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

Laurenz Stinner
Fakultät für Informatik
Technische Hochschule Rosenheim
Rosenheim, Germany
laurenz.p.stinner@stud.th-rosenheim.de

***Zusammenfassung*—Advanced Persistent Threats (APTs) sind ein große Gefahr für jedes Netzwerk. Ihre besonderen Eigenschaften ermöglichen es APTs in nahezu jedes Netzwerk einzudringen. In der Arbeit wird zunächst erklärt, wie sich APTs von anderen Formen der Cyberkriminalität unterscheiden und wie diese im allgemeinen Vorgehen. Anschließend wird gezeigt wie die APT29 im Fall des SolarWinds Compromise vorgegangen ist. Zum Schluss werden Verteidigungsmaßnahmen wie Threat Hunting und das MASFAD Framework vorgestellt.**

***Index Terms*—APT, SolarWinds Compromise, Cybersecurity, APT, Cloudsecurity, Threat Hunting, Killchain, MASFAD**

I. Einführung

Laut Statista belaufen sich die geschätzten jährlichen weltweiten Kosten von Cyberkriminalität auf 8,15 Billionen US-Dollar und steigen bis 2028 um 69,94% auf 13,82 Billionen US-Dollar an [1]. In Deutschland entstehen durch Cyberattacken Schäden in Höhe von 148 Milliarden Euro, was 72% des gesamten Schadens etspricht, der durch Industriespionage, Sabotage und Datendiebstahl verursacht wird. Besonders im Zuge des russischen Angriffskrieg auf die Ukraine hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) viele Phänomene bezüglich Cyberkriminalität in Deutschland festgestellt [2, S. 25]. Das BSI gibt an, das im Durchschnitt täglich 250.000 neue Varianten von Schadprogrammen bekannt werden [2, S. 13]. Dies macht deutlich, wie wichtig es ist, zu verstehen wie APTs agieren, um sich bestmöglich auf Angriffe dieser Art vorzubereiten.

A. Organisierte Kriminalität, Hacker und Advanced Persistent Threats

Bei der Cyberkriminalität wird zwischen verschiedenen Formen unterschieden, siehe Abb. 1. Das National Institute of Standards and Technology beschreibt APTs wiefolgt: 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 [4, S. B-1].

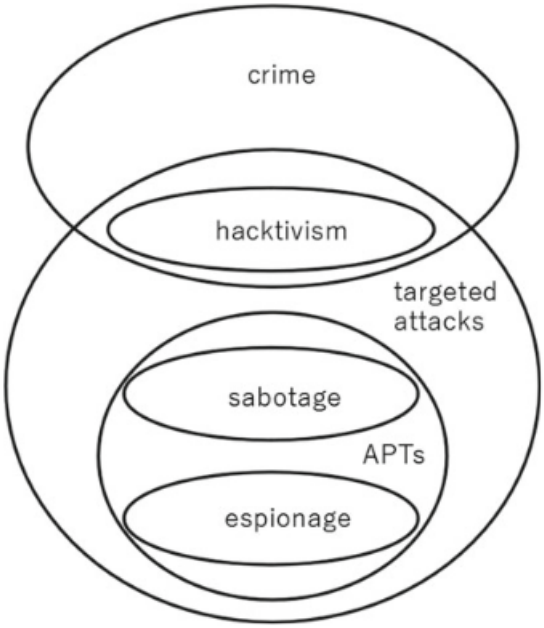

Abbildung 1. Unterscheidung zwischen gezielten Angriffen, Aktivitätes von APTs und Cyberspionage [3, S. 6]

B. SolarWinds Compromise & APT29

Der SolarWinds Compromise war eine Supply-Chain-Attacke der Gruppe APT29 und wurde im Dezember 2020 entdeckt [5]. Das betroffene Softwareprodukt war die Orion Platform des Unternehmens SolarWinds. Die Platform ermöglicht das Überwachen, Analysieren und Verwalten von Resourcen in Cloudumgebungen [6]. Dieser Umfang an Fuktionen hat die Platform zu einem Ziel gemacht, da durch eine mögliche Schwachstelle sehr viele Systeme betroffen sind, was letztendlich eingetreten ist. Der Angriff war so weitreichend, dass das Federal Bureau of Investigation (FBI), Cybersecurity and Infrastruktur Security Agency (CISA), Office of the Director of National Intelligence (ODNI) und die National Security Agency (NSA) eine gemeinsame Erklärung [7] zu dem Angriff herausgegeben haben. Lt. diesem Bericht waren ca. 18.000 öffentliche und private Kunden der Software SolarWinds Orion betroffen. Eine erheblich kleinere Zahl der Kunden wurde durch nachfolgende Aktivitäten kompromittiert. Die Erklärung

enthält bereits die Indizien, dass die verantwortliche APT russischen Ursprungs ist.

Die USA und das Vereinigte Königreich verantworten gemeinsam den russischen Auslandsgeheimdienst für den Angriff [8]. Die Gruppe erhält in späteren öffentlichen Erklärungen u. A. die Beinamen APT29 und Cozy Bear [9].

APT29 operiert seit mindestens 2008 und haben es primär auf Regierungsnetzwerke in Europa und NATO-Mitgliedsstaaten, Forschungsinstitute und Denkfabriken abgesehen [10]. MITRE ordnet der APT29 neben dem SolarWinds Compromise auch die Operation Ghost zu [10].

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.

