KYBERNETICKÉ ÚTOKY: RUSKO? – GRUZIE a SVĚT

Autor: Mgr. Tomáš Sekera, Security Director, Logica CEE

Informační válka „INFOWAR“

Jedná se o soubor aktivit, často vzájemně zkoordinovaných co do cíle, místa a času, které slouží k vytěžení, znepřístupnění, pozměnění, poškození až likvidaci informací anebo jejich zdrojů, s cílem dosáhnout významné výhody v boji nebo vítězství na konkrétním protivníkem. Útoky nejsou jednotlivé, ale většinou kombinované, masivní a zasahující celé vybrané geografické území. Nezanedbatelný je rovněž dominový efekt takového útoku.

Infowar lze podle cílů kategorizovat např. tímto způsobem:

1. charakteristická infowar – omezení efektivní činnosti napadeného subjektu,
2. „hacktivism“ – použití metod hackingu k prosazení politických cílů, spočívající v degradaci či porušení obsahu informačního systému napadeného subjektu, který způsobí neschopnost činnosti subjektů na tomto informačním systému závislým anebo naopak vyvolá nežádoucí reakci na základě dezinformace, včetně šíření poplašných zpráv,
3. zpravodajský (skrytý) charakter napadení, smyslem je získání a analýza informačních zdrojů napadeného subjektu,
4. „perception management“ – vedená za účelem skrytého ovlivnění rozhodování nebo veřejného mínění na základě upravovaných informací,
5. pro úplnost – fyzická likvidace informačních prostředků pomocí bojové akce.

Mimo tyto sofistikované akce stojí tvz. elektroničtí sprejeři, výraz „vypůjčený“ od p. Vondrušky, kteří přepisují webové stránky čistě pro vlastní potěšení, jako důkaz své dovednosti překonat bezpečnostní opatření.

Informační válka v pojetí výše uvedených bodů 2-4 může zásadním způsobem přispět např. až k destabilizaci politické situaci v dané napadené zemi, ovlivnění volebních preferencí. Nástroje informačních technologií ve spojení s PR aktivitami poté dostávají naprosto jiný, silnější náboj. Stávají se rovněž účinným nástrojem propagandy, pozitivní i negativní.

Konflikt Gruzie - Rusko

(dále uváděná zjištění vycházejí z otevřených zdrojů)

Konflikt mezi Gruzií a Ruskem se vedl i na úrovni kybernetického prostoru. V současné době nelze s jistotou říct, jde-li o oficiální útoky vedené jednotlivými stranami na příkaz státní moci, nebo jen o méně či více organizované skupiny lidí – útočníků. Užití pojmu hacker v tomto případě nebylo úplně správným označením útočníka, neboť většinou nešlo o vlámání se do cizích systémů, ale jen o jejich napadení.

Provedení většiny útoků bylo metodou DDoS – tento způsob napadení vzdáleného systému neškodí systému samotnému, ale spíše využívá zahlcení služby, kterou systém provozuje a tím znemožní její normální fungování. Jako příklad lze uvažovat o napadení třeba domény www.www.com :
Útočník, který chce systém napadnout, ovládá tzv. C&C server (command and control). K tomuto serveru jsou pomocí tzv. Botnet sítě připojeni klienti, kteří vykonávají příkazy C&C serveru. Těmito klienty mohou být nedostatečně zabezpečené stanice umístěné po celém světě, jejíž majitelé ani nevědí, že jejich počítač je připojen do Botnet sítě nebo, že napadá jiné systémy. Útočník vydá příkaz, aby se tyto počítače začali automaticky dotazovat webových stránek www.www.com na nesmyslné dotazy. Následkem toho webový server nestíhá odbavit všechny dotazy, neboť jich v

