Security-Webinar

Februar 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

- Security im Januar/Februar
  - OpenSSL
  - Magento
  - Piwik
  - Wordpress
- Botnet verteilt Virenscanner
- Taviso gegen Comodo
- Server-Side Request Forgery
- Ein NSA-Mitarbeiter berichtet

OpenSSL Security

filoo®
member of Thomas Krenn Group

- Kritische Sicherheitslücke in OpenSSL 1.0.2
  - Behoben in 1.0.2f
  - Fehler im Schlüsselaustausch per Diffie-Hellman
  - Kommunikation u.U. entschlüsselbar
  - Betroffene Anwendungen: Unklar
- Sicherheitsproblem in OpenSSL 1.0.2 / 1.0.1
  - Behoben in 1.0.1r, 1.0.2f
  - Client kann (unsichere) SSLv2-Verbindungen forcieren
- Weitere Fixes gegen Logjam u.a.

Magento Security

filoo®
member of Thomas Krenn Group

- Archetypische „Stored XSS“
  - In E-Mail-Adresse von Kunden
  - In Bestell-Kommentaren
  - In HTTP-Header X-Forwarded-For
  - Alle XSS erlauben es, Admin-Cookies zu stehlen
- CSRF-Token nicht validiert
- CSRF führt zu Ausführung von Admin-Aktionen
- Administratoren können PHP-Code ausführen
- Gefixt in Magento CE 1.9.2.3, EE 1.14.2.3, EE 2.0.1
- Betroffen: Alle davor (potentiell)

Piwik 2.16 LTS

filoo®
member of Thomas Krenn Group

- Piwik 2.16.0 bietet LTS-Support (12 Monate)
- Auch über das Release von Piwik 3 hinweg
- Behebt Cross-Site Scripting
  - Keine Details bekannt
  - Einstufung: „Critical“

Botnet verteilt Avira

filoo®
member of Thomas Krenn Group

- Das Botnet „Dridex“ verteilt normalerweise Malware
  - Word-Dokumente mit Makros
  - Keylogger, Bankphishing
- Kürzlich begann es, Avira auszuliefern
  - Aktueller, unmodifizierter (signierter) Installer
- Angegriffene Nutzer erhalten Virenschutz statt Viren
- Unklare Motivation
  - Seltsamer Schachzug der Botnet-Betreiber?
  - Botnet gehacked & Whitehat „repariert“ Clients?

Wordpress Security

filoo®
member of Thomas Krenn Group

- SSRF-Lücke
  - Server-Side Request Forgery
  - Erlaubt Portscans auf IP 0.0.0.0
- Redirect-Lücke
  - Möglichkeit, präparierte URL in Kommentare zu schleusen, um z.B. Spam zu bewerben
  - Laut Changeset URLs mit http://user:pass@host
- Behoben in WP 4.4.2

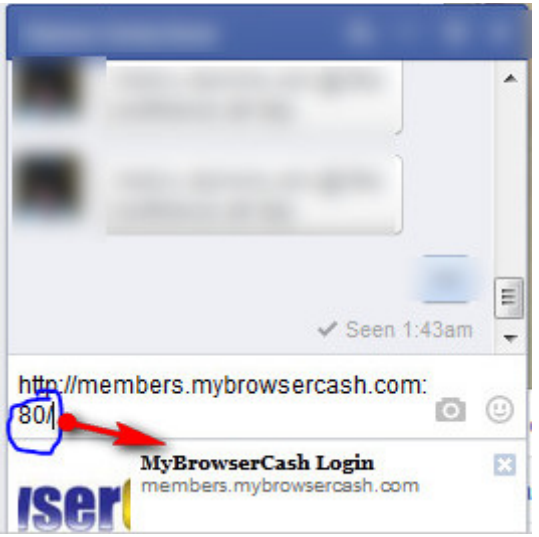
SSRF? Was ist das?

