CESNET

NERD

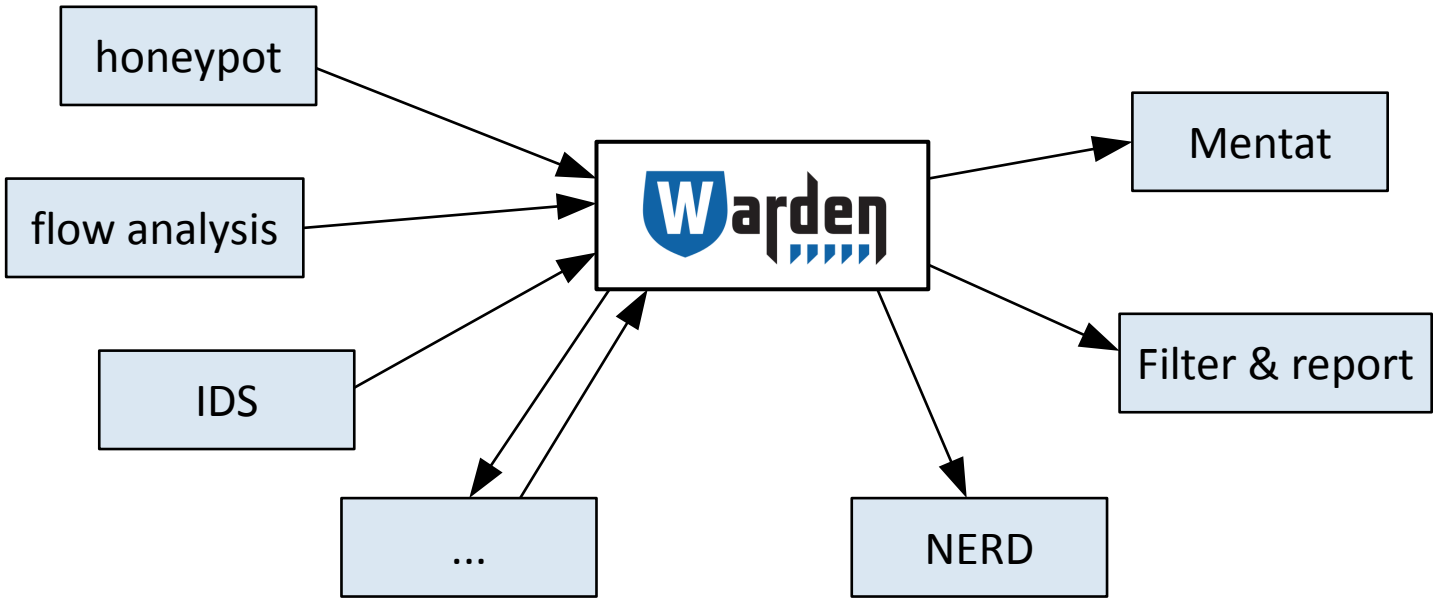
NETWORK ENTITY REPUTATION DATABASE

Václav Bartoš, Martin Žádník

Schůze partnerů SABU
20. 6. 2016

Warden

- Warden – systém pro sdílení informací o bezpečnostích událostech
  - Detektory u nás i v jiných organizací v síti CESNET2, externí zdroje
  - Vyvinuto a provozováno CESNETem (odd. 709)



Warden – data

- Warden – **obrovské množství dat** (>1 mil. hlášení denně)
  - A snažíme se získávat další zdroje
- V současnosti využité **pouze** pro **reporting**
  - Zdrojová adresa uvnitř sítě CESNET2 (nebo partnerské organizace) → email report
  - Pokud je zdroj jinde, **zprávy jsou nevyužité**
- Mnoho dat → lze vydolovat užitečné informace
  - Obecné charakteristiky škodlivého provozu
  - Jaké typy útoků jsou nejčastější?
  - Odkud útoky nejčastěji přichází?
  - Jak jsou vybírány cíle?
  - Jaké bezpečnostní hrozby můžeme v nejbližší době očekávat?

➔ Analýza dat z Wardenu:

  - Technická zpráva CESNET 1/2016, „Analysis of alerts reported to Warden“.

