Das nationale CERT

Ein Tätigkeitsbericht

Otmar Lendl
<lendl@cert.at>

Programm

Geplant:

- Rolle nationales CERT
- Rahmen in AT
  - Einbettung
  - NIS-Umsetzung
- Kooperationen & Datenaustausch
- Status in AT

Oder

- Einfach Fragen

Vorstellung

- Mag. Otmar Lendl
  - Uni Salzburg (erste Debian-Installation per Floppies …)
  - Ping, EUnet, KPNQwest, Eunet2, Tiscali
  - nic.at R&D (ENUM, 2 RFCs geschrieben)
  - Seit 2007 Teamleiter CERT.at

Warum dieser Vortrag?

- Linux?
  - Nicht direkt
- Community!
  - Wir haben spezielle Rolle
  - Wir wollen aktiv kommunizieren

CERT?

- CERT – Computer Emergency Response Team
  - IT Sicherheitsteam
  - Klar definierte Aufgabe
  - Auch von Außen sicht- und ansprechbar

- Hat nichts mit Zertifikaten, X.509 oder ISO27k zu tun

CERT.at?

- Nationales CERT für Österreich
  - nic.at in Kooperation mit dem Bundeskanzleramt
  - Warum wir?
- Aufgaben
  - Proaktiv: Warnungen, Pressearbeit, Community-Building, Networking, ...
  - Netzwerk Hygiene: Was läuft alles schief in Österreich -> Information der Betroffenen
  - Reaktiv: Hilfe bei Vorfällen

Interessante Rolle

- Randbedingungen
  - Keine Weisungsrechte
  - Keine Meldepflichten an uns
  - Zuständig für das ganze Land
- Was geht trotzdem?
  - Überraschend viel

Staatliche Strukturen

- Rechtlicher Rahmen:
  - Österreichs Strategie für Cyber Sicherheit (2013)
  - NIS-Richtlinie (EU) 2016/1148 (2016)
    - Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union
  - Kommt: NIS-Gesetz / Cybersicherheitsgesetz

NIS-D in a nutshell

- Identifikation wesentlicher Dienstleistungen
  - Mindeststandards für IT Sicherheit
  - Meldepflicht bei Vorfällen
- National Etablierung von
  - CSIRTs (CERTs)
  - Zuständigen Behörden
- Kooperation in der EU
  - CSIRT Netzwerk
  - Kooperationsgruppe

Operative Ebene

- Innerer Kreis (IKDOK)
  - GovCERT, Cyber Security Center (BVT), C4, BKA, BMLVS (MilCERT, HNaA, AbwA), BMEIA
- Äußerer Kreis
  - CERT.at, Sektor-CERTs
- Krisenmanagement in das SKKM integriert
- EU: CSIRT Network

Strategische Ebene

- Cyber Security Steuerungsgruppe (CSS)
  - Oberstes Koordinationsgremium auf Beamtenebene
  - Plus zuarbeitende Gruppen eine Ebene drunter
- Cyber Security Platform (CSP)
  - Forum Wirtschaft / Verwaltung
- Cooperation Group

Kooperationen National

- CERT.at / GovCERT
- IKDOK
- CERT-Verbund
- Austrian Trust Circle
  - Sektoren der KI
- Austrian Energy CERT
- Arge Secur
- KSÖ

Kooperationen Internat.

- FIRST (Globaler Dachverband)
- TF-CSIRT (Europäischer Dachverband)
- CSIRT Network
- European GovCERT Group (EGC)
- Nachbarstaaten (CECSP)
- Deutsche CERT-Verbund
- Diverse Trust-Groups

Was heißt das konkret?

- Runter von der abstrakten Ebene!
- Was machen wir wirklich jeden Tag?

- Welche
  - Tools?
  - Daten?

Hard-Core Technik?

- Nationales CERT ist nur < 5% tief security-technisch.
- Sondern:
  - Informationsdrehscheibe
  - Vernetzung von Personen
  - Vermittlung
  - Pressearbeit
  - Vorträge

CERT.at Aufgaben

- Proaktiv: Warnungen, Pressearbeit, Community-Building, Networking, ...
- Netzwerk Hygiene: Was läuft alles schief in Österreich -> Information der Betroffenen
- Reaktiv: Hilfe bei Vorfällen

Networking

- Konferenzen
- Regelmäßige Treffen
  - IT Security Stammtisch (mit Uni Wien)
  - CERT-Verbund
- Mailinglisten
  - discuss / …
- Nicht im Büro hocken
- In Österreich und international

Tech-Watch

- Wir müssen wissen, was los ist
- Warnungen
  - Nur dann, wenn wirklich Feuer am Dach
  - Kein Autoupdate greift
- Tägliche Zusammenfassungen
- Anfragen
  - Aus der Constituency
  - Presse
- Tool dazu: Taranis vom NCSC.nl

Datenaustausch

- „Habt ihr $link schon gesehen?“
- „Wie schätzt ihr das ein?“
- „Hat das schon jemand nachgestellt?“
- „Siehe auch $link2.“