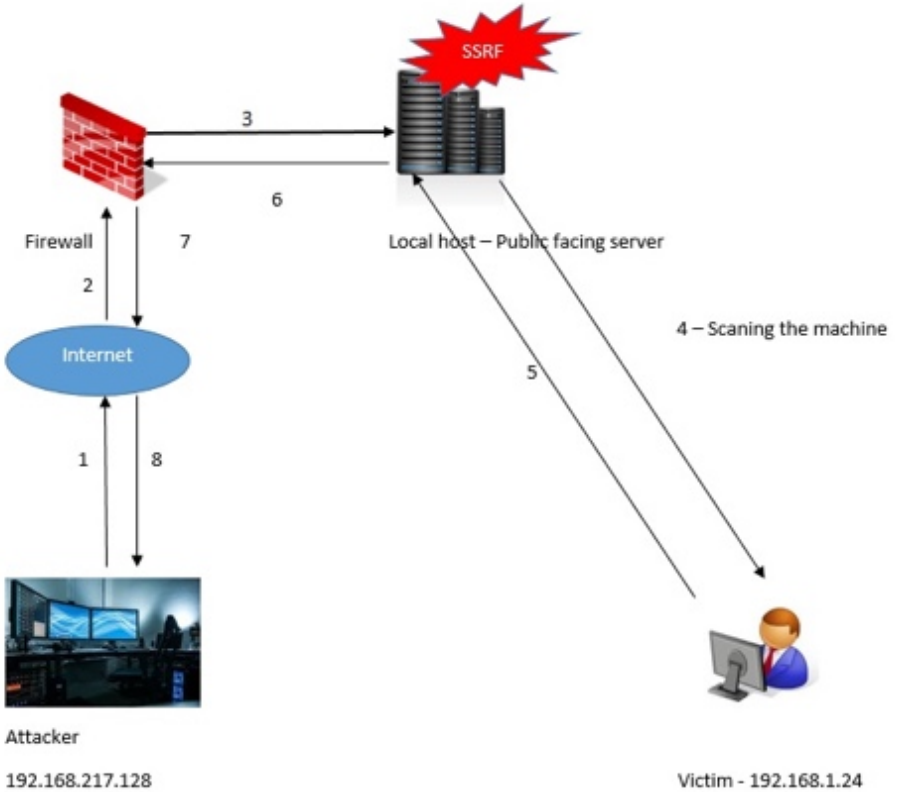
filoo®
member of Thomas Krenn Group

- Angriff gegen interne Server mithilfe ihrer “Kollegen“
  - Webserver mit Interface ins WAN und LAN
  - Sprungbrett ins LAN
- Z.B. über Kommentarfelder etc.
  - Ausnutzen von „Live Previews“ von Links
  - Fehlerhafte Linkvalidierung
- Portscan / RFI / LFI auf interne Maschinen

SSRF

filoo®
member of Thomas Krenn Group





Bildquelle: Network Intelligence Consulting

QEMU Security

filoo®
member of Thomas Krenn Group

- Ein ganzer Stapel Probleme in QEMU/KVM
  - Fehler in verschiedenen Treibern/Emulationen (virtio, pc-net, PCI-Emulator, eepro100, VNC, USB, MegaRAID, IDE, ...)
- Auswirkungen meist: Denial of Service
  - Gast crashed
  - Möglicherweise Ressourcen auf Host verbraucht
- In manchen Fällen „possible code execution“
- Behoben in aktuellen Versionen
  - Debian Jessie: 1:2.1+dfsg-12+deb8u5a

Tavis Ormandy vs. Chromodo

filoo®
member of Thomas Krenn Group

- Comodo Internet Security installiert einen „sicheren“ Browser
  - Chrome mit Addons
- Chromodo beachtet „Same Origin Policy“ nicht
  - Das führt zu extrem simplem Cookie-Klau
- Comodo reagiert extrem professionell
  - Proof of Concept Code wird blockiert
  - Lücken im Browser noch vorhanden
- Lustiges Bug-Ticket:
  - https://code.google.com/p/google-security-research/issues/detail?id=704

NSA / TAO Mitarbeiter

filoo®
member of Thomas Krenn Group

- Vortrag auf USENIX Enigma 2016
  - Rob Joyce, Chief of Tailored Access Operations, NSA
- Wie verteidigt man sich gegen einen Angreifer vom Geheimdienst?
  - „If you want to defend your network, you have to know your network.“
  - „You know what devices you intended to run, we know what devices you actually run.“
  - Reduce the attack surface
  - Angriffe meist über: E-Mail, Web, USB-Medien
- https://www.youtube.com/watch?v=bDJb8WOJYdA

Vorschau

filoo®
member of Thomas Krenn Group

_ Nächster Termin: 09.03.2016

_ 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