CYBER CRIME
Dezernat 54

Wir wollen,
dass Sie
sicher leben!

Täterprofiling und Phänomene

Matthias Schmidt

Cybercrime

TÄTERPROFIL

Zeitreiserätsel

Täter

Fotolia

Kriminalistische Betrachtung der Modi Operandi

Fotolia

Modus Operandi

Fotolia

Vorgehensweise

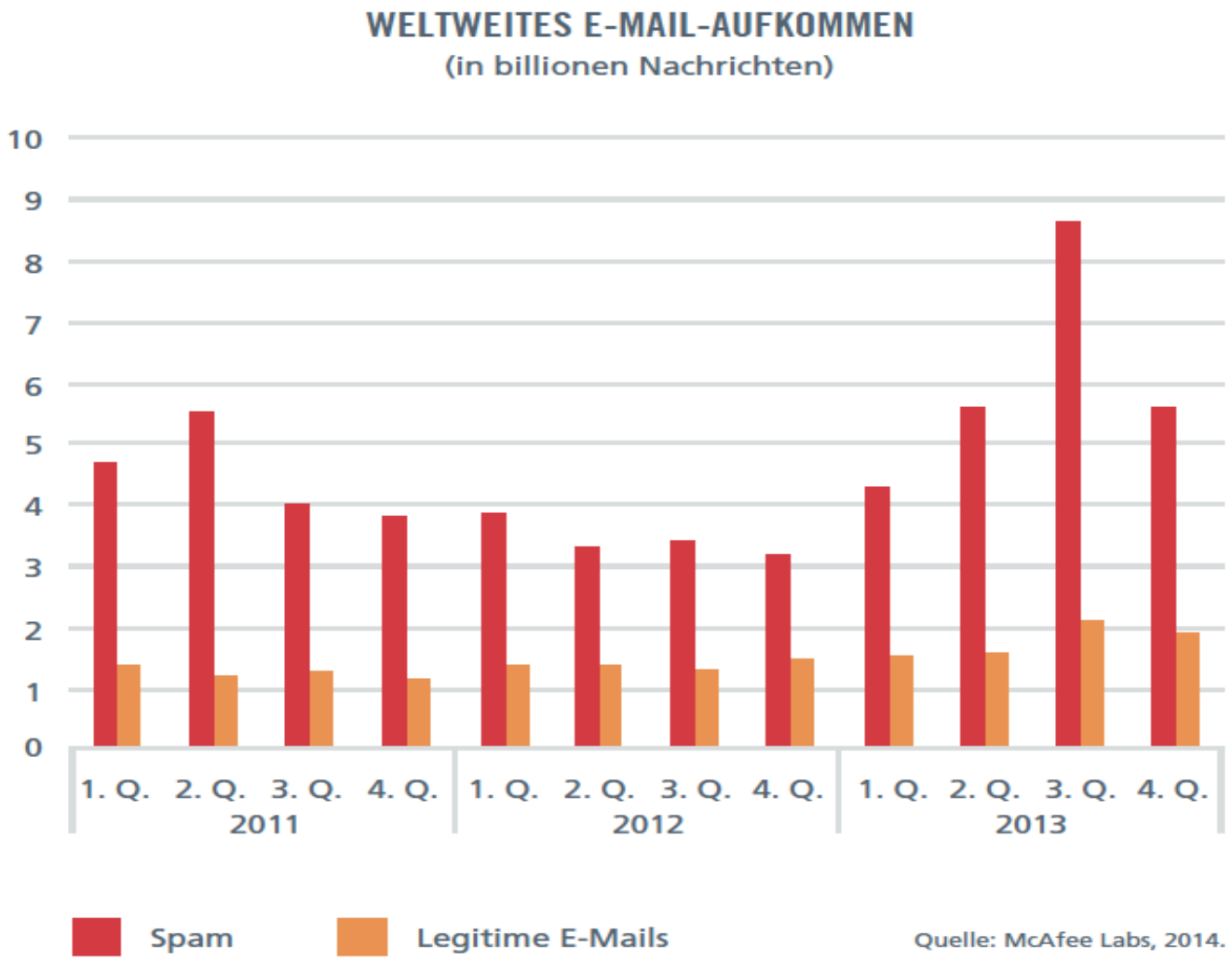
- Nutzung bekannter Schwächen
  - Passwort
  - Neugierde
  - Autoritätsgläubigkeit
  - Anstand
  - Bequemlichkeit
  - Verdrängung/Verschiebung
  - Wissenslücken
  - Verwahrung von Geräten
  - alles was sich anbietet

