



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatikstrategieorgan Bund ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI



Lauernde Gefahren im Internet

Max Klaus, Stv. Leiter MELANI



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatikstrategieorgan Bund ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI




Inhalte:

1. Teil Auftrag und Rahmenbedingungen

2. Teil Aktuelle Bedrohungslage



BR-Auftrag / PPP

	SCHWEIZERISCHER BUNDESRAT	Beschluss	20. August 2003
	CONSEIL FÉDÉRAL SUISSE	Décision	
	CONSIGLIO FEDERALE SVIZZERO	Decisione	

Aufbau und Betrieb einer Melde und Analysestelle Informationssicherung MELANI



Schutz kritischer Infrastrukturen in der Schweiz nur in enger Zusammenarbeit mit der Wirtschaft möglich → Public Private Partnership



Rahmenbedingungen



- Keine Meldepflicht



- Subsidiarität



- Keine Weisungsbefugnis



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatikstrategieorgan Bund ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI



Inhalte:

- 1. Teil Auftrag und Rahmenbedingungen
- 2. Teil Aktuelle Bedrohungslage**



Veränderung der Bedrohungslage

Vor 150 Jahren



derstandard.at

Vor 10 Jahren



augsburgerallgemeine.de

heute



Jdpower.com

morgen?



infosecisland.com

- Modernere Mittel
- Vernetzte Bevölkerung
- Zu geringes Sicherheitsbewusstsein

Angriffe heute



Opfer



Internet



Krimineller



auch ein
Krimineller



Defacements

STAATEN MIT EINGESCHRÄNKTER RELIGIONSFREIHEIT:

Soweit darf es nicht kommen! Ja zur Religionsfreiheit. Nein zur Minarettverbots-Initiative.
 Spenden mit dem Vermerk „Religionsfreiheit“ nimmt die Gesellschaft Minderheiten in der Schweiz dankend entgegen. Postkonto 85-515412-1. www.minarettverbot-nein.ch

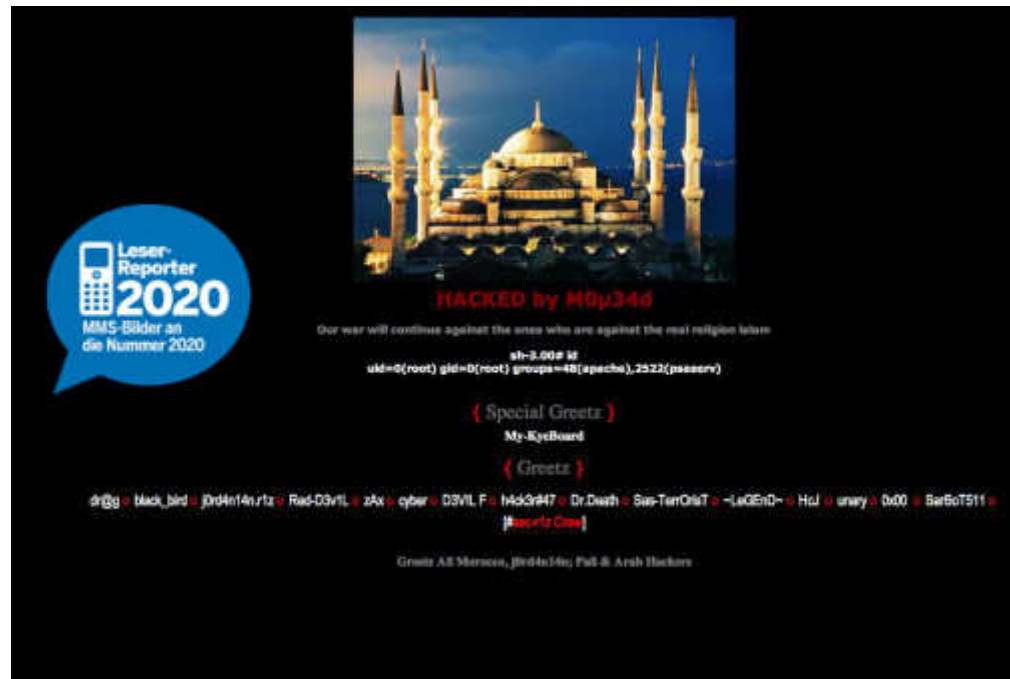
español.eu trios.es



Results de búsqueda: No se han encontrado Resultados !!
 Error: PROHACK
 img opens search: Gm&search=PROHACK: Búsqueda de "query"