Analýza dat z Wardenu – výsledky

- Klíčová zjištění:

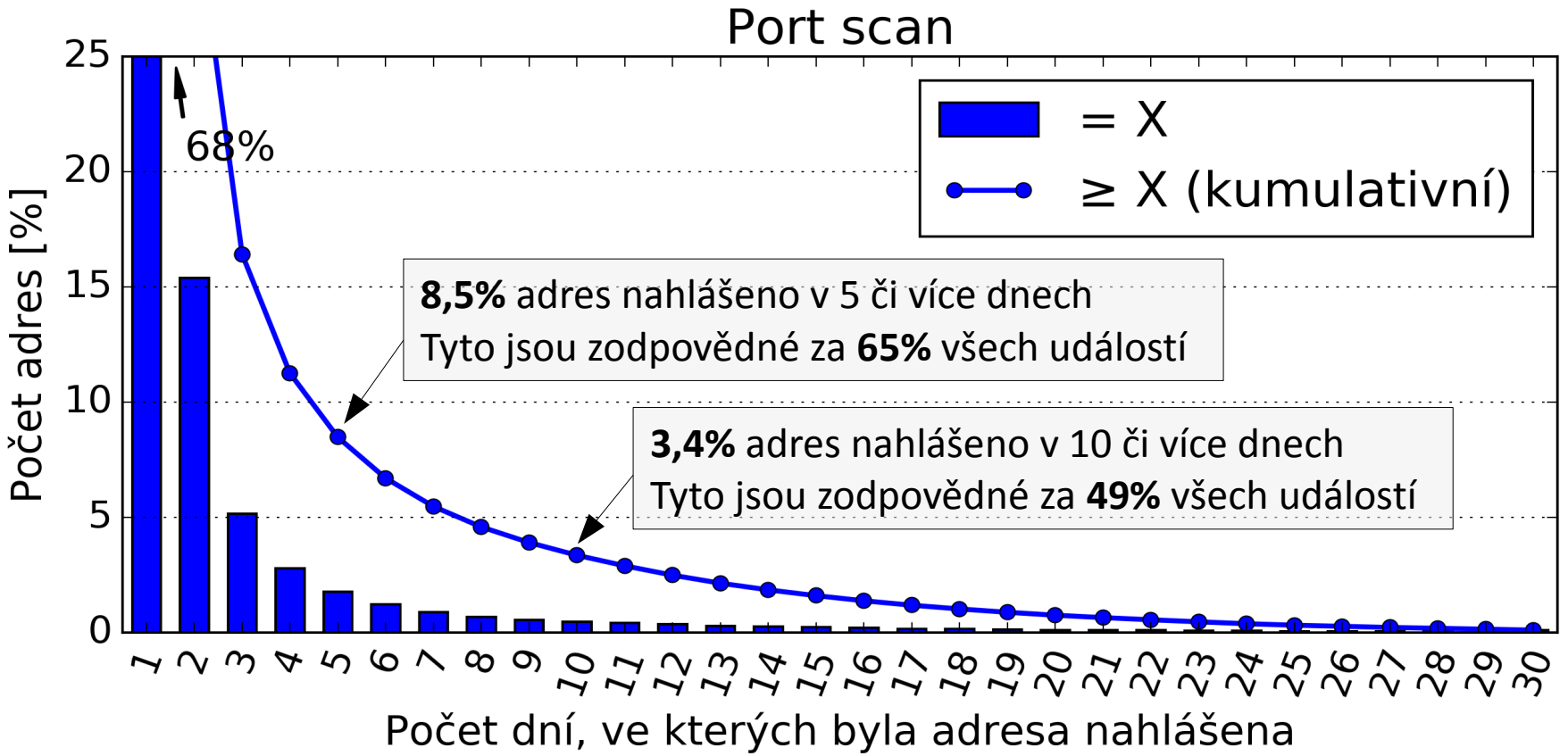
1) Velká část IP adres se objevuje opakovaně.
    - Některé velmi často a dlouhodobě.

2) Některé sítě (AS) a země produkují mnohem více škodlivého provozu než jiné.