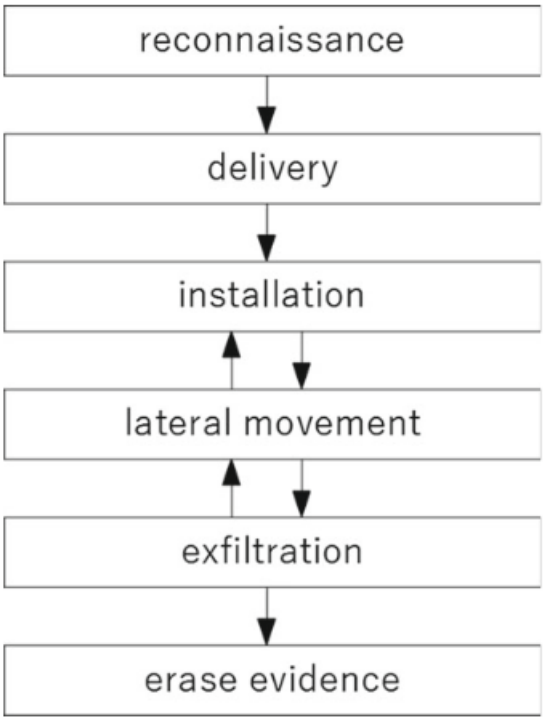

Abbildung 2. Killchain: Idealisiertes Modell der Stufen eines APT-Angriffs [3, S. 8]

von Lockheed Martin [11], welche einfachheitshalber nicht weiter in betracht genommen werden. MITRE unterscheidet sogar noch detailierter zwischen den verwendeten Taktiken [12].

Im Folgenden werden die Schritte der *Killchain* aus Abb. 2 erklärt und Taktiken gelistet die durch APTs genutzt werden, um das Ziel des Schrittes zu erreichen.

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. 10ff].

In der Regel werden öffentlich zugängliche Informationen über ein Ziel gesammelt, um dessen Arbeitsweise besser zu verstehen und potenzielle Angriffsvektoren zu identifizieren [13].

MITRE [14] 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 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.

B. Auslieferung

Die Auslieferung ist sehr verbunden mit der Aufklärung. Häufig wird für eine gewählte Auslieferungsstrategie entsprechende Aufklärung durchgeführt. Wird beispielsweise der Angriffsvektor E-Mail ausgewählt, müssen vorab über diverse Aufklärungstaktiken Informationen gefunden werden, um zu

gewährleisten, dass beispielsweise der Inhalt der Mail geöffnet wird. Vgl. zu diesem Abschnitt Steffens [3, S. 10ff].

MITRE [15] 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 Hardware 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, ...)

Viele Angriffe von APTs werden im nachhinein durch IT-Sicherheitsunternehmen beschrieben, jedoch ist es meist unmöglich herauszufinden, wie die Angreifer in das Netzwerk gelangt sind [3, S. 14]. Wie in Abschnit I-A beschrieben, verfügen APTs über erhebliche Ressource und können desshalb über Wochen oder Monate hinweg den Angriff ausführen. In dieser Zeit können Angreifer ihre Spuren verwischen, bzw. viele Unternehmen halten Log-Dateien nicht entsprechend lange vor, um diese Auswerten zu können [3, S. 15].

C. Installation

Ziel dieses Schritts ist es die Kontrolle über ein System im Netzwerk des Ziels zu bekommen. Der Schritt Auslieferung, aus Abschnitt II-B, und dieser Schritt sind in der Regel die größte Herausforderung und entscheidend für den Erfolg eines Angriffs. Im Zuge diese Schritts wird eine Verbindung zwischen dem kompromittierten System und einem *Control Server* mittels sog. *Backdoors* hergestellt, um den Zugriff zu tarnen. Vgl. zu diesem Abschnitt Steffens [3, S. 15].

MITRE [12] unterscheidet in diesem Punkt zwischen Taktiken für die Ausführung von schadhaftem Code, *Execution*, und Taktiken, um den Zugriff auf längere Zeit zu sichern [12]. Zu den Taktiken für die Ausführung von schadhaftem Code listet MITRE [16] folgende auf:

- **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 [17]. Dazu gehören nach MITRE [17] folgende Taktiken:

- **Account Manipulation** - Aktionen um den Zugriff auf ein Konto aufrechtzuerhalten. z. B. durch Ändern von Anmeldedaten.
- **BITS Jobs** - Windows Brackground Intelligent Transfer Services (BITS) können genutzt werden um Malware als Hintergrundaufgabe dauerhaft auszuführen.
- **Boot or Logon Autostart Execution** - Systemeinstellungen konfigurieren, damit ein Programm bei Systemstart oder Anmeldung automatisch ausgeführt wird.
- **Boot or Logon Initialization Scripts** - Verwendung