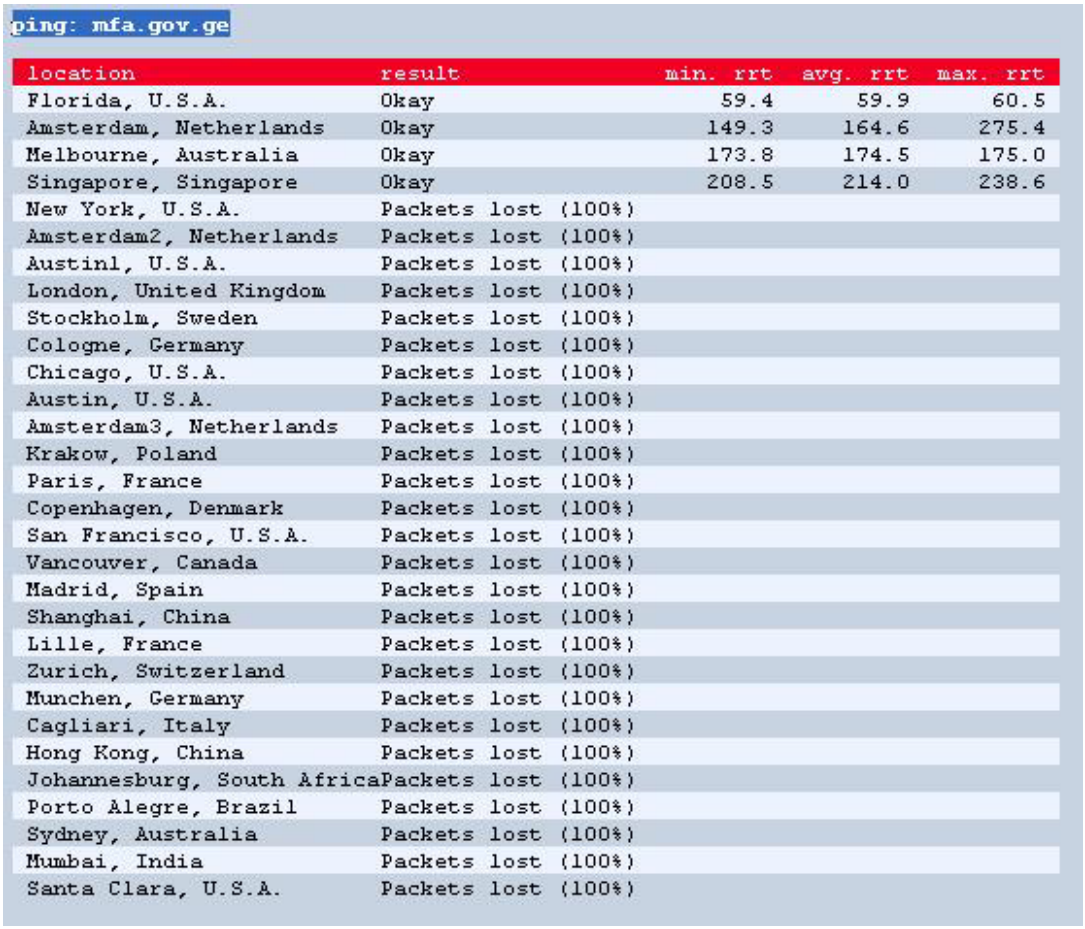
krátkém období přichází velké množství a buď se zastaví anebo neodpovídá na dotazy regulérních návštěvníků. Tento typ útoku vyžaduje dostatečné množství klientů botnetu kteří útočí na napadený systém. Uváděná/odhadovaná cena takového útoku je 0.04 US Cent na jeden útočící počítač.

Útoky na gruzínské webové stránky probíhaly již od cca 19.-20. července 2008. Bezpečnostní experti z USA potvrzují rozsáhlé útoky na oficiální webové stránky Gruzie. Podle mluvčího Gruzínského velvyslanectví nabraly útoky vyšší obrátky v okamžiku napadení Jižní Osetije. Útokům z ruské strany předcházela distribuce veřejného seznamu vládních webových stránek po ruských fórech. Tímto způsobem byla zajištěna informovanost zejména ruský hovořících uživatelů Internetu, které webové stránky budou atakovány. Jednou ze skupin, která se podílí na kyber útocích, je stopgeorgia.ru, v případě nedostupnosti www.stopgeorgia.info . V další fázi došlo k distribuci velmi jednoduchého nástroje na http zahlcení zvolené IP adresy. O víkendu 9.-10. srpna byla většina gruzínských webových stránek nedostupná. Gruzie musela požádat o podporu z jiných zemí, aby mohla o vojenském zásahu informovat okolní svět pomocí Internetu. Většina webových stránek velkých firem a státních orgánů byla přesunuta na hosting do jiných zemí. Na základě napadení stránek prezidenta Saakašviliho (zobrazení fotografie Hitlera), které byly také přesunuty (USA - Georgie), lze nyní hovořit až o „otevřené válce mezi mocnostmi“, neboť američtí hackeři si toto nenechali líbit a provedli odvetné útoky na stránky umístěné v Rusku. Zároveň je ale nutné podotknout, že z pohledu míst zdrojů útoku se jedná o celosvětovou „válku“ neboť útočící počítače jsou z různých zemí světa.