Netzwerk Hygiene

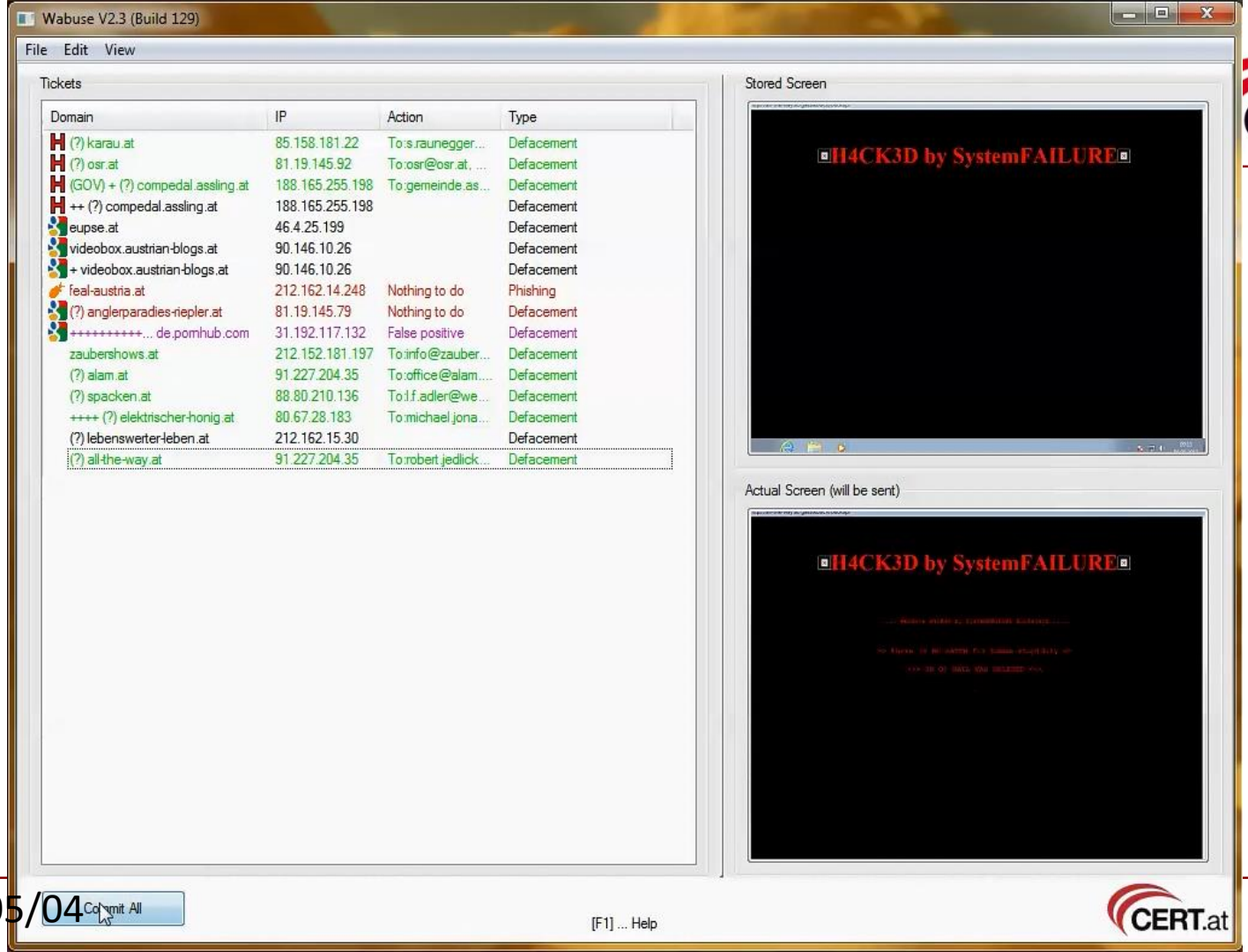
- Web
  - Defacements
  - Phishing
  - Exploit-Packs
- Infektionen
  - Botnetze
- Fehlkonfigurationen
  - TLS Fehler (Poodle, DROWN, …)
  - DDoS Reflectors

