Václav Bartoš

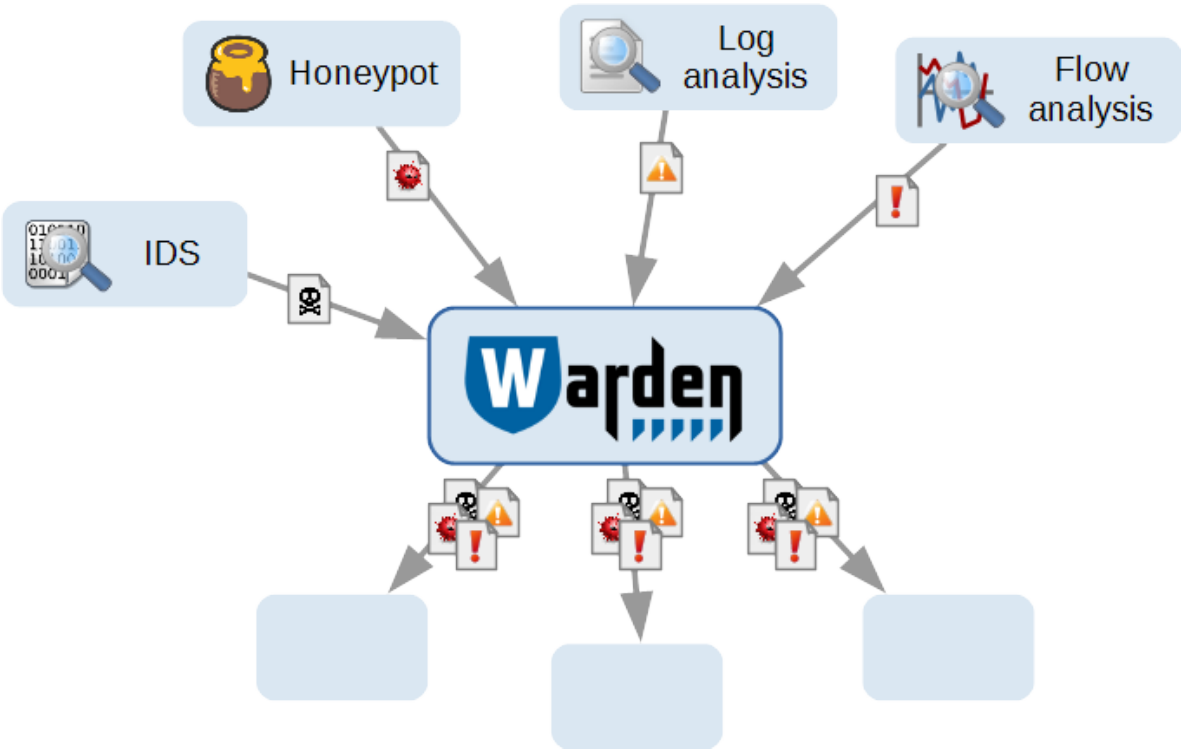
Meeting projektu SABU
12. 10. 2016, Vranovská ves

Osnova

1) Co je (má být) reputační databáze
2) Jak to funguje
3) Aktuální stav
    a) Ukázka
    b) Co je hotovo
    c) Co zbývá dodělat
4) Výpočty reputačního skóre

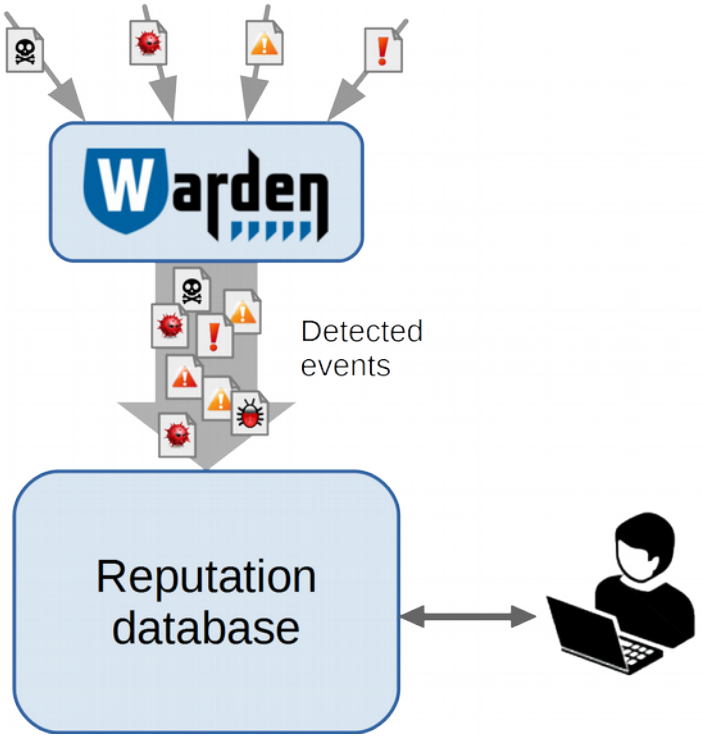
Detekce útoků a zpracování alertů

- V síti CESNET2 je mnoho detektorů škodlivého provozu
  - NEMEA, FTAS, různé honeypoty, …
- Sdílení přes Warden
  - Zapojování dalších organizací
  - cca 2 mil. hlášení denně
- Zpracování – Mentat
  - uložení
  - reportování incidentů, jejichž zdroj je uvnitř CENSET2 (a několika partnerských sítí)
  - zbytek nevyužit



