Bezpečná VLAN v NIX.CZ

Ing. Tomáš Hála
ACTIVE 24, s.r.o.
www.active24.cz

O čem byla přednáška loni?

Březnový DoS na portál ihned.cz

- samostatné přednášky na toto téma:
  - Internet a Technologie 2013 (CZ.NIC)
  - Bezpečnost (pro studenty FIT ČVUT v rámci předmětu "BI-BEZ")

Březnový DoS na portál ihned.cz

- útok na hosting pro ihned.cz, respekt.cz, ekonom.cz aj. (Economia)
- malý datový tok (desítky až stovky Mbps), ale miliony pps
- podvržené adresy (SYN flood a odražený SYN/ACK)
- nebyl příliš distribuovaný
- urychlil nasazení IPv6 ;)
- neznámý motiv, ale evidentně někdo dobře znalý českého prostředí
- zastihl nás uprostřed výběrového řízení na nové FW

Zkušenosti

Zkušenosti

- vygenerovat takový útok je velmi levné a snadné

- zásadně nevýhodný je poměr nákladů na útok a opatření proti němu

- potvrzuje se, že je nutné být na tyto situace dobře připraven

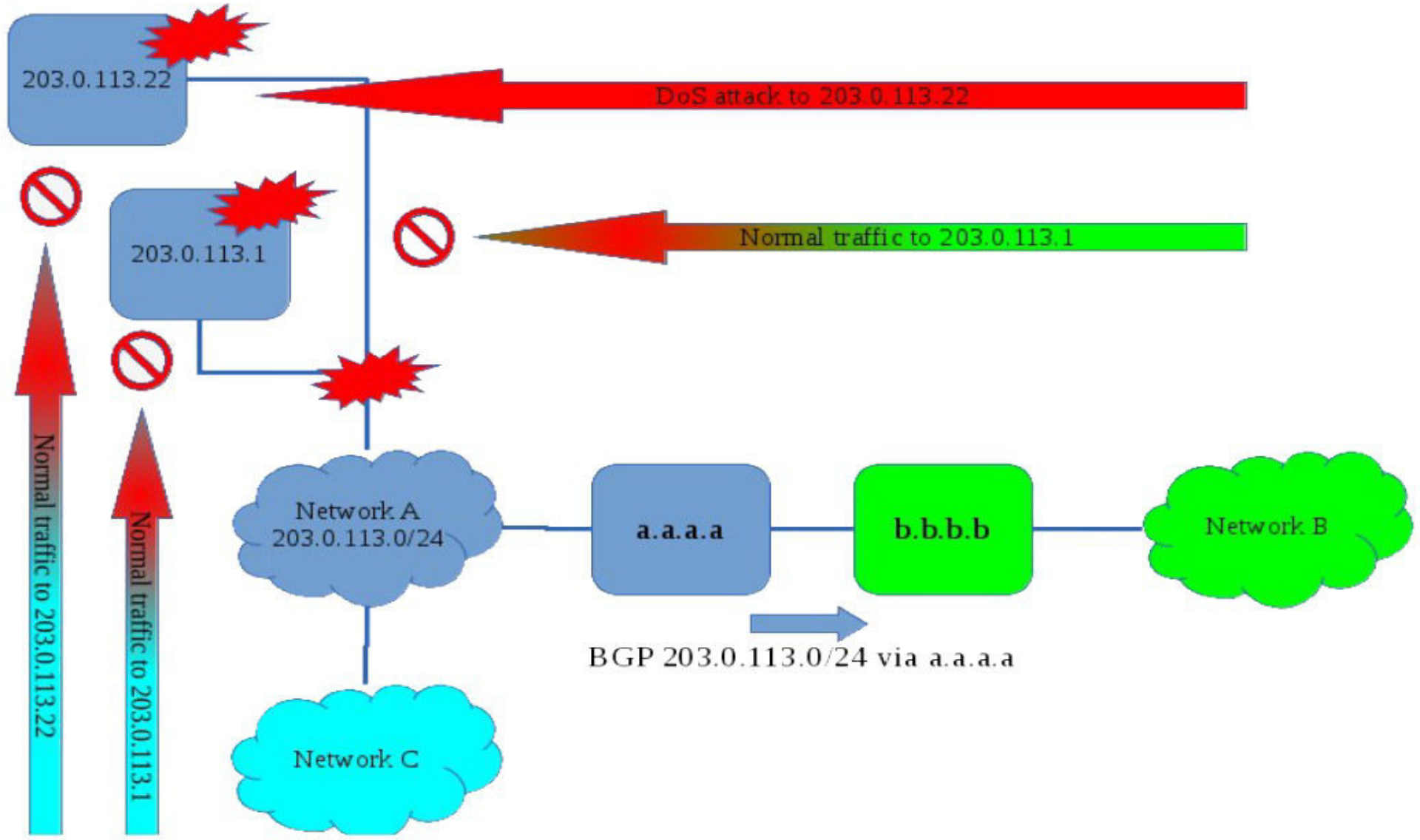
- testování nových FW ve spolupráci s CZ.NIC