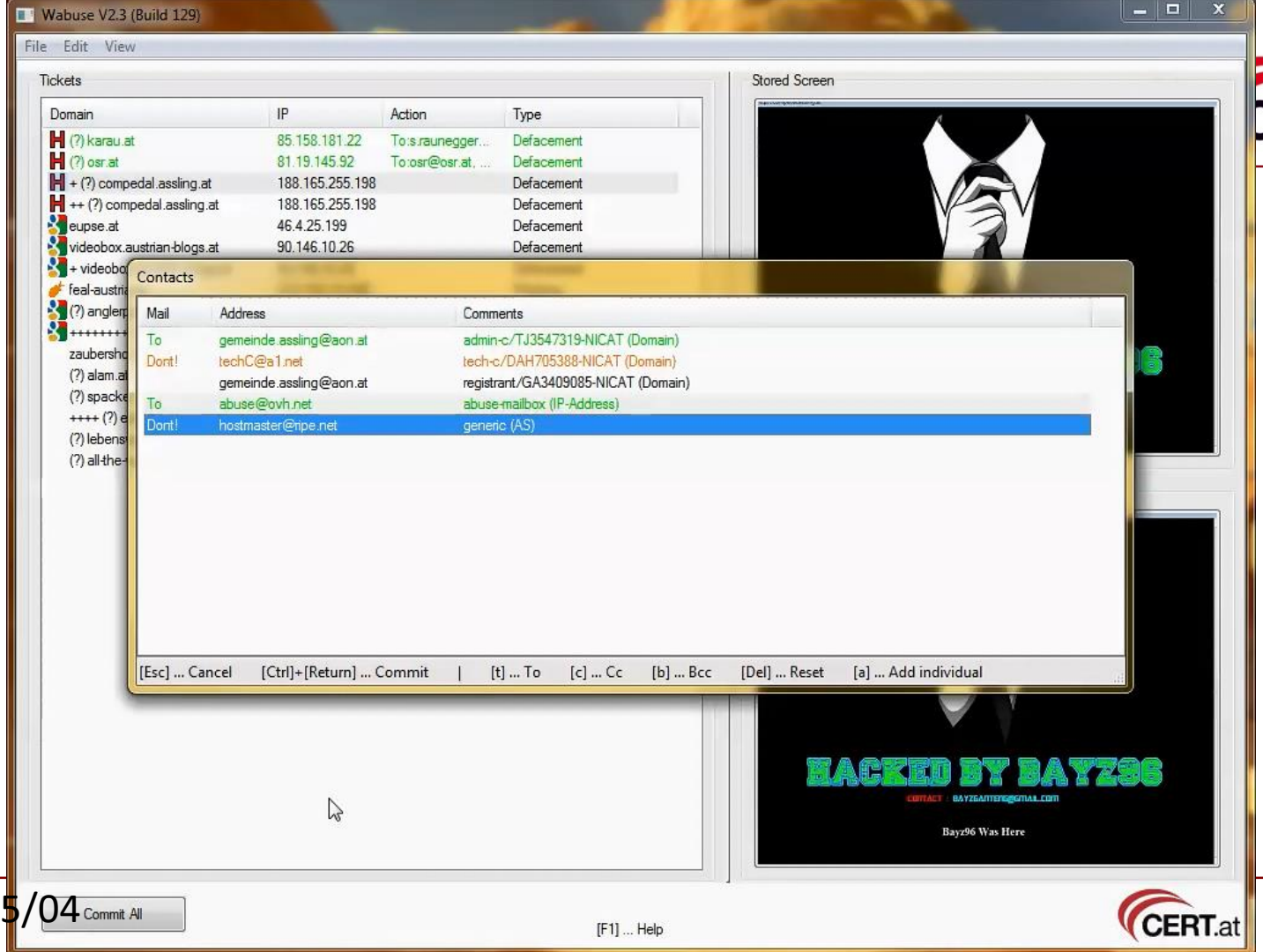
Datenquellen?

- Community der CERTs und anderer Sicherheitsteams
- Non-Profits
  - Shadowserver, Spamhaus, …
  - Researcher
- Große Service-Provider:
  - Google / Bing Malicious URLs feeds
  - Microsoft Digital Crimes Unit
  - Search Engines
- Kommerzielle Datenanbieter (Threat Intel)
  - Zone-H, Virustracker, AnubisNetworks, …
- Eigene Recherchen
- Siehe auch https://www.enisa.europa.eu/publications/proactive-detection-report

Beispiel WebHacks

- Beispiele:
  - Defacements
  - Phishing
  - Google conditional hacks
  - …
- Eigenes Tool für
  - Visueller Check auf False Positive
  - Auswahl des Empfängers
  - Anpassbare Standard-Texte