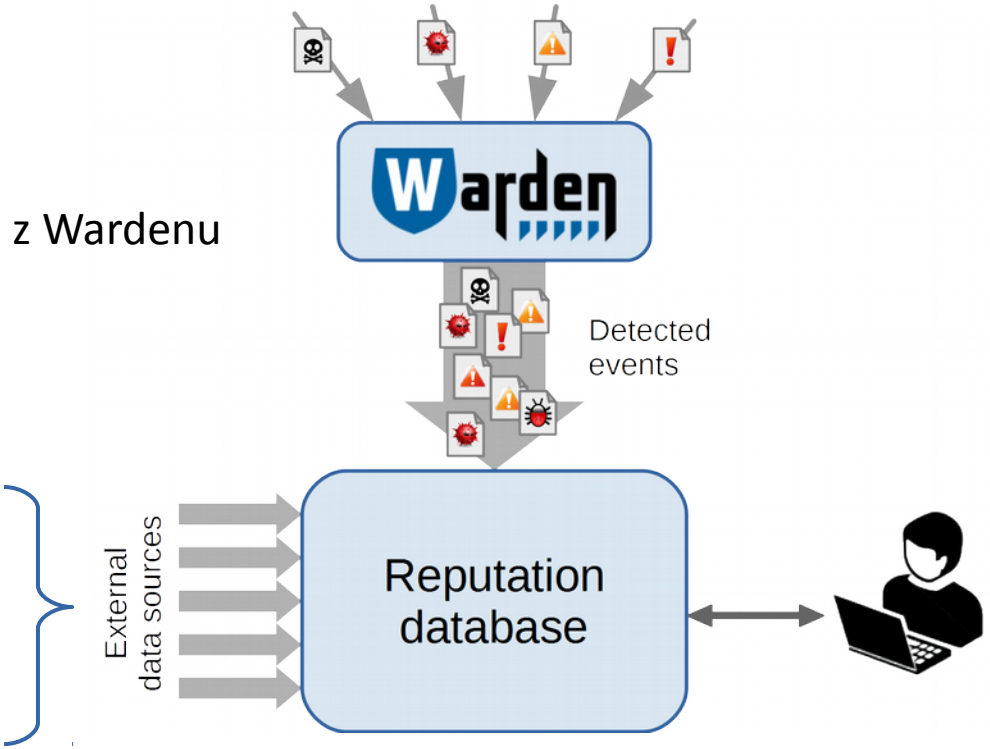
Reputační databáze

- 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



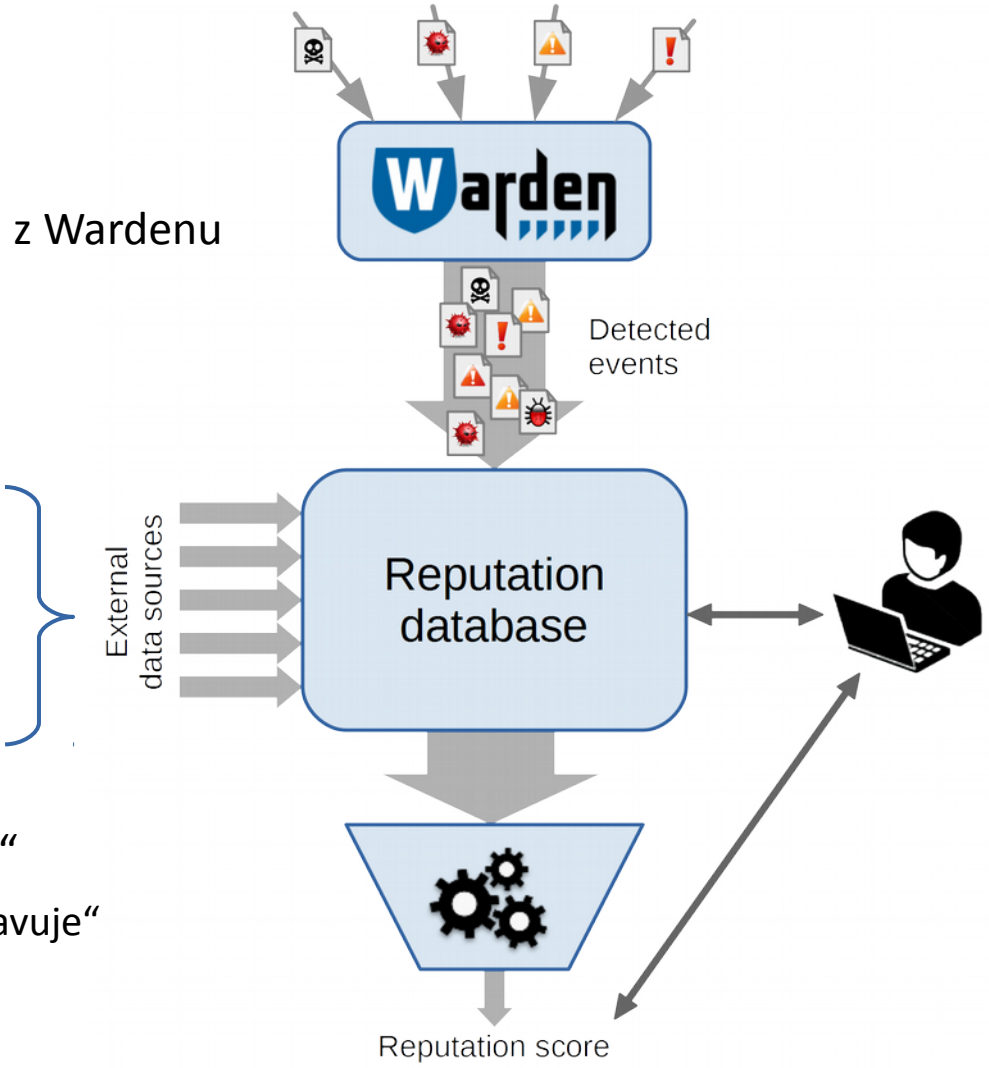
Reputační databáze

- 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
    - Open[DNS,NTP,…] resolvers
    - TOR exit nodes
    - …

