



Was Dein ist, ist Mein: Datensicherheit aus der Angreiferperspektive

Jens Liebchen - RedTeam Pentesting GmbH
jens.liebchen@redteam-pentesting.de
<http://www.redteam-pentesting.de>

Welttag des geistigen Eigentums, Aachen, 26. April 2016



Einleitung
Krypto-Trojaner
Die „typische“ IT
Social Engineering
Physische Sicherheit
Fazit

RedTeam Pentesting, Daten & Fakten
Datensicherheit

RedTeam Pentesting, Daten & Fakten

- ★ Gegründet 2004 in Aachen
- ★ Spezialisierung ausschließlich auf Penetrationstests
- ★ Weltweite Durchführung von Penetrationstests
- ★ Forschung im Bereich der IT-Sicherheit





Einleitung

Krypto-Trojaner

Die „typische“ IT

Social Engineering

Physische Sicherheit

Fazit

RedTeam Pentesting, Daten & Fakten

Datensicherheit

Datensicherheit

Woran denken Sie, wenn Sie an
Datensicherheit denken?



Einleitung
Krypto-Trojaner
Die „typische“ IT
Social Engineering
Physische Sicherheit
Fazit

RedTeam Pentesting, Daten & Fakten
Datensicherheit

Datensicherheit

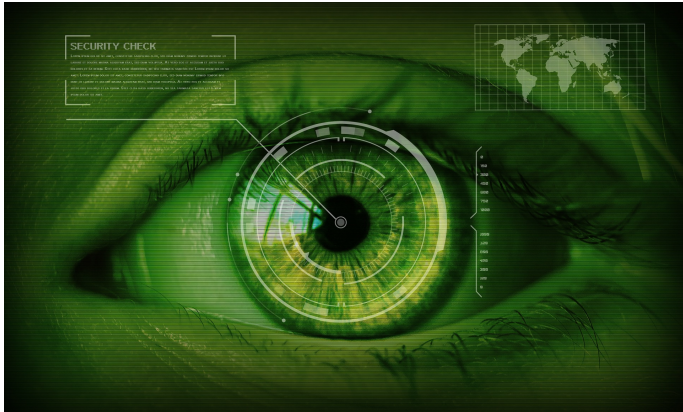




Einleitung
Krypto-Trojaner
Die „typische“ IT
Social Engineering
Physische Sicherheit
Fazit

RedTeam Pentesting, Daten & Fakten
Datensicherheit

Datensicherheit





Einleitung
Krypto-Trojaner
Die „typische“ IT
Social Engineering
Physische Sicherheit
Fazit

RedTeam Pentesting, Daten & Fakten
Datensicherheit

Datensicherheit





Datensicherheit aus der Angreiferperspektive

- ★ Sicherheit muss ein Gesamtkonzept sein, denn ein Angreifer sucht sich die schwächste Stelle
- ★ Kurz: Egal wie ein Angreifer an die Daten kommt, Hauptsache, er erreicht sein Ziel!
- ★ Im Folgenden: Einige Beispiele





Einleitung
Krypto-Trojaner
Die „typische“ IT
Social Engineering
Physische Sicherheit
Fazit

Aktuelles
Krypto-Trojaner: Was tun?
Backup
Was ist passiert?

Phänomen Krypto-Trojaner



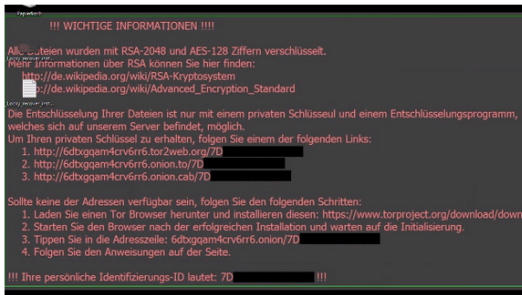


Phänomen Krypto-Trojaner

Krypto-Trojaner Locky wütet in Deutschland: Über 5000 Infektionen pro Stunde

19.02.2016 06:15 Uhr - Ronald Eikenberg

 vorlesen



!!! WICHTIGE INFORMATIONEN !!!!