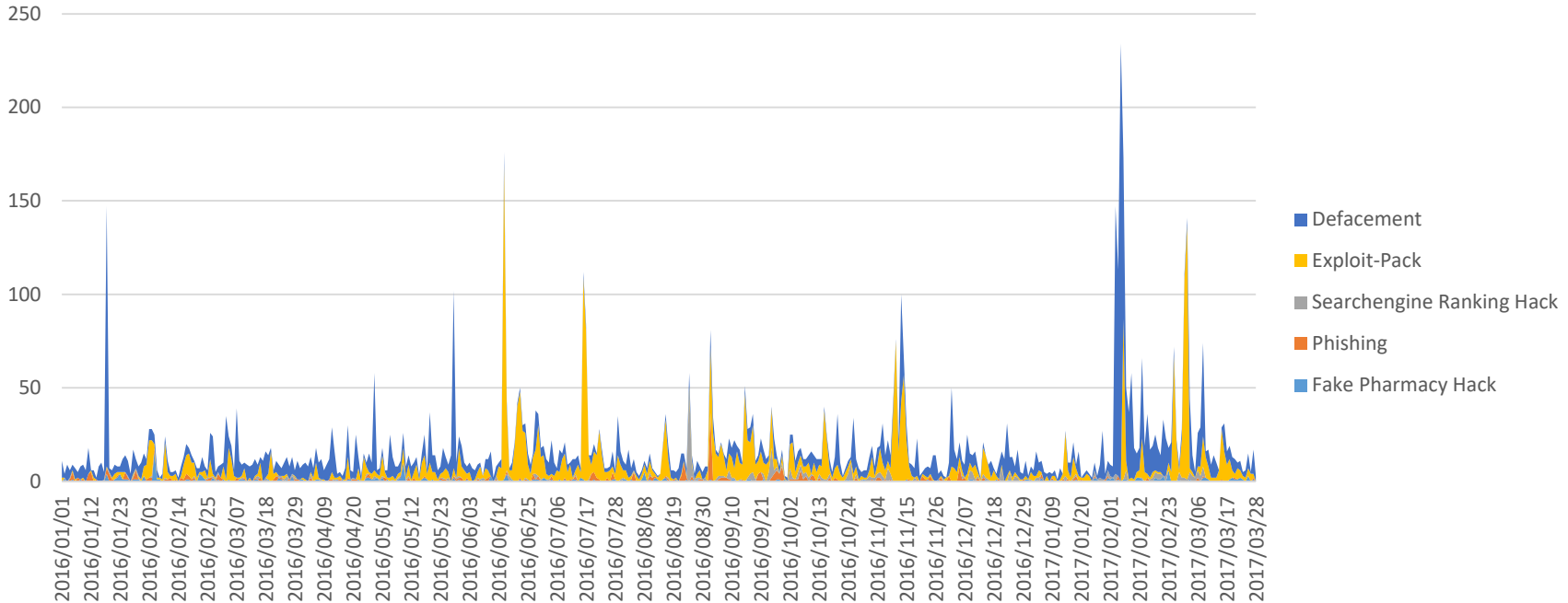

Wabuse V2.3 (Build 129)
File Edit View
Tickets
Domain IP Action Type
(?) karau.at 85.158.181.22 To:s.raunegger... Defacement
(?) osr.at 81.19.145.92 To:osr@osr.at, ... Defacement
(GOV) + (?) compedal.assling.at 188.165.255.198 To:gemeinde.as... Defacement
++ (?) compedal.assling.at 188.165.255.198 Defacement
eupse.at 46.4.25.199 Defacement
videobox.austrian-blogs.at 90.146.10.26 Defacement
+ videobox.austrian-blogs.at 90.146.10.26 Defacement
feal-austria.at 212.162.14.248 Nothing to do Phishing
(?) anglerparadies-riepler.at 81.19.145.79 Nothing to do Defacement
++++++++++... de.pornhub.com 31.192.117.132 False positive Defacement
zaubershows.at 212.152.181.197 To:info@zauber... Defacement
(?) alam.at 91.227.204.35 To:office@alam.... Defacement
(?) spacken.at 88.80.210.136 To:l.f.adler@we... Defacement
++++ (?) elektrischer-honig.at 80.67.28.183 To:michael.jona... Defacement
(?) lebenswerter-leben.at 212.162.15.30 Defacement
(?) all-the-way.at 91.227.204.35 To:robert.jedlick... Defacement
Stored Screen
H4CK3D by SystemFAILURE
Actual Screen (will be sent)
H4CK3D by SystemFAILURE
Commit All
[F1] ... Help


Wabuse V2.3 (Build 129)
File Edit View
Tickets
Domain IP Action Type
(?) karau.at 85.158.181.22 To:s.raunegger... Defacement
(?) osr.at 81.19.145.92 To:osr@osr.at, ... Defacement
+ (?) compedal.assling.at 188.165.255.198 Defacement
++ (?) compedal.assling.at 188.165.255.198 Defacement
eupse.at 46.4.25.199 Defacement
videobox.austrian-blogs.at 90.146.10.26 Defacement
Stored Screen
Contacts
Mail Address Comments
To gemeinde.assling@aon.at admin-c/TJ3547319-NICAT (Domain)
Dont! techC@a1.net tech-c/DAH705388-NICAT (Domain)
gemeinde.assling@aon.at registrant/GA3409085-NICAT (Domain)
To abuse@ovh.net abuse-mailbox (IP-Address)
Dont! hostmaster@ripe.net generic (AS)
[Esc] ... Cancel [Ctrl]+[Return] ... Commit | [t] ... To [c] ... Cc [b] ... Bcc [Del] ... Reset [a] ... Add individual
HACKED BY BAYZ96
Bayz96 Was Here
Commit All
[F1] ... Help

Datenaustausch

- Eingehend:
  - Listen von URLs
  - Manchmal mit Metadaten
- Ausgehend:
  - Mails an Domaininhaber/Hoster/Registrare

Defacements / EP



IP-Adressen

- Infektionen
  - Typischerweise per Sinkhole erkannt
- Fehlkonfigurationen
  - Scan auf Basis Adressen oder Domains
- DDoS Reflekoren
  - Scans

Datenaustausch

- Eingehend:
  - Meist csv files mit IP-Adressen + Metadaten
- Ausgehend
  - Mail an ISPs: in eurem Netz gibt es folgende Probleme

