-

Controlware GmbH

WHITEPAPER

Supply Chain-Angriffe

www.controlware.de

Version: 1.0 Verfasser: Benjamin Heyder, Martin Ruffertshöfer, Andreas Unrath Klassifizierung: EXTERN

Controlware GmbH
Waldstraße 92
63128 Dietzenbach

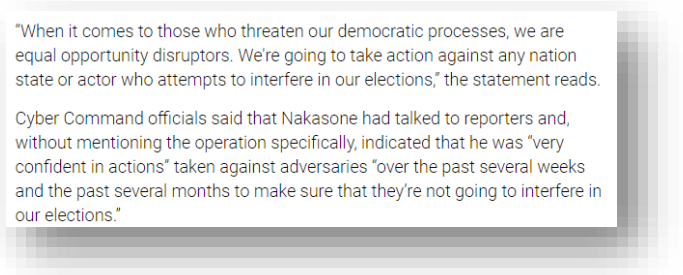
Telefon +49 6074 858-00
Telefax +49 6074 858-108
info@controlware.de
www.controlware.de
blog.controlware.de

Sitz: Controlware GmbH Kommunikationssysteme ■ Waldstraße 92 ■ 63128 Dietzenbach ■ GERMANY
Tel. +49 6074 858-00 ■ Fax +49 6074 858-108 ■ info@controlware.de ■ www.controlware.de
Sitz Dietzenbach ■ Registergericht Offenbach a.M. ■ HRB Nr. 6431 ■ USt-IdNr. DE 113 539 225 ■ Steuernummer 3523035235
Geschäftsführer: Bernd Schwefing, Oliver Thome

Supply Chain-Angriffe – Ein Blick hinter die Kulissen

One Vendor. One Platform. One Supply Chain to compromise them all….

Am Tag der US-Wahl meldete sich General Paul Nakasome, Direktor der NSA und Oberbefehlshaber des US Cyber Command, über Journalisten zu Wort und gab bekannt, dass die Wahlen frei von ausländischer Einflussnahme durchgeführt wurden.


"When it comes to those who threaten our democratic processes, we are equal opportunity disruptors. We're going to take action against any nation state or actor who attempts to interfere in our elections," the statement reads.

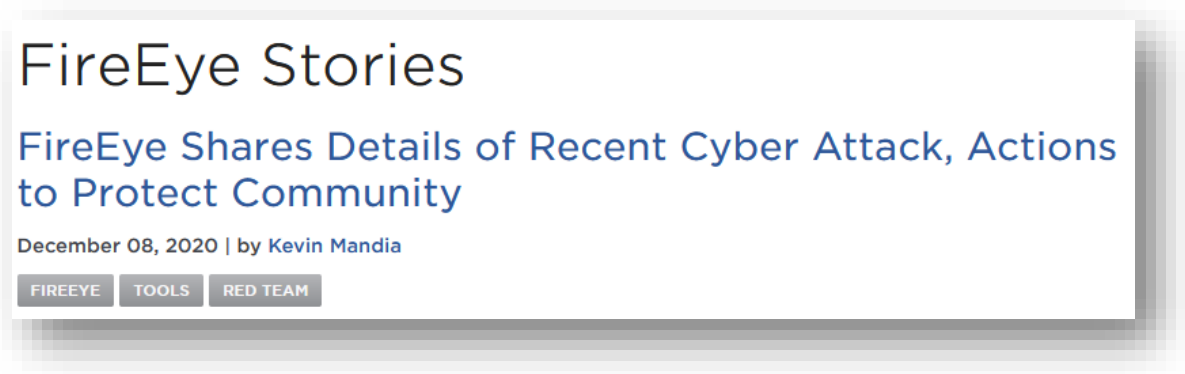
Cyber Command officials said that Nakasone had talked to reporters and, without mentioning the operation specifically, indicated that he was "very confident in actions" taken against adversaries "over the past several weeks and the past several months to make sure that they're not going to interfere in our elections."

