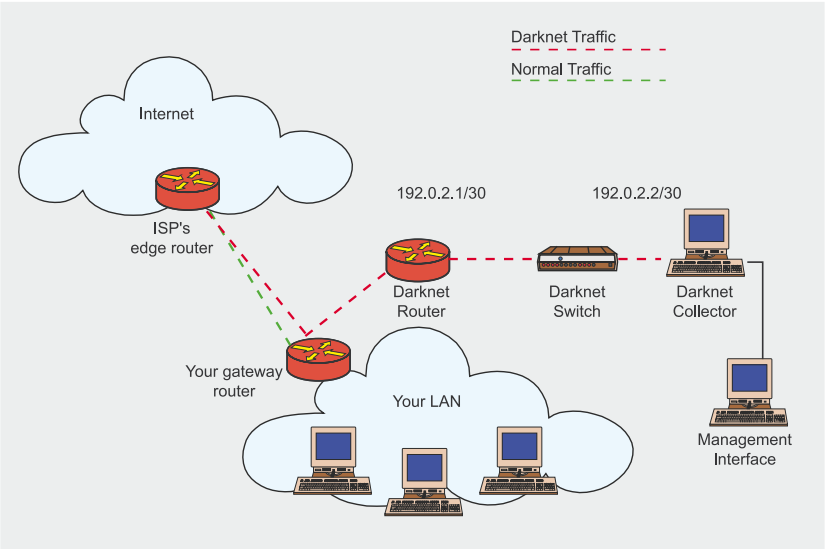
Dalším pro nás zajímavým úkolem, je způsob práce s pakety, které se dostanou do *temné sítě*. Cílový server by měl být nakonfigurován tak, aby neposílal žádné odpovědi v souvislosti s objevujícími se daty. Je jasné, že server musí posílat ARP zprávy (na nastavenou adresu, v našem případě: 192.0.2.2/30) pro navázání komunikace s routerem, ale všechny další pakety musí být odmítnuty, nejlépe s použitím firewallu – stejného, jaký se používá na běžných hostech. Již dříve jsem zmiňoval, že na rozhraní *temné sítě* není možné zprovoznit nějaké služby spojené se zpracováním. K tomu musíme nastavit odlišné ethernetové rozhraní a skrz něj provádět veškeré administrační operace. Protože budeme používat firewall, záleží výběr platformy především na preferovaném řešení. Osobně doporučuji systémy založené na BSD a software *pf* nebo *ipfw2* jako firewall. Bez ohledu na konečný výběr nástroje je také dobré zamyslet se nad přidáním mechanismu logování firewallu. Já nechávám logování vždy zapnuté – hlavně vzhledem k používaným nástrojům pro analýzu logů, které umí parsovat objevující se informace a v krizové situaci vygenerovat příslušné varování. Z druhé strany, zapnuté logování může dosti značně a negativně působit na výkon celého podsystému. Jako dodatečný bezpečnostní mechanismu (firewally také umí spadnout nebo mohou být neúmyslně vypnuty) je dobré nastavit přesměrování provozu v *temné síti* na odmítací rozhraní (černou díru). Přesměrování by mělo být aktivováno v situaci, kdy nejsou z nějaké příčiny filtrovány přicházející pakety. Ukázková konfigurace tohoto mechanismu v systému FreeBSD vypadá následovně:

```
route add -net 10.0.0.0/8 ←┘
127.0.0.1 -blackhole
```

Máme fungující a zabezpečenou síť typu *darknet* a musíme promyslet mechanismus ukládání zachytávaných informací – nejlépe v takovém formátu, který bude adekvátní pro nástroje používané k analýze. Nejobecnějším výběrem je zapsání dat v binárním formátu *pcap*, protože tento formát podporuje drtivá většina aplikací určených pro analýzu provozu na síti. Tento úkol můžeme provést velmi jednoduše použitím programu *tcpdump*, vytvořený skupinou zkoumající síťové technologie v Lawrence

Výpis 3. *Ukázková konfigurace na straně klienta*

```
router bgp XXXX (ASN klienta)
# klient popisuje statické přesměrování,
# které je distribuované BGP
route-map static-to-bgp permit 5
# kontrola čísla,
# zadaného na obou stranách
match tag NNNN
set community additive XXX:NNNN
ip route 192.168.0.1 255.255.255.255 Null0 tag NNNN
```