3) Je možné předpovídat, jaké zdroje budou v blízké době znovu útočit.
    - Na základě historie detekovaných útoků
    - Příslušnosti do sítě, země a dalších informací

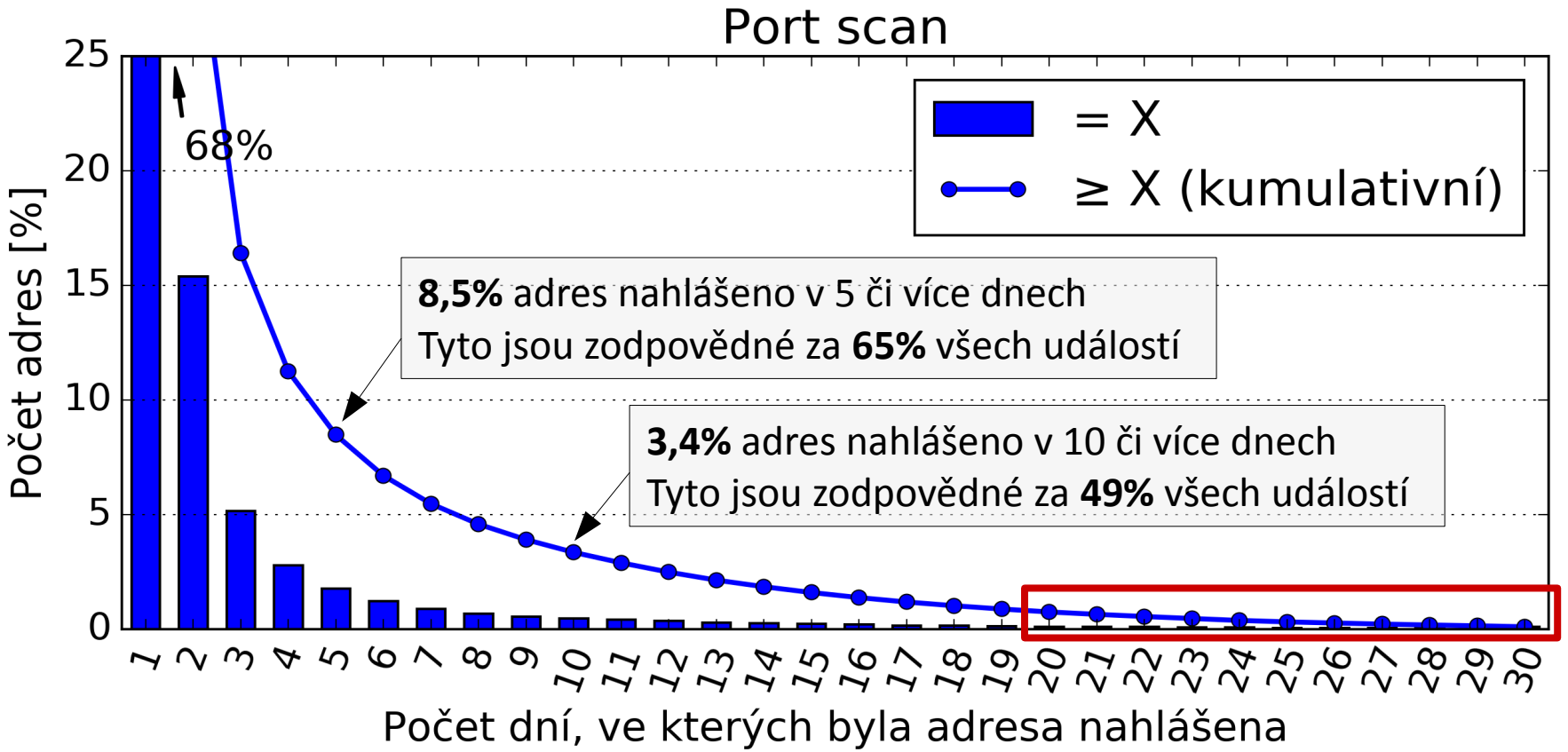
Analýza dat z Wardenu – výsledky

1) Velká část IP adres se objevuje opakovaně.
   - Některé velmi často a dlouhodobě.