Aktuell: StringBleed

- https://cert.at/services/blog/20170427115946-1972.html
- Rohdaten von Shadowserver:

```
"timestamp","ip","protocol","port","hostname","sysdesc","sysname","asn","geo","region","city","version","naics","sic","sector"
"2017-05-01 03:13:54","62.93.124.X","udp",161,"62.93.124.X.jm-data.at","D-Link Wireless Voice Gateway <<HW_REV: B3; VENDOR: D-Link; BOOTR: 2.4.0alpha14; SW_REV: EU_DCM-704_1.10; MODEL: DCM-704>>","CableHome",25447,"AT","NIEDEROSTERREICH","KREMS AN DER DONAU",2,0,0,
"2017-05-01 03:14:59","92.39.165.X","udp",161,,"D-Link Wireless Voice Gateway <<HW_REV: B3; VENDOR: D-Link; BOOTR: 2.4.0alpha14; SW_REV: EU_DCM-704_1.10; MODEL: DCM-704>>","CableHome",50920,"AT","OBEROSTERREICH","BRAUNAU AM INN",2,0,0,
[…]
```

- Eigene Tests zur Verifikation

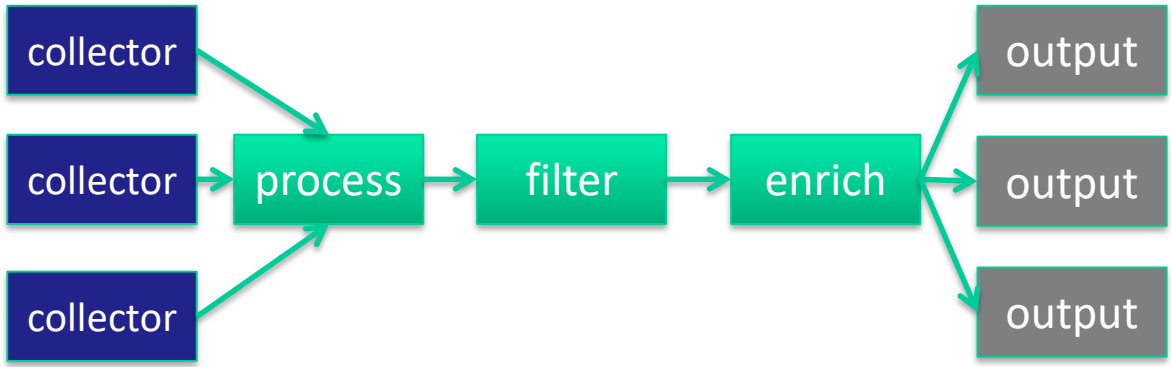
Tool dafür

- https://github.com/certtools/intelmq
- https://github.com/certtools/intelmq-manager

- Mailing list for developers: ask kaplan@cert.at for subscription

What is it?

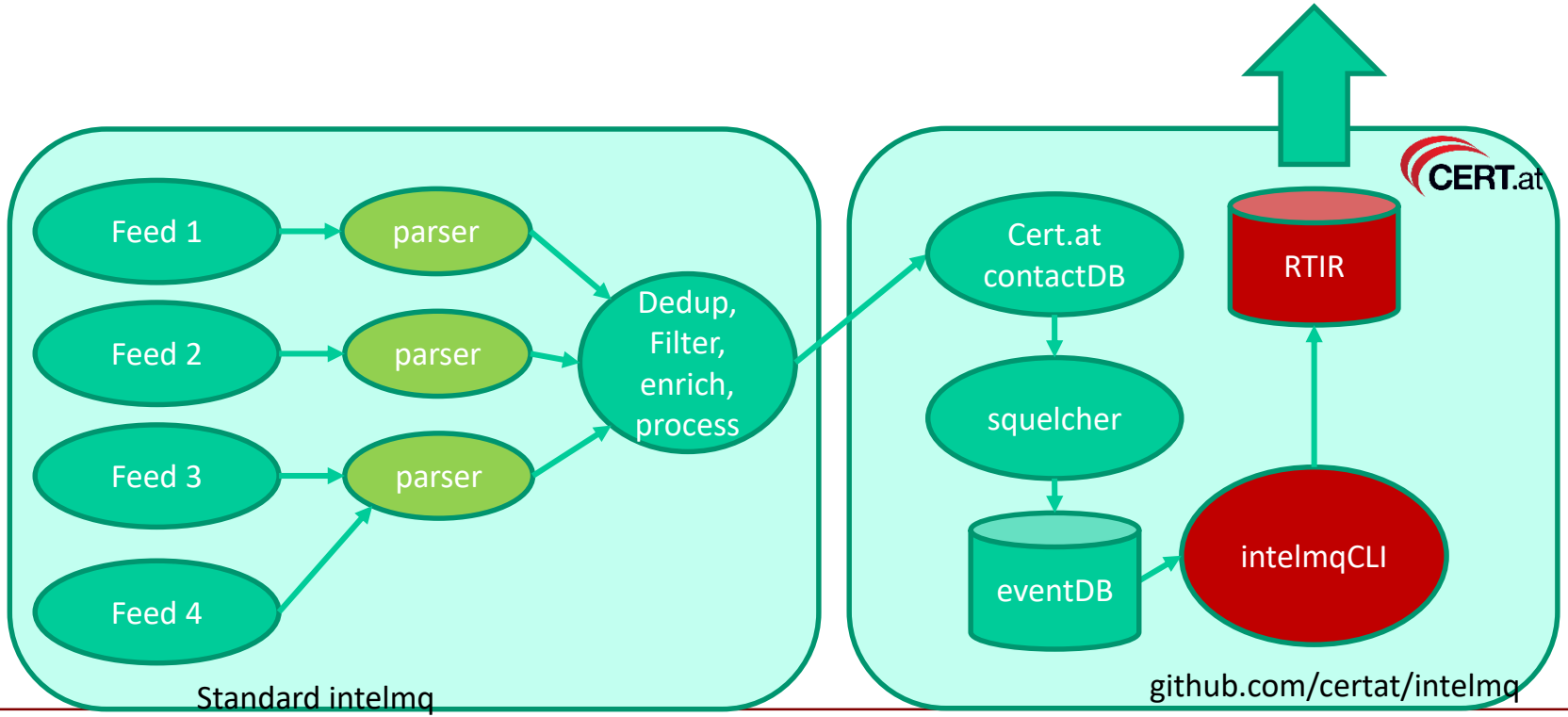
- Open Source Data flow oriented toolkit to:
  - Automatically collect & handle events/incidents
  - Process and enrich these events
  - And send them to some output



