

ACTIVE 24 CSIRT na Cyber Europe 2012



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



4.10.2012 - pracovní den jako každý jiný

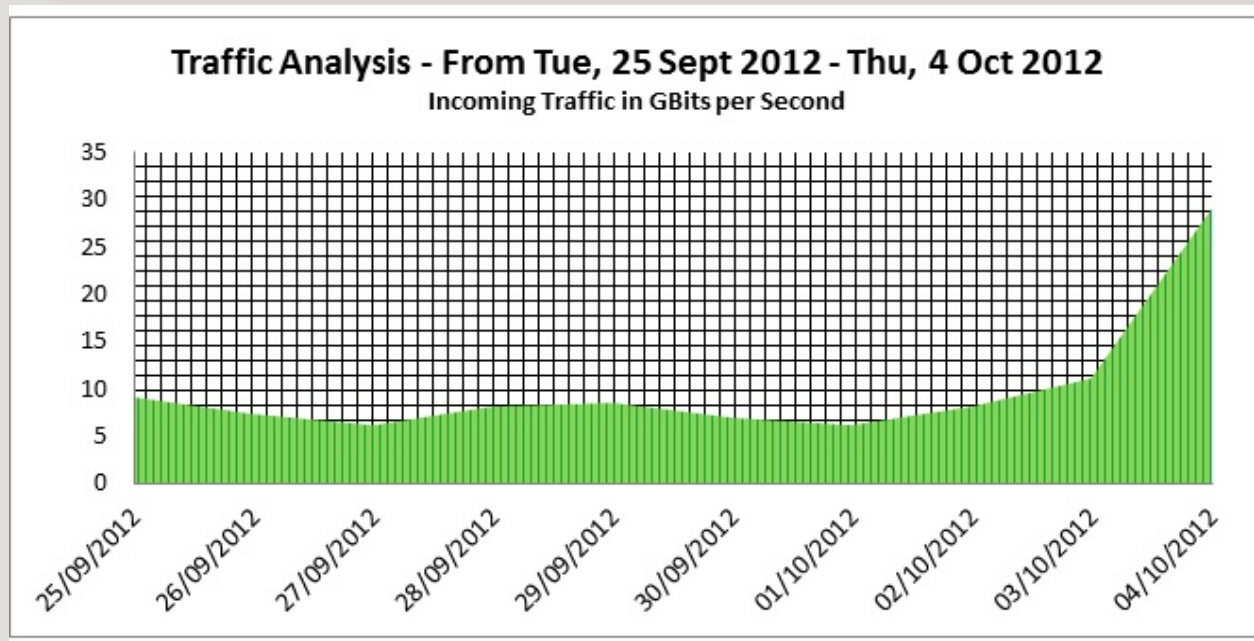


8:00

- přicházím do práce
- uvařím si kávu
- otevřu poštu a koukám do kalendáře, co mě dnes čeká
- začínám řešit každodenní pracovní úkoly

9:08

- náš dohled zjišťuje abnormálně vysoký a stále rostoucí provoz v síti
- směřuje na jednoho konkrétního klienta – Policejní akademii ČR
- možné spojení s útokem, o kterém se šíří informace na Twitteru



9:15 – 9:31

- situace se rychle zhoršuje a začíná ohrožovat naši síť
- o útoku informujeme klienta
- hledáme zdroje útoků a analyzujeme síťový provoz
- prostřednictvím CSIRT.CZ vyrozumíme též hlavní zdroje útoků

9:32

- na pozadí provozních problémů s probíhajícím DDoS náš bezpečnostní tým odhaluje množství napadených webových stránek na našem hostingu
- k napadení je zneužívána chyba v ovládacím panelu třetí strany a weby jsou zneužívány k infikaci PC návštěvníků stránek malwarem
- později se ukáže, že tímto způsobem roste jeden z botnetů, který útočí na další cíle v jiných zemích