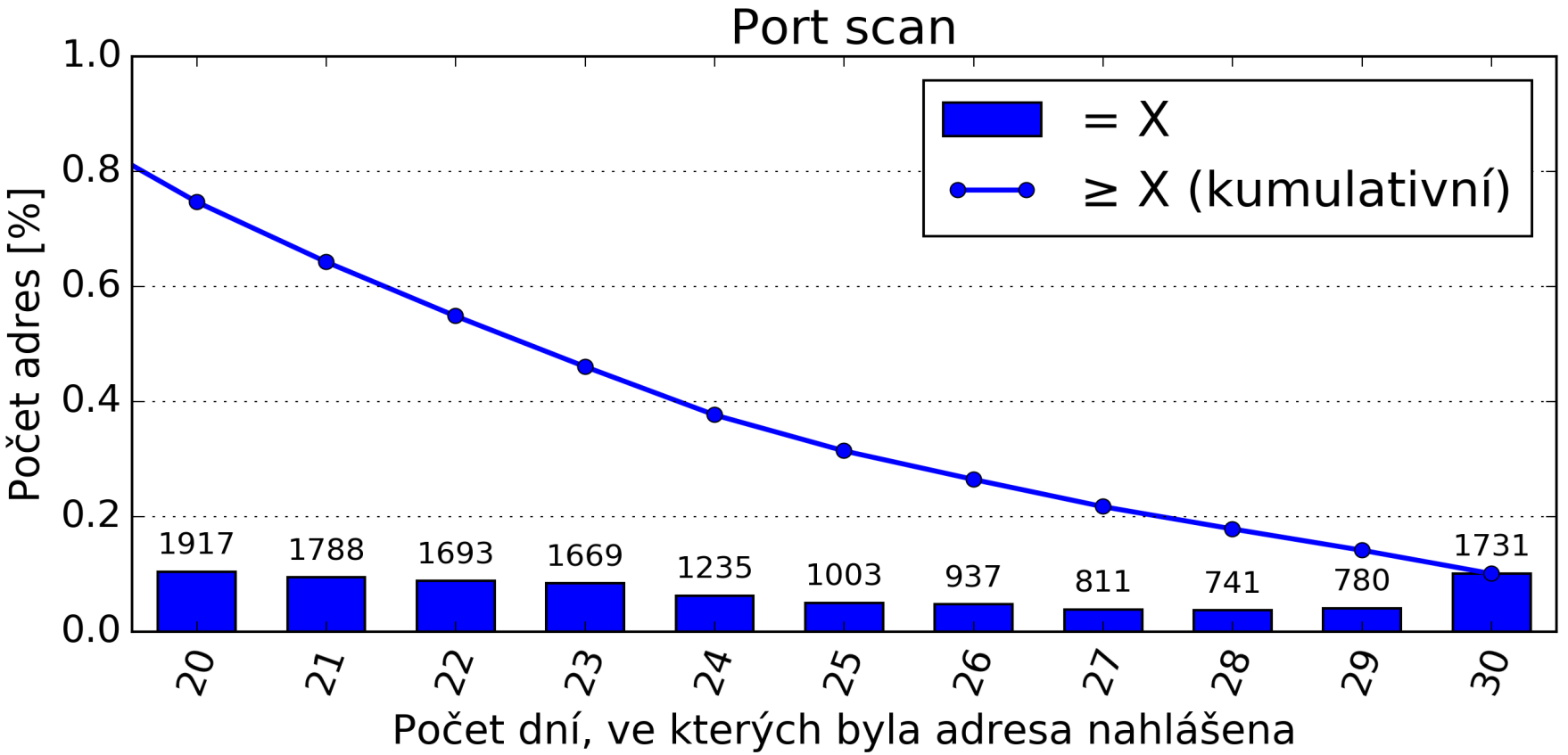
Analýza dat z Wardenu – výsledky

1) Velká část IP adres se objevuje opakovaně.
   - Některé velmi často a dlouhodobě.