Stojí Rusko opravdu za útoky v Gruzii?

Dle analýz U.S.CERT nejsou tyto kybernetické útoky součástí žádného většího plánu k napadení země. V minulosti se toto projevilo např. v Estonsku, Litvě a dalších zemích, které se jakýmkoliv způsobem dotkly cítění ruských hackerů. Nelze s jistotou potvrdit či vyvrátit, má-li Rusko či jiný stát organizovanou skupinu útočníků. Problematika cybercrime a zpravodajských her je kapitola sama pro sebe. Jako pravděpodobnější se vzhledem k charakteru útoku jeví možnost neorganizovaných skupin dostatečně kvalifikovaných (ale i nekvalifikovaných) jedinců, kteří berou útoky jako svou “vlasteneckou” povinnost ke svému státu a mohou se tak zapojit do samotného aktu kybernetické války. Dle informací z webových stránek zabývajících se touto problematikou je pravděpodobné, že za masivní částí útoku stojí skupina RBN (Russian Business Network). Nicméně je nutné na základě komplexního útoku a protiútoků připustit organizovanost těchto skupin.

Zda útočníky jsou hackeři izolovaní od státní moci, či při konkrétním napadení byla uplatněna státní vůle, může ukázat forenzní vyšetřování jednotlivých caus. Pravděpodobnějším se ale jeví, že skutečná fakta vyjdou najevo až otevřením archivů bezpečnostních složek, ovšem po uplynutí doby určené k možnosti zveřejnit jejich obsah. Z pohledu bezprostředního zajištění bezpečného Internetu není však rozhodné, kdo jej napadá.



ping: mfa.gov.ge

location	result	min. rrt	avg. rrt	max. rrt
Florida, U.S.A.	Okay	59.4	59.9	60.5
Amsterdam, Netherlands	Okay	149.3	164.6	275.4
Melbourne, Australia	Okay	173.8	174.5	175.0
Singapore, Singapore	Okay	208.5	214.0	238.6
New York, U.S.A.	Packets lost (100%)			
Amsterdam2, Netherlands	Packets lost (100%)			
Austinl, U.S.A.	Packets lost (100%)			
London, United Kingdom	Packets lost (100%)			
Stockholm, Sweden	Packets lost (100%)			
Cologne, Germany	Packets lost (100%)			
Chicago, U.S.A.	Packets lost (100%)			
Austin, U.S.A.	Packets lost (100%)			
Amsterdam3, Netherlands	Packets lost (100%)			
Krakow, Poland	Packets lost (100%)			
Paris, France	Packets lost (100%)			
Copenhagen, Denmark	Packets lost (100%)			
San Francisco, U.S.A.	Packets lost (100%)			
Vancouver, Canada	Packets lost (100%)			
Madrid, Spain	Packets lost (100%)			
Shanghai, China	Packets lost (100%)			
Lille, France	Packets lost (100%)			
Zurich, Switzerland	Packets lost (100%)			
Munchen, Germany	Packets lost (100%)			
Cagliari, Italy	Packets lost (100%)			
Hong Kong, China	Packets lost (100%)			
Johannesburg, South Africa	Packets lost (100%)			
Porto Alegre, Brazil	Packets lost (100%)			
Sydney, Australia	Packets lost (100%)			
Mumbai, India	Packets lost (100%)			
Santa Clara, U.S.A.	Packets lost (100%)			

Obrázek převzat z článku: Coordinated Russia vs Georgia cyber attack in progress http://www.infowar-monitor.net/