von Skripten die automatisch beim Booten oder bei der Anmeldung auseführt werden.
- **Browser Extensions** - Missbrauchen von Browser-Erweiterungen, um sich dauerhaften Zugang zu verschaffen.
- **Compromise Client Software Binary** - Schadhaften Code in Client-Software-Binärdateien einschleusen.
- **Create Account** - Eigenes Konto für den Systemzugang erstellen.
- **Create or Modify System Process** - Erstellen oder Ändern von Prozessen auf Systemebene (z. B. Windows-Dienste). Diese werden beim Start des Betriebssystems hochgefahren.
- **Event Triggered Execution** - Mit Hilfe von Systemmechanismen können bei bestimmten Ereignissen Prozesse ausgeführt werden. Besonders in Cloud-Umgebungen, werden Cloud-Ereignisse überwacht und bei entsprechende Ereignissen Funktionen oder Dienste ausgeführt.
- **External Remote Services** - Über Remote-Dienste kann der Zugriff auf ein Netzwerk persistiert werden (z. B. VPNs).
- **Hijack Execution Flow** - Missbrauch der Art und Weise, wie Betriebssystem Programme ausführen (Ausführungsfluss). Durch umgeleitete Ausführungen kann schadhafter Code immer wieder geladen werden.
- **Implant Internal Image** - Einsetzen von schadhaftem Code in Cloud- oder Container-Images.
- **Modify Authentication Process** - Modifizieren von Authentifizierungsmechanismen- und -prozessen, um auf Benutzeranmeldeinformationen zuzugreifen.
- **Office Application Startup** - Verwendung von Office-Vorlagenmakros oder Add-Ins, um schadhaften Code in Office-basierten Anwendungen zu persistieren.
- **Power Settings** - Beeinträchtigen der Systemfunktionen in den Ruhezustand zu gehen, neu zu starten oder herunterzufahren, um zu verhindern, dass schadhafter Code gestoppt wird.
- **Pre-OS Boot** - Nutzen von Pre-OS-Boot-Mechanismen, um während des Bootvorgangs schadhafte Firmware und verschiedene bösartige Startdienste vor dem Betriebssystem zu laden.
- **Scheduled Task/Job** - Erstellen oder Modifizieren von geplanten Aufgaben, um schadhaften Code wiederholt auszuführen.
- **Server Software Component** - Ausnutzen von legitimen, erweiterbaren Entwicklungsfunktionen von Servern, die ermöglichen Software oder Skripte zu schreiben und zu installieren.
- **Traffic Signaling** - Verbergen von offenen Ports oder anderen bösartigen Funktionen. Ein magischer Wert oder eine Sequenz muss verwendet werden, um eine Reaktion auf dem System auszulösen, z. B. das Öffnen eines Ports oder die Ausführung einer bösartigen Aufgabe.
- **Valid Accounts** - Durch erbeutete Anmeldeinformationen bestehender Konten, können diese Wiederholt missbraucht werden, um den Zugriff aufrechtzuerhalten.

Neben MITRE beschreibt auch Steffens die Kombination mehrerer Techniken, um das Ziel zu erreichen [3, S. 16]. Trotz der erheblichen Ressourcen die einer APT zur Verfügung stehen, werden durch die wenigsten *zero-day exploits* verwendet, denn meist sind genügend alte Sicherheitslücken vorhanden [1, S. 15] Bereits 2019 wurden 70% der Angriffe über MS Office Produkte ausgeführt [18], was Steffens auf die Makro- und Skript-Funktionalität der Office-Produkte zurückführt [3, S. 15] Trotz standardmäßige Blockierung von Skripten und Makros in Office-Produkten [19], schaffen es Angreifer die Benutzer dazu zu verleiten diese auszuführen.

D. Verbreitung

Besonders dieser Schritt ist charakteristisch für APTs, denn andere Angreifer beschränken sich normalerweise auf ein System, um beispielsweise Zugangsdaten von Onlinebanking zu stehlen. Zunächst müssen auf dem kompromittierten System erweiterte Rechte ergattert werden. Hierzu werden Techniken zur *privilege escalation* eingesetzt. Vgl. dazu Steffens [3, S. 16f].

MITRE [20] listet hierzu die folgenden Techniken:

- **Abuse Elevation Control Mechanism** - Umgehen von Mechanismen zur Kontrolle der Berechtigungserweiterung, um sich höhere Berechtigungen zu verschaffen.
- **Access Token Manipulation** - Verändern eines Zugriffstokens, sodass z.B. ein Prozess so aussieht, als gehöre er zu einem Benutzer mit erweiterten Berechtigungen.
- **Account Manipulation** - Manipulieren von Kontent, um den Zugang zu erweitern.
- **Boot or Logon Autostart Execution** - Systemeinstellungen so konfigurieren, dass Programme bei Systemstart oder Anmeldung automatisch mit erweiterten Berechtigungen gestartet werden.
- **Boot or Logon Initialization Scripts** - Verwenden von Skripten, die beim Booten oder der Anmeldung eines Benutzers mit erweiterten Berechtigungen ausgeführt werden und somit in dessen Sicherheitskontext laufen.
- **Create or Modify System Process** - Erstellen von Prozessen auf Systemebene die u. U. mit Administrationsberechtigungen ausgeführt werden [21].
- **Domain Policy Modification** - Verändern von beispielsweise Domänen-Gruppenrichtlinien, um die Berechtigungen innerhalb der Domäne zu erweitern.
- **Escape to Host** - Ausbrechen aus einem Container, um auf das zugrunde liegende Hostsystem zuzugreifen.
- **Event Triggered Execution** - Mit Hilfe von Systemmechanismen Code bei bestimmten Ereignissen ausführen, der mit erweiterten Berechtigungen startet.
- **Exploitation for Privilege Escalation** - Ausnutzen von Software-Schwachstellen, um die Berechtigungen zu erweitern.
- **Hijack Execution Flow** - Missbrauchen der Art und Weise wie Betriebssysteme Programme ausführt. Dabei werden in den Ausführungsfluss schadhafter Code oder schadhafte Nutzdaten eingeschleust und diese u. U. mit erweiterten Berechtigungen verarbeitet.