Minarettinitiative (1/2)

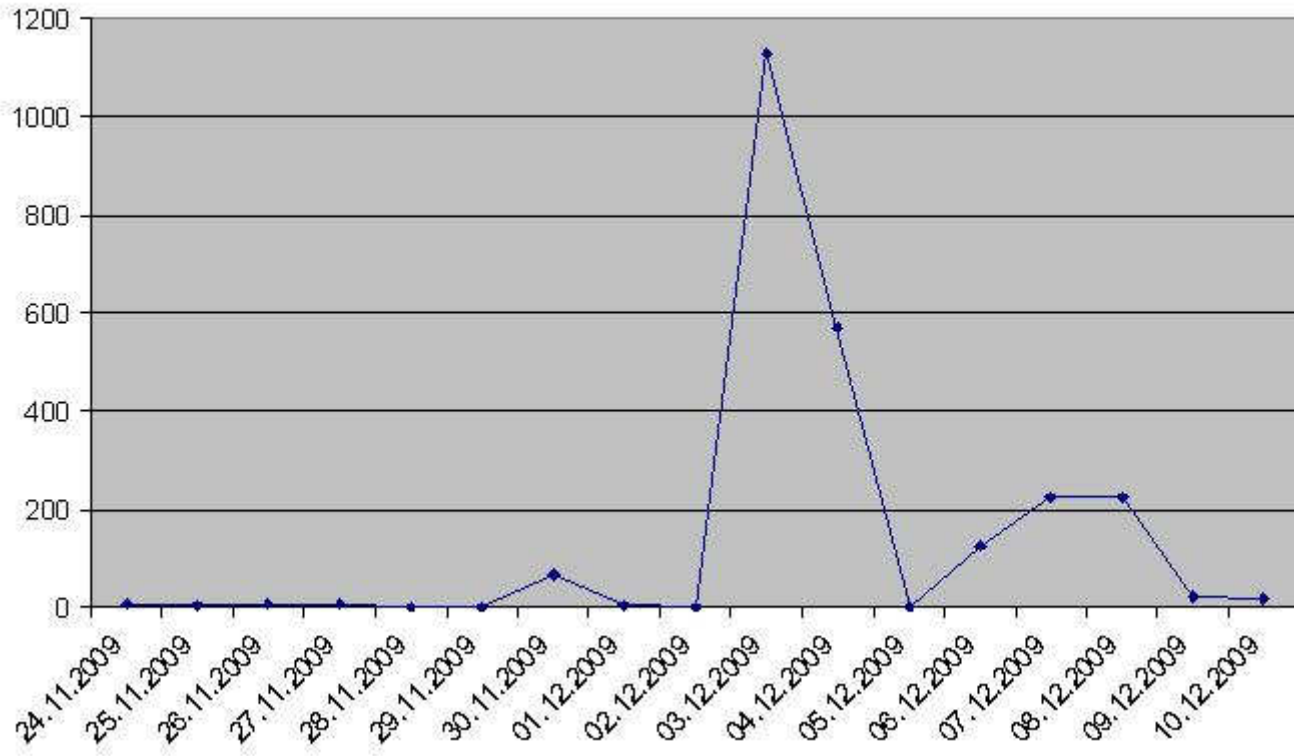


«Unser Krieg gegen die Gegner der wahren Religion Islam wird weitergehen»,
verbreiten Cyberkriminelle auf Webseiten wie boutiq.ch und fruitcake.ch.



Minarettinitiative (2/2)

Anzahl Defacements gegen Schweizer Webseiten



ca. 3000 gehackte Webseiten



Denial of Service

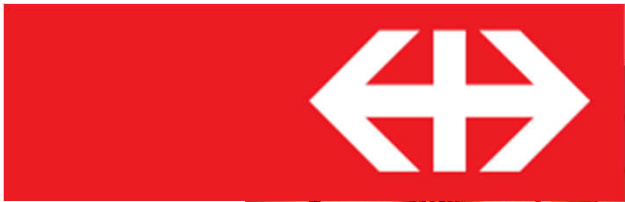


ISB / NDB

Melde- und Analysestelle Informationssicherung MELANI



Der „Schwarze Montag“



SBB



Subject: DDOS ATTACK!!!
Date: Wed, 9 Mar 2016 XX:XX:XX +0000

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!



