IOCS UND THREAT INTEL

SCHNELLERE AUFKLÄRUNG VON SICHERHEITSVORFÄLLEN

DATUM: OKT 04.OKTOBER 2016

Mathias Fuchs

MANDIANT
A FireEye® Company

Vorstellung

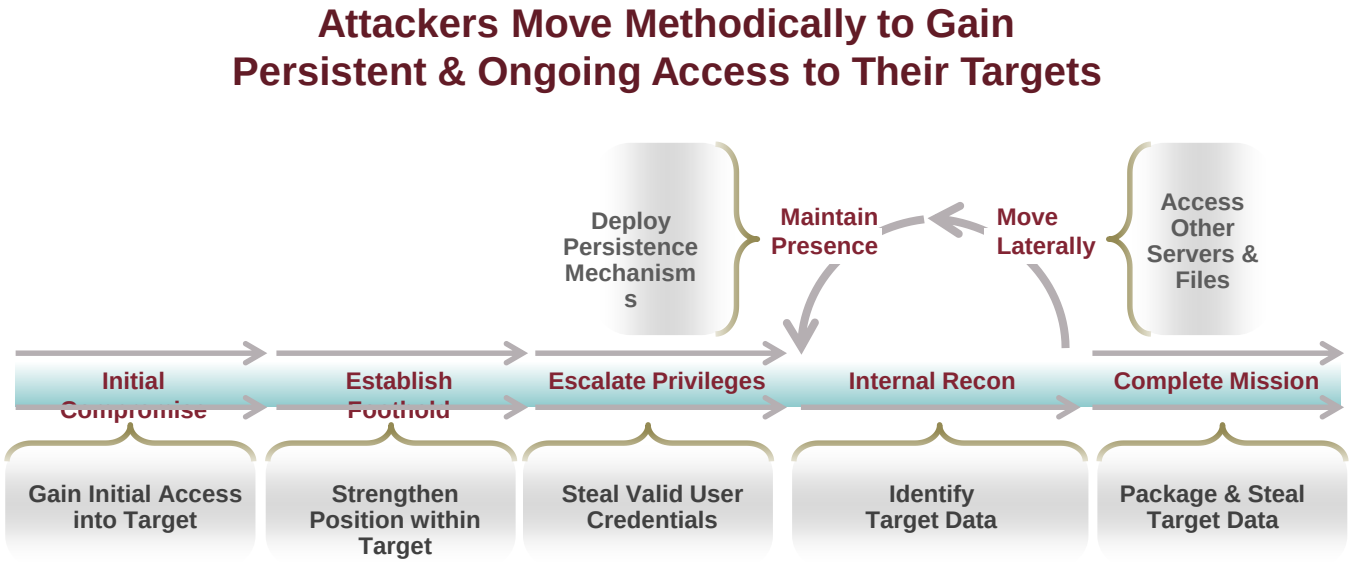
MATHIAS FUCHS

- Senior Consultant
  - Incident Response
  - Redteaming
  - QSA
- SANS Instructor
  - FOR508
  - Advanced Digital Forensics and Incident Response
- Twitter
  - @mathias_fuchs

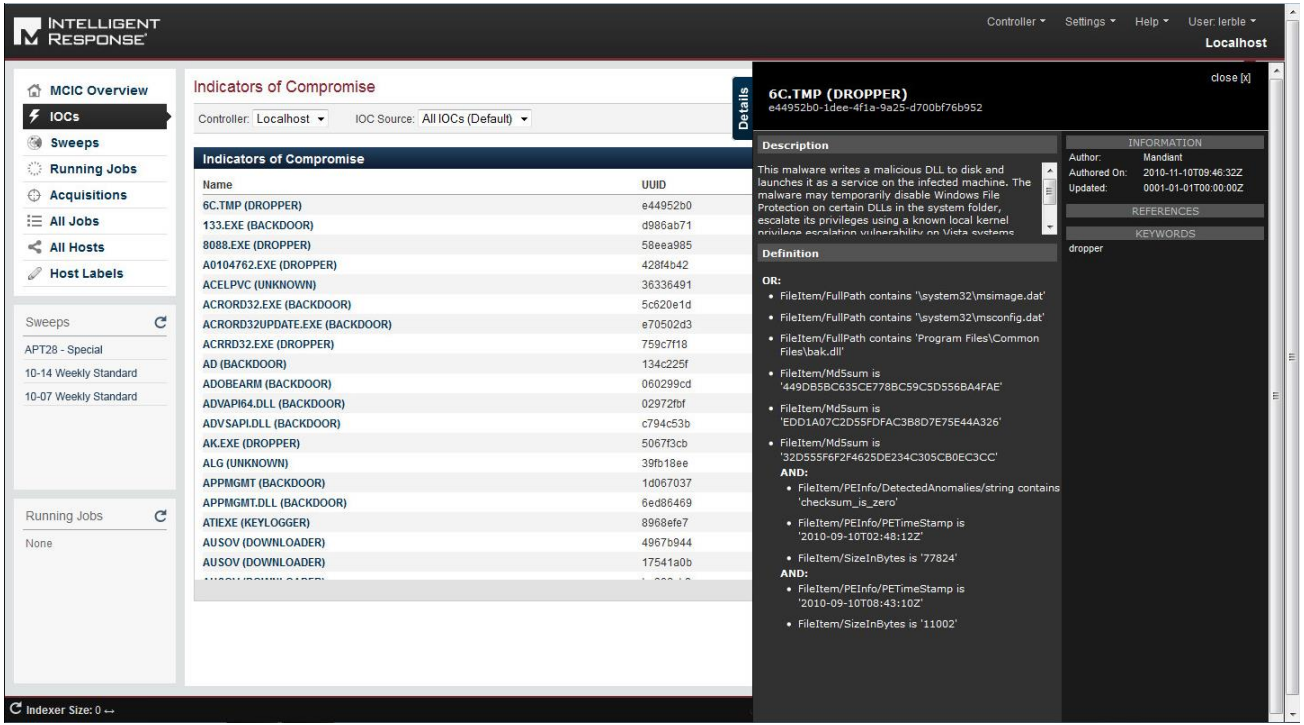
Übersicht

- ***Was sind IOCs***
- ***Aufbau von Threatintelligence***
- ***Beispiele aus dem echten Leben***