- **Process Injection** - Hierbei wird Code in einen Prozess eingeschleust. Läuft der Prozess mit erweiterten Berechtigungen, wird auch der eingeschleuste Code mit diesen Berechtigungen ausgeführt.
- **Scheduled Task/Job** - Ausnutzen der Aufgabenplanung eines Systems. Geplante Aufgaben können u. U. mit erweiterten Berechtigungen ausgeführt werden.
- **Valid Accounts** - Verschaffen von Anmeldeinformation bestehender Konten, die bereits erweiterte Berechtigungen haben.

Einige dieser Taktiken werden auch in anderen Schritten verwendet, wesshalb die klare Abtrennung zwischen den Schritten nicht ganz so leicht möglich ist. Nachdem Angreifer administrative Berechtigungen erlangt haben, wird das System z. B. auf Anmeldeinformation zu anderen System durchsucht, um mit Hilfe dieser auf andere Systeme im Netzwerk zu gelangen [3, S. 17]. MITRE [22] kennt einige weitere Taktiken, um sich im Netzwerk zu verbreiten:

- **Exploitation of Remote Services** - Ausnutzen eines Remote-Dienstes innerhalb eines Netzwerkes, um sich unerlaubten Zugang zu weiteren internen Systemen zu verschaffen. Dabei werden Software-Schwachstellen in Programmen und Betriebssystemen ausgenutzt.
- **Internal Spearphishing** - Angreifer können sich mittels internem Spearphishing Zugang zu zusätzlichen Information verschaffen. Es handelt sich dabei um ein mehrstufiges Verfahren, bei dem z. B. ein E-Mail-Konto eines Benutzers in Besitz genommen wird.
- **Lateral Tool Transfer** - Übertragen von Tools oder anderen Dateien zwischen Systemen in einer kompromittierten Umgebung.
- **Remove Service Session Hijacking** - Kontrolle über bereits bestehende Sitzungen in Remote-Diensten übernehmen.
- **Remote Services** - Verwenden von gültigen Kontent, um sich bei einem Dienst anzumelden, der Remote-Verbindungen akzteptiert, z. B. SSH.
- **Replication Through Removable Media** - Wechselmedien können verwendet werden, um sich auch in getretten Netzwerken zu verbreiten. Dabei wird Malware auf das Wechselmedium gespielt und mittels Autorun-Funktion auf dem getrennten System ausgeführt.
- **Software Deployment Tools** - Zugang zu Softwarebereitstellungssystemen von Drittanbietern zu verschaffen, um diese zur Verbreitung zu nutzen.
- **Taint Shared Content** - Schadprogramme auf gemeinsam genutzten Speicherorten (Netlaufwerke, Code-Repositorien) in vertrauenswürdigen Dateien ablegen. Sobald ein Nutzer den freigegebenen Inhalt öffnet, kann so der Schadcode verbreitet werden.
- **Use Alternate Authentication Material** - Verwenden von alternativem Authentifizierungsmaterial (Kennwort-Hashes, Kerberos-Tickets, Token, usw.), um sich weiter im System zu verbreiten.

In Abb. 2 ist zu sehen, dass *installation*, *lateral movement* und *exfiltration* als Kreislauf dargestellt werden. Dies erklärt Steffens damit, dass für Systeme die durch die Verbreitung zugreifbar werden der Zyklus erneut beginnt und die Schritte durchlaufen werden [3, S. 18].

E. Exfiltration

Die Exfiltration von Dokumenten und Daten ist das eigentliche Zeil von APTs, die anderen Schritte sind nur ein Mittel zum Zweck. Im Groben geht es darum, die Dokumente und Daten an einen Server zu übermitteln der unter voller Kontrolle der APT steht. Dafür greifen APTs auf Wortlisten zurück, um nach interessanten und relevaten Daten zu filtern. Dabei werden Dokumentnamen, Ordnernamen oder auch Dateiendungen berücksichtigt, die einen Hinweis auf wichtige Daten liefern. Einerseits wird dieses Vorgehen gewählt, damit der Aufwand des Durchsuchens der Dateien realisierbar bleibt, andererseits birgt das Exfiltrieren großer Datenmengen die Gefahr schneller entdeckt zu werden, da ungewöhnlich großer Netzwerkverkehr erzeugt wird. Vgl. dazu Steffens [3, S. 18].

MITRE [23] listet dafür folgende Taktiken auf:

- **Automated Exfiltration** - Automatisches exfiltrieren von z. B. sensiblen Dokumenten. Dafür wird diese Technik meist mit anderen Exfiltrationstechniken kombiniert [24].
- **Data Transfer Size Limit** - Exfiltrieren von Daten in kleineren Paketen, um z. B. zu vermeiden, dass Schwellenwerte für die Datenübertragung im Netzwerk nicht überschritten werden.
- **Exfiltration Over Alternative Protocol** - Daten über andere Protokolle, als das der bestehenden Verbindung, exfiltrieren.
- **Exfiltration Over C2 Channel** - Daten über das Protokol der bestehenden Verbindung exfiltrieren.
- **Exfiltration Over Other Network Medium** - Nutzen von anderen Netwerkmedien, wie WiFi-Verbindungen, mobile Datenverbindungen oder Bluetooth, um Daten zu exfiltrieren.
- **Exfiltration Over Physical Medium** - Stehlen von Daten mittels physischer Medien, z. B. USB-Laufwerke oder Mobiltelefone.
- **Exfiltration Over Web Services** - Verwenden von Webdiensten zur Exfiltration, z. B. über Fileshare-Dienste.
- **Scheduled Transfer** - Planen von Datenexfiltrationen, damit nur zu bestimmten Tageszeiten oder in bestimmten Zeitabständen. Diese Taktik wird u. U. genutzt, um den Datenverkehr mit normalen Aktivitäten zu vermischen. Andere Taktiken werden meist mit dieser verbunden [25].
- **Transfer Data to Cloud Account** - Übertragen von Daten, einschließlich Backups von Cloud-Umgebungen, auf ein anderes Cloud-Konto, um Exfiltrationserkennung zu umgehen.