- mají několikanásobně vyšší odolnost než byl útok na nás v březnu

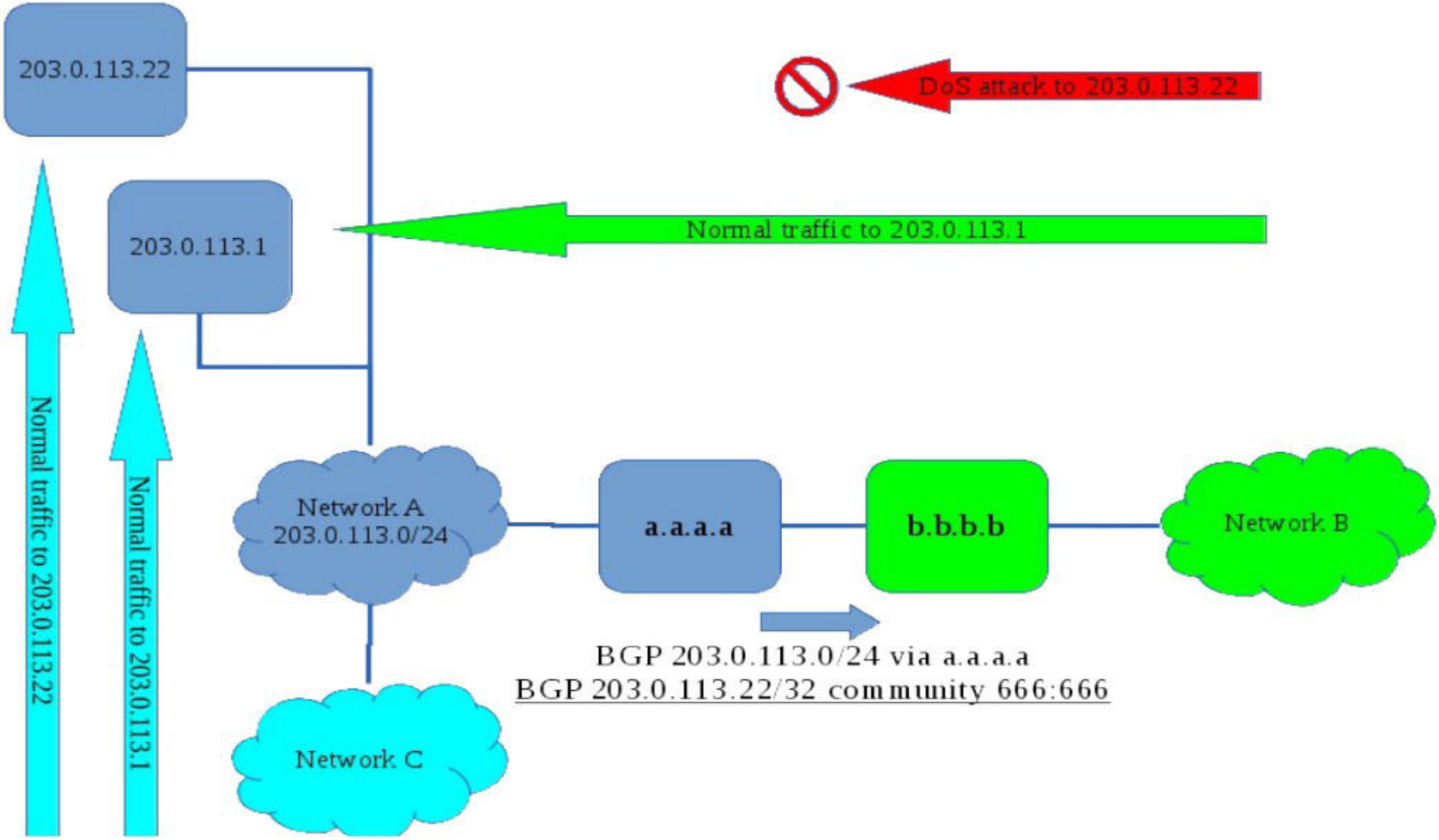
- síla útoku byla očividně přizpůsobována cíli, tedy to rozhodně samo o sobě nedává záruku bezpečí