Collective.
bert.admin.ch
ers



GALAXUS

All your servers will be DDOS
don't pay protection - 25 BTC
17j7onEtLgS2pd6qLekKQCteqTr

If you don't pay by Monday, attack will start, price to stop will increase to 50 BTC and will continue.

This is not a joke.

Our attacks are extremely powerful. If you don't pay protection will be implemented.



second.



at all with just 25 BTC

reply, we will not respond. WE WILL AGAIN HEAR FROM US

AFXZVS

AND YOU

Bitcoin is anonymous, nobody will ever know you cooperated.





Phishing (Kunstwort aus: **P**assword, **H**arvesting und **F**ishing)



Graphic Design by **Panda Software**





Beispiel eines Phishingmails



Kantonalbank

de | fr | it | en

Home

Sehr geehrte Kunden der Kantonalbank,

wie Sie wissen, wird unser e-banking stets aktualisiert, um immer den höchsten Standard an Synchronität und Sicherheit beizubehalten. Um sicherzustellen, dass Sie das neue System des e-bankings problemlos und synchron nutzen können, **müssen Ihre persönlichen Address- und Telefondaten noch einmal von Ihnen bestätigt werden.** Dies ist notwendig um keine alten Daten in das neue e-banking zu übernehmen. Um Ihre persönlichen Daten zu aktualisieren, melden Sie sich hier bitte zunächst bei Ihrem e-banking an:

Klicken Sie hier - >

Nachdem Sie das Formular im e-banking ausgefüllt haben, wird von Ihnen kein weiterer Schritt zur Aktualisierung benötigt. Sie werden innerhalb von 48 Stunden nach dem Ausfüllen des Formulars von einem Mitarbeiter unserer e-banking Abteilung telefonisch kontaktiert, um die Aktualisierung Ihres e-bankings abzuschließen. Vielen Dank für Ihr Verständnis und Ihr Vertrauen in die Kantonalbank.

Mit freundlichen Grüßen,

e-banking Abteilung,
Die Schweizer Kantonalbanken.