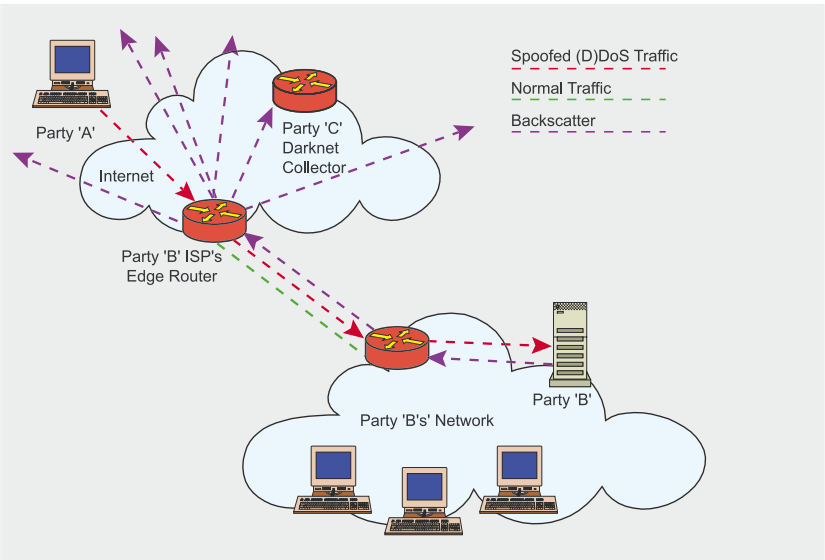
Obrázek 4. *Referenční logická topologie sítě typu darknet*

Berkeley National Laboratory. Zde je jednoduchý příklad použití tohoto nástroje z příkazové řádky:

```
tcpdump -i en0 -n -w darknet_dump -C125
```

V tomto příkladě je nástroj *tcpdump* nastaven tak, aby zachytával data z rozhraní *en0*, s vypnout podporou DNS. Po načtení dalších 125 milionů bajtů jsou data zapsána do souboru pojmenovaného *darknet_dumpN* (hodnota N je zvýšena po každém zápisu, pro zachování unikátnosti jména). Data jsou zapsána v binárním formátu *pcap*. Výsledné soubory mohou být použity jako vstup pro určité nástroje, které provedou potřebné analýzy. Ve většině scénářů může být program *tcpdump* využit pro prohledání zachycených dat – v reálném čase – dělá se to pomocí BPF výrazů (anglicky *Berkeley Packet Filter*). Samozřejmě, pokud máme uložen celý tok informací ze sítě *darknet* v souborech, nemusíme se bát, že přijdeme o nějakou podstatnou informaci. Později můžeme pohodlně provést bádání a analýzu s pomocí jiných, specifických aplikací.

Dalším užitečným nástrojem, pomáhající ve vizualizaci toku dat v síti, je *argus*. Tento nástroj je vyvíjen firmou QoSient. Konfigurace tohoto programu je trochu komplikovanější, abychom ji mohli popsat v rámci to-



Obrázek 5. *Příklad vstupního rozptylu v případě DDoS útoku*

hoto textu, proto doporučuji seznámit se s jeho možnostmi. Tato aplikace umožňuje mimo jiné pravidelně sledovat tok dat v *temné síti,* odchytávat zajímavé události a generovat hlášení, které jsou velmi užitečné, protože pomáhají dobře porozumět specifikům objevujících se hrozeb.

Pro vizualizaci toku dat v síti *darknet*, ve statistickém kontextu, je možno použít nástroj MRTG (*http://www.mrtg.org/*) Tobiase Oetikera. Tento program umí vygenerovat pěkné grafy toku paketů v *temné síti.*

Existují samozřejmě tuny jiných nástrojů, které mohou být užitečné pro extrakci a analýzu informací na základě dat z *temné sítě*. Pro začátek můžu doporučit několik tříd nástrojů, kterým můžete věnovat pozornost:

- IDS senzory (*Bro*, *Snort*, atd.)
- Paketové sniffery (např. *tcpdump*)
- Analyzátory provozu (*argus*, *SiLK*, atd.)
- Parsery logů generovaných firewallem
- Počítadla toku dat (např. *MRTG*)
- Nástroje pro hledání kategorií platforem infikovaných/skenovaných zařízení (např. *p0f* Michała Zalewského)

