Methoden und Techniken von Advanced Persistent Threats am Beispiel des Solarwinds Compromise

Maria Mustermann
Fakultät für Informatik
Technische Hochschule Rosenheim
Rosenheim, Germany
maria.mustermann@stud.th-rosenheim.de

***Zusammenfassung*—Am des Solarwinds Compromise der APT 29 wird gezeigt, welche Methoden und Techniken durch APTs angewandt werden. ?? Deshalb ist es für Organisationen und Firmen unerlässlich sich gegen böswillige Akteure zu schützen.**

Paper soll anhand des Solarwinds Compromise der Advanced Persistent Threat (APT) 29 zeigen, wie diese Vorgehen, welche Techniken verwendet werden und welche Ziele APTs verfolgen. ?? Im Schlussteil werden die wichtigsten Maßnahmen aufgezeigt oder eine raffinierte Maßnahme im Detail erklärt

***Index Terms*—APT, Solarwinds, Cybersecurity, Machine Learning, Artificial Intelligence**

I. Einführung

Als APTs werden Gruppierungen oder Personen bezeichnet, die über ein hohes Maß an Fachwissen und erhebliche Ressourcen verfügen, die es Ermöglichen mehrere Angriffsvektoren zu nutzen. Zusätzlich verfolgen APTs ihre Ziele wiederholt über einen längeren Zeitraum, passen sich den Bemühungen der Verteitiger an und sind entschlossen die Ziele zu erreichen. Zu diesen Zielen gehören u. a. das Exfiltrieren von Informationen, kritische Aspekte einer Organisation zu stören und sich im System des Ziels zu verbreiten und festzusetzen [1, S. B-1]. Die geschätzten jährlichen Kosten von Cyberkriminalität sollen laut Statista im Jahr 2023 auf 8,15 Billionen US-Dollar belaufen und bis 2028 um 69,94% auf 13.82 Billionen US-Dollar steigen [2].

A. Organisierte Kriminalität, Hacker und Advanced Persistent Threats

Abgrenzung von APT zu anderen Formen der Cyberkriminalität ist in Abb. 1 dargestellt.

B. Solarwinds Compromise

II. Vorgehensweise von Advanced Persistent Threats

Die Techniken der APTs werden immer komplexer und vielfältiger und bestehen aus vielschichtigen und zeitaufwändigen Prozessen [3, S. 7f]. Um sie besser zu verstehen, werden die verschiedenen Teile eines Anriffs in eine *killchain* sortiert [3, S. 8], siehe Abb. 2. Es gibt weitere Killchain-Modelle, u. a. von Lockheed Martin [4], welche einfachheitshalber nicht weiter in betracht genommen wurden.

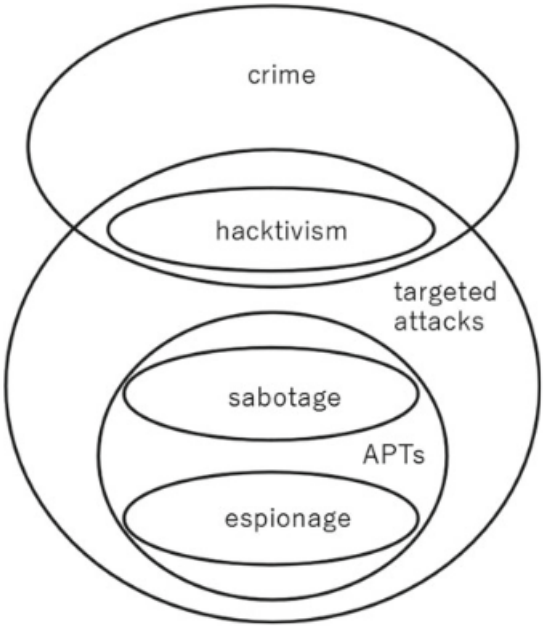

Abbildung 1. Unterscheidung zwischen gezielten Angriffen, Aktivitätes von APTs und Cyberspionage [3, S. 6]

A. Aufkärung

Das Ziel des ersten Schritts ist es nicht nur Information über das Ziel zu finden, sondern auch das Ziel festzulegen. Wie und warum Ziele ausgewählt werden lässt sich schwer bis nicht feststellen. Meist wird angenommen, dass APTs einen Auftrag durch Kunden bekommen, beispielsweise durch Geheimdienste, und danach ihre Ziele suchen. Nachdem das Ziel feststeht beginnt die weitere Aufklärung. Vgl. zu diesem Abschnitt Steffens [3, S. 10-13]. In der Regel werden öffentlich zugängliche Informationen über ein Ziel gesammelt, um dessen Arbeitsweise besser zu verstehen und potenzielle Angriffsvektoren zu identifizieren [5]. MITRE [6] listet zehn Techniken auf, mit deren Hilfe Informationen über das Ziel gefunden werden können:

- **Active Scanning** - Direkte Interaktion mit der Infrastruktur des Ziels (IP-Adressblöcke finden, Schwachstellenscanns, Wortlistsuche)
- **Gather Victim Host Informatiomn** - Harware- und