Etwas mehr als acht Wochen danach, erleben wir die Auswirkungen eines der größten und weitreichendsten Cyberangriffe, den die Welt je gesehen hat. Mehrere tausend Unternehmen und Behörden sind weltweit betroffen, mit ungewissen Auswirkungen. Handelt es sich um eine „einfache“ Spionage-Aktion oder wurde die Kompromittierung dazu genutzt, Hintertüren in betroffene Unternehmen, Behörden und Versorger zu integrieren? Was aktuell wie Panikmache oder pure Fiktion klingt, ist bittere Realität.

Supply Chain-Angriffe lassen sich vor allem in der Phase des initialen Zugriffs kaum verhindern. Ziel sollte es also sein, zumindest eine Ausbreitung und Folgeaktivitäten des Angreifers zu erkennen und in der Lage zu sein, Fragen nach dem Ausmaß des Angriffs zu beantworten und entsprechende Maßnahmen abzuleiten.

Mit diesem Whitepaper möchten wir das bisher Geschehene aufarbeiten, einordnen und dem geneigten Leser eine Möglichkeit bieten, Entscheidungen auf Basis solider Informationen zu treffen. Am Ende des Dokuments befinden sich eine Quellensammlung und ein Glossar. Eine Anmerkung der Autoren sei noch gestattet: In diesem Dokument möchten wir niemandem etwas vorwerfen und in keiner Art und Weise Schuldzuweisungen aussprechen. Die meisten der betroffenen oder beteiligten Unternehmen haben sich vorbildlich und uneigennützig verhalten. Besonders die Rolle des Netzwerksicherheits- und Dienstleistungsanbieters FireEye sei hier hervorzuheben.

Am 08.12.2020 meldete FireEye über seine Webseite und per E-Mail, dass der Security-Experte Opfer einer ausgefeilten Cyberattacke wurde und ein sogenannter Nation State Actor dahinter vermutet wird, da der Angriff besonders komplex und zielgerichtet wirkte.


FireEye Stories

FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community

December 08, 2020 | by Kevin Mandia

FIREEYE TOOLS RED TEAM

Nach weiteren Untersuchungen gab FireEye am 11.12.2020 bekannt, dass die Angreifer das Unternehmen über eine sogenannte Supply Chain-Attacke kompromittiert haben. Der kompromittierte Zulieferer war SolarWinds, von dem FireEye das Netzwerkmanagement-System Orion nutzt.

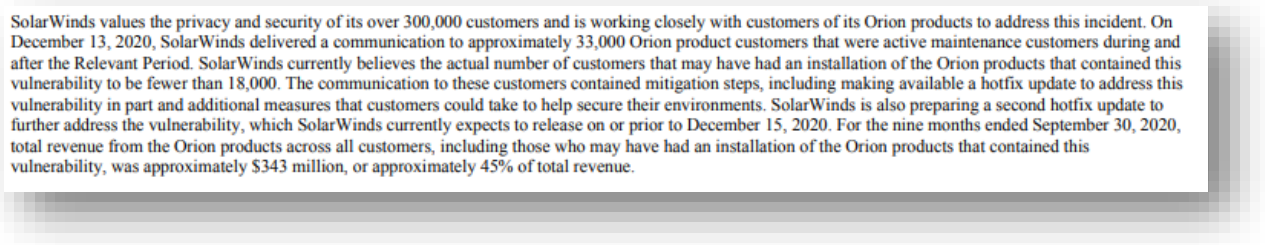

FireEye Stories

Global Intrusion Campaign Leverages Software Supply Chain Compromise

December 13, 2020 | by Kevin Mandia

FIREEYE

Wie sich herausstellte, war FireEye nur eines der Opfer in dieser weitreichenden Angriffskampagne. Erste Schätzungen vermuteten über 500 betroffene Unternehmen, aktuell geht man allerdings von mehr als 18.000 potentiellen Unternehmen aus. Bis heute ist nicht ganz klar, wie SolarWinds genau kompromittiert wurde.


