Security-Webinar

März 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: Stefanie Jerchel
  - 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 März
  - Glibc-Lücke
  - DROWN-SSL-Lücke
  - Cachebleed
  - Linux Mint Hack
  - Ransomware
  - Drupal Sicherheitsupdate

Glibc Bug

filoo®
member of Thomas Krenn Group

- Stack-based buffer Overflow in glibc
- In Funktion getaddrinfo()
  - “The getaddrinfo() function is used to get a list of IP addresses and port numbers for host hostname and service servname.“
- Kann mit bösartigem DNS-Paket ausgelöst werden
  - 2048+ Bytes groß
- Buffer Overflow – sorgt für Anwendungs-Crashes
  - Kein funktionierender Exploit mit Code-Ausführung bekannt

Glibc Bug - Mitigation

filoo®
member of Thomas Krenn Group

- Glibc updaten!
  - Alle Versionen seit 2.9 verwundbar
  - Aktuelle Distro-Pakete für relevante Distributionen
  - Embedded Devices / Appliances nicht vergessen!
- Synology / QNAP NAS Patches
- Vmware ESXi 5.5/6.0
  - 5.5, 6.0 gefixt mit Patch
- Bei eigenen Appliances: Hersteller-Support fragen!
- Mitigation per Firewall: Übergroße DNS-Responses filtern (>2048 Bytes UDP/TCP)

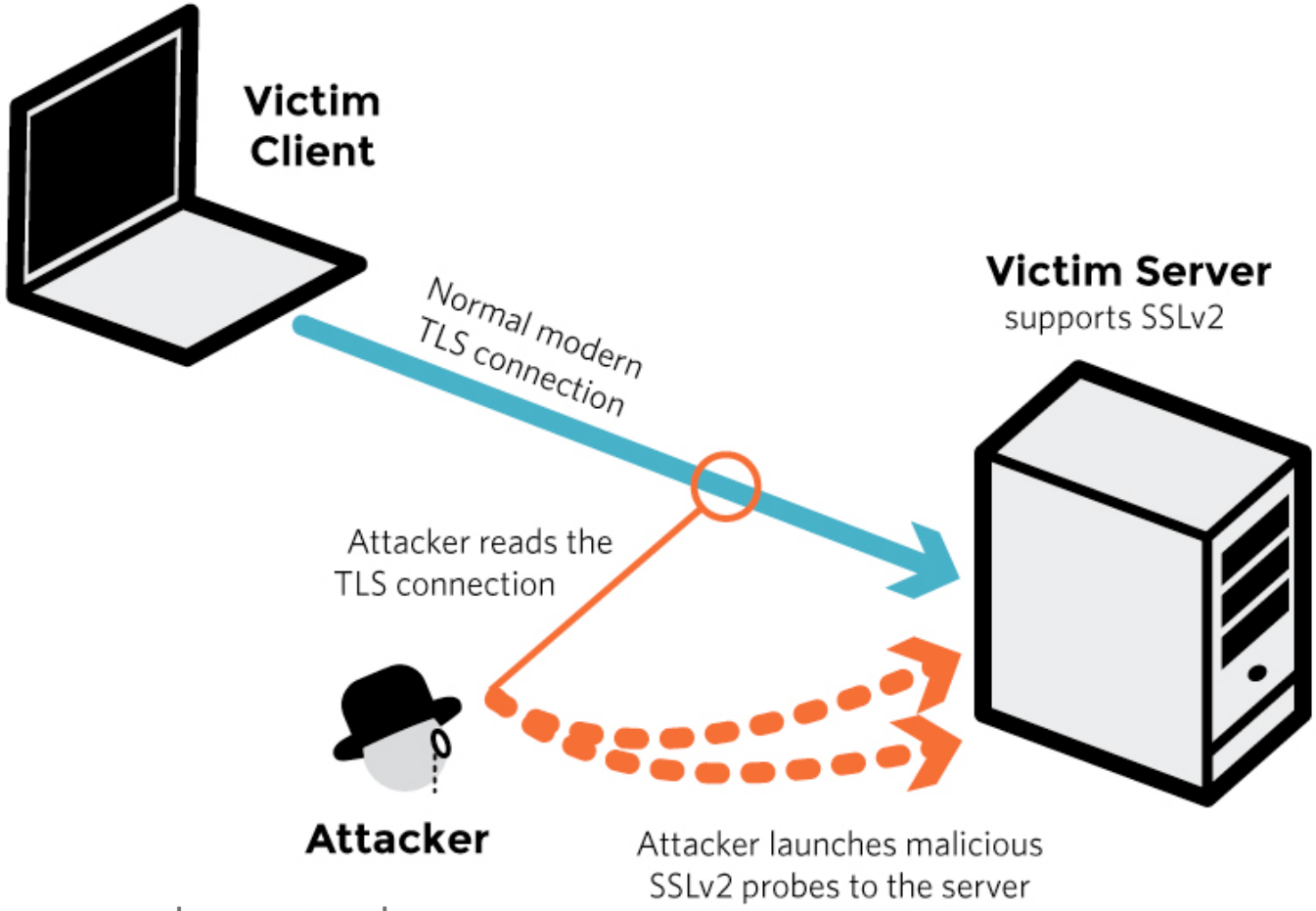
DROWN

filoo®
member of Thomas Krenn Group

- Sicherheitslücke in SSLv2
- Kann genutzt werden, um TLS Sessions nachträglich zu entschlüsseln
  - Rechenaufwand notwendig: Ca. 440$ und Amazon-Cloud
- Angreifbar: Alle Serverdienste, die SSLv2 noch unterstützen
- Durch mehrfach genutzte Schlüssel/Zertifikate u.U. indirekte Angriffe
  - Z.B: Mailserver angreifbar, Webserver nicht
  - Über shared Key: Angriff auch auf Webserver