Anatomie eines gezielten Angriffs



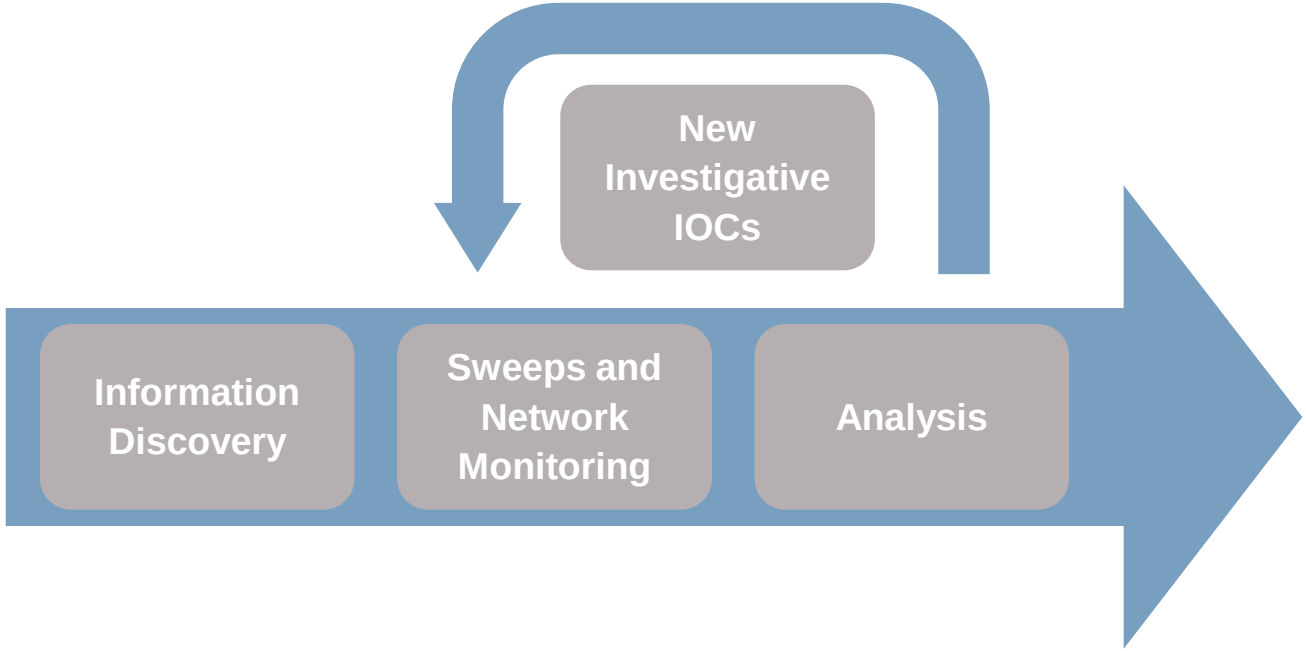
Indicators of Compromise



Untersuchungszyklus

Informationsquellen

- Host Untersuchung
- Netzwerk Monitoring
- Log Analyse (SIEM)
- Malware Reverse Engineering



Threat Intelligence

- 3 Arten von Spuren
  - Atomic
  - Computed
  - Behavioural
- Hoher Informationsfluss
- Attributionsfehler
- Dynamisches Gegnerfeld
- Teuer
- Aktive vs. Passive Informationsgewinnung

Threat Intel Sharing

- Vielzahl an Plattformen
- Einbahnstraßen scheinen attraktiver für Unternehmen
- Interessensverbände
- CERTs

Ihr Intel Team

- Erfahrung im Intelligence/Ermittlungs Bereich
- Mindestens 2 Personen
- Verknüpft in Community
- Informationseingänge
  - Incident Response Untersuchungen
  - Internet & Darknet Analysen
  - Öffentliche Stellen
  - Malware Analysen
  - Hersteller
  - Certs
  - Medien, ...

Fallbeispiel APT3

- APT3 ist eine technische sehr ausgereifte Angreifergruppe
- Bekannt durch „Operation Clandestine Wolf“
- Ziel mit hohem wissenschaftlichen Wert

- Intelligence Einsatz um weitere infizierte Rechner zu finden
- Aufbau weiterer Intelligence durch Fehler der Angreifer

Incident Response Hotline

Phone

- Germany 0800 181 7231
- Switzerland 0800 848 030
- Austria: 0800 296 251
- International: +1 (703) 996 3012

Email

- To: investigations@mandiant.com
- CC: dachconsulting@mandiant.com

MANDIANT
A FireEye® Company

Kontaktdaten

Mathias Fuchs
MANDIANT, a FireEye Company
Senior Security Consultant
Mobile: **+43 660 31337 99**
Email: mathias.fuchs@mandiant.com

Jan Korth
MANDIANT, a FireEye Company
Director of Security Consulting Services
Mobile: +**49 (160) 2723362**
Email: jan.korth@mandiant.com


MANDIANT
A FireEye® Company
FRAGEN & ANTWORTEN