Alle Dateien wurden mit RSA-2048 und AES-128 Ziffern verschlüsselt.
Mehr Informationen über RSA können Sie hier finden:
<http://de.wikipedia.org/wiki/RSA-Kryptosystem>
http://de.wikipedia.org/wiki/Advanced_Encryption_Standard

Die Entschlüsselung Ihrer Dateien ist nur mit einem privaten Schlüssel und einem Entschlüsselungsprogramm, welches sich auf unserem Server befindet, möglich.
Um Ihren privaten Schlüssel zu erhalten, folgen Sie einem der folgenden Links:

1. <http://6dbxgqam4crv6rr6.tor2web.org/7D>
2. <http://6dbxgqam4crv6rr6.onion.to/7D>
3. <http://6dbxgqam4crv6rr6.onion.cab/7D>

Sollte keine der Adressen verfügbar sein, folgen Sie den folgenden Schritten:

1. Laden Sie einen Tor Browser herunter und installieren diesen: <https://www.torproject.org/download/download>
2. Starten Sie den Browser nach der erfolgreichen Installation und warten auf die Initialisierung.
3. Tippen Sie in die Adresszeile: 6dbxgqam4crv6rr6.onion.to/7D
4. Folgen Sie den Anweisungen auf der Seite.

!!! Ihre persönliche Identifizierungs-ID lautet: 7D [redacted] !!!

Quelle: <https://www.heise.de/-3111774>



Einleitung
Krypto-Trojaner
Die „typische“ IT
Social Engineering
Physische Sicherheit
Fazit

Aktuelles
Krypto-Trojaner: Was tun?
Backup
Was ist passiert?

Phänomen Krypto-Trojaner

SPIEGEL ONLINE NETZWELT Login | Registrierung

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Reise | Auto | Stil

Nachrichten > Netzwelt > Web > Internetkriminalität > Lösegeld-Trojaner: US-Polizisten gehen auf Erpressung ein

Ransomware: US-Polizisten zahlen Lösegeld für ihre Daten



Technik im Polizeiauto: Die Polizisten überwiesen den Erpresser Bitcoin

Eine amerikanische Polizeistation ist Opfer eines Lösegeld-Trojaners geworden. Doch statt ruhig zu bleiben, zahlten die Polizisten rund 600 Dollar an die Erpresser. Dabei hätte es vielleicht eine viel einfachere und preiswertere Lösung gegeben.

Quelle: <http://spon.de/aervi>



Einleitung
Krypto-Trojaner
Die „typische“ IT
Social Engineering
Physische Sicherheit
Fazit

Aktuelles
Krypto-Trojaner: Was tun?
Backup
Was ist passiert?

Phänomen Krypto-Trojaner

Cyber-Attacke auf Aachener Krankenhaus

Von Dieter Haack



Kriminelle haben das Computersystem des Aachener Marienhospitals lahmgelegt. Nach einer sogenannten Cyber-Attacke sind alle Computer-Systeme der Klinik abgeschaltet worden.

Die Folgen für die Klinik sind gravierend: Bis voraussichtlich Ende der Woche kann das Krankenhaus nicht am Notaufnahme-System der Feuerwehr teilnehmen. Denn auch die Radiologie, die für die schnelle Untersuchung von Notfallpatienten wichtig ist, ist betroffen. Alle Patientendaten seien gerettet worden, heißt es.

Quelle: <http://www1.wdr.de/nachrichten/rheinland/cyber-attacke-auf-krankenhaus-100.html>



Einleitung
Krypto-Trojaner
Die „typische“ IT
Social Engineering
Physische Sicherheit
Fazit

Aktuelles
Krypto-Trojaner: Was tun?
Backup
Was ist passiert?

Krypto-Trojaner: Was jetzt?

★ Bezahlen?



Einleitung
Krypto-Trojaner
Die „typische“ IT
Social Engineering
Physische Sicherheit
Fazit

Aktuelles
Krypto-Trojaner: Was tun?
Backup
Was ist passiert?

Krypto-Trojaner: Was jetzt?

- ★ Bezahlen?
 - ★ Führt zu mehr/besseren/teureren Erpressungen



Krypto-Trojaner: Was jetzt?