What is it (2)?

- Written in Python
- Based on message queues („MQ“) – redis, (RabbitMQ, zmq)
- Fast
- Very easy to extend
- GUI interface to create pipelines

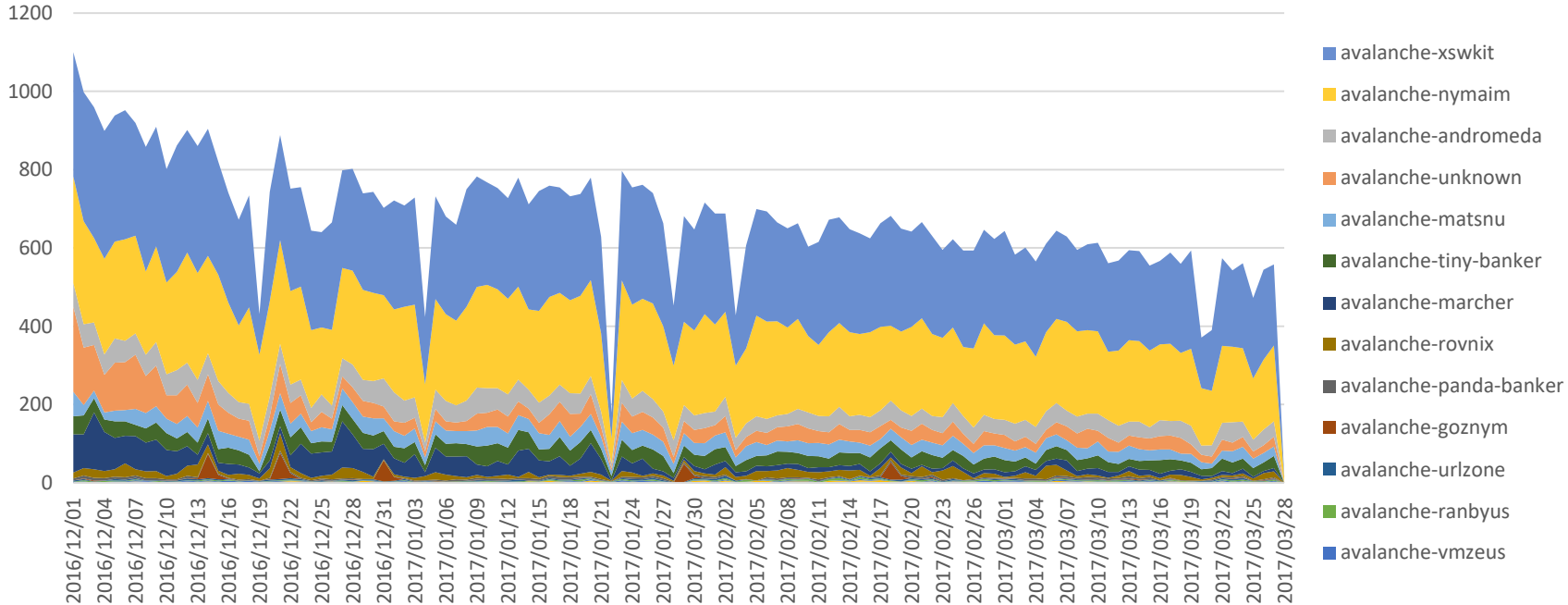
Status bei CERT.at



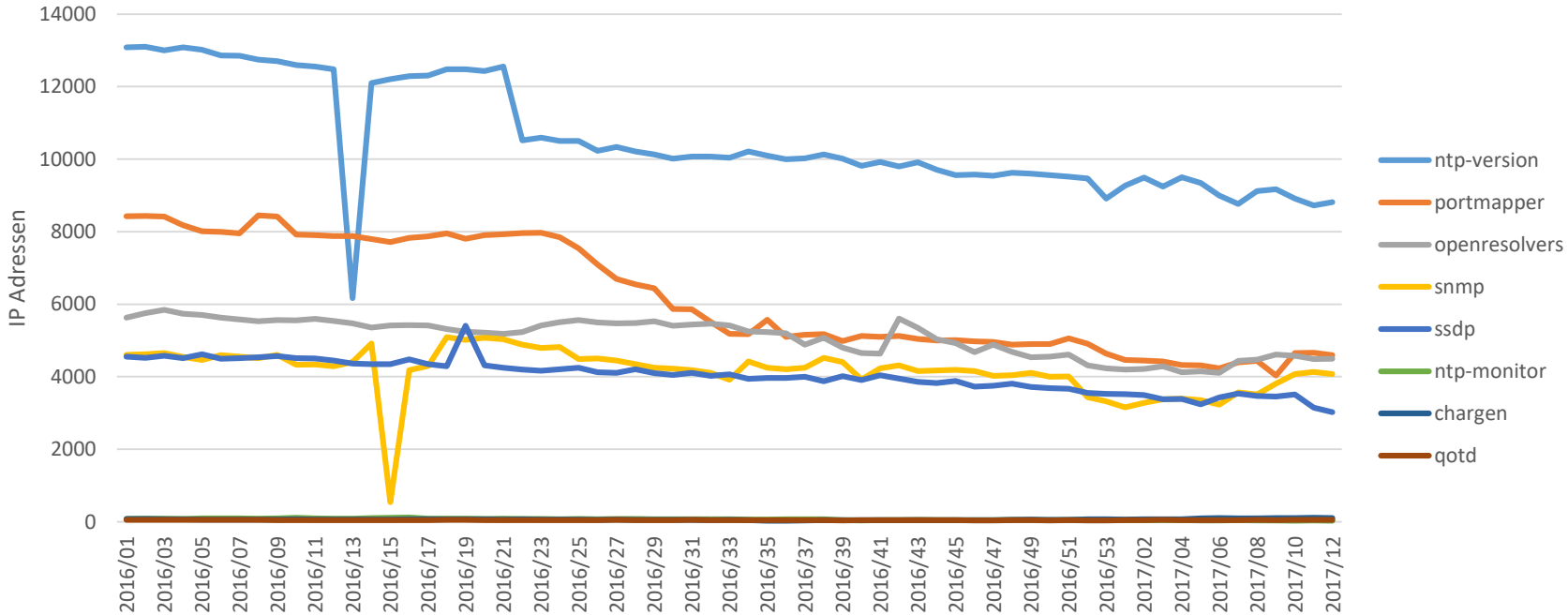
Avalanche Takedown

- Jurisdictions: 30
- Arrests: 5
- Premises searched: 37
- Servers seized: 39