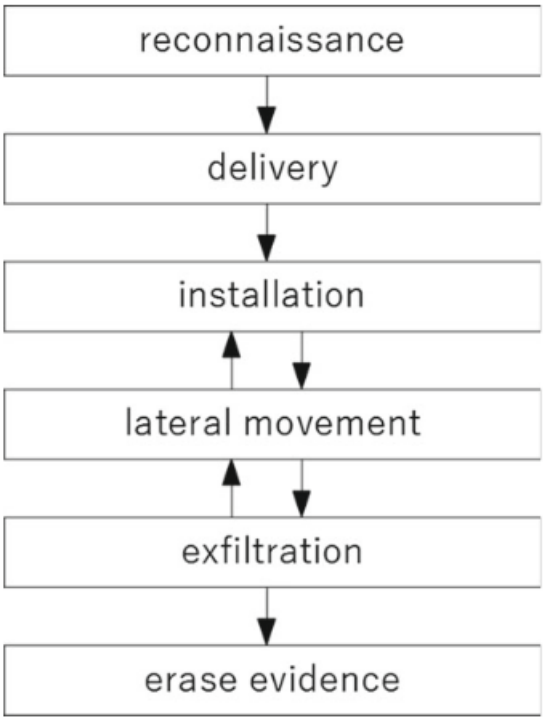

Abbildung 2. Killchain: Idealisiertes Modell der Stufen eines APT-Angriffs [3, S. 8]

Softwareinformation über das Zielsystem finden (Betriebssystem, Konfigurationen, Firmware, usw.)
- **Gather Victim Identity Information** - Informationen über Mitarbeiter (Daten von Personen, E-Mail Adressen, Zugangsdaten)
- **Gather Victim Network Information** - Grundlegende Informationen über das Netzwerk (IP-Adressen, DNS- & Domain-Informationen, Netzwerktopologie, usw.)
- **Gather Victim Org Information** - Informationen über das Unternehmen sammeln, die für weiter Schritte genutzt werden können (Geschäftsbeziehungen, Personalstruktur und -hierarchie, usw.)
- **Phishing for Information** - Erlangen von vertraulichen Informationen mithilfe von u. a. Social-Engineering Taktiken (Telefonate, E-Mails, usw.)
- **Search Closed Sources** - Informationen über das Ziel kaufen (Dark-Web Schwarzmärkte, usw.)
- **Search Open Technical Databases** - Technische Informationen über das Ziel in frei verfügbaren Online-Datenbanken finden (WHOIS, DNS, CDNs, usw.)
- **Search Open Websites/Domains** - Informationen über Suchmaschienen, Social-Media oder Coderepositorien finden.
- **Search Victim-Owned Websites** - Durchsuchen von Webseiten nach Informationen, die dem Ziel gehören (E-Mail Adressen, Mitarbeitername, usw.)

Viele der Techniken werden kombiniert, um am Ende das eigentliche Ziel zu erreichen. Beispielsweise werden auf der Webseite des Ziels wichtigen Mitarbeitern gesucht, weitere Informationen über Social-Media gewonnen, um anschließend vertrauliche Informationen über das Ziel mittels Social-Engineering Taktiken zu gewinnen.

?? Solarwinds Compromise

B. Auslieferung

Die Auslieferung ist sehr verbunden mit der Aufklärung. Häufig wird für eine gewählte Auslieferungsstrategie entsprechende Aufklärung durchgeführt. ?? Vgl. zu diesem Abschnitt Steffens [3, S. 10-13]. MITRE [7] bezeichnet diesen Schritt als initialen Zugriff und unterscheidet zwischen zehn Techniken:

- **Content Injection** - Nutzen von bereits kompromittierten Datenübertragungskanälen.
- **Drive-by Compromise** - Ziel wird aktiv zu bösartigen Nutzdaten auf einer kompromittierten Webseite gelockt, z.B. Abgreifen von Anwendungszugriffstoken.
- **Exploit Public-Facing Application** - Ausnutzen einer Schwachstelle eines Systems.
- **External Remote Services** - Nutzen von unzureichend abgesicherten Remote-Diensten, wie VPNs.
- **Harware Additions** - Einbringen neuer Hardwaer in ein System oder Netzwerk, z.B. Wechseldatenträger.
- **Phishing** - Versenden von Phishing-Nachrichten, um einen Zugang zum System des Ziels zu erhalten.
- **Replication Through Removable Media** - Eindringen in abgetrennte Netzwerke, z.B. mittels Wechselmedien in Kombination mit Autorun-Funktionen
- **Supply Chain Compromise** - Einschleusen von bösartigem Code durch Auslieferungsmechanismen von Anwendungen.
- **Trusted Relationship** - Ausnutzen von vertrauenswürdigen Dritten, um Zugang zu einem Netzwerk zu erhalten.
- **Valid Accounts** - Nutzen von Anmeldeinformationen bestehender Konten (VPNs, Outlook, Remote-Desktop, ...)