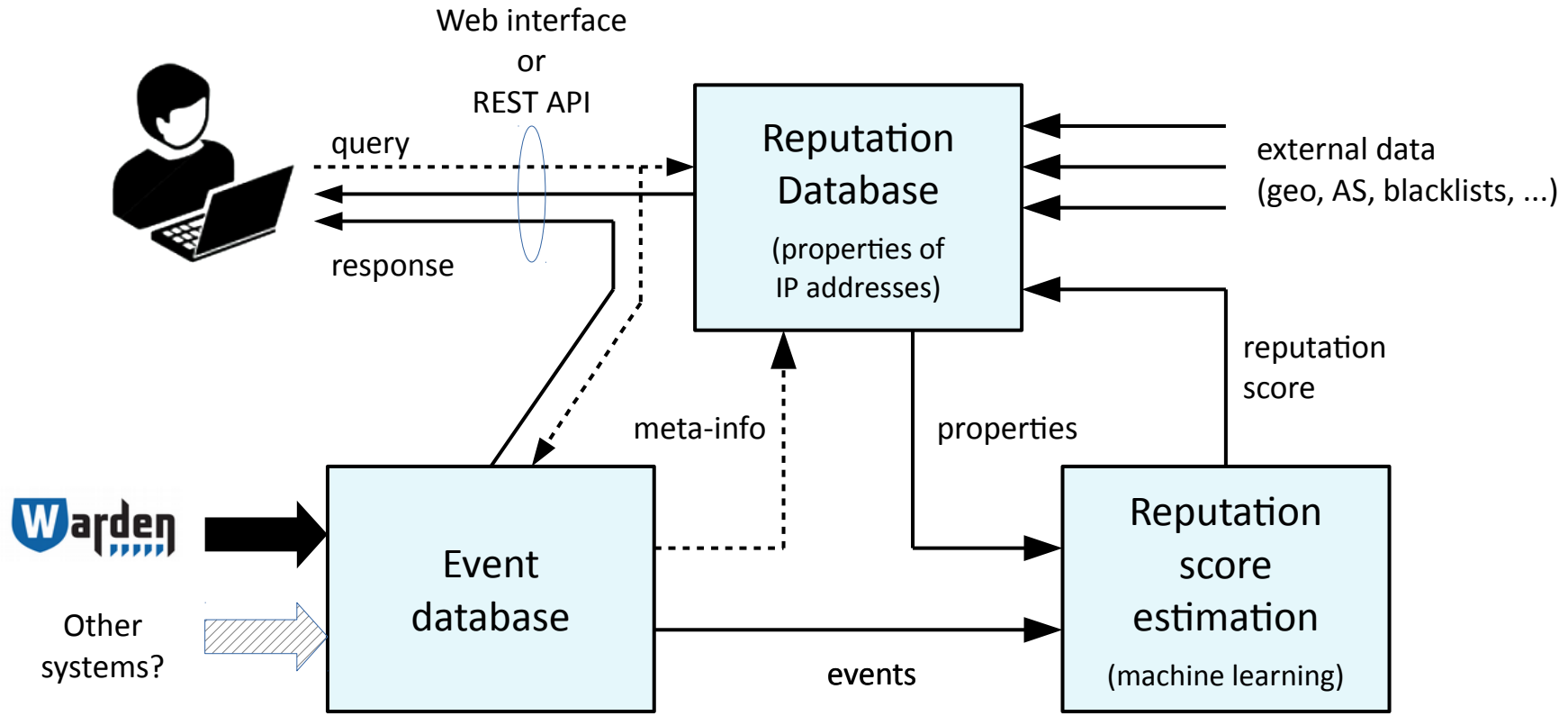


Reputační databáze

- 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
    - Open[DNS,NTP,…] resolvers
    - TOR exit nodes
    - …
  - Shrnutí všech informací do „reputation score“
    - Ohodnocení „jak velkou hrozbu entita představuje“



NERD – Logická architektura

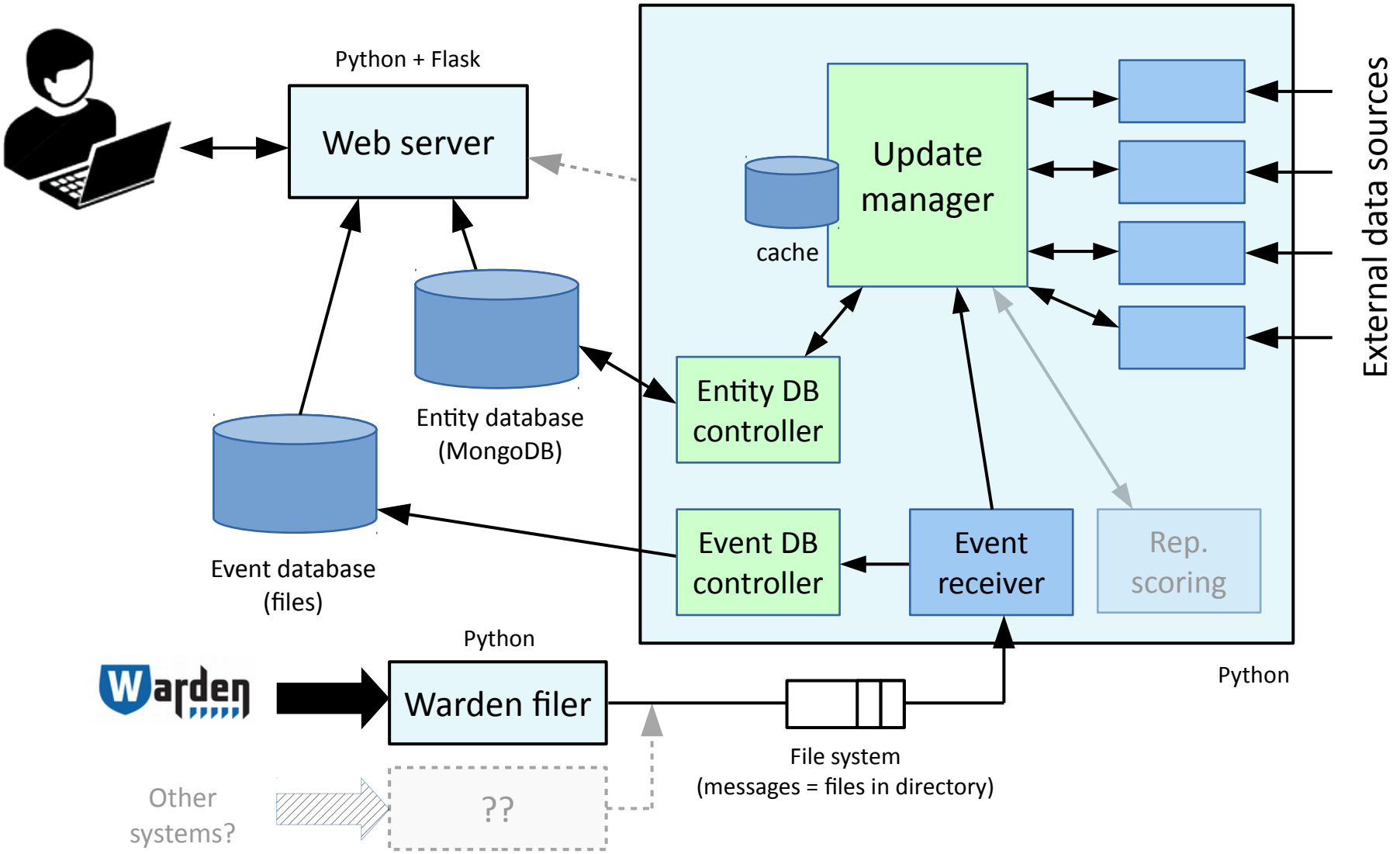


Implementace

- Backend – Python daemon
- Modulární architektura
  - O každou vlastnot se stará určitý modul
  - Snadná rozšiřitelnost

- Frontend – Web-based
  - Python + Flask
  - HTML5, CSS, JavaScript + jQuery, ...