SolarWinds values the privacy and security of its over 300,000 customers and is working closely with customers of its Orion products to address this incident. On December 13, 2020, SolarWinds delivered a communication to approximately 33,000 Orion product customers that were active maintenance customers during and after the Relevant Period. SolarWinds currently believes the actual number of customers that may have had an installation of the Orion products that contained this vulnerability to be fewer than 18,000. The communication to these customers contained mitigation steps, including making available a hotfix update to address this vulnerability in part and additional measures that customers could take to help secure their environments. SolarWinds is also preparing a second hotfix update to further address the vulnerability, which SolarWinds currently expects to release on or prior to December 15, 2020. For the nine months ended September 30, 2020, total revenue from the Orion products across all customers, including those who may have had an installation of the Orion products that contained this vulnerability, was approximately $343 million, or approximately 45% of total revenue.

Bildunterschrift: Auszug aus dem SEC Report von SolarWinds

Bekannt ist nur, dass es den Angreifern gelungen ist, sich in die Software-Updates und in den Software-Signierprozess des Unternehmens einzuklinken und über die offiziellen Update-Server maliziöse Programmbibliotheken zu verteilen. Die Programmbibliotheken waren Teil der SolarWinds Orion-Plattform. Dabei handelt es sich um ein zentrales Netzwerkmanagement-System, das zur Verwaltung diverser Netzwerk- und Security-Produkte genutzt wird. Die Update-Server dienten den Angreifern als Verteilmechanismus, um die maliziöse Software zu verteilen. Dabei wurde die Tatsache ausgenutzt, dass Update-Server oftmals geringeren Sicherheitskontrollen ausgesetzt sind und häufig als vertrauenswürdig gelten. Wer an dieser Stelle beim Lesen stutzt, dem sei ein Blick in seine eigenen Firewalls oder Proxy Whitelists nahegelegt. Den Angreifern ist es gelungen, sich so tief in den Software-Entwicklungs- und Bereitstellungsprozess bei SolarWinds einzuklinken, dass die maliziösen Programmbibliotheken sogar offiziell signiert wurden. Man geht aktuell nicht davon aus, dass irgendwelche CAs kompromittiert wurden. Die Angreifer taten alles dafür, um die Kampagne möglichst lange geheim zu halten. Laut Dokumenten der Börsenaufsichtsbehörden geht SolarWinds davon aus, seit März 2020 kompromittiert worden zu sein.

Auch die Auswahl von SolarWinds geschah keinesfalls zufällig. Durch die Art der Software und dem Betätigungsfeld ist das Unternehmen interessantes Einfallstor für diese Art von Angriffen. Die Situation ist aktuell noch immens in Bewegung und täglich kommen neue Details ans Licht, wie zum Beispiel, dass Microsoft ebenfalls zu den Opfern gehört und die Angreifer in der Lage waren, den Quellcode von Windows-Betriebssystemen einzusehen.

Die Auswirkungen lassen sich im Grunde wie folgt zusammenfassen:

- Der „Erfolg“ des SolarWinds Hacks gab den Angreifern weitreichenden Zugriff auf unterschiedlichste Firmen- und Regierungssysteme.
- Hervorzuheben ist, dass es sich bei den Opfern des Angriffs um extrem gut gesicherte Unternehmen gehandelt hat, die eine durchdachte Cybersecurity-Policy „adopted“ haben.
- Es handelt sich höchstwahrscheinlich um staatliche Akteure.
- Eine der Konsequenzen könnten „Cyber-physische“ Auswirkungen sein. (Stromausfall)
- Die langwierige und weitreichende Angriffskampagne macht ein Abschätzen der konkreten Auswirkungen so gut wie unmöglich.
- Cisco und Microsoft waren Opfer des Angriffs. Die Unternehmen haben zwar ihre Erkenntnisse transparent geteilt, die finalen Konsequenzen sind aber nicht abzusehen.
- Die SUNBURST/Teardrop Malware war nur das Vehikel, das weitere Angriffe und Eingriffe in die Unternehmensnetzwerke ermöglicht.
- Es ist nicht auszuschließen, dass sich die Angreifer bereits anderweitig im Netzwerk persistiert haben.
- Eine 100%ige Sicherheit, dass alle potentiellen Hintertüren im Unternehmen geschlossen sind, sofern die initiale Infektion mit SUNBURST/Teardrop bestätigt ist, ist nur durch eine komplette Neuinstallation der gesamten IT-Infrastruktur zu realisieren. Auch wenn dies utopisch klingt, so entspricht es doch der aktuellen Lage.
- Der Angriff wirft ein Schlaglicht auf das Risiko, das durch Zulieferer innerhalb einer Wertschöpfungskette besteht.
- Der Angriff zeigt auch, warum Unternehmen schnell einen Least Privilege-Ansatz adaptieren sollten.
- Die aktuell vorhandenen Threat-Modelle bilden das Risiko eines solchen Angriffs meist nur rudimentär ab und müssen überarbeitet werden.
- Software-Signaturen sind kein Garant für sichere Software.
- Unternehmen sollten ständig die benötigten Privilegien von Software und den angrenzenden Prozessen validieren.