Erpressung



<http://www.trustedwatch.de>

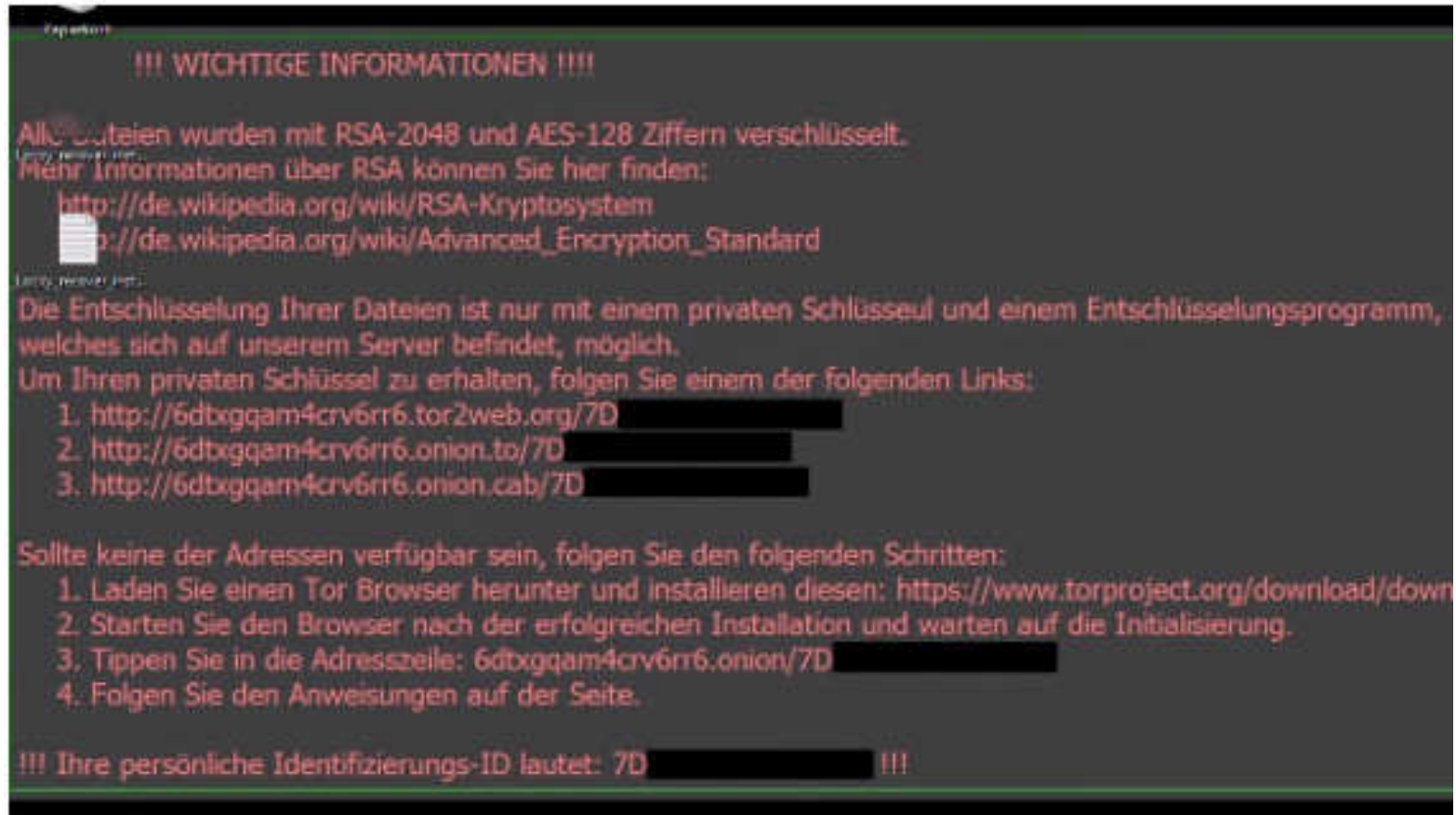
ISB / NDB

Melde- und Analysestelle Informationssicherung MELANI





Verschlüsselungstrojaner «Locky» (1/2)





Verschlüsselungstrojaner «Locky» (2/2)



- USA: IT für eine Woche lahm gelegt
- Deutschland: aktuell 5'000 Infektionen / Stunde
- Schweiz: einzelne Fälle bekannt



Betrug





Betrug: President Scam

Re: RE: Dossier confidentiel - N

DATEI NACHRICHT

Ignorieren Ignorieren X

Junk-E-Mail Löschen

Antworten Antworten

Allen antworten

Weiterleiten

Besprechung

Chat

Weitere

Verschieben in: ?

Team-E-Mail

Antworten und I...

An Vorgesetzte(n)

Erledigt

Neu erstellen

QuickSteps

Versenden

Kategorisieren Nachverfolgung

Übersetzen

Suchen

Verwalten

Markieren

Bearbeiten

Mo 17.11.2014 16:26

m. [redacted].w [redacted]@ [redacted].com [redacted]

Re: RE: Dossier confidentiel

An [redacted]

Wenn [redacted]

Bitte betrachten Sie die Darstellung dieser Nachricht. Wenn Probleme mit der Darstellung dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

Parfait

Nous espérons que vous trouverez les coordonnées bancaires du bénéficiaire à créditer :

Cette opération est soumise à la validation de la banque.

Je vous prie de bien vouloir trouver ci-joint les coordonnées bancaires du bénéficiaire à créditer :

Merci de votre retour.

Par mes soins, je reste dans la vive l'attente de l'ordre de virement.

Veillez à bien vouloir confirmer la conformité du protocole de confidentialité vis à vis de la banque ?

Cordialement,

M. W.

Directeur Général

Directeur

[redacted]

t en mesure d'effectuer un paiement

ation afin de respecter la norme de cette opération.

[redacted]

ISB / NDB

Melde- und Analysestelle Informationssicherung MELANI





Spionage






Spionageangriffe gegen das EDA



Das Mail an Mitarbeiter des EDA

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidg. Volkswirtschaftsdepartement EVD

Staatssekretariat für Wirtschaft SECO

Strategische Tourismuspolitik

Sehr geehrter Herr Max Muster !