RTBH – kladivo na (D)DoS

RTBH filtering



RTBH filtering



RTBH – kladivo na (D)DoS

- blokace provozu směřujícího na cíl z vybraných linek (typicky ze zahraničí)

- uvolní zahlcené linky, ale blokuje i regulérní provoz

- velice efektivní u služeb, kdy je cíl i většina jeho regulérních uživatelů propojených ve stejném peering uzlu (např. NIX) a útok přichází ze zahraničí (např. botnet)

- moc nám nepomůže, pokud hostujeme projekt určený z většiny pro zahraniční návštěvníky (pomůže infrastruktuře, ale ne cíli)

- a co když i útok přichází přes stejný peering uzel (NIX)?

Bezpečná VLAN

Bezpečná VLAN

- reakce na proběhlé útoky

- iniciativa vznikla na půdě NIX.CZ

- lepší udělat něco sami, než státní orgán vymyslí nějaký nesmysl

- vše řeší na L2, nezasahuje do L3, kam NIX zasahovat nemá a nechce

- funguje na dobrovolnosti, důvěře a přirozené motivaci, nic nevnucuje

- vyžaduje plnění přísných pravidel

- vytváří oddělený peering subjektů, které se zaváží pravidla plnit

Jaká jsou ta pravidla?

- BCP38
- funkční ochrana proti generování amplifikačních útoků ze své sítě (DNS, NTP, SNMP aj.)
- RFC6192 (protecting the router control plane)
- funkční dohledové středisko v režimu 24/7
- registrovaný CSIRT tým
- monitorovat hraniční a zákaznické linky na anomálie
- smluvně zakazovat svým zákazníkům zneužívání sítě (VOP)
- zahájit práce na odstranění/omezení incidentu nejpozději do 30 minut
- aktivně používat IPv6
- domény podepisovat DNSSECem
- provozovat redundantní, nepřetížené přípojky min. do dvou uzlů NIX
- a další..

Co přináší nového pro český internet

Co přináší nového pro český internet

- RTBH na L2 v rámci NIXu

- možnost ostrovního provozu

- důvěryhodná platforma pro efektivní a rychlou výměnu informací ohledně obrany a prevence proti útokům

- definuje, co by měl dodržovat odpovědný ISP

- zvyšuje rozsah nasazení těchto opatření ve významných sítích v ČR

- zvyšuje povědomí o pravidlech a tím motivuje i ostatní

Kdo je těch šest statečných :)

Kdo je těch šest statečných :)

- ACTIVE 24

- CESNET

- CZ.NIC

- Dial Telecom

- Seznam.cz

- Telefonica O2

- další stojí frontu nebo vyčkávají, jak dopadneme. Je žádoucí mít členů co nejvíce, i z řad našich obchodních konkurentů.

Co obnášela implementace v ACTIVE 24

Co obnášela implementace v ACTIVE 24

- bezpečnosti se věnujeme dlouhodobě, proto jsme drtivou většinu požadavků měli splněnu ještě před vstupem do projektu BV (BCP38, DNSSEC, IPv6, zákaz otevřených resolverů..)

Dodělat zbývalo:

- implementace RRL (měli jsme řešeno inhouse scripty)

- doplnit control plane policy i na IPv6

- znemožnit zneužití našeho veřejného NTP serveru

- ověřit plnění ostatních pravidel

Jaký je aktuální stav

Jaký je aktuální stav

- zakládající členové plní všechna definovaná kritéria

- podepsána zakládající listina se závazky k plnění pravidel

- vytvořena VLAN, přiděleny peering IP rozsahy

- funkční konference členů BV

- samotné navazování odděleného peeringu a implementace RTBH na L2 začíná právě v těchto dnech

- následovat bude ostrý test ostrovního provozu

Co vám přinese vybrat si služby od člena BV

Co vám přinese vybrat si služby od člena BV

- vaše stránky budou ze sítí členů BV dostupné i v případě DoS útoků o intenzitě, jakou ČR ještě nezažila (srovnatelné s r. 2007 v Estonsku)

- obdobně v případě připojení od ISP v BV budete mít funkční přístup minimálně na služby poskytovatelů obsahu v BV

- jistota, že váš provider dělá pro bezpečnost českého internetu podstatně více, než je běžný standard

Děkuji za pozornost

www.active24.cz

www.hosting.cz

www.domeny.cz

www.servery.cz

twitter.com/active24cz