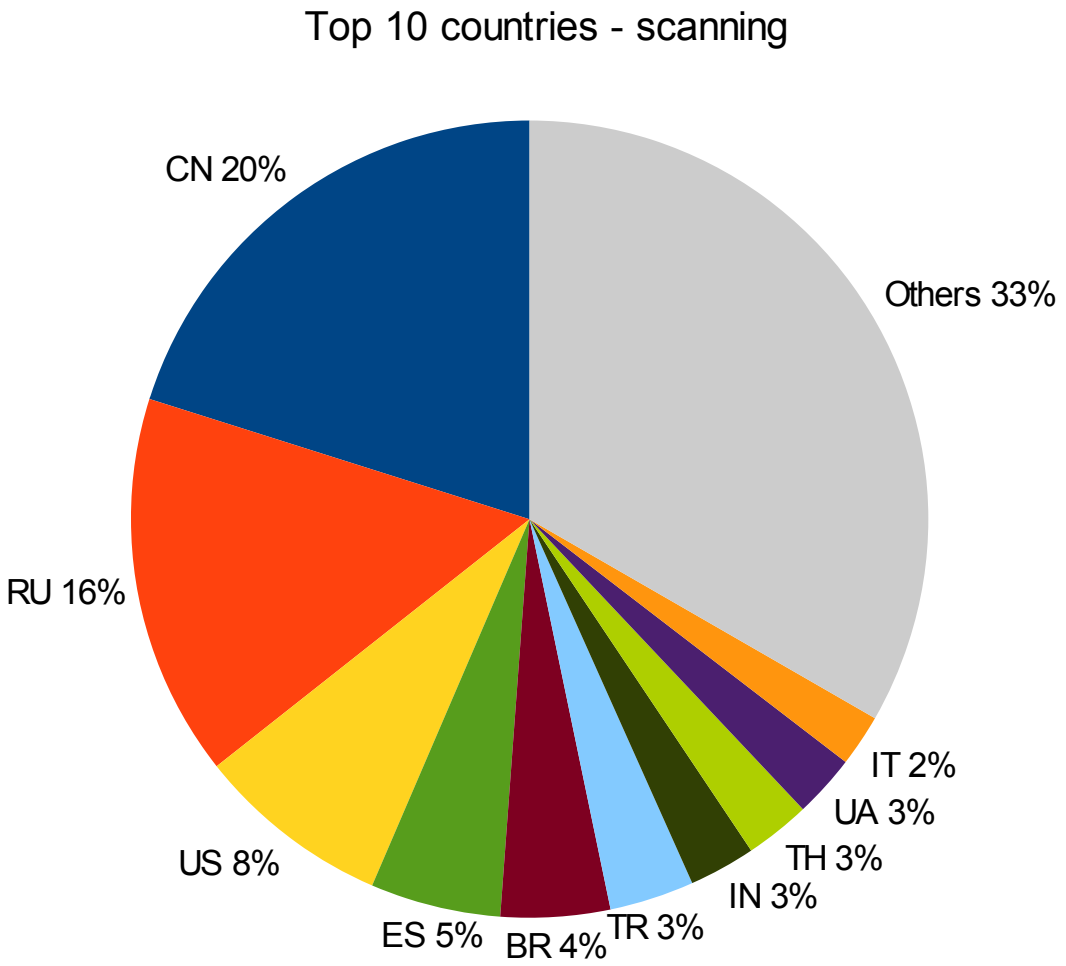
Analýza dat z Wardenu – výsledky

1) Velká část IP adres se objevuje opakovaně.
   - Některé velmi často a dlouhodobě.



