Cyber Incident Response

Einblicke in die tägliche Arbeit von Incident Respondern bei EY

1. Oktober 2021
IT-SECX

EY
Building a better working world

EY Forensics

Cyber Kill Chain & MITRE ATT&CK®

PRE-ATT&CK

- Reconnaissance
- Resource Development

ENTERPRISE ATT&CK

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact

Quellen: https://attack.mitre.org/ und https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Vorfall 1

Lockdown, Freitag 19:47 Uhr

Das Security Operations Center („**SOC**“) eines weltweit agierenden Industrieunternehmens meldet zwei Alerts:

1) Login mit lokalem Admin-Account, welcher in der Regel nur in Ausnahmefällen verwendet wird
2) Meldung des Antiviren-Programms über potenzielles Credential Dumping (LSASS Dump)

Cyber Kill Chain & MITRE ATT&CK®

PRE-ATT&CK

- Reconnaissance
- Resource Development

ENTERPRISE ATT&CK

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact

Quellen: https://attack.mitre.org/ und https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Cyber Kill Chain & MITRE ATT&CK®

PRE-ATT&CK

- Reconnaissance
- Resource Development

ENTERPRISE ATT&CK

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact

Quellen: https://attack.mitre.org/ und https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Modus Operandi

Initial Access

Diebstahl von Zugangsdaten durch Ausnutzung von Sicherheitslücken in einer Firewall

Persistence

Sammlung von Passwörtern mit Hilfe eines lokalen Admin-Accounts

Privilege Escalation

Verwendung von Mimikatz zur Erlangung von administrativen Rechten

Discovery & Lateral Movement

Scannen des Netzwerks mit diversen Discovery Skripten und Verbindungen über RDP

Exfiltration

Sammlung von Firmendaten auf einem internen Server – es erfolgte keine Ausleitung

Impact

Keine Lösch- oder Verschlüsselungs-vorgänge

Vorfall 2

Dienstag 10:31 Uhr

Ein Softwareunternehmen wurde Opfer eines Cyberangriffs und hat Lösegeld bezahlt.

Nach dem Neuaufsetzen sämtlicher IT-Systeme beauftragt uns das Unternehmen mit der Überwachung und Überprüfung des „neuen“ Firmennetzwerks und ausgewählter Kernsysteme.

TA505

Als finanziell motivierte Gruppe bekannt operiert TA505 weltweit und setzt dabei auf hoch entwickelte, spezialisierte und sich ständig ändernde Malware.

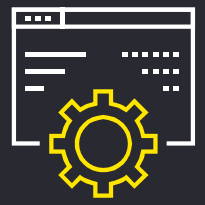
Modus Operandi

Exploitation

- Get2 und TrickBot

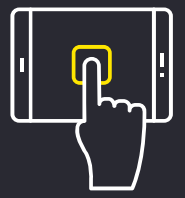
Command & Control (C2)

- Dridex, FlawedAmmyy und FlawedGrace



Installation

- SDBot und ServHelper



Actions on Objectives

- runmel.bat, wsus.exe und Cl0p

MITRE ATT&CK®

Quelle: https://attack.mitre.org/

Cyber Forensics Analyst (w/m/d)

Schwerpunkte:
Cyber Incident Response, eDiscovery und IT-Forensik

Standort: Wien
Stundenausmaß: Vollzeit, ab sofort

Fragen?

EY Building a better working world

Christoph Wiedner
Forensic & Integrity Services

+43 664 60003 1851
christoph.wiedner@at.ey.com

EY Building a better working world

Juliane Gorgasser
Forensic & Integrity Services

+43 664 60003 4047
juliane.gorgasser@at.ey.com

EY

Vielen Dank

Building a better working world

EY | Assurance | Tax | Strategy and Transactions | Consulting

ey.com/at