In der Regel werden Dateien die exfiltriert werden sollen zuvor in passwortgeschützte und komprimierte Archive RAR gepackt, um das Opfer daran zu hindern, herauszufinden welche Dateien gestohlen wurden [3, S. 19].

F. Beweise löschen

Die sog. Operational Security (OpSec) korreliert stark mit der Raffinesse von APTs. Besonders Gruppen die der NSA und CIA zugeordnet werden, sind stark im Thema OpSec. Dabei geht es darum genutzte Tools zu löschen, Logs richtig zu löschen und sonstige Spuren zu entfernen oder zu verwischen, um zu verhindern entdeckt zu werden. Viele APTs führen diesen Schritt nicht sorfältig durch. Dadurch lassen sich viele Spuren finden, aber nicht alle. Viele System löschen selbst die Spuren von Anreifern, z. B. durch Logrotation. Zusätzlich wird dieser Schritt gemieden, da gute System das Löschen von Logs überwachen und Alarm schlagen. Vgl. dazu Steffens [3, S. 19f].

III. Vorgehensweise im SolarWinds Compromise

Der Angriff auf SolarWinds wurde als Supply-Chain-Attacke eingestuft, was bedeutet, dass das Ziel des Angriffs nicht SolarWinds selbst, sondern die Kunden von SolarWinds waren. Das US-amerikanische Cybersicherheitsunternehmen FireEye entdeckte als erstes den Angriff [26].

Da keine festen Beweise gefunden wurden, wie APT29 auf die internen System von SolarWinds gelangt sind, um in deren Software eine Backdoor einzubauen, wird im Folgenden nur die Kompromittierung der Kunden von SolarWinds analysiert. Dabei wird der Angriff auf eine nicht näher benannte us-amerikanische Denkfabrik genauer betrachtet, der durch das Unternehmen Volexity beobachtet wurde.

A. Zeitlicher Ablauf

Der Begin der Attacke wird auf den 06.08.2019 datiert, dort wurde die erste bekannte Infrastruktur für die Attacke angelegt. Die erste Modifikation der SolarWinds Software geht auf den 26.10.2019 zurück, wobei die erste ausnutzbare Schwachstelle in den Softwareupdates ab März 2020 enthalten war, die als SUNBURST-Malware bezeichnet wird. Am 13.12.2020 wurde der SolarWinds Report von Fireeye veröffentlicht und somit der Angriff öffentlich bekannt. Ein Tag später wurde von SolarWinds ein Sicherheitshinweis zur Attacke herausgegeben. Am 15.12.2020 wurde die SUNBURST C2 (Command and Control) Domaine durch Microsoft beschlagnahmt [27]. Im durch Veloxity beobachteten Angriff wurde im Juli 2020 die Malware in SolarWinds Orion ausgenutzt [28].

B. Aufklärung

Die Aufklärungsphase ist im SolarWinds Compromise etwas schwammig. Die Malware SUNBURST, die durch ein Update der SolarWinds Orion Platform mit installiert wurde, dient u. A. dazu, Aufklärung im Netzwerk der Opfer zu betreiben [29]. Jedoch wurde die Malware zuerst ausgeliefert und installiert, wesshalb hier die Reihenfolge der Killchain nicht exakt wiedergegeben wird. Wie in Abb. 2 vermerkt ist, ist die Killchain auch nur ein idealisiertes Modell, und der SolarWinds Compromise unterstützt diese Aussage durch das verdrehen der Schritte.

C. Auslieferung und Installation

Die Malware SUNBURST wurde durch ein Softwareupdate durch authorisierte Systemadministratoren heruntergeladen und installiert [30].

SUNBURST wurde in die SolarWinds.Orion.Core.BusinessLayer.dll eingeschleust. Dort wurde die Malware in einer Methode aktiviert die in regelmäßigen Abständen aufgerufen wurde. Das stellte sicher, dass die Persistenz der Malware gewährleistet ist und neustart eines Systems immer wieder ausgeführt wurde. Neben einigen Bedingungen, prüft die Malware vor ihrem Start, ob Prozesse laufen, die einer Sicherheitssoftware zugeordnet werden können, um sich vor diesen zu verstecken. Sobald die Malware gestartet ist, baut sie eine Verbindung zu einem C2 (Command and Control) Server auf, um grundlegende Informationen über das System zu übermitteln. Über den C2 Server können Befehle an die Malware übermittelt werden und ermöglichen eine vollen Zugriff auf das System [29].

D. Erneute Aufklärung

Im durch Veloxity beobachteten Angriff wurde nach dem Eindringen in das Netzwerk erneut Aufklärungsarbeit betrieben. Es wurden mittels Powershell Konfigurationseinstellung im Exchange der Organisation ausgelesen. Darunter befanden sich Informationen über Exchange-Nutzer und deren aktuellen Rollen. Vgl. zu diesem Abschnitt Cash et al. [28].