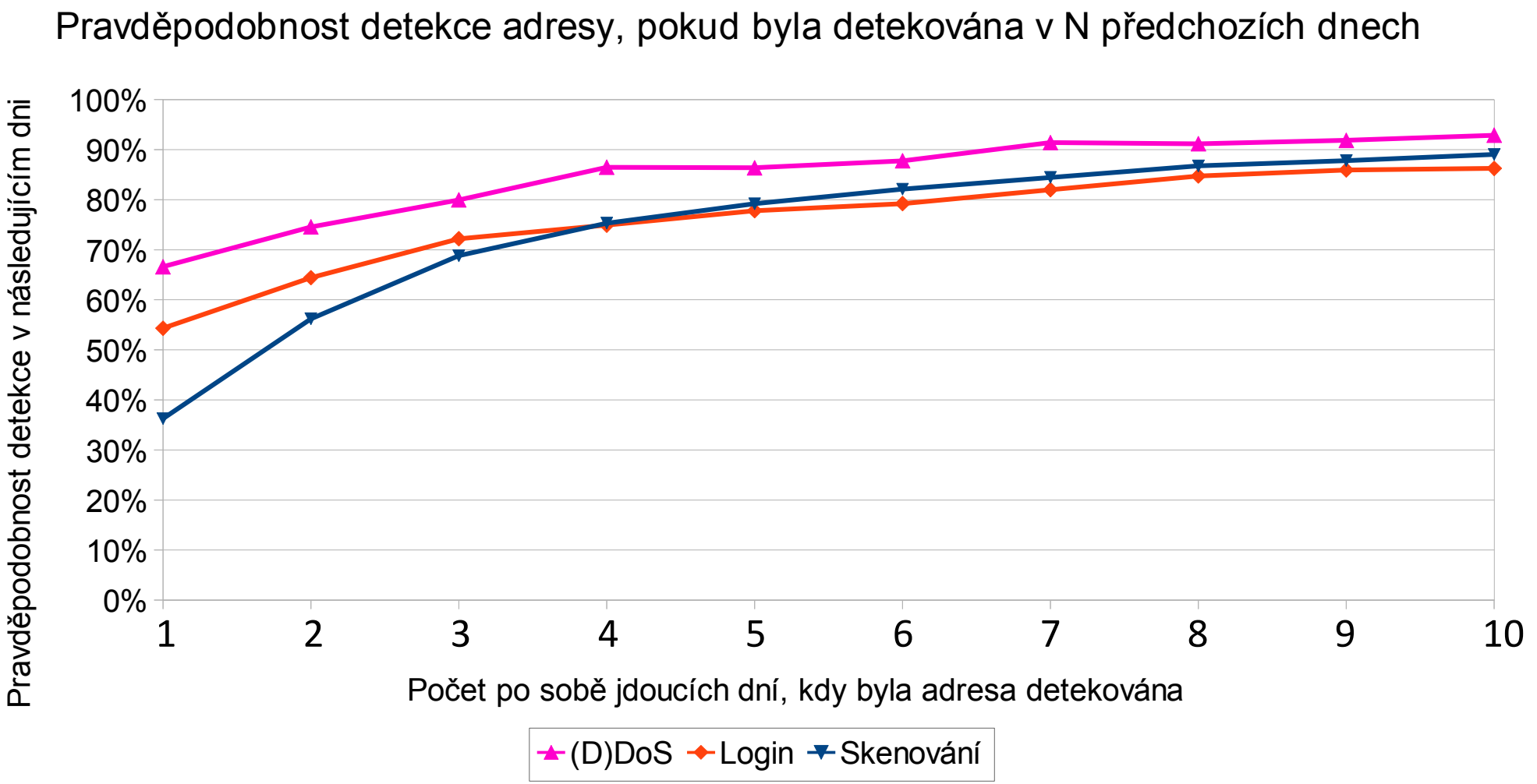
Analýza dat z Wardenu – výsledky

2) Některé sítě (AS) a země produkují mnohem více škodlivého provozu než jiné.



Analýza dat z Wardenu – výsledky

3) Je možné předpovídat, jaké zdroje budou v blízké době znovu útočit.
   - Na základě historie detekovaných útoků
   - (Příslušnosti do sítě, země a dalších informací)



Reputační databáze

- Databáze ***síťových entit*** (**IP adresy**, sítě, domény, …)
  - Seznam známých zdrojů škodlivých aktivit na internetu a všeho, co o nich víme

- Hlavní cíle:
  - Přijímat hlášení o bezpečnostních událostech z Wardenu
    (příp. i z jiných obdobných systémů)
    - Agregace podle zdrojové adresy
  - Obohacení o další data z externích zdorjů
    - Hostname, ASN, geolokace, …
    - Přítomnost na blacklistech
    - …
  - Shrnutí všech informací do „reputation score“
    - „jak velkou hrozbu entita představuje“
      - Formálně: pravděpodobnost, že bude adresa v blízké době útočit, kombinovaná se závažností předpokládaného útoku