- Servers taken offline through abuse reports: 221
- Countries with victim IP's: 180+
- Domains blocked or sinked: Over 800,000 in 60+ TLDs

Entwicklung



DDoS Reflektoren



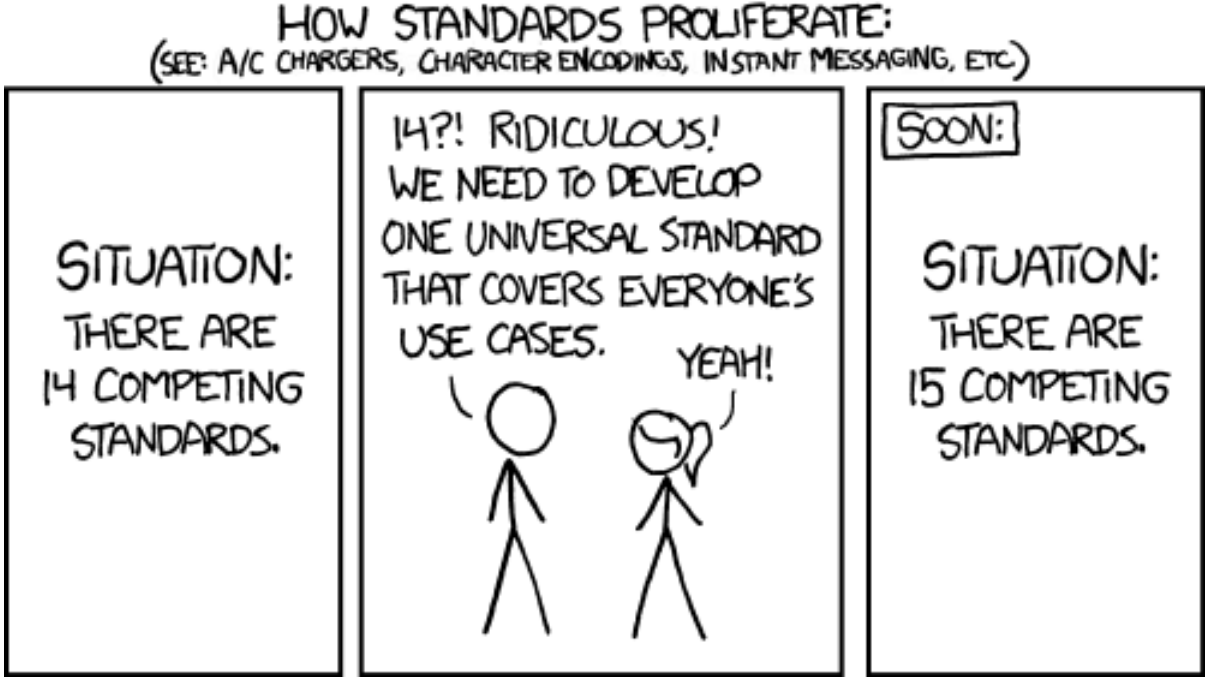
Threat Intel

- Auf was sollte man schauen?
- Beispiele:
  - Eckpunkte eines Spear-Phishes
  - C2 Domains/IP-Adressen
  - Filenamen/Hashes/Mutexe/Registry einer Malware