E. Verbreitung

Um sich im Netzwerk zu verbreiten erstellten die Angreifer mittels PowerShell neue geplante Aufgaben auf weiteren Systemen [28].

F. Exfiltration

Der Zugriff auf den Exchange Server der Denkfabrik ermöglichte es den Angreifern via PowerShell-Kommands Mailboxen zu extrahieren. Diese wurden in ein passwort-geschütztes Archiv verpackt, um durch eine HTTP-Anfrage exfiltriert werden zu können. Um Verteidigungsmechanismen zu umgehen wurde das Archiv als PNG Bilddatei über eine URL zur verfügung gestellt. Zusätzlich fügten die Angreifer ein eigenes Gerät als zulässige ID für die aktive Synchronisierung für eine Reihe an Postfachern hinzu, um weiterhin Zugriff auf die Postfächer zu erhalten. Vgl. zu diesem Abschnitt Cash et al. [28].

G. Beweise löschen

Nach der erfolgreichen Exfiltration der E-Mails, wurde die Export-Anfrage aus dem Exchange Server gelöscht.

IV. Verteidigung gegen Advanced Persistent Threats

A. Threat Hunting

Unter Theat Hunting versteht man die Kombination von Netwerkverkehr, Logs, Code und anderen mehrquelligen Daten, um den Host, Angriffspfad, den Angreifer und die Angrifssorganisation, die den Angriff gestartet hat, durch die

verschiedenen Techniken und Methoden zu lokalisieren [31]. Sicherheitsunternehmen haben in den letzten Jahren viele Forschungsberichte zu APT-Angriffen veröffentlicht, jedoch meist nach den Angriffen [31]. Durch die Entwicklung von Deep-Learning und traditionellen maschinellen Lern-Technologien, hat es fortschritte bezüglich Erkennung und Rückverfolgung von APT-Angriffen basierend auf der Analyse von Provenance Graphen gegeben [31].

1) UNICORN: UNICORN ist ein Angriffserkennungssystem, welches versucht Angriffe auf mehrere Hosts gleichzeitig zu erkennen [32]. Als Eingabe nutzt UNICORN einen Provenence Graphen mit benannten Kanten, der dauerhaft aktualisiert wird. Daraus wird ein Histogramm konstruiert, siehe Abb. 3 Schritt 2, wobei jedes Histogrammelement eine eindeutige Substruktur des Graphen beschreibt. UNICORN reduziert dabei den Einfluss von Histogrammelementen, die in keinen kausalen Zusammenhang mit den aktuellen Ereignissen im System stehen. Aufgrund der Datenmenge wendet UNICORN eine ähnlichkeitserhaltende Hashing-Technik an und wandelt so das Histogramm in eine Graphenskizze um, siehe Abb. 3 Schritt 3. Daraus erstellt UNICORN ein normales Systemausführungsmodell und identifiziert abnormale Aktivitäten ohne Wissen über Angriffe. Dafür erfasst das Modell Verhaltensänderungen innerhalb einer einzelnen Ausführung, indem es Systemaktivitäten in verschiedenen Phasen der Ausführung clustert und Veränderungen erkennt. Das Modell wird dabei nicht dynamisch während der Laufzeit angepasst, desshalb ist es besser geeignet für lang laufende Systeme, die vorher analysiert werden können. Vgl. zu diesem Abschnitt Han et al. [32].

2) HOLMES: HOLMES ist ein System, welches versucht aus Ereignisspuren auf effiziente Weise Alarme zu generieren. Zuerst sammelt HOLMES Audit-Protokolle von veschiedenen Systemen, die Ereignisse, von beispielsweise Dateiveränderungen, Prozessen und Netzwerkverbindungen, enthalten. Diese Daten werden in einem Provenance Graphen abgebildet, bei dem die Knoten des Graphen Subjekte (Prozesse) und Objekte (Dateien, Sockets) bilden und die Kanten die Abhängigkeiten mit Ereignisnamen zwischen diesen darstellen. Zur weiteren Verarbeitung der Daten ist eine Sammlung an Taktiken, Techniken und Prozeduren von APTs nötig. Diese Sammlung verbindet Taktik, Technik und Prozedurs (TTPs) mit Ereignissen, Vorbedingungen und Schweregrad und Gruppiert diese in die Schritte der Killchain. Aus dem Graphen der Ereignisse und der Sammlung von TTPs wird ein High-Level Szenario Graph (HSG) erstellt. Bei diesem bilden die Knoten die TTPs ab, die Kanten den Informationsfluss zwischen den Elementen die zur TTP zugeordnet sind. Dazu wird der Provenance Graph nach den Vorbedingungen der TTPs analysiert und wenn alle Vorbedingugen einer TTP erfüllt sind, wird diesen in den HSG hinzugefügt. Um den HSG zu bewerten, wird aus den TTPs der höchste Schweregrad einer TTP der Aufklärungsphase gewählt. Vgl. zu diesem Abschnitt Milajerdi et al. [33].