10:02 – 10:36

- DDoS útoky dále sílí
- zákazníci si stěžují na nedostupnost služeb
- že se něco děje, už si začínají všímat i média

10:46-12:15

- zjišťujeme řadu podrobností o probíhajících útocích, ale bez spolupráce dalších zahraničních subjektů se je nedaří zastavit – naopak dále sílí
- instituce z nejrůznějších zemí nás informují, že také čelí DDoS útokům, které pocházejí mj. i z naší sítě
- bezpečnostní tým objevuje sofistikovaný kód, který zneužívá SOHO zařízení našich zákazníků k útokům na jiné cíle
- BBC news píše o rozsáhlém kybernetickém útoku, který se šíří napříč Evropou..

Probouzím se ze špatného snu?

Cyber Europe 2012



Cyber Europe 2012

- cvičení obrany proti rozsáhlému koordinovanému kybernetickému útoku směřovanému na klíčové státní i komerční instituce EU

Cíle:

- ověření efektivity různých způsobů komunikace
- ověření možností spolupráce privátního a veřejného sektoru
- hledání možností na zlepšení účinnosti obrany proti reálným hrozbám



Organizace a účastníci cvičení

- ENISA
- National Moderator
- National Monitor

Hráči:

- za ČR: CSIRT.CZ, ACTIVE 24, CESNET, Policejní akademie
- stovky dalších hráčů z 25 zemí Evropy



ACTIVE24-CSIRT

- Computer Security Incident Response team
- <http://www.active24.cz/csirt/>
- první a dosud jediný oficiálně registrovaný CSIRT tým z komerční sféry v ČR
- u Trusted Introducer registrován 9.2.2012 – status Listed
- bez registrace fungoval již řadu let přes abuse@active24.cz
- registrací navázal přímou spolupráci s ostatními týmy v ČR i po celém světě
- z této spolupráce vzešla i účast na cvičení Cyber Europe 2012



Jak cvičení probíhá

- vytvořen oddělený virtuální svět, ve kterém se vše odehrává
- EXERCISE EXERCISE EXERCISE
- žádný útok ve skutečnosti neprobíhá
- důraz na vytvoření realistického prostředí (stres, zahlcení požadavky, Twitter, BBC, blogy, CSD apod.)
- cvičení je řízeno zasíláním tzv. injectů
- cílem je komunikovat s ostatními partnery a vzájemnou spoluprací najít efektivní protiopatření, jak útokům čelit

Poznátky z průběhu

- bylo to připraveno lépe, než jsem čekal
- simulovaný útok se skládal z řady zcela reálných hrozeb, které v menším měřítku v A24 každodenně řešíme
- je dobré si to zažít – psychicky vás to na podobnou situaci připraví
- národní POC používat až jako last resort contact
- v případě krizí se na řešení musí podílet odpovídající počet osob
- používat selský rozum, nebojovat se scénářem



Poznátky z průběhu

- filtrovat ze záplavy podnětů to, co je důležité
- je potřeba být připraven používat různé způsoby komunikace a vědět, kde hledat kontakty
- komunikaci pomáhá, když osobně znáte partnery z ostatních institucí, se kterými musíte spolupracovat
- je potřeba se více přiblížit realitě pokud jde o interní pravidla a zvyklosti v různých organizacích (sdělování informací, odpojování..)
- reálný DoS na závěr :-)



Závěr

- pro pořádný efekt je potřeba výrazně větší zastoupení veřejného i privátního sektoru
- CSIRT týmů je v ČR stále velmi málo – zakládejte je, má to smysl
- cvičení je potřeba opakovat a připravovat na různé typy hrozeb, podobně jako cvičí bezpečnostní složky státu (hasiči, policie..)
- účast na cvičení vás obohatí o nové zkušenosti a v případě reálné hrozby už budete chladněji reagovat s využitím naučených postupů
- v A24 používáme takto nabyté zkušenosti i k preventivnímu posilování bezpečnosti služeb, které nabízíme