- ★ Bezahlen?
 - ★ Führt zu mehr/besseren/teureren Erpressungen
 - ★ Keinerlei Garantie, dass Daten wiederherstellbar sind



Krypto-Trojaner: Was jetzt?

- ★ Bezahlen?
 - ★ Führt zu mehr/besseren/teureren Erpressungen
 - ★ Keinerlei Garantie, dass Daten wiederherstellbar sind
- ★ Hoffen, dass die Programmierer Fehler gemacht haben?



Krypto-Trojaner: Was jetzt?

- ★ Bezahlen?
 - ★ Führt zu mehr/besseren/teureren Erpressungen
 - ★ Keinerlei Garantie, dass Daten wiederherstellbar sind
- ★ Hoffen, dass die Programmierer Fehler gemacht haben?
 - ★ Fehler bei der Verschlüsselung kamen in der Vergangenheit vor, aber auch Programmierer von sog. Ransomware lernen dazu



Krypto-Trojaner: Was jetzt?

- ★ Bezahlen?
 - ★ Führt zu mehr/besseren/teureren Erpressungen
 - ★ Keinerlei Garantie, dass Daten wiederherstellbar sind
- ★ Hoffen, dass die Programmierer Fehler gemacht haben?
 - ★ Fehler bei der Verschlüsselung kamen in der Vergangenheit vor, aber auch Programmierer von sog. Ransomware lernen dazu
- ★ Seien Sie dankbar! :-)



Backup

⇒ Sie können endlich unter realistischen Bedingungen testen, ob das Wiederherstellen des Backups funktioniert!

- ★ Nur Backups helfen
- ★ Viele Benutzer haben kein Backup
- ★ Viele Benutzer, die denken, Sie hätten ein Backup, haben den Wiederherstellungsprozess nicht getestet
- ★ ⇒ Machen Sie Backups und testen Sie vorher!



Backup

⇒ Sie können endlich unter realistischen Bedingungen testen, ob das Wiederherstellen des Backups funktioniert!

- ★ Nur Backups helfen
- ★ Viele Benutzer haben kein Backup
- ★ Viele Benutzer, die denken, Sie hätten ein Backup, haben den Wiederherstellungsprozess nicht getestet
- ★ ⇒ Machen Sie Backups und testen Sie vorher!



Backup

⇒ Sie können endlich unter realistischen Bedingungen testen, ob das Wiederherstellen des Backups funktioniert!

- ★ Nur Backups helfen
- ★ Viele Benutzer haben kein Backup
- ★ Viele Benutzer, die denken, Sie hätten ein Backup, haben den Wiederherstellungsprozess nicht getestet
- ★ ⇒ Machen Sie Backups und testen Sie vorher!



Backup

- ⇒ Sie können endlich unter realistischen Bedingungen testen, ob das Wiederherstellen des Backups funktioniert!
- ★ Nur Backups helfen
 - ★ Viele Benutzer haben kein Backup
 - ★ Viele Benutzer, die denken, Sie hätten ein Backup, haben den Wiederherstellungsprozess nicht getestet
 - ★ ⇒ Machen Sie Backups und testen Sie vorher!



Backup

⇒ Sie können endlich unter realistischen Bedingungen testen, ob das Wiederherstellen des Backups funktioniert!

- ★ Nur Backups helfen
- ★ Viele Benutzer haben kein Backup
- ★ Viele Benutzer, die denken, Sie hätten ein Backup, haben den Wiederherstellungsprozess nicht getestet
- ★ ⇒ Machen Sie Backups und testen Sie vorher!



Glück gehabt?

- ★ Ein Angreifer hat beliebigen Programmcode auf Ihrem Rechner ausgeführt
- ★ Diesen Angriff haben Sie bemerkt...
- ★ ... leider aber nur, weil der Angreifer es so wollte!

⇒ Andere Angriffe/Industriespionage bemerken Sie normalerweise nicht so einfach!



Glück gehabt?

- ★ Ein Angreifer hat beliebigen Programmcode auf Ihrem Rechner ausgeführt
- ★ Diesen Angriff haben Sie bemerkt...
- ★ ... leider aber nur, weil der Angreifer es so wollte!

⇒ Andere Angriffe/Industriespionage bemerken Sie normalerweise nicht so einfach!



Glück gehabt?