Rozmisťování sítí typu honeynet

Stejně jako *darknet*, *honeynet* znamená zjednodušeně rozsah podporovaného IP adresového prostoru. Ale v případě sítí typu *honeynet* nezůstávají pakety bez odpovědi – tato síť simuluje správně fungující službu (nebo více služeb) umožňující – dle potřeby – provedení vstupní výměny dat (anglicky *handshake*) nebo i navázání kompletní, obousměrné komunikace. Se sítěmi typu *honeynet* je spojen pojem *honeypot*. *Honeypot* je systém, který simuluje originální službu. Je to od základů velmi precizně kontrolovaný a neustále monitorovaný zdroj, který má sloužit jako návnada pro potencionální nepřátele útočících na systém. Existuje několik různých druhů sítí *honeynet*, ačkoliv jejich základní myšlenka fungování je společná: poznat taktiku protivníka a získat o něm co nejvíce informací.

Fyzické systémy typu honeypot

Fyzické systémy typu *honeypot* jsou celé počítače umístěné uvnitř sítě *honeynet*, mající vlastní IP adresu, operační systém a je vybaven nástroji podporující simulaci cílové služby.

Virtuální systémy typu honeypot

Virtuální systémy typu *honeypot* jsou plně softwarově simulované služby umístěné uvnitř sítě *honeynet*, simulující takové podmínky prostředí jako je operační systém, síťová fronta a služby nabízené jako vábnička. Jeden fyzický server může nabízet síť tisíců virtuálních *honeypotů*.

Systémy typu honeypot s nízkou úrovní interakce

Systémy typu *honeypot* s nízkou úrovní interakce (v dnešních době – nejčastěji používané systémy tohoto typu) jsou navrhovány tak, aby nalákaly potencionálního útočníka skrz zpřístupnění jednoho nebo více slabých míst, navázat vstupní dialog a uložit si několik prvních paketů příchozích dat. Samozřejmě, že útočník nebo zlomyslný software provádějící útok, rychle zjistí že cílový systém nemůže být použit – ale než se to stane – existuje velká šance na získání cenných informací o taktice nebo schopnostech protivníka. Systémy tohoto typu jsou momentálně využívány pro analýzu taktiky používané generátory spamu.

Existuje několik komerčních implementací řešení typu *honeynet* ale nejčastěji používaným je *honeyd* – projekt typu *open source*, jehož autorem je Niels Provos. Informace o tom, jak získat a nastavit *honeyd* můžete najít na domovské stránce projektu na adrese *http://www.honeyd.org*. Zde se zmíním pouze o tom, že *honeyd* je navržen jako virtuální *honeypot/honeynet*, jenž umí simulovat mnoho různých operačních systémů a programových komponent.

Jiný *honeypot*, pracující v módu malé interakce, který stojí za to zmínit, je *LaBrea*: inovativní řešení autora Toma Listona. Komponenta funguje jako služba spuštěná na pozadí a umožňuje generování nezávislých odpovědí na příchozí požadavky v zadaném bloku IP adres. Práce tohoto programu spočívá (velmi zjednodušeně) na tom, že vytváří a zpřístupňuje prostředí, které se jeví jako velmi atraktivní – z pohledu viděného potencionálními útočníky. *LaBrea* však disponuje jednou velmi zajímavou vlastností, která tuto aplikaci odlišuje od konkurence: umí zpomalit síťovou frontu atakujícího subjektu – přičemž to dělá velmi účinně. Informace o specifikaci této procedury můžete nalézt na domovské stránce projektu na adrese *http://labrea.sourceforge.net/labrea-info.html*.

Systémy typu honeypot s velkou úrovní interakce

Systémy typu *honeypot* s velkou úrovní interakce jsou používány méně často, ale disponují neocenitelnou hodnotou. Oproti systémům s malou úrovní interakce, jsou navrženy takovým způsobem, aby atakující subjekt mohl úspěšně provést úplnou infiltraci cílového systému. Díky tomu může správce, kromě získání základních informací, plně poznat záměry a nástroje, které má útočník k dispozici. Existuje nevýdělečná organizace, známá pod jménem *Honeynet Project* (*http://www.honeynet.org/*), která se zabývá shromažďováním informací a nástrojů zjednodušujících vývoj *honeypot* systémů s velkou úrovní interakce. Na domovské stránce projektu můžete najít mnoho fantastických nástrojů připravených k použití ve vlastních sítích typu *honeynet*. Zvláštní pozornost byste měli věnovat programům *Honeywall*, *Termlog* a *Sebek*.