Im Rahmen unseres [Programms zur Foerderung des Inlandtourismus](#) wurde ein Amateurfotowettbewerb unter eidgenössischen Zivilbeamten durchgefuehrt. Ziel war ein solches auszuwaehlen das moeglichst umfassend das Gesamtbild der Naturschoenheiten unseres Landes darstellen wuerde. Unter der Mehrzahl der an unsere Adresse eingegangenen [Bilder](#) hat unsere Jury 6 ausgewaehit. Ihre Meinung ist uns sehr wichtig und wir moechten Sie darum bitten uns mit dem Wahl der endgueltigen Sieger zu helfen.

Haben Sie kurz Zeit uns zu helfen? Ihre Stimme hilft uns ueber den besten Amateurfotokuenstlerfuer zu entscheiden. Die Wettbewebsbilder sind auf unserer [Web-seite](#) abrufbar. Dort koennen Sie auch Ihre Stimme fuer ein das Ihnen besonders gefallen hat abgeben. Um Ihnen die Ansicht der Fotos benutzerfreundlicher zu machen werden Fotoalben aller Teilnehmer in Form einer Diaschau dargestellt so dass die Panoramabilder mit den Ansichten der Schweiz nacheinander praesentiert werden. Alle Bilder die Ihnen besonders gefallen haben koennen Sie ruhig auf Ihren Arbeits-oder Home PC ohne jegliche Copyrightverletzung herunterladen. Fuer Ihre Stimme danken wir Ihnen im voraus.

[Uebergang zur web-seite zur Stimmabgabe](#)

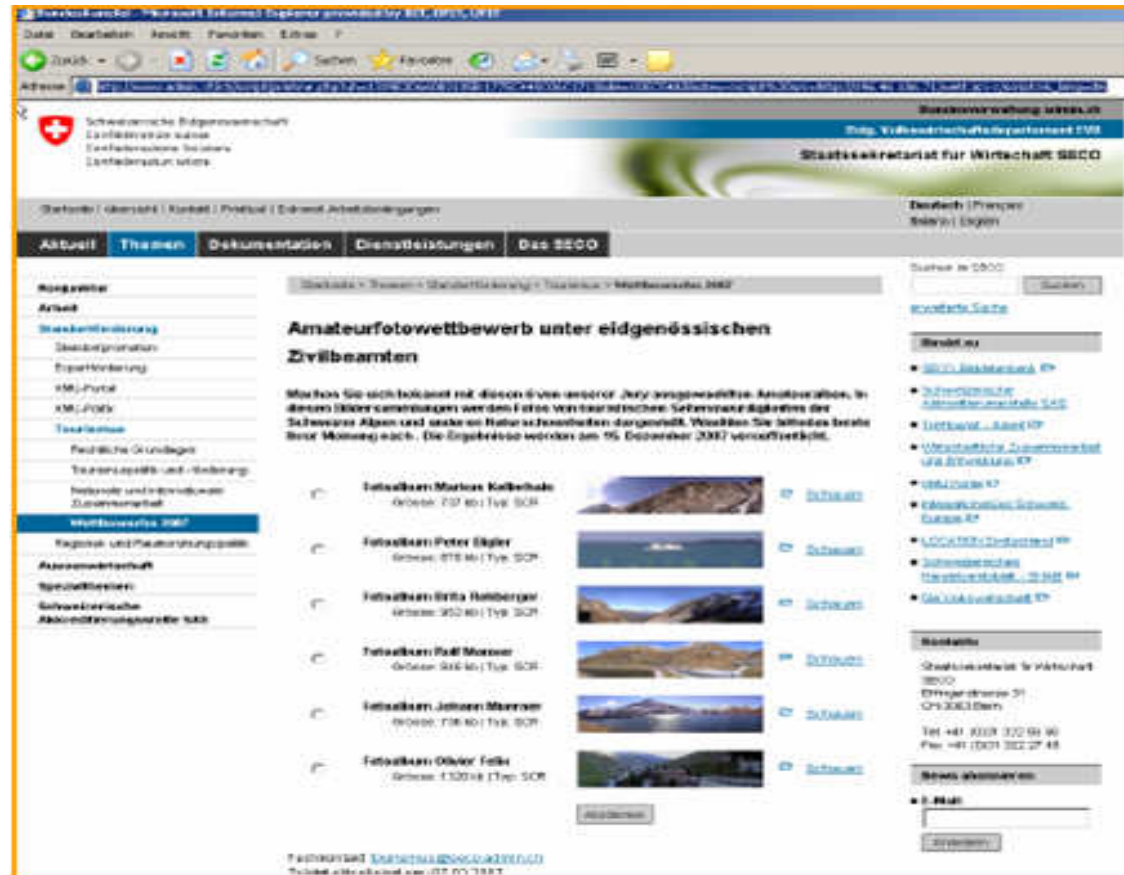
Diese Mitteilung ist kein Spam, ihre Absendung ist mit der Verwaltung der Domain admin.ch abgestimmt.