Architektura (implementace)



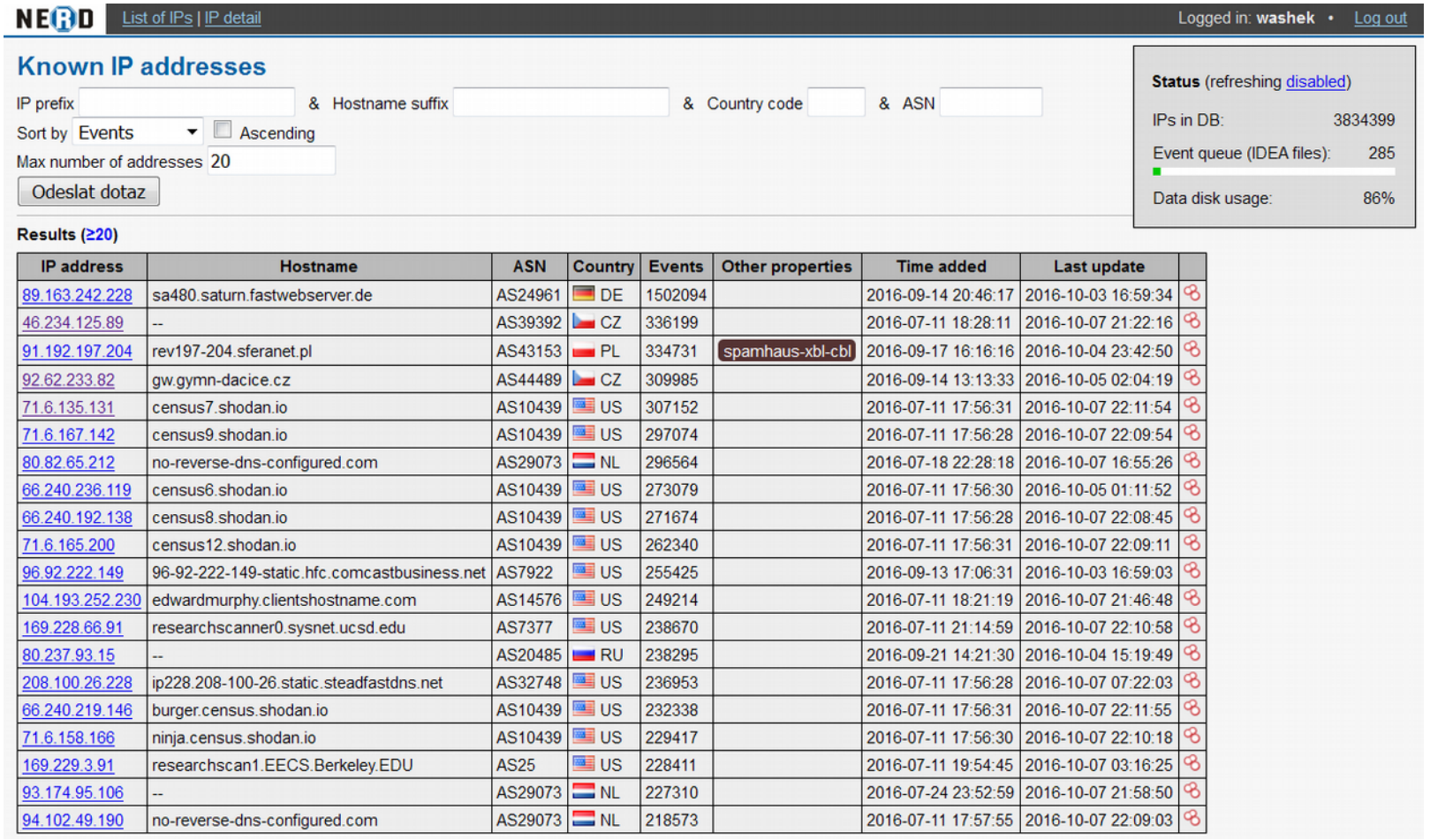
Aktuální stav

- Co je hotovo:
  - Databáze běží a sbírá data (od července)
  - Moduly pro:
    - Příjem dat z Wardenu a ukládání událostí
    - DNS (hostname)
    - ASN
    - Geolokace
    - Blacklisty – DNSBL i lokálně stahované, mj. i TOR
    - Shodan (připraveno, zatím nespuštěno)
  - Frontend
    - Zobrazení dat
    - Vyhledávání podle většiny položek
    - Login přes lokální účet nebo eduID/eduGAIN

Web frontend

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

Login/heslo: **sabu/sabu**



IP address	Hostname	ASN	Country	Events	Other properties	Time added	Last update	
89.163.242.228	sa480.saturn.fastwebserver.de	AS24961	DE	1502094		2016-09-14 20:46:17	2016-10-03 16:59:34	
46.234.125.89	--	AS39392	CZ	336199		2016-07-11 18:28:11	2016-10-07 21:22:16	
91.192.197.204	rev197-204.sferanet.pl	AS43153	PL	334731	spamhaus-xbl-cbl	2016-09-17 16:16:16	2016-10-04 23:42:50	
92.62.233.82	gw.gymn-dacice.cz	AS44489	CZ	309985		2016-09-14 13:13:33	2016-10-05 02:04:19	
71.6.135.131	census7.shodan.io	AS10439	US	307152		2016-07-11 17:56:31	2016-10-07 22:11:54	
71.6.167.142	census9.shodan.io	AS10439	US	297074		2016-07-11 17:56:28	2016-10-07 22:09:54	
80.82.65.212	no-reverse-dns-configured.com	AS29073	NL	296564		2016-07-18 22:28:18	2016-10-07 16:55:26	
66.240.236.119	census6.shodan.io	AS10439	US	273079		2016-07-11 17:56:30	2016-10-05 01:11:52	
66.240.192.138	census8.shodan.io	AS10439	US	271674		2016-07-11 17:56:28	2016-10-07 22:08:45	
71.6.165.200	census12.shodan.io	AS10439	US	262340		2016-07-11 17:56:31	2016-10-07 22:09:11	
96.92.222.149	96-92-222-149-static.hfc.comcastbusiness.net	AS7922	US	255425		2016-09-13 17:06:31	2016-10-03 16:59:03	
104.193.252.230	edwardmurphy.clientshostname.com	AS14576	US	249214		2016-07-11 18:21:19	2016-10-07 21:46:48	
169.228.66.91	researchscanner0.sysnet.ucsd.edu	AS7377	US	238670		2016-07-11 21:14:59	2016-10-07 22:10:58	
80.237.93.15	--	AS20485	RU	238295		2016-09-21 14:21:30	2016-10-04 15:19:49	
208.100.26.228	ip228.208-100-26.static.steadfastdns.net	AS32748	US	236953		2016-07-11 17:56:28	2016-10-07 07:22:03	
66.240.219.146	burger.census.shodan.io	AS10439	US	232338		2016-07-11 17:56:31	2016-10-07 22:11:55	
71.6.158.166	ninja.census.shodan.io	AS10439	US	229417		2016-07-11 17:56:30	2016-10-07 22:10:18	
169.229.3.91	researchscan1.EECS.Berkeley.EDU	AS25	US	228411		2016-07-11 19:54:45	2016-10-07 03:16:25	
93.174.95.106	--	AS29073	NL	227310		2016-07-24 23:52:59	2016-10-07 21:58:50	
94.102.49.190	no-reverse-dns-configured.com	AS29073	NL	218573		2016-07-11 17:57:55	2016-10-07 22:09:03	