Musíme také zmínit, že skupina pracující na projektu *Honeynet* vytvořila skvělou knihu popisující nástroje, taktiku a psychologické aspekty týkající se síťových útoků – vše v kontextu zkušeností získaných při vytváření a používání technologií typu *honeynet*. Více informací o zmiňované knize, jejíž titul zní: *Poznej svého nepřítele* (anglicky *Know Your Enemy*), je možno najít na stránkách projektu. Výtěžek z prodeje této knihy pomáhá projektu z finanční stránky.

Doporučené způsoby použití sítí typu honeynet

Pro výzkumné organizace a pro firmy, které mají mnoho volného času a peněz (znáte byť jen jednu takovou firmu?) jsou systémy typu *honeypot* neocenitelným nástrojem, ale já osobně – hlavně vzhledem k vysokým provozním nákladům – bych nedoporučoval použití tohoto typu systémů v každodenní praxi. Sítě typu *honeynet* je vhodné provozovat spíše v módu *na požádání* – ve chvíli kdy vzrůstá aktivita útoků a je těžké určit je zjistit pomocí jednoduchých nástrojů. Jiným scénářem, kdy je dobré používat *honeypoty,* je nutnost ověřit potencionální pokusy o infiltraci do systému.

V této chvíli je dobré zmínit příklad implementace tohoto typu systému, používané jedním z čelních výrobců integrovaných čipů. V této organizaci se využívá linuxový server na kterém je spuštěn VMWare. Na základě tohoto software jsou spouštěny 4 virtuální počítače – po jedné pro každý z momentálně používaných firemních variant systému Windows (NT, 2000, 2003 a XP). Na každém systému je udržován systém aktuálních záplat. Na nižší úrovni fungující Linux monitoruje tok dat a změny provádějící se v příslušných systémech s cílem zachycení nové havěti (a jiných hrozeb), která by mohla mít negativní vliv na komerční služby. Více informací o této implementaci najdete na adrese *http://phoenixinfragard.net/meetings/past/200407hawrylkiw.pdf.*

Implementace kanálů jako obrany před útoky typu DDoS

Jiným novátorským způsobem využití technologie kanálů je jejich použití jako obranný mechanismus před (potencionálně rozprášenými) útoky spočívajícími v blokování služeb. V bodě *Základní pojednání a příklady využití* jsem ukázal nejjednodušší způsob přesměrování protivníka do *černé díry.* Ve chvíli, kdy přesně známe cíl útoku, přesměrujeme IP adresu na dočasné rozhraní nacházející se na okraji sítě. Toto jednání úplně uvolní atakovaný systém od

Tabulka 1. *ICMP pakety*

ICMP pakety	Popis
3.0	Nedostupná síť
3.1	Host nedostupný
3.3	Port nedostupný
3.4	Vyžadována fragmentace
3.5	Chyba ve zdrojové cestě
3.6	Chyba: cílová síť není známa
3.7	Chyba: cílový host není znám
3.10	Host blokován správcem
3.11	Nedostupný typ síťové služby
3.12	Nedostupný typ služby hosta
3.13	Komunikace zablokována správcem
11.0	Vypršení TTL při předávání
11.1	Reasemblace fragmentace: chybí odpověď ve stanoveném čase

TCP pakety	Popis
Nastavený bit RST	Resetování TCP

celkového zahlcení způsobeného bombardováním zlomyslnými požadavky – bohužel ne vždy umožní obejít vedlejší, negativní efekty útoku – takových jako je zvýšené zatížení sítě poblíž bodu útoku (v topologickém smyslu).

Aby se vyhnuli tomuto nežádoucímu efektu, mnoho zprostředkovatelů síťových služeb – zvláště těch, kteří podporují největší telekomy – se rozhodlo pro využití pokročilých technik obrany před útoky typu DDoS, stanovující integrální část síťové infrastruktury a implementovaných již ve chvíli návrhu celého systému. V mnoha případech jsou řešení tohoto typu vybavena pokročilými technologiemi sledování umožňující lokalizovat bezprostřední vstupní bod útoku a již v této části přesměrovat nepřátelské pakety na rozhraní černé díry, nezpůsobujíc žádné další přetížení a zatížení sítě. Tyto systémy umožňují zachytit škodlivý tok dat a bezprostředně jej blokovat přímo ve vstupním bodě – v reálném čase. Co víc, v některých případech je kontrola nad tímto systémem možná v podobě dedikovaného rozhraní z úrovně klienta. Pak mluvíme o *uživatelsky řízených černých dírách v reálném čase* (anglicky *customer-triggered real-time blackholes*).