B. Visuelle Analytik mit dem MASFAD-Framework

Das Multi-agent System for Advanced Persistent Threat Detection (MASFAD) bietet die Möglichkeit APTs mittels Anomalie- und verhaltensbasierter Analyse zu erkennen. Dabei fokusiert sich das Framework auf das erkennen von zuvor nicht erkannter oder unbekannter Bedrohungen. MASFAD konzentriert sich stärker auf die von verschiedenen Sensoren im Netzwerk gesammelten Daten, als auf die Topologie des Netzwerks. Dabei steht der Analyst selbst im Mittelpunkt und dessen Fachwissen wird durch die vorgeschlagene Visualisierung von MASFAD erweitert. Durch die verschiedenen Visualisierungsformen sollen dem Analysten die Daten verständlich aufbereitet werden und verhelfen korrekte Annahmen über Aktivitäten im Netzwerk zu treffen. Vgl. zu diesem Abschnitt Nikolov und Mees [34].

V. Fazit

APT sind Aufgrund ihres Durchhaltevermögens eine besondere Gefahr für Unternehmen, Regierungen und sonstige Organisationen. Die in der Arbeit gezeigte Vorgehensweise von APTs macht deutlich, wie Aufwändig und Schwierig es ist sie zu erkennen, gar zu bekämpfen. Das zeigt besonders der SolarWinds Compromise der sogar amerikanische Behörden bedroffen hat, die selbst in der Informationssicherheit tätig sind. Durch diverse Maßnahmen wie Mitarbeiterschulungen und gute Systemadministration können zwar Hürden geschaffen werden, jedoch keine APT wirklich davon abgehalten werden, das System zu kompromittieren. Wird ein Weg blockiert, sucht sich eine finanzkräftige und personenstarke APT den nächsten Weg und wiederholt alles, bis das Ziel erreicht ist.

Die vorgestellten Verteidigungstechniken wie HOLMES, UNICORN und das MASFAD-Framework können bei der Sicherung von Systemen unterstützend wirken. Jedoch sind Ressource, v. a. Fachpersonal, weiterhin notwendig, um die Erkenntnisse der Verteidigungstechniken anzuwenden.

Literatur

[1] Statista. Estimated cost of cybercrime worldwide 2017-2028. Accessed on: Oct. 30, 2023. [Online]. Available: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

[2] Bundesamt für Sicherheit in der Informationstechnik, "Die lage der it-sicherheit in deutschland."

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

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

[5] MITRE Corporation. Solarwinds compromise. MITRE Corporation. Accessed on: Nov. 7, 2023. [Online]. Available: https://attack.mitre.org/versions/v14/campaigns/C0024/

[6] SolarWinds Worldwide, LLC. Orion platform. Accessed on: Dec. 07, 2023. [Online]. Available: https://www.solarwinds.com/de/orion-platform

[7] Cybersecurity and Infrastructure Security Agency. Joint statement by the federal bureau of investigation (fbi), the cybersecurity and infrastructure security agency (cisa), the office of the director of national intelligence (odni), and the national security agency (nsa). Accessed on: Nov. 4, 2023. [Online]. Available: https://www.cisa.gov/news-events/news/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

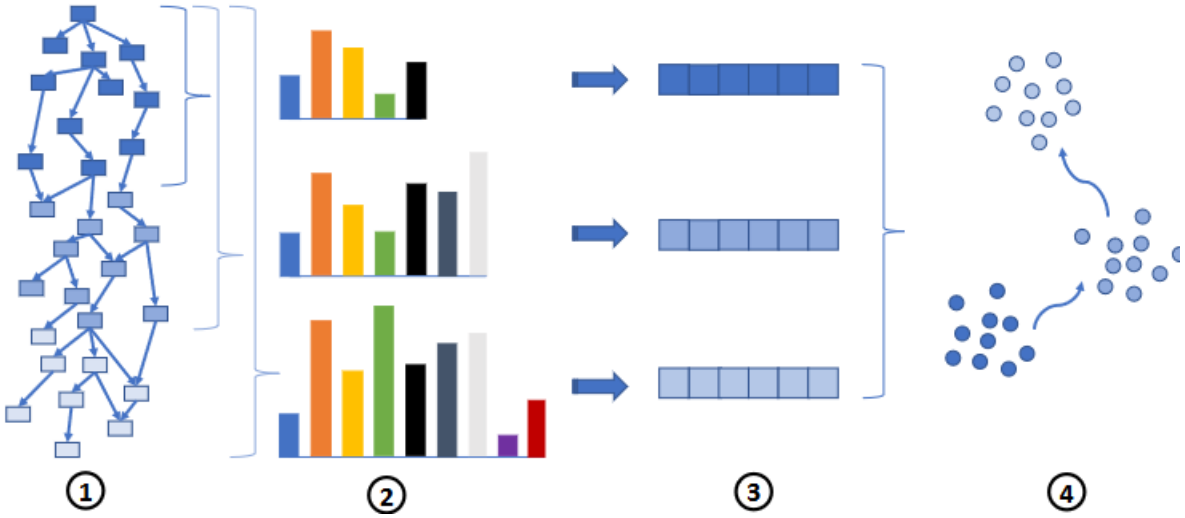

Abbildung 3. Schematischer Aufbau von UNICORN; Quelle: [32]