Da die Situation noch eine extreme Dynamik vorweist und sich die Nachrichtenlage beinahe täglich verändert, fokussieren wir uns in diesem Dokument ausschließlich auf den Vorfall SolarWinds/SUNBURST. An notwendigen Stellen wird auf das entsprechende Datum der Quellinformation verwiesen, um Transparenz über die Aktualität zu schaffen.

Von der Forensik innerhalb eines Unternehmens zur weltweiten Zusammenarbeit

Die Timeline der medialen Berichterstattung über den Vorfall veranschaulicht sehr gut, was bei den meisten Sicherheitsvorfällen in Firmen im Hintergrund passiert. Hier lässt sich anschaulich zeigen, was Analysten im Bereich der Forensik leisten und welche Bereiche in die Aufarbeitung und Schadensbegrenzung involviert sind. Es handelt sich nämlich nicht nur um IT-Abteilungen und Dienstleister, sondern auch um Vorstände, Marketingverantwortliche, Pressesprecher etc. sowie andere Abteilungen. Im ungünstigsten Fall kann auch eine Prüfung der Börsenaufsicht erfolgen.

08.12.2020:
FireEye: Der Netzwerksicherheits- und Dienstleistungsanbieter FireEye Informiert über das Eindringen in das eigene Netz und die Entwendung von Red Team Tools.
Link. *https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html*

09.12.2020:
SolarWinds: SolarWinds gibt Veränderungen im Vorstand bekannt.
Aktienhandel: CPP Investments (Canada Pension Plan Investment Board) kauft SolarWinds Anteile von Private Equity-Firmen (Silver Lake, Thoma Bravo und deren Co-Investoren).

11.12.2020:
FireEye: Der Netzwerksicherheits- und Dienstleistungsanbieter FireEye findet bei der Angriffsanalyse ein kompromittiertes Update der SolarWinds Orion Software.

12.12.2020:
FireEye: Der Netzwerksicherheits- und Dienstleistungsanbieter FireEye Informiert den CEO von SolarWinds über die Findings innerhalb der Software.
Link: *https://seekingalpha.com/filing/5276758*

NSC: Notfallmeeting des National Security Concil (NSC) im Weißen Haus
Link: *https://www.reuters.com/article/us-usa-cyber-amazon-com-exclsuive-idUSKBN28N0PG*

13.12.2020:
FireEye: Offizielle Veröffentlichung der SUNBURST Backdoor durch FireEye
Link: *https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html*