Passwörter

Rank	Password	Change from 2013
1	123456	Unchanged
2	password	Unchanged
3	12345	Up 17
4	12345678	Down 1
5	qwerty	Down 1
6	123456789	Unchanged
7	1234	Up 9
8	baseball	New
9	dragon	New
10	football	New
11	1234567	Down 4
12	monkey	Up 5
13	letmein	Up 1
14	abc123	Down 9
15	111111	Down 8
16	mustang	New
17	access	New
18	shadow	Unchanged
19	master	New
20	michael	New
21	superman	New
22	696969	New
23	123123	Down 12
24	batman	New
25	trustno1	Down 1

[Image credit: Alex E. Proimos/Flickr]

Spam


WELTWEITES E-MAIL-AUFKOMMEN
(in billionen Nachrichten)
10
9
8
7
6
5
4
3
2
1
0
1. Q. 2. Q. 3. Q. 4. Q.
2011
1. Q. 2. Q. 3. Q. 4. Q.
2012
1. Q. 2. Q. 3. Q. 4. Q.
2013
Spam
Legitime E-Mails
Quelle: McAfee Labs, 2014.

Fazit

„Ewige Wachsamkeit ist der Preis der Freiheit.“

(Thomas Jefferson 1743 - 1826)

Cybercrime

PHÄNOMENE

Ransomware – Bundestrojaner

BUNDESPOLIZEI

Bundesnetzagentur

Alle Aktivitäten des Computers wurden aufgenommen. Alle Ihre Dateien ist verschlüsselt.

ACHTUNG!

Sie haben die Verletzung von Urheberrechten und Schutzrechten (Video, Musik, Software) und illegal Inhalt unterzogen wurde, verstößt damit gegen Artikel 1, Abschnitt 8, Ziffer 8, die auch als Urheberrecht des Strafgesetzbuches der Deutschland. Artikel 1, Abschnitt 8, 8 Ursache des Strafgesetzbuches sieht eine Geldstrafe von 2-500 Mindestlöhne oder ein Freiheitsentzug von zwei bis acht Jahren.

Sie wurden Anzeigen oder Verteilen verboten pornografischen Inhalten (Kinder Porno Fotos und etc wurden auf Ihrem Computer gefunden). So gegen Artikel 202 des Strafgesetzbuches der Deutschland, bestimmt Artikel 202 des Strafgesetzbuches für einen Freiheitsentzug von vier bis zwölf Jahren.

Illegaler Zugriff von Ihrem PC wurde ohne Ihr Wissen oder Ihre Zustimmung eingeleitet, Ihren PC von Malware infiziert werden können, so verstoßen Sie gegen das Gesetz über die nachlässige Verwendung von Personal Computer. Artikel 210 des Strafgesetzbuches sieht eine Geldstrafe von bis zu 100.000€ und / oder Freiheitsentzug von vier bis neun Jahren.

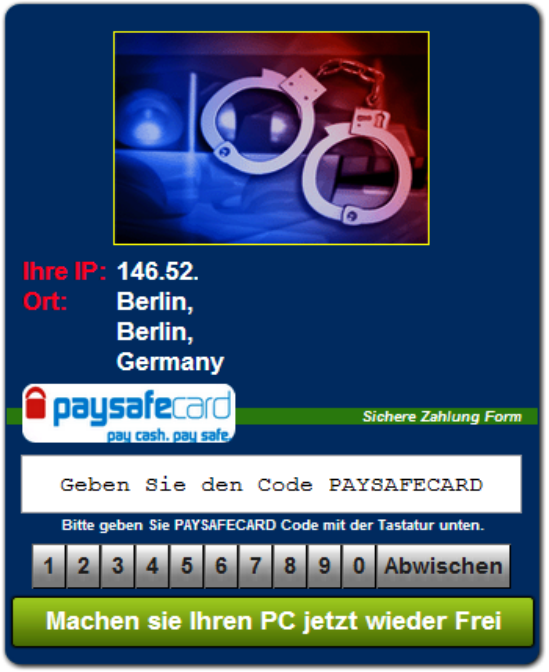
Nach der Änderung des Strafgesetzbuches der Deutschland vom 28. Mai 2011, diese Rechtsverletzung (wenn es sich nicht wiederholt - zum ersten Mal) als bedingte berücksichtigt werden, wenn Sie die Geldbuße von den Staaten zahlen.