?? Solarwinds compromis supply chain compromise

C. Installation

?? MITRE [8] unterscheidet in diesem Punkt zwischen Taktiken für die Ausführung von schadhaftem Code, *Execution*, und Taktiken, um den Zugriff auf längere Zeit zu sichern [8]. Zu den Taktiken für die Ausführung von schadhaftem Code listet MITRE [9] folgende:

- **Cloud Administration Command** - Missbrauchen von Cloud-Verwaltungsdiensten, wie AWS Systems Manager und Azure Runcommand.
- **Command and Scripting Interpreter** - Befehls- und Skriptinterpreter, wie Unix-Shell und PowerShell, werden zum ausführen von schadhafem Code verwendet.
- **Container Administration Command** - Über Containerverwaltungsdienste kann schadhafter Code innerhalb eines Containers ausgeführt werden.
- **Deploy Container** - Einsetzen von schadhaften Containern, um beispielsweise Prozesse auszuführen die Malware ausführen oder herunterladen.

- **Exploitation for Client Execution** - Ausnutzern von Software-Schwachstellen in Client-Anwendungen, um Code auszuführen.
- **Inter-Process Communication** - Manipulieren von prozessübergreifender Kommunikation, um Befehle oder Code auszuführen.
- **Native API** - Verwenden von nativen Betriebssystemschnittstellen.
- **Scheduled Task/Job** - Ermöglicht bösartigen Code erstmalig oder wiederholt auszuführen, indem Fuktionen zur Aufgabenplanung missbraucht werden.
- **Serverless Execution** - Missbrauchen von Serverless Computing, Integrations- und Automatisierungsdiensten, um Code in Cloudumgebungen auszuführen.
- **Shared Modules** - Schadhafter Code kann über gemeinsame Module (z.B. DLLs) ausgeführt werden.
- **Software Deployment Tools** - Bei Zugang zu installierten drittanbieter Softwares für Systemadministration, -monitoring und Softwarebereitstellung kann beliebe Malware in großen Teilen des Netzwerks installiert werden. Dadurch wird auch die Verbreitung im Netzwerk erzielt.
- **System Services** - Verwenden von Systemdiensten oder Daemons zur Ausführung von Code. Kann bereits zum erreichen von Persistenz verwendet werden.
- **User Execution** - Bösartiger Code wird hierbei durch einen Benutzer ausgeführt, der durch Social Engineering dazu gebracht wurde.
- **Windows Management Instrumentation** - Ausnutzen der Windows Management Insturmentation, um Befehle auszuführen.

Die größte Teil der genannten Taktiken ermöglichen es, schadhaften Code einmalig auszuführen, jedoch werden diese Prozesse nach neustart eines Systems beendet. Um den Zugang über Neustarts hinweg zu sichern, werden Taktiken zu persistierung eingesetz [10]. Dazu listet MITRE [10] folgende Taktiken auf:

- **Account Manipulation** -
- **BITS Jobs** -
- **Boot or Logon Autostart Execution** -
- **Boot or Logon Initialization Scripts** -
- **Brwoser Extensions** -
- **Compromise Client Software Binary** -
- **Create Account** -
- **Create or Modify System Process** -
- **Event Triggered Execution** -
- **External Remote Services** -
- **Hijack Execution Flow** -
- **Implant Internal Image** -
- **Modify Authentication Process** -
- **Office Application Startup** -
- **Power Settings** -
- **Pre-OS Boot** -
- **Scheduled Task/Job** -
- **Server Software Component** -
- **Traffic Signaling** -
- **Valid Accounts** -

D. Verbreitung

E. Exfiltration

F. Beweise löschen

III. Verteidigung gegen Advanced Persistent Threats

A. Threat Hunting

B. Visual Analytics with the MASFAD framework

IV. Fazit ??

Acknowledgment

References

Literatur

[1] National Institute of Standards and Technology, "Managing information security risk :," U.S. Department of Commerce, Tech. Rep.

[2] Statista. Estimated cost of cybercrime worldwide 2017-2028. [Online]. Available: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

[3] T. Steffens, *Attribution of Advanced Persistent Threats*. Springer-Verlag.

[4] Lockheed Martin Corp. Chiber kill chain. Accessed on: Nov. 20, 2023. [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[5] E. Cole, *Advanced persistent threat*. Syngress.

[6] MITRE Corporation. Reconnaissance. Accessed on: Nov. 21, 2023. [Online]. Available: https://attack.mitre.org/versions/v14/tactics/TA0043/

[7] ——. Initial access. Accessed on: Nov. 21, 2023. [Online]. Available: https://attack.mitre.org/versions/v14/tactics/TA0001/

[8] ——. Enterprise tactics. Accessed on: Nov. 21, 2023. [Online]. Available: https://attack.mitre.org/tactics/enterprise/

[9] ——. Execution. Accessed on: Nov. 25, 2023. [Online]. Available: https://attack.mitre.org/tactics/TA0002/

[10] ——. Persistence. Accessed on: Nov. 25, 2023. [Online]. Available: https://attack.mitre.org/tactics/TA0003/