Reputační databáze – použití

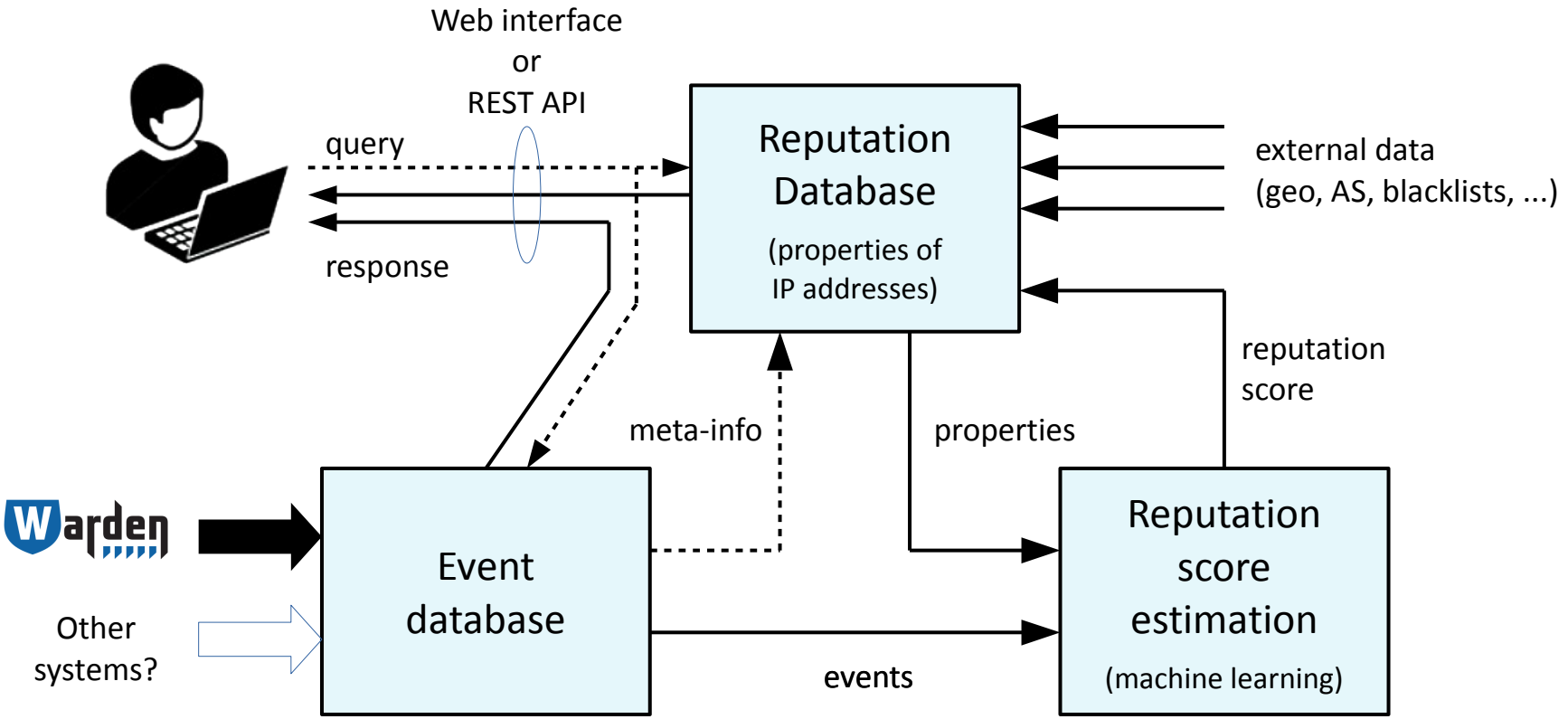
- Způsoby použití:
  - „Vrať mi vše, co víš o této IP adrese“
  - Informace o seznamu adres (entit)
  - Vyhledávání entit podle zadaných kritérií
  - Statistiky

- K čemu to bude dobré?
  - Incident handling / vyšetřování
  - Block listy pro firewally
    - Např. mitigace DDoS (blokování adres se špatnou reputací)
    - Blokování SSH spojení od známých SSH útočníků
  - Bezpečnostní výzkum
  - Vizualizace, „marketing“, PR
    - Statistiky, grafy, ...
  - Uživatelé určitě přijdou s dalšími způsoby použití ...