Um Ihren Computer zu entsperren und andere rechtliche Konsequenzen zu vermeiden, sind Sie verpflichtet, einen Erlass-Gebühr von 100€ zu zahlen. Vor Ort durch PAYSAFECARD (Sie müssen PAYSAFECARD Karte kaufen, laden Sie es mit 100€ und geben Sie den Code). Sie können den Code an jeder Werkstatt oder Tankstelle kaufen. PAYSAFECARD ist in den Filialen bundesweit verfügbar.

Wie bezahle ich die Geldbuße auf meinem PC zu entsperren?

1. Finden Sie einen Einzelhandel in der Nähe von PAYSAFECARD:

2. Pick up the PAYSAFECARD bei Prepaid-Auswahl und laden Sie es mit Bargeld an der Kasse auf.
3. Geben Sie Ihre PAYSAFECARD Code und Eintragen "Machen sie Ihren PC jetzt wieder Frei"



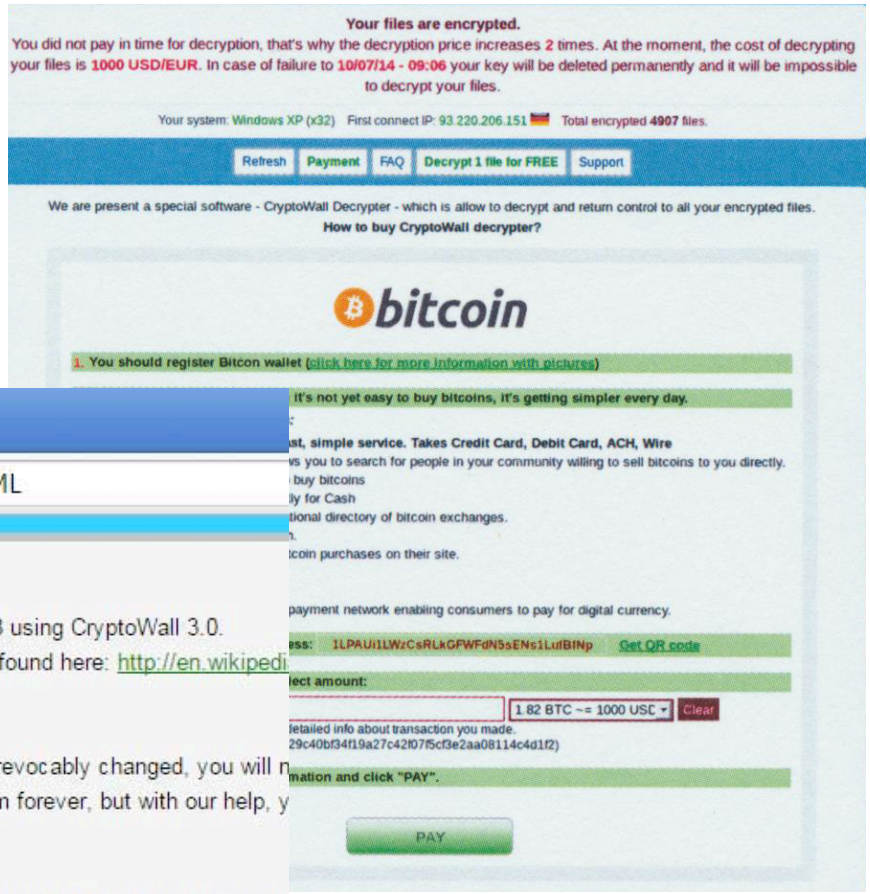
Bitte beachten Sie: Geldbuße kann nur innerhalb von **12** Stunden bezahlt werden. Sobald 12 Stunden verstreichen, verfällt die Möglichkeit, die Geldbuße zu zahlen.

Alle PC-Daten werden festgenommen und Strafverfahren gegen Sie eingeleitet werden, wenn die Geldbuße nicht bezahlt wird.