„Law 1: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore. “

(10 Immutable Laws of Security, Microsoft)



Die „typische“ IT

Egal welche Branche, IT sieht ähnlich aus:

- ★ Windows-Domänen
- ★ Linux-Server
- ★ Clients (meist Windows)
- ★ Standard-Soft- und Hardware
- ★ Spezielle Branchensoftware

Aus Angreifersicht: Angriffe sind
größtenteils unabhängig von der Branche

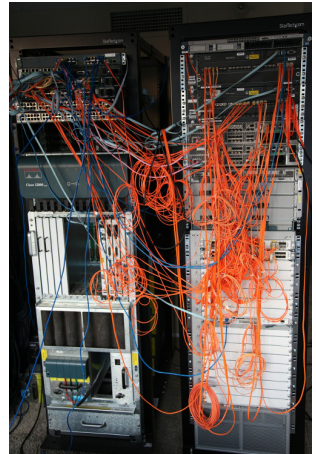




Standard-IT: Probleme

Ähnliche IT-Landschaft heißt leider auch ähnliche oder gleiche Probleme:

- ★ Mangelnde physische Sicherheit (z.B. einfacher Zugriff auf Netzwerke bis hin zu Serverräumen)
- ★ Fehlende Separierung / nur Segmentierung von Netzen
- ★ Keine Updates, d.h. komplett veraltete Systeme mit bekannten Sicherheitslücken

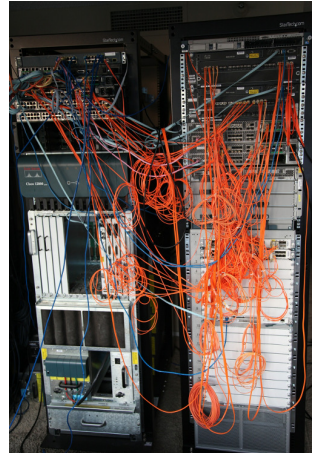




Standard-IT: Probleme

Ähnliche IT-Landschaft heißt leider auch ähnliche oder gleiche Probleme:

- ★ Schwache Passwörter, Standardpasswörter
- ★ Fehlende Authentifizierung und/oder Autorisierung
- ★ Keine oder mangelhafte Verschlüsselung
- ★ Unnötige Dienste
- ★ ...

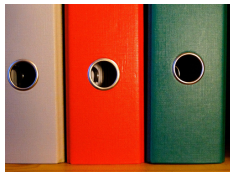




Standard-IT: Lösungen

Jeder Betrieb ist heute abhängig von IT und sollte sich daher Gedanken über diese Abhängigkeit machen:

- ★ Dedizierte IT-Sicherheitsverantwortliche
- ★ Sicherheitskonzepte
 - ★ Update-Management
 - ★ Separierung von Netzen
 - ★ Regelmäßige Überprüfung der eigenen Maßnahmen
- ★ Notfallplan („roter Ordner“)
 - ★ Wer wird im Verdachtsfall informiert?
 - ★ Welche Maßnahmen dürfen/müssen getroffen werden?





Einleitung
Krypto-Trojaner
Die „typische“ IT
Social Engineering
Physische Sicherheit
Fazit

Definition
Hintergründe
Beispiel klassisches Social Engineering

Social Engineering

„Social Engineering [...] nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, unberechtigt an Daten oder Dinge zu gelangen.“

(Wikipedia)



Faktor Mensch

Warum sind Social Engineering-Attacken erfolgreich?

- ★ sensitive Informationen oft nicht intuitiv als solche erkennbar
- ★ spontane Einschätzung von Risiken schwierig
- ★ Stress (evtl. gezielt aufgebaut)
- ★ (anerzogene) Hilfsbereitschaft
- ★ Macht der Gewohnheit
- ★ Egoismus / Egozentrik bei jedem vorhanden



Aufgefallen im Gebäude, und dann?

- ★ Klassisches Social Engineering hilft weiter, wenn ein Angreifer „entdeckt“ wird
- ★ Selbst professionelle Mitarbeiter des Objektschutzes im Hochsicherheitsbereich verhalten sich bei gut gewählten Erklärungen falsch

Beispiel:

„Wir führen hier gerade eine Sicherheitsüberprüfung im Auftrag der Geschäftsleitung durch. Ich notiere Ihren Namen, damit ich sie lobend erwähnen kann. Bitte behalten sie über die Prüfung Stillschweigen, damit wir weiter testen können.“



Aufgefallen im Gebäude, und dann?