DROWN

filoo®
member of Thomas Krenn Group



_ Quelle: www.drownattack.com

DROWN-Vorgehen

filoo®
member of Thomas Krenn Group

- Angreifer benötigt eine Möglichkeit, SSL-Traffic abzuhören
  - Abhören von 1000 TLS-Sessions
- Aufbau von 40000 SSLv2-Verbindungen
- Durchführen von 2^50 symmetrischen Verschlüsselungsoperationen
  - Dadurch Herausfinden eines TLS-Session-Keys
  - Dadurch Entschlüsseln von TLS-Traffic möglich
- Zeitaufwand: 8h mit EC2
  - Stark reduzierter Zeitaufwand durch Ausnutzen einer weiteren OpenSSL-Lücke: Unter 1 Minute auf Standard-PC

DROWN-Schutz

filoo®
member of Thomas Krenn Group

- SSLv2 komplett abschalten
  - Apache: SSLProtocol All -SSLv2 -SSLv3
  - Nginx: ssl_protocols TLSv1 TLSv1.1 TLSv1.2
  - Postfix (SSLv2 per Default aus):
    - smtp_tls_protocols = !SSLv2, !SSLv3
    - smtpd_tls_protocols = !SSLv2, !SSLv3
- Auf allen Servern, die dasselbe Zertifikat nutzen, prüfen
- Auf aktuelles OpenSSL upgraden

Drown-Links

filoo®
member of Thomas Krenn Group

- https://www.openssl.org/blog/blog/2016/03/01/an-openssl-users-guide-to-drown/
- https://drownattack.com/
- https://drownattack.com/drown-attack-paper.pdf
- https://test.drownattack.com/

Cachebleed

filoo®
member of Thomas Krenn Group

- Angriff gegen CPU-Caches auf Sandy-Bridge-CPUs
- Auslesen von (Teilen von) RSA-Schlüsseln
- Funktioniert nur unter Nebenbedingungen
  - Angreifer-Prozeß muß im selben Hyperthread laufen wie Opfer
- Rauschen durch paralelle Cachezugriffe (VMs etc.) erschwert Angriff
- Praktische Realisierbarkeit: Gering
- Angriff wird mit aktuellem OpenSSL ausgehebelt

Linux-Mint-Hack

filoo®
member of Thomas Krenn Group

- Linux Mint ist eine Linux-Distribution
  - U.A. für unsere Cloud-Plattform verfügbar
- Wurde in mindestens zwei Anläufen gecrackt
- „Laxe Rechtevergabe“ in Wordpress war verantwortlich
- Resultat: Schadcode in Distributions-Downloads
- Mehr Informationen inkl. Signaturen:
  - http://blog.linuxmint.com/?p=2994

Locky-Ransomware

filoo®
member of Thomas Krenn Group

- „Locky“ hat zehntausende Rechner infiziert
  - Eintrittsvektor über infizierte Mails mit Office-Dokumenten
  - Bösartiges Javascript in Webseiten
  - Exploit-Kits (Flash-, Java-, Browser-Bugs)
- Alle Dateien, die der Rechner erreicht, werden crypted
  - Auch Dateien auf Netzwerkshares
  - AES-Verschlüsselung, derzeit nicht leicht knackbar
- Lösegeldforderung von 0,5 BC
  - Ca. 180 €

OSX-Ransomware

filoo®
member of Thomas Krenn Group

- Kryptotrojaner (Ransomware) meist für Windows
- Erste bekannte Version für MacOSX „KeRanger“
- Kommt huckepack mit Transmission (BT-Client)
  - Download-Server von Transmission wurde gehacked
  - Kompromittierte .dmg-Datei
- Verschlüsselt verschiedene Dateitypen
  - 1 BC Lösegeld (ca. 370 €)
  - Beginn der Verschlüsselung nach 3 Tagen
  - Command&Control-Server muß erreichbar sein
- Haben Sie Transmission 2.90? Sofort auf 2.92 updaten!

Webserver-Ransomware

filoo®
member of Thomas Krenn Group

- CTB-Locker befällt Websites
- Schädling in PHP entwickelt
- Befällt schreibbare Dateien des Users
  - Oft der Webserver-user (httpd / www-data)
  - Fast 600 Dateitypen vom PHP-Skript bis zum Nintendo-Emulator
- AES-Verschlüsselung
- Lösegeld von initial 0,4 BC
  - Steigt nach erstem Termin an

Drupal

filoo®
member of Thomas Krenn Group

- Verschiedene Security-Bugs im Drupal-Core
  - Versionen 6.x, 7.x, 8.x
  - Advisory ID: SA-CORE-2016-001
- Offener Redirect, HTTP Header Injection, Userverwaltung etc.
- Gefixte Versionen:
  - 6.38
  - 7.43
  - 8.0.4

Vorschau

filoo®
member of Thomas Krenn Group

- Wir stellen auf zweimonatigen Turnus um!
- Im April gibt's ein Webinar zum Absichern von Rootservern
- Nächster Termin für dieses Webinar: 11.05.2016
- 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