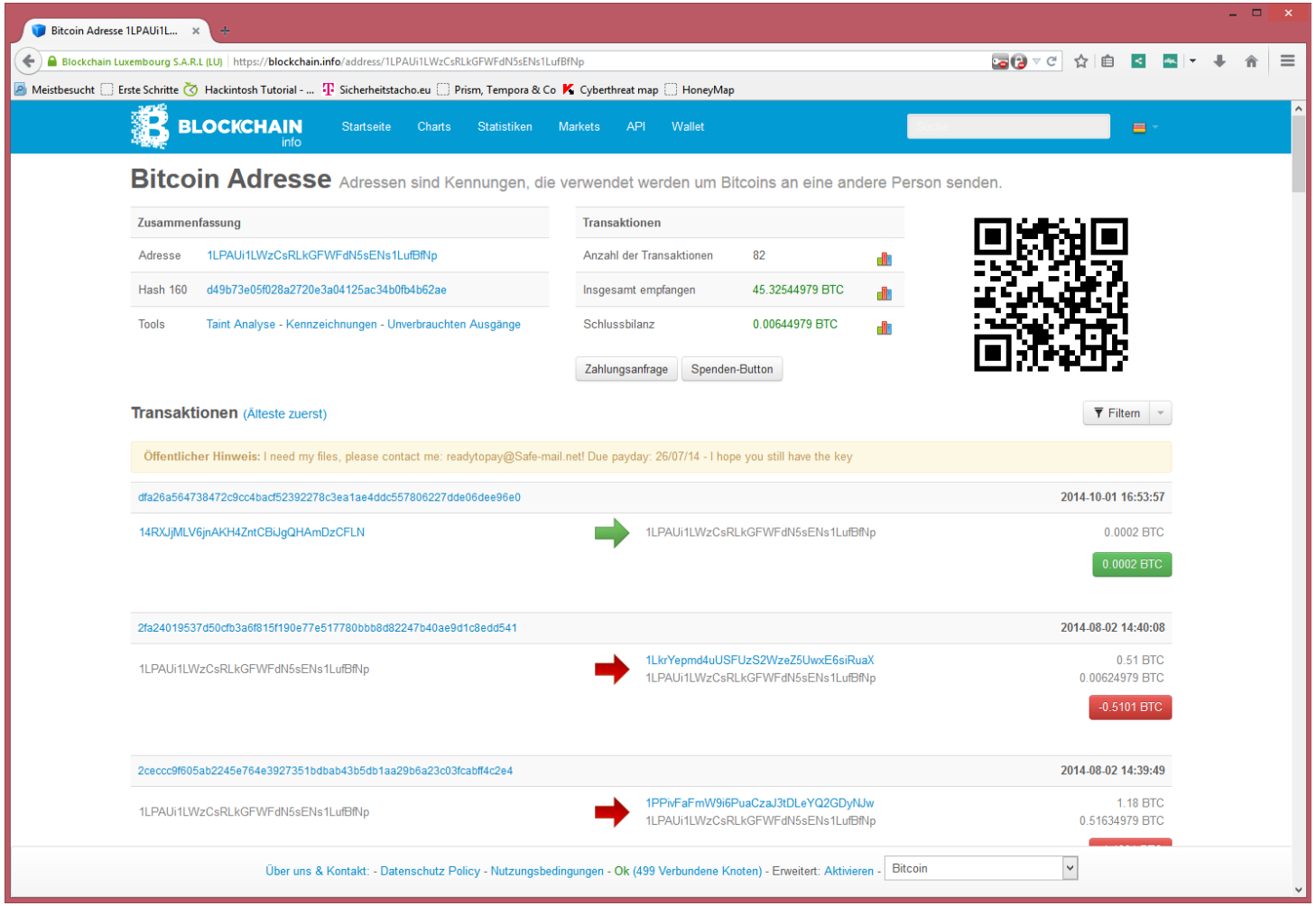
Support

- Cmd → assoc → ZFSendToTarget=CLSID\{888DCA60-FC0A-11CF-8F0F-00C04FD7D062} (vorlesen lassen)
- Ereignisanzeige öffnen Fehlerprotokoll ☺
- Fernwartungssoftware z. B. Ammy Admin (http://www.ammyy.com/de/s_home.htm)
- Kontodaten oder Kreditkartendaten werden abgefragt und abgebucht ……
- Rechner ist unbrauchbar

Ransomware – Cryptowall



Cryptowall



Quelle: www.blockchain.info

Briefe von der Bank etc.