Řízené přesměrování do černé díry

Jak jsem již zmiňoval výše, mnoho velkých ISP subjektů implementuje rozprášené, automatické systémy umožňující řízení přesměrování do černé díly (anglicky *blackhole routing*) pro zadaný rozsah IP adres. Toto vyvolání může být provedeno jak na straně zprostředkovatele Internetu tak i u klienta – a v závislosti na potřebě – manuálně nebo automaticky. Tato technika se opírá o využití jednoduchých kanálů – tak jak je popsáno v podbodu *Základní pojednání a příklad využití*. Cílový kanál se obvykle nastavuje na všech vstupních (čtěte: okrajových) routerech v síti ISP subjektu – čili ve všech bodech toku dat s vnějším světem. Ve chvíli identifikace útoku, jak zprostředkovatel tak i klient, mohou ohlásit atakovaný prefix v tabulce přesměrování BGP. Tento prefix je pak příslušně označen, takže příchozí data na všechny okrajové routery jsou staticky přesměrovány na rozhraní *blackhole*.

Z pohledu ISP, jsou pro implementaci rozprášeného mechanismu přesměrování do černé díry, vyžadovány následující kroky:

- Výběr ne globálně přesměrovaného prefixu (např. Test-Net (RFC

3330) 192.0.2.0/24), který bude používán jako následující skok pro libovolný atakovaný prefix. Použití prefixu o délce 24 umožňuje použití mnoha různých IP adres pro specifické typy přesměrování.
- Konfigurace statické trasy na každém vstupním/naslouchajícím routeru, pro prefix 192.0.2.0/24 tak, aby vedla na rozhraní černé díry. Například: `ip route 192.0.2.0 255.255.255.0 Null0`
- Konfigurace BGP a taktiky map přesměrování s cílem ohlášení, že dane předčíslí je atakováno (viz Výpis 1).

V ukázkové konfiguraci rozšiřujeme statická přesměrování (shodná se zápisem *tag 199*) v BGP, nastavíme další skok na IP adresu přesměrovanou na rozhraní černé díry, nastavíme lokální prioritu na hodnotu 50 a ujistíme se, že cílové přesměrování nebude propojeno na žádné vnější připojení (`no-export`).

Při této základní konfiguraci může ISP subjekt inicializovat mechanismus ovládání skrz statické přesměrování pro atakovaný prefix (nebo hosta) například:

```
ip route 172.16.0.1 255.255.255.255
192.0.2.1 Null0 tag 199
```

Toto statické přesměrování vlastně vyvolává iniciátor, který spustí celý výše popsaný proces. Router na kterém je definováno toto přesměrování jej oznámí jiným vnitřním routerům pomocí iBGP – tato informace bude předávána tak dlouho až se dostane ke všem okrajovým routerům.

Navíc ISP subjekt může zpřístupnit možnost ovládání popsaného procesu pomocí BGP, díky čemuž mohou uživatelé BGP spouštět celý mechanismus nezávisle na intervenci zprostředkovatele. ve skutečnosti je to nejmocnější aspekt této techniky. Abyste získali výsledek tohoto typu, musíte trochu změnit konfiguraci na straně ISP (viz Výpis 2).

ISP subjekt přesměrovává statickou adresu < *blackhole-ip* > na rozhraní černé díry – a dokud klient oznamuje cílový prefix, do té doby jej zprostředkovatel propaguje uvnitř své sítě. Ve výsledku, tak jako ve výše popsaném případě – veškerý provoz přicházející na určenou adresu je pak přesměrován na okrajových routerech sítě ISP subjektu.

Základní konfigurace na straně klienta je ukázána na Výpise 3.

Když je BGP konfigurace na svém místě (definovaná na straně zprostředkovatele), musí klient pouze nainstalovat statické přesměrování pro atakovaný prefix #. Tímto způsobem, s nevelkou pomocí ISP subjektu, má klient k dispozici velmi rychlý mechanismus reakce na útoky typu DoS, stejně pro jednotlivé hosty i v oblasti celého prefixu.