Odvetné útoky Gruzie a její obrana

Gruzie provedla odvetné útoky na webové stránky ruských médií avšak s daleko menšími následky než pocítila sama. V současné době provádí Gruzie filtrování, cenzuru a monitorování internetu na úrovní ISP. Caucuses On-Line, největší Internet Service Provider, nemá díky omezením přístup k doménám s koncovkou ".ru" Podobný filtrovací systém byl zaveden i v GRENA (Georgian Academic and Research Network (obdoba naší akademické sítě). Není zřejmé, zda jde o rozhodnutí jednotlivých ISP nebo o součást státního plánu v případě ohrožení. Gruzie požádala o odbornou pomoc z okolních států. Polsko a Estonsko nabídlo Gruzii odbornou pomoc a kapacitu k přemístění důležitých internetových stránek. Dva z estonských odborníků CERT se vypravili do Gruzie, aby pomohli se zabezpečením internetové sítě v zemi. Estonsko tak pomáhá vytvořit jakousi kybernetickou alianci zemí, které byly napadeny ruskými hackery. Gruzie tvrdí, že nedošlo jen k napadení stránek prezidenta a státních institucí, ale také bankovního systém, který musel být na několik dní vyřazen. Většinu odborníků znepokojuje fakt, že za všemi útoky pravděpodobně stojí civilní skupiny hackerů a kybernetická válka se tak dostává do nové roviny. Nelze tedy obviňovat přímo jednotlivé státy, z nichž hackeři zřejmě pocházejí. Proto nelze ani požadovat nápravu stavu po těchto státech. Maximálně prevenci – jejíž návrh částečného řešení je dále uveden.

Zdroj: Moscow *Moskovskiy Komsomolets* in Russian 12 Aug 08 p3

Obrázek převzat z Information Warfare Monitor http://www.infowar-monitor.net/

Další související útoky v Gruzii

Došlo také k zneužití emailových adres gruzínských politiků, seznam byl původně vytvořen lobbistickou organizací. Emailové schránky byly zahlceny (SPAM) a cíleně byly podstrčeny URL s malware přes live exploity.

Byl zaznamenán útok na mobilní telefon gruzínského premiéra, který spočíval v zahlcení telefonu nesmyslnými textovými zprávami a voláním.

Dalším typem útoku bylo přerušení běžných komunikačních kanálů. Jedno z nejpopulárnějších hackerských fór v Gruzii bylo nedostupné 24 hodin pod stálým útokem DDoS, aby byla znemožněna komunikace mezi gruzínskými hackery.

Cílem útoků byla kompromitace několika vládních www stránek zejména:

- www.president.gov.ge
- www.rustavi2.com
- www.parliament.ge
- www.government.gov.ge/eng/
- www.mfa.gov.ge
- www.mod.gov.ge
- www.police.ge
- www.nsc.gov.ge
- www.mof.ge
- www.nbg.gov.ge

Cíle gruzínských hackerů:

- osinform.ru – jihoosetinská televizní a rozhlasová stanice
- osradio.ru – jihoosetinská televizní a rozhlasová stanice

Ovládací C&C servery jsou zejména:

79.135.167.22

- emultrix.org
- yandexshit.com
- ad.yandexshit.com
- a-nahui-vse-zaebalo-v-pizdu.com
- killgay.com
- ns1.guagaga.net
- ns2.guagaga.net
- ohueli.net
- pizdos.net

Symantec: Kybernetický útok na Litvu byl veden z Ruska

Společnost Symantec se prostřednictvím svého country managera pro ČR Radka Smolíka vyjádřila k červencovému (2008) koordinovanému kybernetickému útoku na několik tisíc litevských webových serverů, a to jak vládních institucí, tak i soukromých společností.

„Podle našich analýz, kterými disponujeme, se jedná s nejvyšší pravděpodobností o útok cíleně vedený z Ruska. To, že za útokem stojí ruští hackeři, potvrzuje i podvržený obsah plný komunistických a nacistických symbolů a nacionálních replik. Ostatně napjaté vztahy mezi Litevci a silnou ruskou menšinou žijící v Litvě tuto domněnku potvrzují."