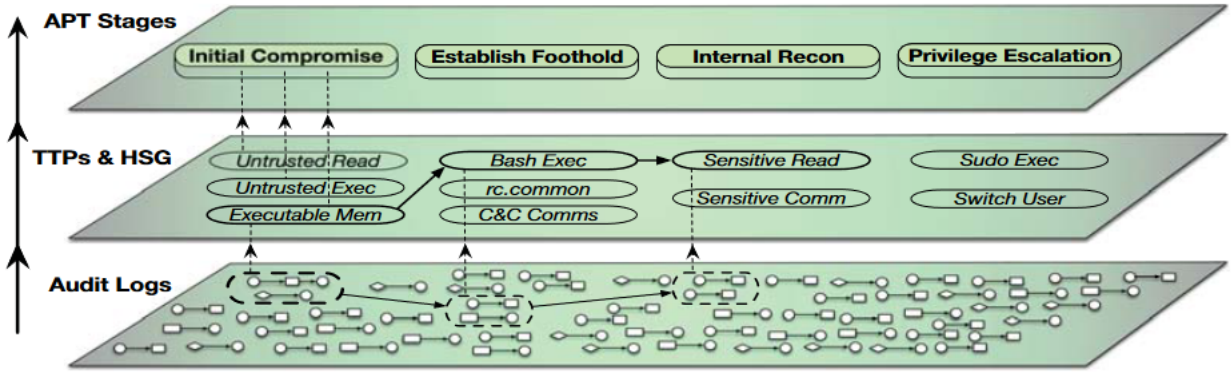

Abbildung 4. Schematischer Aufbau von HOLMES; Quelle: [33]

[8] Foreign Commonwealth and Development Office and The Rt Hon Dominic Raab MP. Russia: Uk and us expose global campaign of malign activity by russian intelligence services. Accessed on: Dec. 07, 2023. [Online]. Available: https://www.gov.uk/government/news/russia-uk-and-us-expose-global-campaigns-of-malign-activity-by-russian-intelligence-services

[9] NSA. Russian svr targets u.s. and allied networks. U/OO/132340-21.

[10] MITRE Corporation. Apt29. Accessed on: Dec. 07, 2023. [Online]. Available: https://attack.mitre.org/versions/v14/groups/G0016/

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

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

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

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

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

[16] ——. Execution. Accessed on: Nov. 25, 2023. [Online]. Available: https://attack.mitre.org/versions/v14/tactics/TA0002/

[17] ——. Persistence. Accessed on: Nov. 25, 2023. [Online]. Available: https://attack.mitre.org/versions/v14/tactics/TA0003/

[18] Statista. Wo hacker angreifen. Accessed on: Dec. 06, 2023. [Online]. Available: https://de.statista.com/infografik/17721/verteilung-von-cyberattacken-nach-betroffenen-plattformen/

[19] nicholasswhite, DHB-MSFT, skeith92, and kellieei. Macros from the internet are blocked by default in office. Accessed on: Dec. 06, 2023. [Online]. Available: https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked

[20] MITRE Corporation. Privilege escalation. Accessed on: Dec. 07, 2023. [Online]. Available: https://attack.mitre.org/versions/v14/tactics/TA0004/

[21] ——. Create or modify system process. Accessed on: Dec. 07, 2023. [Online]. Available: https://attack.mitre.org/versions/v14/techniques/T1543/

[22] ——. Lateral movement. Accessed on: Nov. 28, 2023. [Online]. Available: https://attack.mitre.org/versions/v14/tactics/TA0008/

[23] ——. Exfiltration. Accessed on: Dec. 05, 2023. [Online]. Available: https://attack.mitre.org/versions/v14/tactics/TA0010/

[24] ——. Automated exfiltration. Accessed on: Dec. 05, 2023. [Online]. Available: https://attack.mitre.org/versions/v14/techniques/T1020/

[25] ——. Scheduled transfer. Accessed on: Dec. 05, 2023. [Online]. Available: https://attack.mitre.org/techniques/T1029/

[26] R. Alkhadra, J. Abuzaid, M. AlShammari, and N. Mohammad, "Solar winds hack: In-depth analysis and countermeasures," in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2021.

[27] Unit 42. Solarstorm supply chain attack timeline. Accessed on: Dec. 07, 2023. [Online]. Available: https://unit42.paloaltonetworks.com/solarstorm-supply-chain-attack-timeline/

[28] D. Cash, M. Meltzer, S. Koessel, S. Adair, and T. Lancaster. Dark halo leverages solarwinds compromise to breach organizations. Accessed on: Dec. 07, 2023. [Online]. Available: https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/

[29] Microsoft Theat Intelligence. Analyzing solorigate, the compromised dll file that started a sophisticated cyberattack, and how microsoft defender helps protect customers. Accessed on: Nov. 6, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

[30] FIREEYE. Highly evasive attacker leverages solarwinds supply chain to compromise multiple global victims with sunburst backdoor. Accessed on: Dec. 07, 2023. [Online]. Available: https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

[31] L. Chen, R. Jiang, C. Lin, and A. Li, "A survey on threat hunting: Approaches and applications," in *2022 7th IEEE International Conference on Data Science in Cyberspace (DSC)*. IEEE.

[32] X. Han, T. Pasquier, A. Bates, J. Mickens, and M. Seltzer, "Unicorn: Runtime provenance-based detector for advanced persistent threats," 2020.

[33] S. M. Milajerdi, R. Gjomemo, B. Eshete, R. Sekar, and V. Venkatakrishnan, "Holmes: Real-time apt detection through correlation of suspicious information flows," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE.

[34] G. Nikolov and W. Mees, "Detection of previously unknown advanced persistent threats through visual analytics with the masfad framework," in *2023 International Conference on Military Communications and Information Systems (ICMCIS)*. IEEE.