Zbývá dodělat

- Frontend:
  - Přehlednější detail IP adresy
    - Včetně časové osy událostí, grafů, vyhledávání v událostech
  - Spousta drobných dodělávek
  - Veřejná verze (jak data anonymizovat a přitom stále poskytovat zajímavé informace?)
- Backend:
  - Další zdroje:
    - Další blacklisty (ne vždy lze snadno stáhnout, potřeba speciálně vyjednat přístup) - kromě spam např. Dial-up prefixy, OpenDNS/NTP
    - Jiné „reputační databáze“
    - Jiné zdroje událostí než Warden (DShield, MISP, AlienVault OTX, …?)
  - Agregace zpráv (nejlépe kdyby se dělala jinde než v NERD)
  - Přechod z MongoDB na PostgreSQL (nebo něco jiného?)
  - Updaty (blacklisty, hostname)
  - Vylepšit odmazávání starých dat
- Podpora jiných entit než IP adres (ASN, domény, země, prefixy)
- Whitelisty
- **API**
- **Výpočet reputation score**

Výpočet reputačního skóre

- Reputační skóre
  - Shrnuje všechny informace v DB
  - Hodnota vyjadřující, jak moc je IP adresa „nebezpečná“.
    - Nemusí být nutně jen jedno číslo
    - „Nebezpečnost“ v určitém kontextu, např. vzheldem k určitému typu útoku.

- Formální definice:
  - **Pravděpodobnost**, že daná entita (IP adresa) bude **v blízké budoucnosti** (např. příštích 24h) vykazovat **škodlivou činnost**, *kombinovaná s mírou závažnosti této činnosti.*

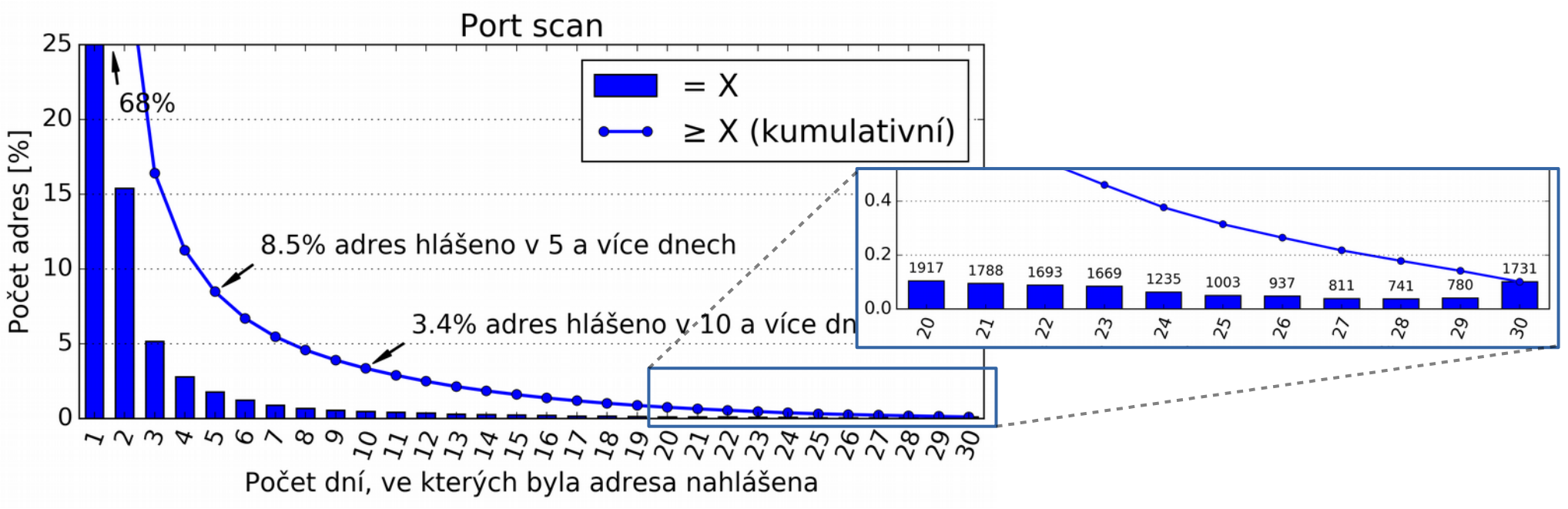
(a ta bude detekována)

→ Předvídání útoků

Je to vůbec možné?

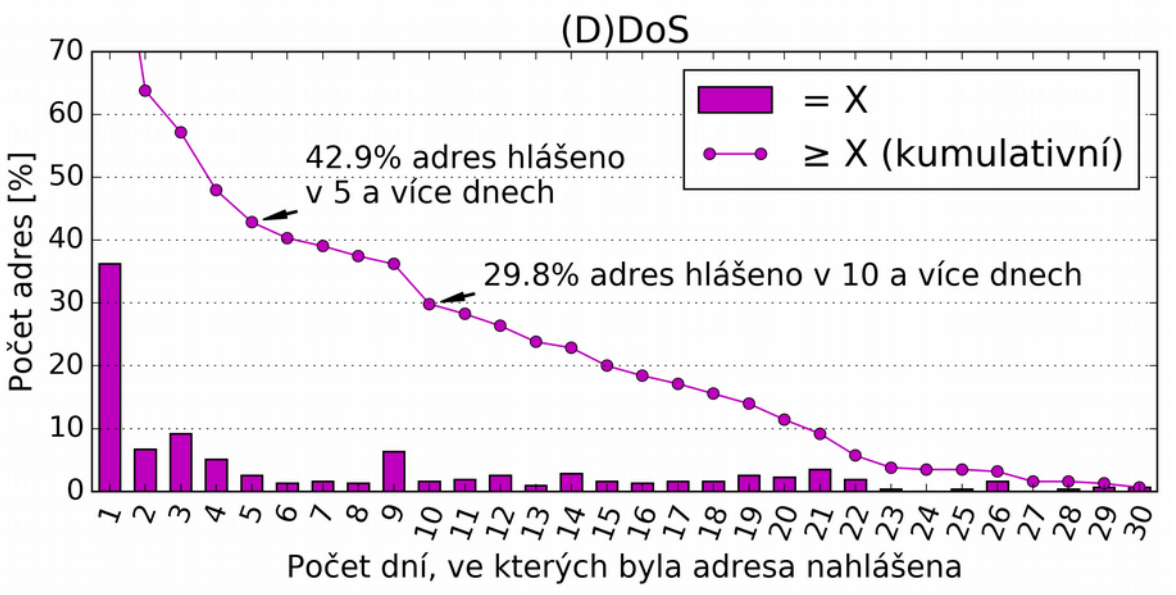
Predikce útoků

- Analýza dat ze systému Warden.
  - 70 mil. hlášení from ze dvou měsíců (dva měsíční vzorky z r. 2015).
- 68% IP adres je detekováno jen v jednom dni z měsíce.
  - Ale 8.5% je nahlášeno v 5 a více dnech.
    - Tyto jsou zodpovědné za 65% všech hlášení.
  - Tisíce adres jsou detekovány (téměř) každý den.