VISA MasterCard

[redacted]

München, 20.07.2012

Aktualisierung unserer Sicherheitssysteme:
Anlegung Ihres neuen Online-Passworts

[redacted] ist das Kreditkartenverwaltungscenter der Deutschen Bundesbank. Damit sind wir für die Sicherheit Ihrer MasterCard/VISA-Kreditkarte verantwortlich.

Aufgrund des zunehmenden Betruges mittels rechtswidrig erlangter Daten von Zahlungskarten im Internet sehen wir uns dazu gezwungen, national ein neues Sicherheitssystem einzuführen. Das bisherige 3D-Secure-System wird somit ergänzt.

Für Ihre Kreditkarte müssen Sie online ein neues persönliches Passwort für Internetzahlungen anlegen.

Anlegung Ihres Sicherheitspasswortes

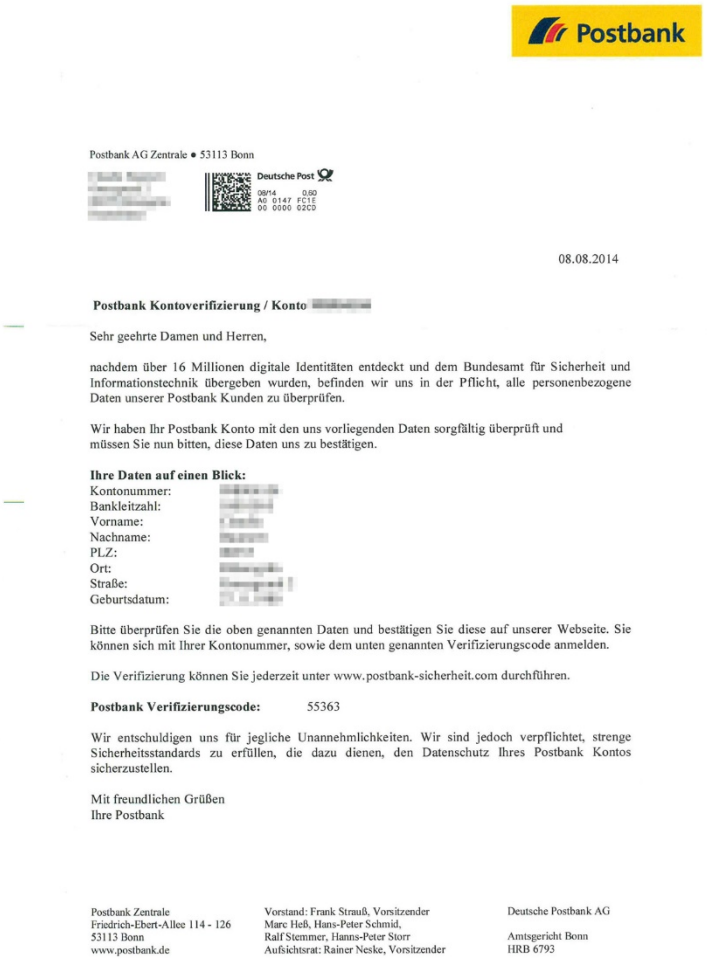
Bitte legen Sie Ihre persönliches Sicherheitspasswort unter folgender Internetseite an:
http://www.initiative-online-passwort.com/

MasterCard VISA

[redacted]

Sollten Sie Ihrer Karte binnen 14 Tagen keinen Sicherheitscode hinzugefügt haben, können Sie leider keine weitere Transaktionen mit Ihrer Kreditkarte tätigen!

Mit freundlichen Grüßen



Postbank

Postbank AG Zentrale • 53113 Bonn

[redacted]

Deutsche Post
08/14 0,60
A0 0147 FC1E
00 0000 02C0

08.08.2014

Postbank Kontoverifizierung / Konto [redacted]

Sehr geehrte Damen und Herren,

nachdem über 16 Millionen digitale Identitäten entdeckt und dem Bundesamt für Sicherheit und Informationstechnik übergeben wurden, befinden wir uns in der Pflicht, alle personenbezogene Daten unserer Postbank Kunden zu überprüfen.