- ★ Klassisches Social Engineering hilft weiter, wenn ein Angreifer „entdeckt“ wird
- ★ Selbst professionelle Mitarbeiter des Objektschutzes im Hochsicherheitsbereich verhalten sich bei gut gewählten Erklärungen falsch

Beispiel:

„Wir führen hier gerade eine Sicherheitsüberprüfung im Auftrag der Geschäftsleitung durch. Ich notiere Ihren Namen, damit ich sie lobend erwähnen kann. Bitte behalten sie über die Prüfung Stillschweigen, damit wir weiter testen können.“



Einleitung
Krypto-Trojaner
Die „typische“ IT
Social Engineering
Physische Sicherheit
Fazit

Mobile IT-Hardware
Hotels
Datenvernichtung
Empfehlungen Datenvernichtung

Mobile IT-Hardware: Laptops

Problem: Ihre Mitarbeiter tragen ihre vertraulichen Daten bei Geschäftsreisen aus dem Unternehmen.





Mobile IT-Hardware: Laptops

Problem: Ihre Mitarbeiter tragen ihre vertraulichen Daten bei Geschäftsreisen aus dem Unternehmen.





Hotels

Daten außerhalb Ihres Unternehmens:

- ★ Die meisten Hoteltüren sind nicht sicher abschließbar
- ★ Über Hotelsafes könnte man eigene Vorträge halten

⇒ Hotels sind kein guter Ort, um wichtige Daten zu lagern!





Einleitung
Krypto-Trojaner
Die „typische“ IT
Social Engineering
Physische Sicherheit
Fazit

Mobile IT-Hardware
Hotels
Datenvernichtung
Empfehlungen Datenvernichtung

Hoteltüren





Einleitung
Krypto-Trojaner
Die „typische“ IT
Social Engineering
Physische Sicherheit
Fazit

Mobile IT-Hardware
Hotels
Datenvernichtung
Empfehlungen Datenvernichtung

Hoteltüren





Datenvernichtung

- ★ Eine richtige (und konsequente) Datenvernichtung ist wichtig
- ★ Im digitalen Bereich:
Festplatteninhalte sicher löschen
(überschreiben)
- ★ Vorsicht bei SSDs!
- ★ Im analogen Bereich:
Shredder/Aktenvernichter





Beispiel Lebenszyklus vertraulicher Papierdaten

Ein Kunde stellt folgendem Ablauf dar:

- ★ Morgens erhält Callcenter-Mitarbeiter Papierliste
- ★ Einträge werden abgehakt
- ★ Notizen während der Telefonate auf extra Papier notiert
- ★ Einträge und Notizen werden in EDV übertragen
- ★ Abends wird Liste in spezielle Ablage gelegt
- ★ Notizen kommen in Papiermüll
- ★ Ablage wird abends geleert und sicher verwahrt
- ★ Mülleimerinhalt wird abends per Shredder vernichtet



Beispiel Lebenszyklus vertraulicher Papierdaten

Es zeigte sich:

- ★ Notizen finden sich nicht auf extra Papier, sondern auf Listen



Beispiel Lebenszyklus vertraulicher Papierdaten

Es zeigte sich:

- ★ Notizen finden sich nicht auf extra Papier, sondern auf Listen
- ★ Notizen und Listen werden nicht täglich in EDV übertragen



Beispiel Lebenszyklus vertraulicher Papierdaten

Es zeigte sich:

- ★ Notizen finden sich nicht auf extra Papier, sondern auf Listen
- ★ Notizen und Listen werden nicht täglich in EDV übertragen
- ★ Listen mit Notizen finden sich überall im Raum



Beispiel Lebenszyklus vertraulicher Papierdaten

Es zeigte sich:

- ★ Notizen finden sich nicht auf extra Papier, sondern auf Listen
- ★ Notizen und Listen werden nicht täglich in EDV übertragen
- ★ Listen mit Notizen finden sich überall im Raum
- ★ Die für die Listen vorgesehene Ablage ist leer