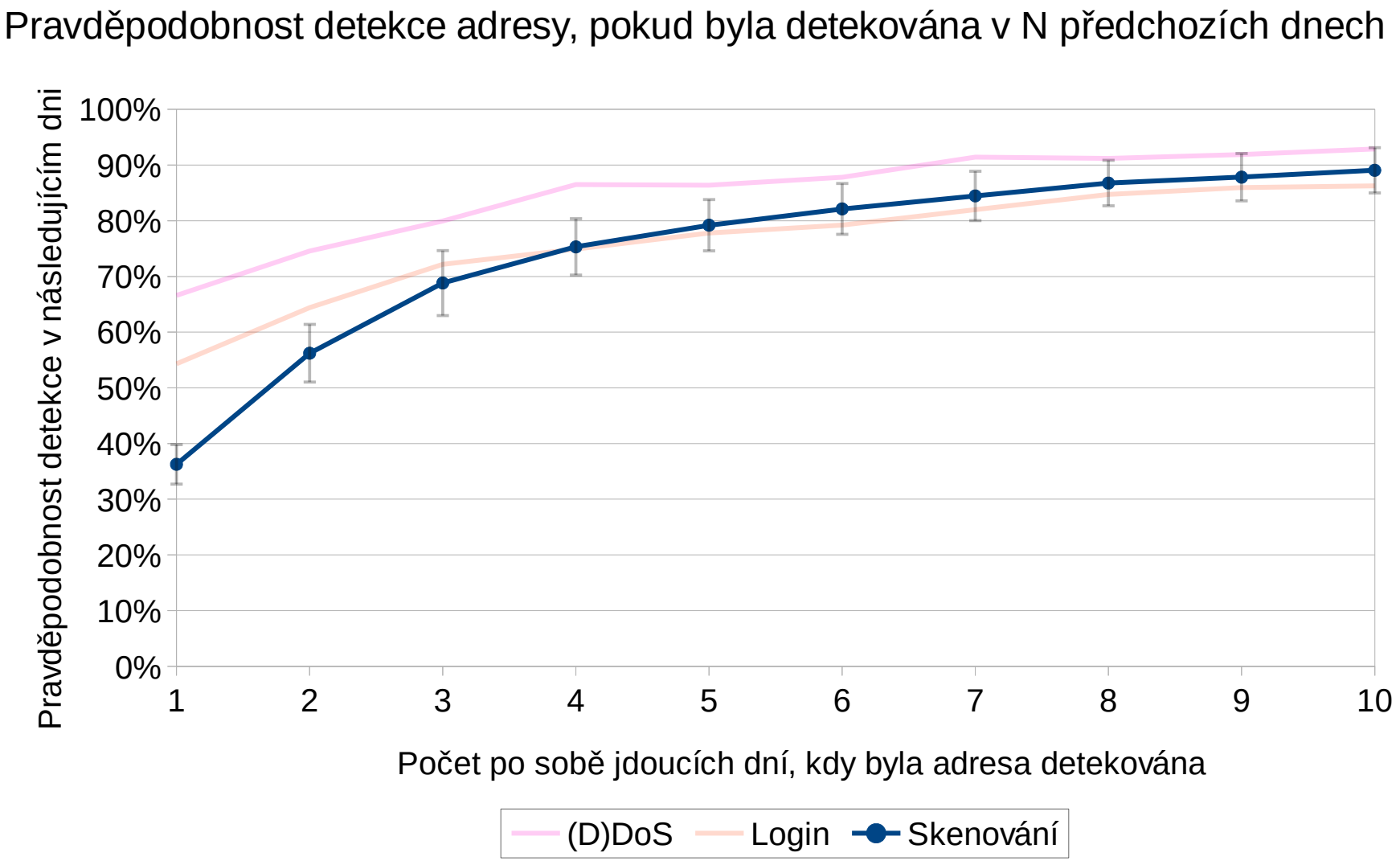


Predikce útoků

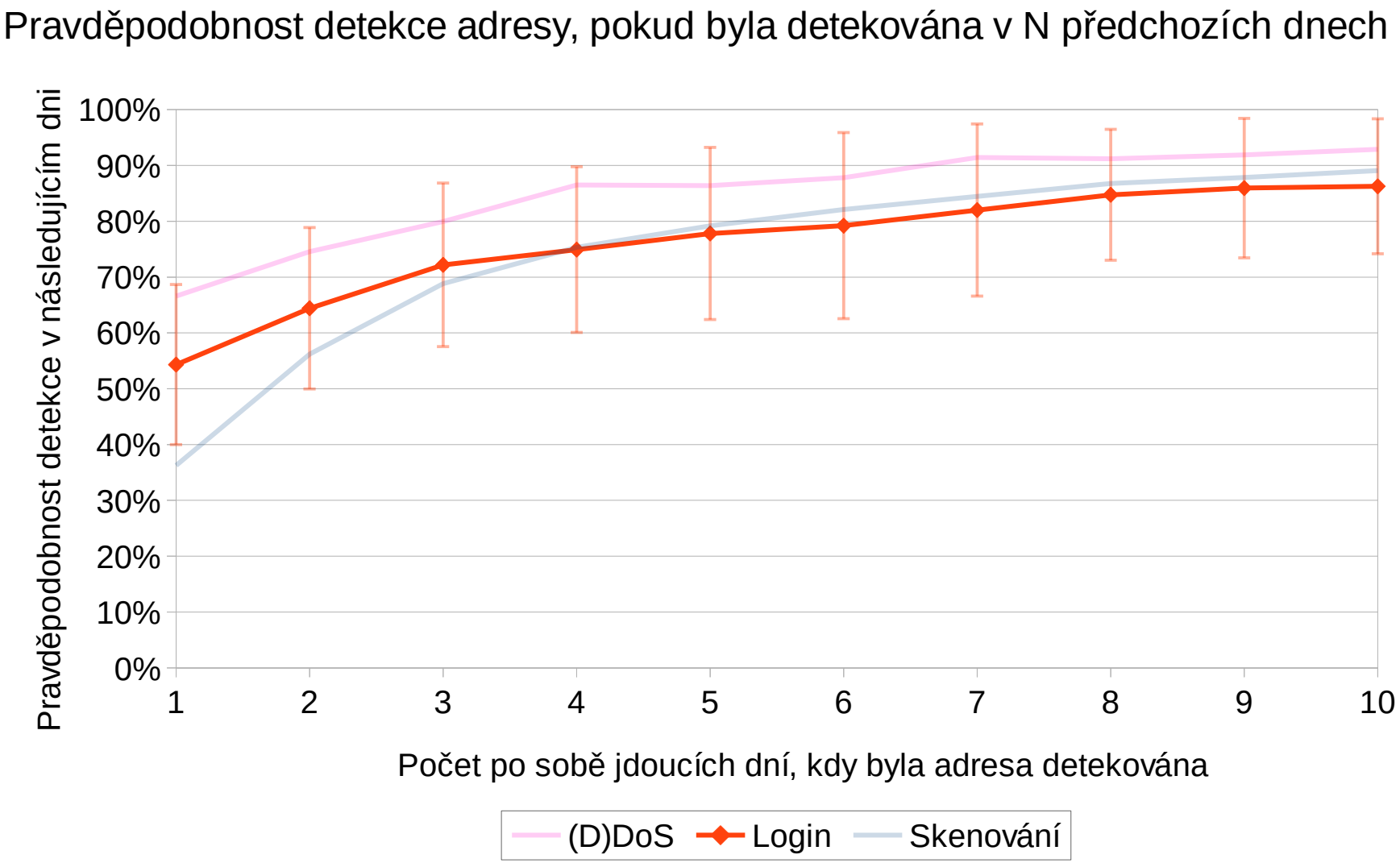
- Analýza dat ze systému Warden.
  - 70 mil. hlášení from ze dvou měsíců (dva měsíční vzorky z r. 2015).
- 68% IP adres je detekováno jen v jednom dni z měsíce.
  - Ale 8.5% je nahlášeno v 5 a více dnech.
    - Tyto jsou zodpovědné za 65% všech hlášení.
  - Tisíce adres jsou detekovány (téměř) každý den.
- Pro (D)DoS útoky je 30% útoků detekováno v 10 a více dnech z měsíce.