Staatssekretariat für Wirtschaft SECO und
Schweizer Tourismus-Verband

Link zu admin.ch mit XSS

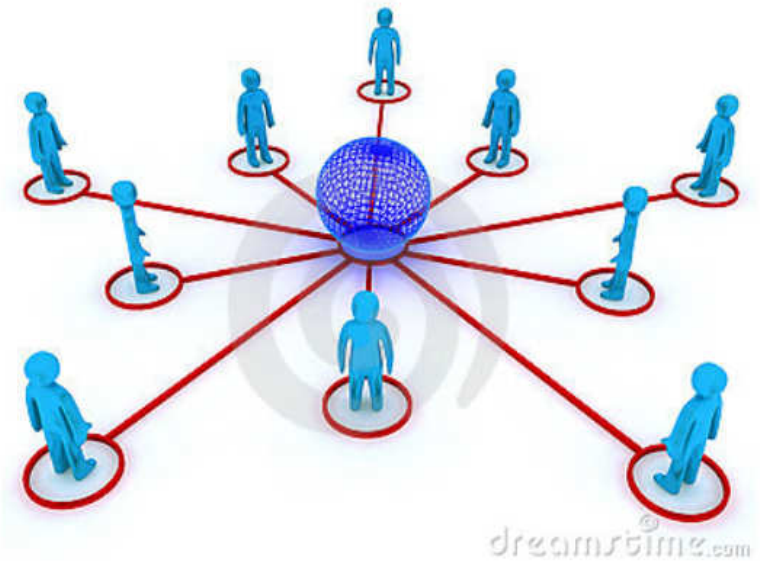


Spionageangriffe gegen das EDA



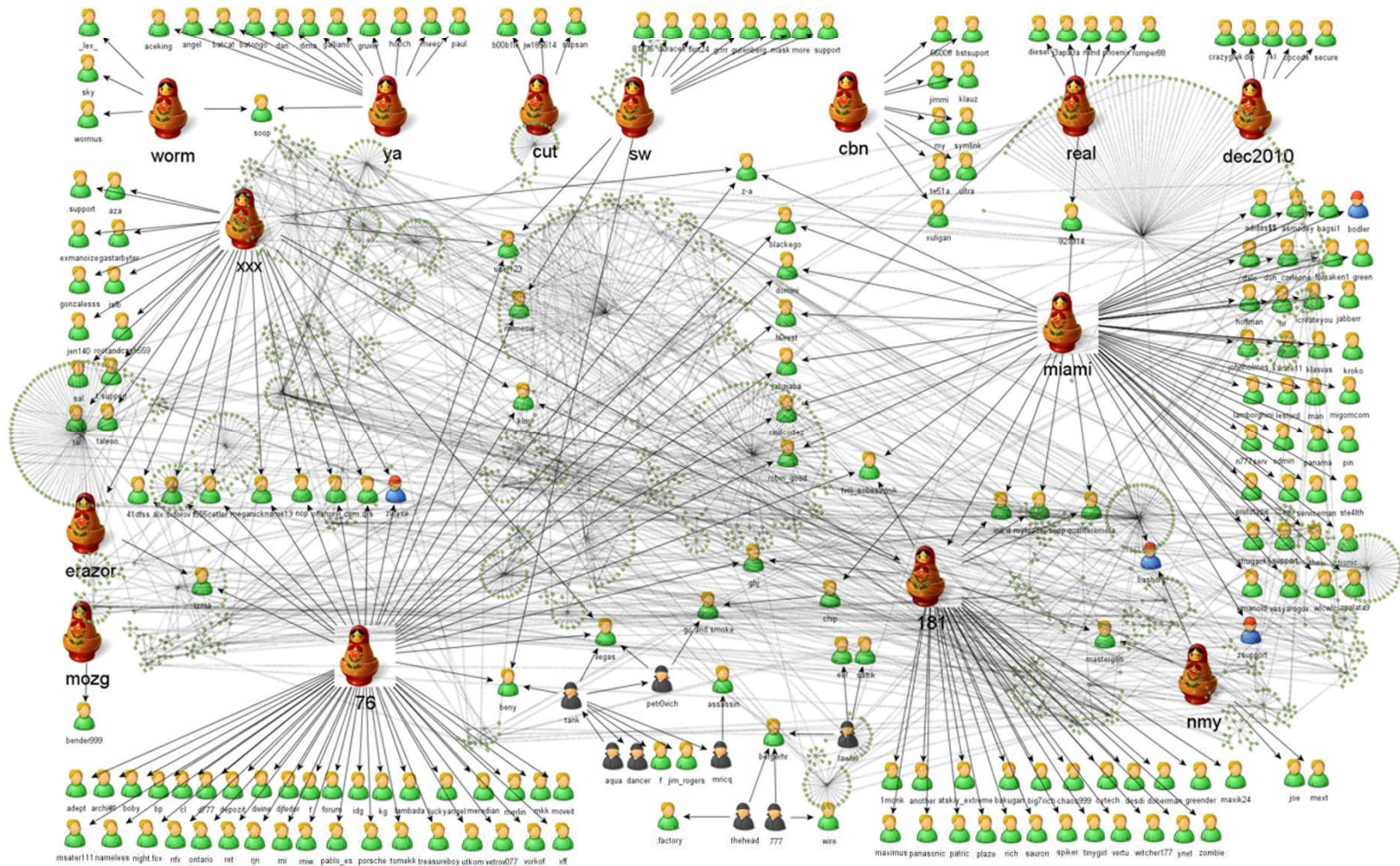


Arbeitsteilung / Vernetzung





Jobsharing bei Cyber-Angriffen



ISB / NDB

Melde- und Analysestelle Informationssicherung MELANI



Wie gut sind die ‚Akteure‘ vernetzt?

Vorfall:

- mittels SQL Injektion Zugang zu Kreditkarten Nummern
- Mit Zusatzprogrammen herausfinden der Pin Nr.
- Erhöhung der Kartenlimite auf **Maximum**
- Produktion und Verteilung der Kreditkarten

Tag X - Weltweit koordinierter Angriff

- Geldbeschaffung an **135** Geldautomaten mit verschiedenen Kreditkarten
- In **49** verschiedenen Ländern
- Zeitaufwand: **30 Minuten**
- **→ Deliktsumme: 9,4 Mio US\$**



Schlussfolgerungen (1/2)

- Informationstechnologie ist allgegenwärtig und ein wichtiger Bestandteil im „daily business“ vieler Unternehmen
- Informationstechnologie als zweischneidiges Schwert: Neue Möglichkeiten, aber auch neue Verletzbarkeit
- Das organisierte Verbrechen verfügt über hervorragende Mittel und setzt diese gewinnbringend ein
- Angegriffen wird vor allem, was **Geld** bringt und/oder einen Informationsvorsprung (Know-How-Gewinn zum Nulltarif)



Schlussfolgerungen (2/2)

- Angegriffen wird über das schwächste Glied, und das ist immer öfter der Mitarbeiter
 - Technische Massnahmen allein reichen nicht aus
 - Schutzmassnahmen beinhalten: Technische Massnahmen, organisatorische Massnahmen, Sensibilisierung, Informationsaustausch



Herzlichen Dank für Ihre Aufmerksamkeit



Max Klaus
Stv. Leiter Melde- und Analysestelle
Informationssicherung MELANI

Schwarztorstrasse 59
3003 Bern
max.klaus@isb.admin.ch