Pravděpodobnou příčinou útoků je přijetí litevským parlamentem nového zákona (ze všech post-sovětských republik dosud nejpřísnější), který zakazuje a přísně trestá publikování komunistických a nacistických symbolů, jako jsou obrazy představitelů těchto režimů, emblémy, vlajky, odznaky a označení, ale také srp a kladivo nebo třeba svastika.

„Z politického hlediska má útok proti několika tisícům litevských webových stránek podobný charakter jako zhruba rok starý útok na Estonsko. Ten byl však svým rozsahem i dopadem mnohem citelnější. Značné dopady loňského útoku na estonský život byly zapříčiněny i velkým pokrokem v oblasti eGovernment, jehož Estonsko dosáhlo – a tím také podstatně větší závislostí na těchto službách."

Zdroj: *SecurityWorld/Internet*, rubrika On-line bezpečnost, 2.7.2008

Obrana – doporučení

Na základě zkušeností se jeví nejdůležitějším v případě napadení internetu takovým to masivním útokem jako v Gruzii, Litvě a Estonsku (dostupnost + integrita), zachovat plné fungování systémů informovanosti občanů, systémů včasného varování, podpůrných systémů kritické infrastruktury (ITC služby, doprava, energetika, finanční služby, vynucování práva, zdravotnictví, sociální zabezpečení, zajištění potravin a vody, ozbrojené síly). Jako malicherné se jeví řešit v danou chvíli nefunkční stránky prezentace hlavy státu (z pohledu bezpečnosti státu nepřinášejí žádné relevantní informace). Jistě jde o prestižní záležitost, ale v době útoku je důležitější zachovat kritické systémy.

Jednou z cest, jak ochránit provoz vybraných veřejných služeb poskytovaných prostřednictvím Internetu, je přiřazení odpovídajícího technicko-organizační opatření na základě

jejich kategorizace. Poskytovatelé těchto služeb přitom nejsou typicky subjekty zařazenými do systému krizového řízení, pro případ války a krizových stavů. Jedná se o běžné služby veřejnosti, jejichž nedostupnost ale způsobuje nemalé problémy – uživatelské, informační, potažmo i politické.

Katalog vybraných služeb by byl analogií, byť významově nižší, mezinárodního, či národního preferenčního schématu (přednostního spojení), kdy se jedná o souhrn technicko-organizačních opatření, která umožňují zařazeným uživatelům v období krizových stavů přístup ke službám elektronických komunikací v mezinárodním nebo národním provozu i v případech, kdy jejich poskytování je omezeno z důvodu narušení infrastruktury sítě nebo její neprůchodnosti. Ochrana by byla poskytována primárně službě, nikoliv subjektu, který ji provozuje, jakkoliv toto spolu úzce souvisí.
Dostupnost služeb zařazených v katalogu by tak byla zvýšenou měrou chráněna i v době mimo krizové stavy. Otázkou je, vzhledem k významu některých služeb, zda i za krizových stavů….

Klasické technické řešení

Státní instituce a významné soukromé subjekty mohou mít mimo vlastní izolovanou krizovou infrastrukturu jako obranu proti DDoS útokům při běžném provozu nasazeny filtry, jež omezí příchod ze shodných adres, či připraveny záložní servery, jež při zvýšeném zatížení převezmou další dotazy účastníků. Smyslem tohoto článku není prezentovat výčet technických možností obrany proti DdoS Attack.

V souvislosti s tímto typem útoků je nutné zmínit problematiku ochrany VoIP systémů. Stává se běžným trendem přechod firem a dalších subjektů na tento typ komunikace a v případě zahlcení serverů obsluhujících tyto služby by byla znemožněna jejich komunikace.

Řešení de lege ferenda

Stát (primárně člen EU – závaznost direktiv EU), pravděpodobně zastoupený regulátorem pro oblast elektronických komunikací, může mít, jako součást krizového řízení připraven projekt, kdy ISP budou povinni průběžně, či na výzvu filtrovat určité IP adresy. V době masivního napadení Internetu by byly řízeně dostupné jen vnitrostátní adresy a případně adresy okolního světa, které by byly určeny k předávání informací. Tento „White list“ by bylo nutné neustále udržovat aktuální na základě vznikajících nebo zanikajících informačních systémů v prostředí Internetu. Díky této metodě by se velice omezila možnost DDoS útoku na ohrožené servery bez zásahu vlastníka serveru. Ovšem cenou za takové řešení by byla dočasná nedostupnost a snížený komfort služeb poskytovaných prostřednictvím Internetu, oproti době mimo útok. K takovému kroku je nutná mj. změna příslušné národní legislativy, spočívající v uložení povinnosti monitoringu a nastavení flitrů provozu pro ISP, dále v povinnosti pro regulátora tuto oblast nad rámec krizového řízení kontrolovat a plnění povinností vyžadovat. V neposlední řadě by bylo nutné řešit i otázku souvisejících nákladů.