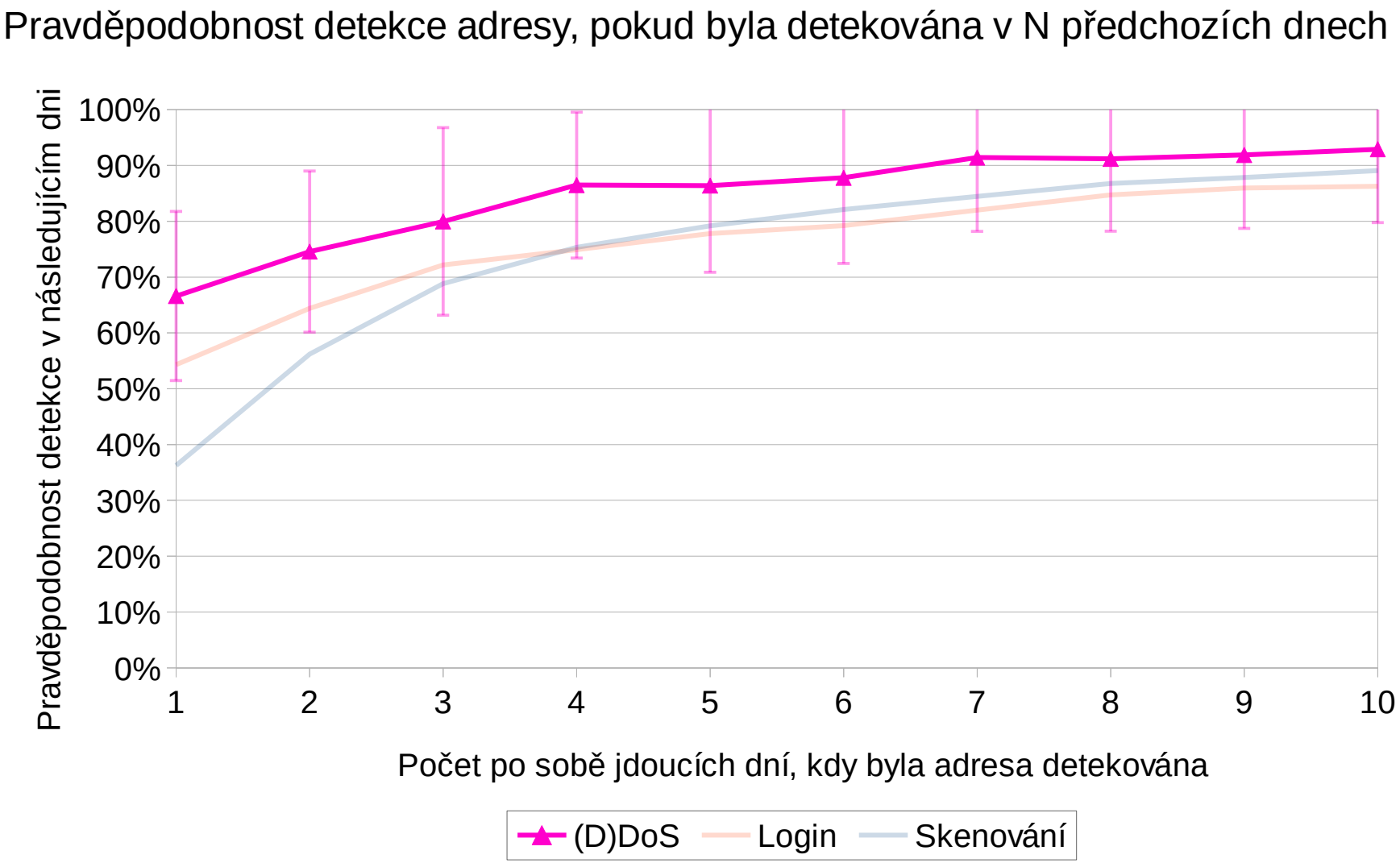
Predikce útoků



Predikce útoků

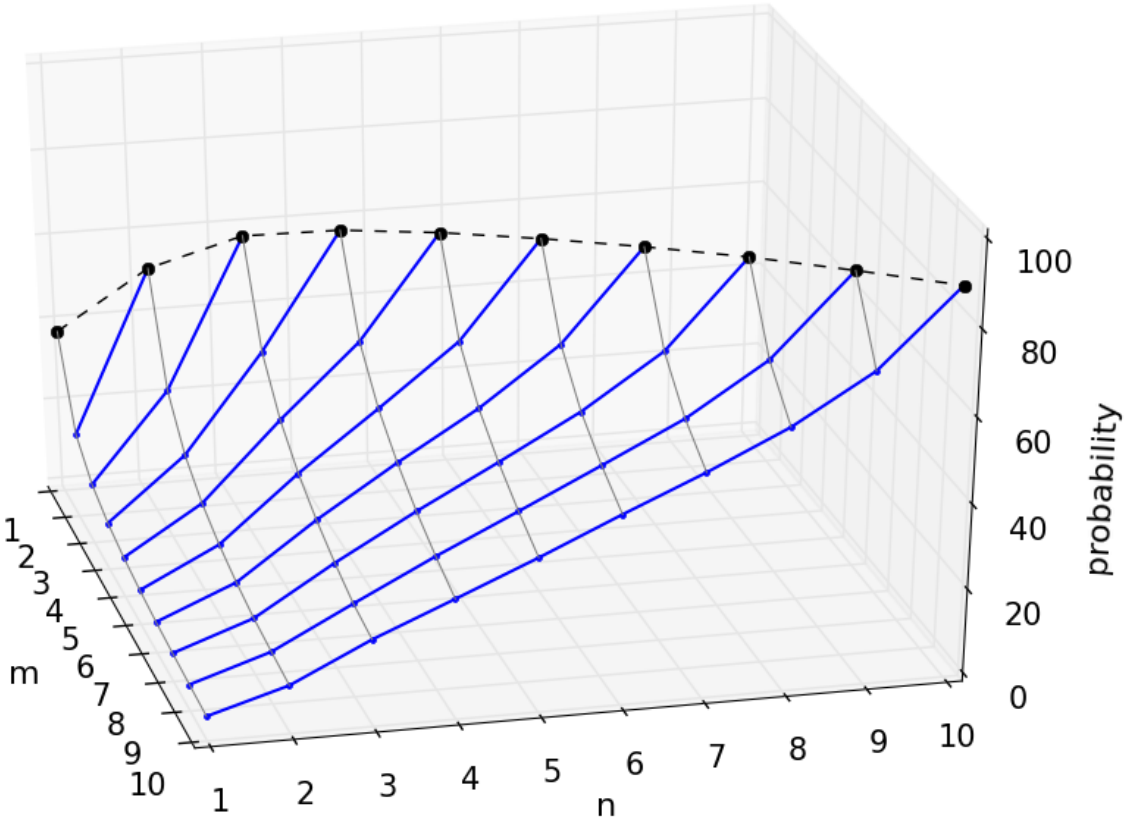


Predikce útoků



Predikce útoků

- Pravděpodobnost detekce, pokud byl adresa detekována v ***n*** z ***m*** předchozích dní.
  - Pouze port scan, pro ostatní útoky příliš málo dat (statisíce útoků; tisíce adres)



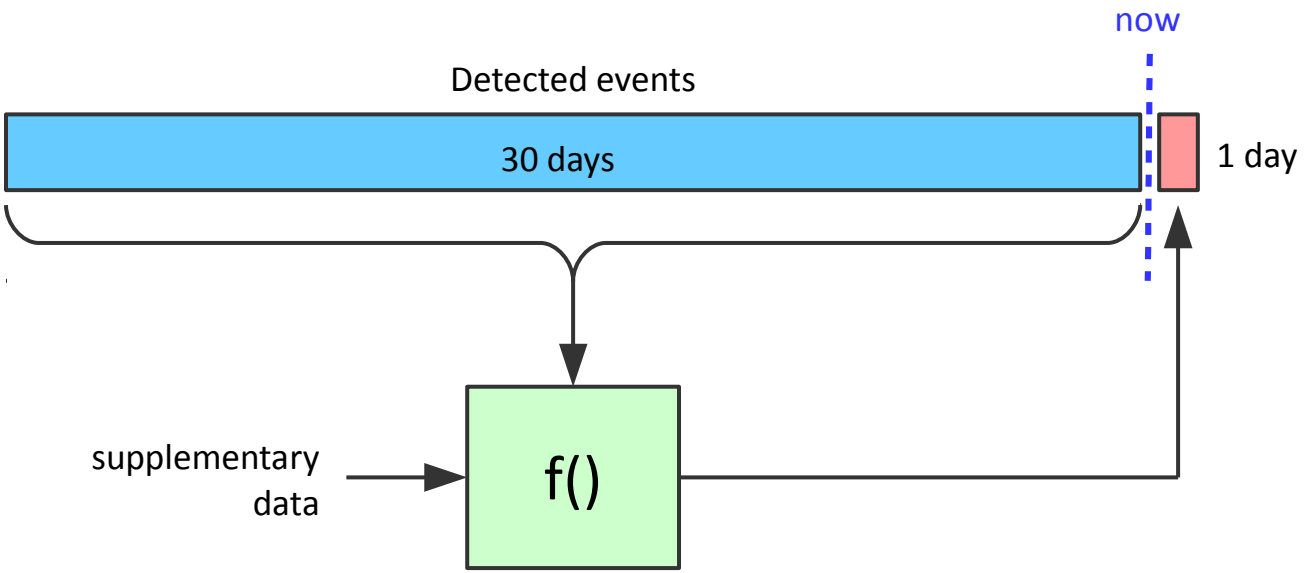
Predikce útoků

- Můžeme přidávat i další vstupní parametry
  - Např. geolokaci, blacklisty
- Problém:
  - pro každou kombinaci vstupních hodnot potřebujeme dostatek vzorků pro výpočet pravděpodobnosti
  - Počet kombinací stoupá exponenciálně
- Řešení:
  - Výpočet pravděpodobnosti je vlastně funkce $\langle X_1 \times X_2 \times \ldots \times X_n \rangle \rightarrow [0,1]$
    - poměrně „hladká“
    - lze aproximovat i s menším množstvím vzorků
  - Máme trénovací data

    --> **Strojové učení** (s učitelem)

Predikce pomocí strojového učení

- Pro každou entitu (IP adresu), a typ škodlivé aktivity:
  - Vstup:
    - historie detekovaných událostí
    - ostatní data o entitě (DNS, AS, geo, blacklisty ...)
  - Výstup:
    - pravděpodobnost, že bude v příštích 24h detekována událost s touto IP



Aktuální stav

- Připravena nová datová sada
  - září 2016
  - 36 mil. záznamů
- První experimenty v SW Weka
  - login attempt
  - na základě informací o detekci v 7 dnech předpověď pro 8. den
  - 96.7% rozhodnuto správně (shodně 3 různé ML metody)

```
1,0,0,0,0,0,0 → 0
0,0,0,1,0,0,0 → 0
0,0,0,0,0,0,1 → 0
1,0,0,0,0,0,0 → 0
0,0,1,0,0,0,0 → 0
0,0,0,0,0,1,1 → 1
1,0,0,0,0,1,0 → 0
0,0,0,0,1,0,1 → 1
      . . .
(59k záznamů)
```

Děkuji za pozornost