Wir haben Ihr Postbank Konto mit den uns vorliegenden Daten sorgfältig überprüft und müssen Sie nun bitten, diese Daten uns zu bestätigen.

Ihre Daten auf einen Blick:
Kontonummer: [redacted]
Bankleitzahl: [redacted]
Vorname: [redacted]
Nachname: [redacted]
PLZ: [redacted]
Ort: [redacted]
Straße: [redacted]
Geburtsdatum: [redacted]

Bitte überprüfen Sie die oben genannten Daten und bestätigen Sie diese auf unserer Webseite. Sie können sich mit Ihrer Kontonummer, sowie dem unten genannten Verifizierungscode anmelden.

Die Verifizierung können Sie jederzeit unter www.postbank-sicherheit.com durchführen.

Postbank Verifizierungscode: 55363

Wir entschuldigen uns für jegliche Unannehmlichkeiten. Wir sind jedoch verpflichtet, strenge Sicherheitsstandards zu erfüllen, die dazu dienen, den Datenschutz Ihres Postbank Kontos sicherzustellen.

Mit freundlichen Grüßen
Ihre Postbank

Postbank Zentrale
Friedrich-Ebert-Allee 114 - 126
53113 Bonn
www.postbank.de

Vorstand: Frank Strauß, Vorsitzender
Marc Heß, Hans-Peter Schmid,
Ralf Stemmer, Hanns-Peter Storr
Aufsichtsrat: Rainer Neske, Vorsitzender

Deutsche Postbank AG

Amtsgericht Bonn
HRB 6793

Fallbeispiele – E-Mail

Fotolia

Fallbeispiel

Dropbox & Howrse

CEO - Fraud

Schützen

Wirksame Mechanismen

- IT-Basisschutz wehrt etwa 80 % der Angriffe ab
- IT-Sicherheitskonzept
- Awareness
- Policies
- Prozesse
- **Krisenmanagement → 100%igen Schutz gibt es nicht!!!**

Krisenmanagement

- Szenarien → **Risikobewertung durch Experten**
- Klassifizierung von Daten
- Eskalationsstufen
- Dokumentation
- Verantwortlichkeiten
- Gremien
- Informationsfluss intern/extern
- Berichtspflichten und Öffentlichkeitsarbeit
- Handlungsempfehlungen

Handlungsempfehlung für die Wirtschaft

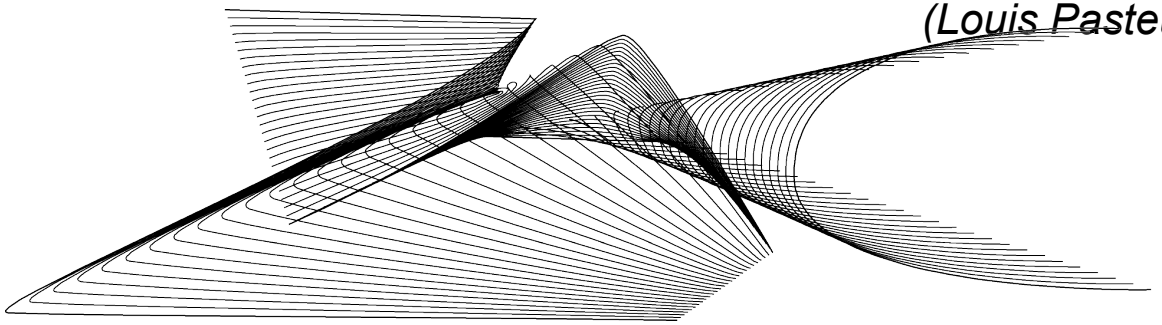
Bundeskriminalamt

Zeitreiserätsel - Lösung

Fazit

„Das Glück bevorzugt den, der vorbereitet ist“

(Louis Pasteur 1822-1895)



Zentrale Ansprechstelle Cybercrime – ZAC
Maillingerstraße 15, 80636 München
Telefon 089/1212-3300
zac@polizei.bayern.de

Matthias Schmidt
Tel: 089/1212-3533
matthias.schmidt@polizei.bayern.de