White list by ovšem mohl vzniknout i na základě dobrovolnosti, resp. komerčních dohod mezi ISP a jeho klienty s chráněnými zájmy - službami. Jednalo by se o z pohledu práva dobrovolné zavedení restrikcí nežádoucího provozu, v návaznosti na podmínky vyplývající z národních a mezinárodních propojovacích smluv a smluv o přístupu k sítím elektronických komunikací a přiřazeným prostředkům.

Poškozený by se následně při nedostupnosti služby z důvodu nezajištění přiměřené bezpečnosti mohl dožadovat nápravy přímo u ISP (jakkoliv se ISP obecně v jejich všeobecných

obchodních podmínkách nyní předem vyviňují z nedostupnosti služby cizím zaviněním), jež by tak byl nucen na základě smluvního závazku nebo zákonné povinnosti konat a předcházet takovým nežádoucím stavům, např. navrhovaným monitorováním a filtrováním provozu.

Obchodní model naprosté regulace vs. model dobrovolnosti (smluvního vztahu ISP/uživatel), lze pro danou situaci kombinovat i regulací částečnou. Regulován by příslušným způsobem byl pouze povinný obsah smluv o propojení a o připojení, kdy by ISP měl povinnost zavést monitor a filtr, současně s právem nežádoucí provoz přerušit.

Ale již v současné době je možno zřejmě uvažovat také o uplatnění náhrady vzniklé škody stranou poškozenou (spotřebitelem/uživatelem) přímo na ISP. Využívání tohoto právního prostředku, resp. navazujících soudních rozhodnutí – precedentů, by mohlo být spouštěcím impulsem a přispět k systematickému a preventivnímu řešení situace, ze strany samotných ISP. Uživatel služby nemůže totiž situaci příliš ovlivnit a dle mého názoru není ani možné po něm spravedlivě požadovat zajištění takové ochrany vlastními prostředky. Jakkoliv je nutné konstatovat,že stále řada uživatelů, včetně institucí, nemá nastaveny základní zabezpečovací funkce. Na místě je patrná jistá analogie s užíváním služeb elektronického bankovnictví, kdy povinnost zajistit bezpečnost v této rovině je jednoznačně přenášena na poskytovatele služeb – banky, čemuž v prostředí ČR svědčí rozhodnutí finančního arbitra.

Pokud navrhovaná řešení shrneme – bezpečnost internetu je záležitostí všech zúčastněných a je žádoucím „do hry“ vtáhnout zvláště poskytovatele služeb elektronických komunikací, ať již formou úplné, či částečné regulace anebo formou zvláštní bezpečnostní služby poskytované ISP za úplatu (garance dostupnosti). Tlak ovšem musí primárně vzejít ze strany poškozených nebo ohrožených uživatelů, kterými jsou stát, právnické i fyzické osoby.

Poznámka na závěr. Existuje celá řada aktivit mezinárodních organizací a států, spojených s kritickými infrastrukturami. V Evropě se jedná zejména o ITU, G8, IOCE/HTC, OECD, GTSC, GRSC, IEFT, ETSI. V Kanadě vytvořil ministerský předseda Úřad pro ochranu kritických infrastruktur spadající pod obecnou pravomoc ministra národní obrany. Ve Spojených státech je vytvořena Prezidentské rada pro ochranu kritických infrastruktur. Problematika je pochopitelně řešena i na úrovni vojenské (NATO a další).

Tomas Sekera

Digitally signed by Tomas Sekera
DN: CN = Tomas Sekera, C = CZ, OU = end user
Reason: I am the author of this document
Date: 2008.12.03 15:30:12 +01'00'