Tabulka 2. *Shrnutí*

Krok	Opis
Plně pochopte jak vám zprostředkovatel Internetu může pomoci v případě DDoS útoku.	Vytvořte si plán činností při vyskytnutí se útoku DDoS, vytvořte strategii, která využije možností vašeho zprostředkovatele v oblasti přesměrování útoku do černé díry (v reálném čase).
Zvažte implementaci vnitřní sítě typu *darknet*.	Pamatujte, že vnitřní síť typu darknet vám dává možnost chycení síťové havěti rychleji než to udělá váš antivirový software. Navíc, použití tohoto řešení odhalí těžce detekovatelné chyby v konfiguraci vaší sítě.
Zvažte implementaci vnější sítě typu *darknet*.	Vnitřní síť typu darknet vám umožní získat nástroj pro nepřetržité monitorování hrozeb přicházejících z vás obklopujícího prostředí; tento nástroj vám umožní ukládat a analyzovat nevyžádaný provoz objevující se ve vaší síti. Prozkoumáním dat spojených se zpětným rozptylem pak již víte, že vaše síť se stává spoluúčastníkem útoku na jiný subjekt.
Pokud máte čas a příslušné zdroje, použijte systém typu *honeypot*.	Většina organizací nevidí nutnost používání sítě typu *honeynet* (a pokud ano, tak již po nějaké škodě). Z druhé strany však jsou takovéto sítě neocenitelným zdrojem informací pro výzkumníky mechanismů bezpečnosti systémů. Vždy je dobré zamyslet se nad dopady implementace sítě *honeynet* – toto poznání může mít výrazný vliv na vaše konečné rozhodnutí.

Vstupní rozptyl a metoda Traceback

V této sekci popíšeme promyšlené způsoby využívání sítě návnad pro detekci útoků a také získávání důvěrných informací a stopování útočícího subjektu.

Vstupní rozptyl

Než přejdeme k věci, chtěl bych definovat pojem vstupní rozptyl. Použiji k tomu jednoduchý příklad. Celý semestr, v době mého prvního roku na škole, jsem psal dopisy (ty obyčejné – na papír) mým přátelům, kteří v té době cestovali po světě. Při mé neustálé schopnosti zapomínat se mi velmi často stávalo, že jsem zapsal na obálku nesprávnou zpáteční adresu. Jednou se jeden z mých kamarádů přestěhoval na nové místo a dopis, který jsem mu napsal byl vrácen odesílateli. Protože zpáteční adresa nebyla správná – dopis se nevrátil mě, ale na recepci kolejí a teprve poté se dostal do správných (mých) rukou.

Tento případ návratu k odesílateli je právě formou vstupního rozptylu. V tomto případě rozptyl byl založen na tom, že dopis byl doručen na recepci – a ne přímo mně.

V kontextu Internetu, ve chvíli, kdy jistý subjekt A provádí útok

Nove číslo již v prodeji

Časopis lze zakoupit také na naší internetové stránce:
http://buyitpress.com

www.lpmagazine.org/cz

typu DoS na subjekt B, přičemž A touží zůstat anonymní vzhledem k B – pak obvykle v zasílaných paketech zadá falešnou zdrojovou adresu (IP hlavičky jsou příslušně upraveny, v případě Ipv4 je množství možných permutací 2^32). Ve chvíli útoku, routery a jiná síťová zařízení nacházející se na cestě toku dat posílají velké množství návratových informací, které se vrací k úplně náhodným adresátům, kteří úplně bez příčiny získávají informace o útoku na subjekt B (stejně jako se recepce na kolejích dozvěděla o mém dopise). Tento stav je zobrazen na Obrázku 5.

Ve skutečnosti je většina zpráv přicházejících v rámci vstupního rozptyl potichu filtrována našimi firewally, protože jsou považovány za odpovědi na požadavky, které nebyly odeslány. Pokud máme implementováno síť typu *darknet*, můžeme čekat na pakety tohoto typu s cílem zjištění jak často je náš adresový prostor spojen s útoky na jiné subjekty. V Tabulce 1 vidíte typy paketů, které je možno kvalifikovat jako zpětný požadavek.

Traceback

Teď, když již víme v čem spočívá smysl vstupního rozptylu, se můžeme zamyslet nad tím, jak jej můžeme využít k vlastním cílům. V síti vybavené mnohonásobnými tranzitními bránami, by mohlo být velmi užitečné lokalizovat vstupní bod *špatných* paketů. Technika, která to umožňuje provést, se nazývá *traceback*. Je velmi užitečná, protože po identifikování ohroženého vstupního bodu do sítě můžeme zredukovat propustnost tohoto vstupu, což je jednoznačně odlehčení atakované služby – přičemž *dobrý* tok paketů může pokračovat alternativním, neohroženým způsobem připojení.