Reputační databáze – uživatelé

- Uživatelé:
  - Lidé – CSIRT týmy, administrátoři sítí, výzkumníci
    - Web interface
    - *Plugin pro browsery – pop-up okénko pro každou IP adresu na stránce*
  - Jiné systémy
    - HTTP-based API
- Kdo bude mít přístup k datům:
  - Přispěvatelé posílající data do Wardenu
  - CSIRT týmy
  - Ve velmi omezené podobě i veřejně
    - Pouze informace z veřejných zdrojů + celkové shrnutí (reputace)
    - Limity na množství dotazů
- Uživatelské účty, skupiny
  - Přístup k určitým položkám omezen na určité skupiny

NERD – Architektura



NERD – reputační databáze

- Dokumentová NoSQL databáze
  - JSON dokument pro každou IP adresu (entitu)
- Záznam o IP adrese:
  - Časové známky (vytvoření záznamu, poslední úprava)
  - Meta informace o událostech
  - Atributy:
    - Hostname (rev. DNS)
    - Geolokace
    - ASN
    - Abuse kontakt
    - Seznam blacklistů, na kterých je adresa přítomna
    - Amplifikátor (Open DNS, NTP, SNMP)
    - TOR exit node
    - VirusTotal
    - Informace ze Shodanu (otevřené porty)
    - ...
  - Odvozené atributy:
    - Statická/dynamická adresa
    - Typ zařízení
    - …
  - Reputation score (možná více než jedna hodnota)
  - Ručně přidané poznámky

Mnoho z těchto atributů s historií či mírou pravděpodobnosti

NERD – ukázka

https://nerd.cesnet.cz/nerd/ips/

List of IPs | IP detail

Known IP addresses

IP prefix & Country code

Sort by Events Ascending

Max number of addresses 20

Odeslat dotaz

IP address	Hostname	ASN	Country	Events	Time added	Last update
149.56.149.51	ip51.ip-149-56-149.net		US	8363	2016-06-03 13:17:57	2016-06-06 15:15:55
71.6.135.131	census7.shodan.io		US	3239	2016-05-30 16:12:52	2016-06-07 13:23:29
169.228.66.91	researchscanner0.sysnet.ucsd.edu		US	2690	2016-06-03 12:40:03	2016-06-07 13:22:55
169.229.3.91	researchscan1.EECS.Berkeley.EDU		US	2513	2016-06-03 12:30:38	2016-06-07 13:22:45
185.110.132.201	--		RU	1811	2016-06-06 15:16:10	2016-06-07 13:22:26
37.49.225.61	--		NL	1571	2016-06-03 12:29:32	2016-06-06 15:29:04
217.174.249.91	server217-174-249-91.live-servers.net		GB	1135	2016-06-03 12:39:32	2016-06-06 15:21:40
141.212.122.81	researchscan336.eecs.umich.edu		US	1021	2016-05-30 16:15:39	2016-06-06 15:29:29
67.50.80.11	mail.clicweb.org		US	1020	2016-06-03 12:40:21	2016-06-03 12:40:29
185.141.24.61	weinee1.com		RO	797	2016-06-06 15:20:27	2016-06-06 15:28:45
178.238.230.81	m1481.contabo.host		DE	785	2016-06-06 15:19:22	2016-06-06 15:28:42
139.196.66.151	--		CN	528	2016-06-03 12:28:55	2016-06-06 15:28:58
45.34.191.181	--		US	514	2016-06-03 13:13:49	2016-06-03 13:16:14
205.204.100.1	--		US	464	2016-06-03 12:29:01	2016-06-06 15:28:59
47.88.134.11	--		CA	443	2016-06-03 12:28:53	2016-06-06 15:28:57
141.212.122.111	researchscan366.eecs.umich.edu		US	407	2016-05-30 16:15:15	2016-06-07 13:22:27
141.212.122.101	researchscan356.eecs.umich.edu		US	406	2016-05-30 16:15:15	2016-06-06 15:29:29
141.212.122.91	researchscan346.eecs.umich.edu		US	401	2016-05-30 16:15:40	2016-06-06 15:29:29
139.196.134.1	--		CN	391	2016-06-03 12:28:57	2016-06-06 15:28:58
61.151.214.71	71.214.151.61.dial.xw.sh.dynamic.163data.com.cn		CN	355	2016-05-30 16:15:36	2016-06-06 15:29:28

Děkuji za pozornost