Datenaustausch

- Viel in normalen Emails
  - Manchmal mit Attachments im CSV Format
- Machine2Machine?
  - Dem heiligen Gral laufen wir schon lange nach

Standards



https://xkcd.com/927/

Aktuell

- CYBOX/STIX/TAXII 1
  - XML basiert
  - Sehr komplex
- STIX 2
  - Einfacher, JSON
- In der Praxis …

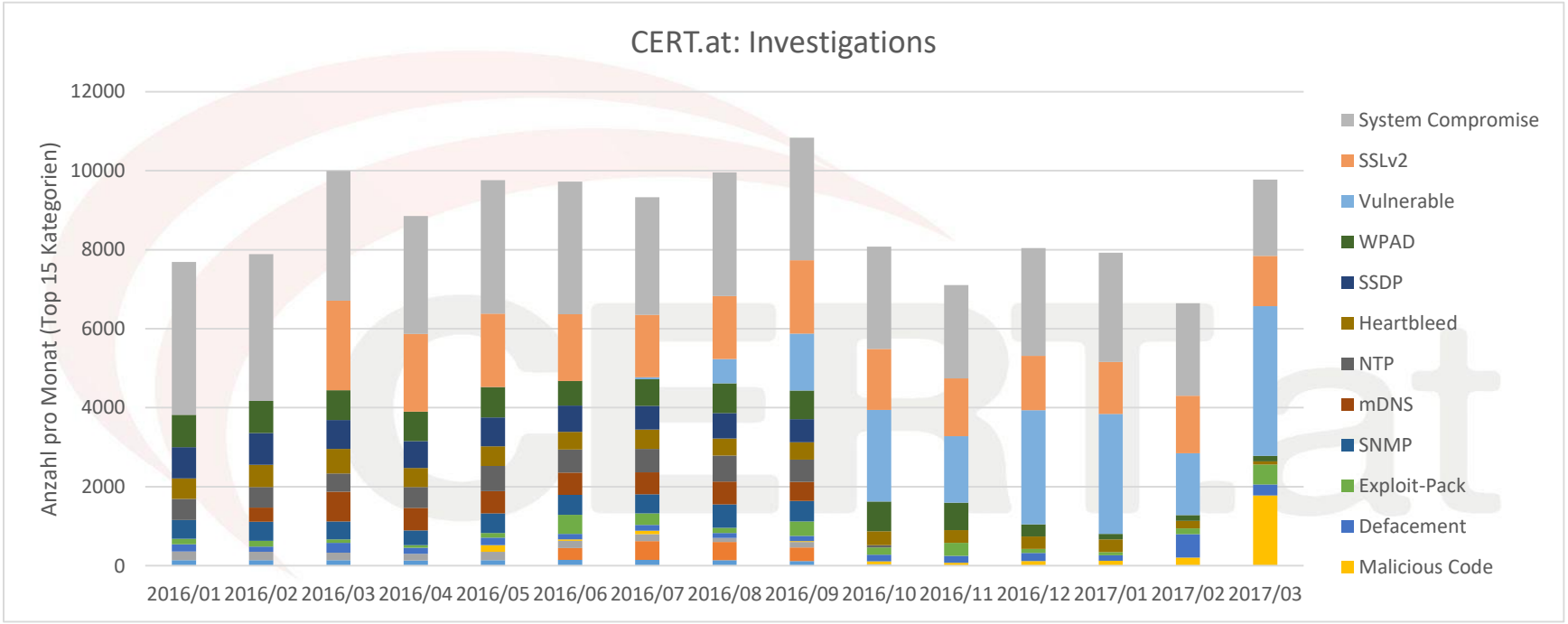
Tool dafür: MISP

- Malware Information Sharing Platform
  - Open Source
  - Das Tool der Wahl für CERTs
  - Synchronisation zwischen Instanzen

Zusammenfassung Daten

- OSINT / Vulnerabilities
  - Freitext, Tool: Taranis
- Standardvorfälle (Bot, Webpages, DDoS)
  - Einfach strukturierte Listen
  - Tool: IntelMQ
- Threat Intel
  - Viel noch manuell
  - Tool: MISP

Ausgehende Mails



Ad Linux

- Ähnlich verwundbar wie Windows
- Am Desktop hilft der Marktanteil
- Am Server gar nicht
- Im Embedded-Bereich auch nicht
- Passt bitte auf eure Systeme auf!
  - Und sei es nur, um Dritte zu schützen.

Fragen?

Otmar Lendl <lendl@cert.at>
+43 1 5056416 711