Technika *traceback* umožňuje využít vstupního rozptylu podporované sítí (nebo sítěmi) typu *darknet*, v kontextu hledání vstupního bodu útočících paketů. tato technika je však dostupná pouze z úrovně ISP subjektu nebo ve velmi velké organizaci vlastnící rozsáhlou síť vybavenou mnoha vstupními internetovými branami.

Když máme síť tohoto typu dostupnou, může být *traceback* proveden vetech jednoduchých krocích (ve chvíli DoS útoku):

- Proveďte identifikaci cíle a ujistěte se zda je současný provoz zapříčiněn útokem.
- Na všech bránách přesměrujte část zvýšeného provozu do černé díry (například hosty z oblasti /32) ale místo odmítání paketů, nastavte rozhraní černé díry tak, aby reagovalo na nesprávné požadavky. To způsobí vygenerování vnitřního provozu obsahujícího zprávy o chybách ICMP, které se budou vracet na své zdrojové body.
- Využijte svůj *darknet* pro zachycení vstupního rozptylu (očekávejte především zprávy o chybách ICMP) – filtrujte pouze ty zprávy, které obsahují IP adresu vašeho routeru. Místa, kde budete dostávat tyto zprávy jsou hledanými vstupními body útoku. Tuto operaci můžete provádět i když nemáte komplikované nástroje pro práci se sítí typu *darknet*. Stačí použít jednoduchý přístupový seznam ve spojení s rozhraním routeru vaší sítě *darknet*: `access-list 105 permit icmp any any unreachables log; access-list 105 permit ip any any`

Po spuštění terminálu v monitorovacím módu (nebo obyčejným prohlížením logu) dostanete zjednodušený report o vstupním rozptylu, který byste měli prohledat s přihlédnutím k objevení se IP adres svých bran. ●

V Síti

- Kniha *Extreme Exploits: Advanced Defenses against Hardcore Hacks*, vydaná vydavatelstvím McGraw-Hill/Osborne v roce 2005 – *http://www.amazon.com/gp/product/0072259558/*
- Dokumenty: Internet RFCs 3330 (*Special-use IPv4 Addresses*) a 3882 (*Configuring BGP to Block Denial of Service Attacks*)
- Projekt *Darknet* skupiny Cymru – *http://www.cymru.com/Darknet/*
- Domovská stránka knihoven *tcpdump* a *libpcap* – *http://www.tcpdump.org/*
- Domovská stránka *ARGUS* – *http://www.qosient.com/argus/flow.htm*
- Domovská stránka *Honeyd* – *http://www.honeyd.org*
- Domovská stránka projektu *HoneyNet* – *http://www.honeynet.org*
- Domovská stránka nástroje *p0f* – *http://lcamtuf.coredump.cx/p0f.shtml*
- Článek Chrise Morrowa a Briana Gemberlinga pojednávající o využití mechanismu černých děr ISP subjekty (anglicky *ISP blackholing*) a analýze výskytu zpětného rozptylu (anglicky *backscatter*) – *http://www.secsup.org/Tracking/*
- Prezentace Dana Hawrylkiwa o sítích typu *honeynet* – *http://phoenixinfragard.net/meetings/past/200407hawrylkiw.pdf*
- FAQ dokument o paketovém filtru v systému OpenBSD *http://www.openbsd.org/faq/pf/*

O autorovi

Victor Oppleman je uznávaným autorem, mluvčím a přednášejícím na poli bezpečnosti počítačových sítí a také konzultantem v nejdůležitějších, mezinárodních korporacích. Jeho software, šířený jako *open source*, je momentálně na stovkách tisíc počítačů po celém světě. Victor Oppleman je také vlastníkem mnoha patentů s takových oblastí jako adaptivní výběr připojení v rozprášených sítích (anglicky *distributed adaptive routing*) a uživatelské bezdrátové aplikace (anglicky *wireless consumer applications*).

Velká část dnešního článku se opírá o materiály prezentované v knize autora: *Extreme Exploits: Advanced Defenses Against Hardcore Hacks*, vydané vydavatelstvím McGraw-Hill/Osborne v roce 2005.