Phishing Infrastructure Knowledge

GITS
27.04.22

Inhaltsverzeichnis

Wer wir sind

- Vincent Donat (Wirtschaftsinformatik)
- Gina Bartenwerfer (Wirtschaftsinformatik)
- Michelle Kirst (Informatik)
- Bernhard Birnbaum (Informatik)
- Abdalla Khalil (Informatik)
- Felix Gretschel (CV)

Die Aufgabe

- Aufbau einer “rauscharmen” IT-Umgebung
- Netzwerkverkehr untersuchen (mitmproxy vs. SSL-Keylogfiles)
- Mailclients forensisch untersuchen
- Methoden entwickeln, um von Spam-/Phishing Attacken betroffen zu werden
- Untersuchung, wie große Dienstanbieter Phishing Attacken wahrnehmen können

Betroffene Sicherheitsaspekte

- Vertraulichkeit (unbefugter Zugriff auf Daten des Betroffenen)
- Authentizität (Angreifer geben sich als andere Entität aus)
- Persönlichkeitsschutz, Selbstbestimmung (Erhalt von Nachrichten ohne Zustimmung)

Gesetzliche Grundlagen

- Bundesamt für Sicherheit in der Informationstechnik (BSI) legt Mindeststandards für die Sicherheit der Informationstechnik des Bundes fest (auf Grundlage des § 8 Abs. 1 BSIG)
- Bei möglicher Strafbarkeit ist nach §269 StGB zwischen Phishing-Mails und Phishing-Webseiten zu unterscheiden
  - Phishing Webseiten machen sich zweifelsfrei der Urkundenfälschung strafbar
  - Bei Phishing Mails bestehen gespaltene Ansichten

Taxonomie

Angreifer	Werkzeuge	Schwachstelle	Aktion	Ziel	Resultat	Absicht
Kriminelle Beauftragte	Malware Websites Nachrichten	Mensch Adressobfuskation	Masquerade Stehlen Auslesen	Account Daten Informationen	Zugriff auf persönliche Daten Unerlaubter Zugriff auf Informationen	Finanziell motiviert

Datenstrom & Datenarten

Datenstrom: Netzwerkdatenstrom DS(N)

Datenarten:

-Raw Data(DT1) (Rohdaten) → Netzwerkpakete
-Details about Data (DT3) → Sequenznummern von Netzwerkpaketen
-Communication Protocol Data (DT5)
-Process Data (DT6) (Prozessdaten)
-Session Data (DT7) (Sitzungsdaten)

Aufgabenverteilung

- Dynamische Arbeitsverteilung
- Mehrere wöchentliche Meetings
- Protokoll der Besprechung inkl. Aufgaben

Aktueller Stand

- Aufbau virtualisierter Systemlandschaft
- Zugänge für Overleaf beantragt
- Ausprobieren von mitmproxy und Wireshark/SSL-Keylogfile

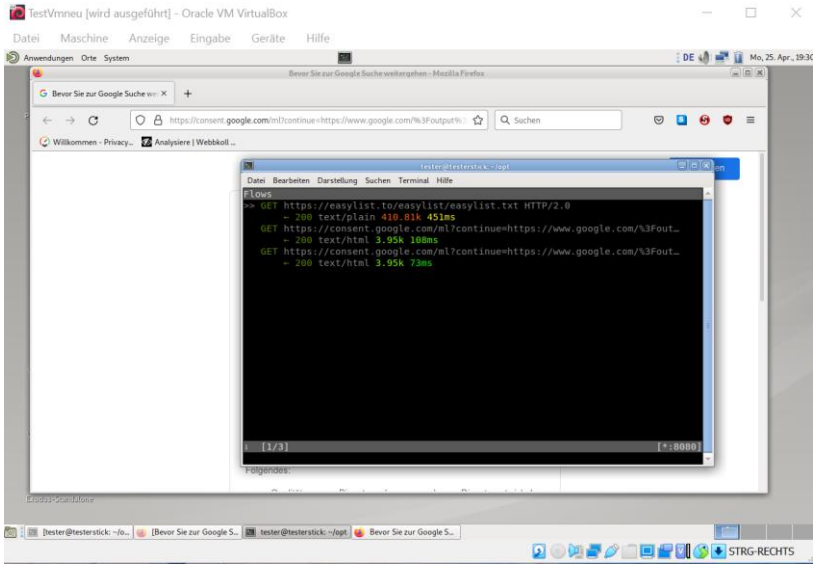

Bild: Ausführung Google über mitmproxy

Aussicht

- konstanten Strom von Phishing-Mails erreichen
- Kategorisierung der Phishing-Mails und Auswahl auf bestimmte Aspekte

Quellen

- https://www.recht-freundlich.de/phishing-online-banking/alles-wichtige-phishing (abgerufen am 23.04.2022)

Fragen?