

Advanced Persistent Threat

Theresa Meiksner

Begriffe

- ▶ Advanced (deutsch: fortgeschritten)

- ▶ **Advanced (deutsch: fortgeschritten)**

Ein APT erfolgt auf bestimmte, selektierte Opfer, Personen oder Institutionen mit erweiterter Technik und Taktiken.

Begriffe

- ▶ **Advanced (deutsch: fortgeschritten)**
Ein APT erfolgt auf bestimmte, selektierte Opfer, Personen oder Institutionen mit erweiterter Technik und Taktiken.
- ▶ **Persistent (deutsch: andauernd)**

Begriffe

- ▶ **Advanced (deutsch: fortgeschritten)**

Ein APT erfolgt auf bestimmte, selektierte Opfer, Personen oder Institutionen mit erweiterter Technik und Taktiken.

- ▶ **Persistent (deutsch: andauernd)**

APT nutzt den ersten infizierten Rechner nur als Sprungbrett in das lokale Netz der betroffenen IT-Struktur, bis das Hauptziel, z. B. ein Rechner mit Forschungsdaten, zum längeren Ausspionieren oder Sabotieren erreicht ist.

Begriffe

- ▶ **Advanced (deutsch: fortgeschritten)**
Ein APT erfolgt auf bestimmte, selektierte Opfer, Personen oder Institutionen mit erweiterter Technik und Taktiken.
- ▶ **Persistent (deutsch: andauernd)**
APT nutzt den ersten infizierten Rechner nur als Sprungbrett in das lokale Netz der betroffenen IT-Struktur, bis das Hauptziel, z. B. ein Rechner mit Forschungsdaten, zum längeren Ausspionieren oder Sabotieren erreicht ist.
- ▶ **Threat (deutsch: Bedrohung)**

Begriffe

- ▶ **Advanced (deutsch: fortgeschritten)**
Ein APT erfolgt auf bestimmte, selektierte Opfer, Personen oder Institutionen mit erweiterter Technik und Taktiken.
- ▶ **Persistent (deutsch: andauernd)**
APT nutzt den ersten infizierten Rechner nur als Sprungbrett in das lokale Netz der betroffenen IT-Struktur, bis das Hauptziel, z. B. ein Rechner mit Forschungsdaten, zum längeren Ausspionieren oder Sabotieren erreicht ist.
- ▶ **Threat (deutsch: Bedrohung)**
Selbsterklärend – APT stellt eine Bedrohung für gefährdete Systeme dar.

Was sind APTs?

- ▶ Im Bereich Cyber Attacks (Cyber Bedrohung)
- ▶ Gezielte Angriffe gegen größere Unternehmen
- ▶ Wirtschaftlich und/oder politisch motiviert
- ▶ Schadsoftware unbemerkt ins Netzwerk einschleußen
- ▶ Ziel: möglichst lange unbemerkt bleiben, damit im Hintergrund Daten sammelt.
- ▶ Daten wird an C&C Server des Angreifers geschickt.

Ideen?

Was wird gesammelt?

- ▶ Infos über
 - ▶ Netzwerk
 - ▶ Betriebssysteme
 - ▶ User Daten
- ▶ Sehr beliebt: AutoCAD Format DXF
 - ▶ Warum?

Was wird gesammelt?

- ▶ Infos über
 - ▶ Netzwerk
 - ▶ Betriebssysteme
 - ▶ User Daten
- ▶ Sehr beliebt: AutoCAD Format DXF
 - ▶ Warum?
 - ▶ **Bau und Produktpläne**

Net Traveler 2010-2013

- ▶ Ziel: 350 Behörden/Unternehmen in 40 Ländern
- ▶ Methode: MS Office Dokumente Exploit
- ▶ über Spear-Phishing Mails
- ▶ Schädling sammelt/protokolliert:
 - ▶ Tastaturanschläge (Keylogger?!)
 - ▶ Office Dateien
 - ▶ **sammelte 22 GB (woaaaah!!!)**

Angriff Trends

- ▶ Zero-Day Exploits
 - ▶ Pen Test z.B einen Web Server
 - ▶ Ziel: Anfragen zu erzeugen mit denen d. Server nicht zu recht kommt.
- ▶ Watering Hole Attacks
 - ▶ Schadcode (z.B: JavaScript) auf einer Website, die vom gezielten Unternehmen gerne angesurft wird.
 - ▶ Warten bis Mitarbeiter des Unternehmens in die Falle tappt.

APTs abwehren

- ▶ Infrastruktur kennen
- ▶ Re-evaluation des Security Konzepts
- ▶ Unvoreingenommene Kontroll Blicke zulassen
- ▶ Schulungen der Mitarbeiter (security awareness)

Danke für eure Aufmerksamkeit!