Beispiel Lebenszyklus vertraulicher Papierdaten

Es zeigte sich:

- ★ Notizen finden sich nicht auf extra Papier, sondern auf Listen
- ★ Notizen und Listen werden nicht täglich in EDV übertragen
- ★ Listen mit Notizen finden sich überall im Raum
- ★ Die für die Listen vorgesehene Ablage ist leer
- ★ Mülleimer ist nicht geleert, es finden sich Listen mit Notizen



Beispiel Lebenszyklus vertraulicher Papierdaten

Es zeigte sich:

- ★ Notizen finden sich nicht auf extra Papier, sondern auf Listen
- ★ Notizen und Listen werden nicht täglich in EDV übertragen
- ★ Listen mit Notizen finden sich überall im Raum
- ★ Die für die Listen vorgesehene Ablage ist leer
- ★ Mülleimer ist nicht geleert, es finden sich Listen mit Notizen
- ★ Weitere Listen finden sich (einmal zerissen) im Papiermüll auf dem Firmengelände. Zugriff für jedermann ist möglich.



Beispiel Lebenszyklus vertraulicher Papierdaten

Es zeigte sich:

- ★ Notizen finden sich nicht auf extra Papier, sondern auf Listen
- ★ Notizen und Listen werden nicht täglich in EDV übertragen
- ★ Listen mit Notizen finden sich überall im Raum
- ★ Die für die Listen vorgesehene Ablage ist leer
- ★ Mülleimer ist nicht geleert, es finden sich Listen mit Notizen
- ★ Weitere Listen finden sich (einmal zerissen) im Papiermüll auf dem Firmengelände. Zugriff für jedermann ist möglich.
- ★ Rekonstruktion von fast 100% der Listen der vergangenen Tage gelingt



Beispiel Lebenszyklus vertraulicher Papierdaten

Es zeigte sich:

- ★ Notizen finden sich nicht auf extra Papier, sondern auf Listen
- ★ Notizen und Listen werden nicht täglich in EDV übertragen
- ★ Listen mit Notizen finden sich überall im Raum
- ★ Die für die Listen vorgesehene Ablage ist leer
- ★ Mülleimer ist nicht geleert, es finden sich Listen mit Notizen
- ★ Weitere Listen finden sich (einmal zerissen) im Papiermüll auf dem Firmengelände. Zugriff für jedermann ist möglich.
- ★ Rekonstruktion von fast 100% der Listen der vergangenen Tage gelingt
- ★ Es existiert firmenweit überhaupt kein Shredder!



Empfehlungen Datenvernichtung

- ★ Nutzen Sie Shredder (mindestens Sicherheitsstufe 4)!
- ★ Prüfen Sie regelmäßig, ob Ihre Mitarbeiter die Aktenvernichter auch nutzen (der Mülleimer ist bequemer!).
- ★ Überprüfen Sie regelmäßig, ob der Shredder auch wirklich (noch) korrekt arbeitet
- ★ Bei externen Datenvernichtungsunternehmen: Was ist mit der Datensicherheit bis zur Vernichtung?



Einleitung
Krypto-Trojaner
Die „typische“ IT
Social Engineering
Physische Sicherheit
Fazit

Fazit

Fazit

- ★ Industriespionage findet statt





Einleitung
Krypto-Trojaner
Die „typische“ IT
Social Engineering
Physische Sicherheit
Fazit

Fazit

Fazit

- ★ Industriespionage findet statt
- ★ Auch/Gerade bei kleineren Unternehmen





Fazit

- ★ Industriespionage findet statt
- ★ Auch/Gerade bei kleineren Unternehmen
- ★ Erkennen Sie Ihre 10% der wirklich wichtigen Daten...





Fazit

- ★ Industriespionage findet statt
- ★ Auch/Gerade bei kleineren Unternehmen
- ★ Erkennen Sie Ihre 10% der wirklich wichtigen Daten...
- ★ ...und schützen Sie diese adäquat!





Einleitung
Krypto-Trojaner
Die „typische“ IT
Social Engineering
Physische Sicherheit
Fazit

Fazit

Fragen?

Vielen Dank für Ihre
Aufmerksamkeit