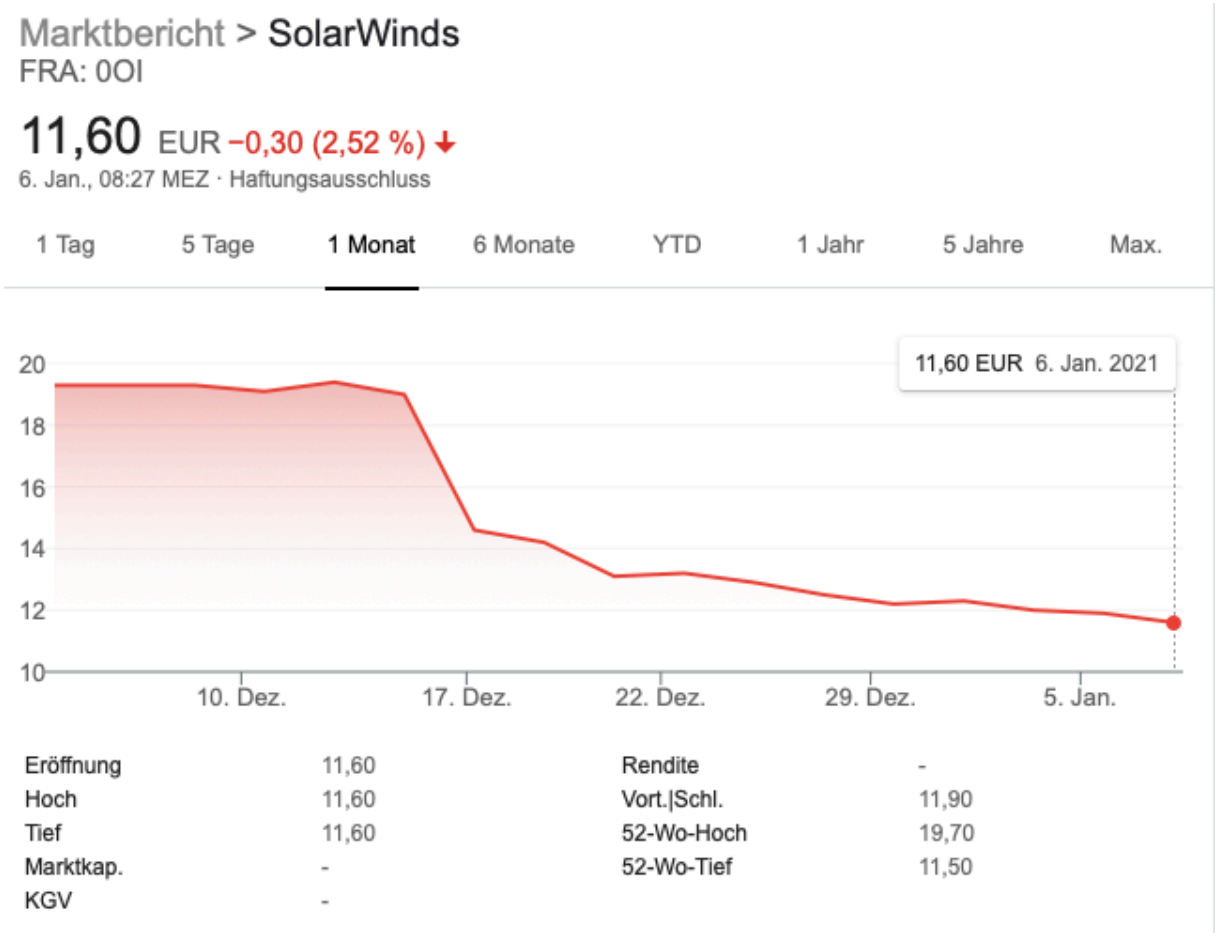
13.12.2020:
DHS-CISA: CISA Emergency Directive (21-01). Order zur Abschaltung aller SolarWinds Orion-Systeme
Link: *https://cyber.dhs.gov/ed/21-01/*

SolarWinds: Security Advisory durch SolarWinds
Links: *https://www.solarwinds.com/securityadvisory; https://www.msspalert.com/cybersecurity-news/solarwinds-orion-vulnerability-investigation/*

https://www.msspalert.com/cybersecurity-news/solarwinds-orion-vulnerability-investigation/
FireEye: Disclosure (Veröffentlichung)
Link: *https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html*

Microsoft: Veröffentlichung Orientierungshilfe
Link: *https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html*

14.12.2020:
SolarWinds/Börse: Das Unternehmen SolarWinds legt die Verwundbarkeit offiziell offen, wonach der Aktienkurs drastisch fällt.
Link. *https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm*



Bildquelle: Google

15.12.2020:

Wall Street Journal: Medienberichte über die Opfer des Angriffs, wonach sich unter den Opfern unter anderem das U.S. Commerce and Treasury Department, das Department of Homeland Security (DHS), das National Institute of Health und das State Department befinden.

Link: *https://www.wsj.com/articles/suspected-russian-hack-said-to-have-gone-undetected-for-months-11607974376?mod=tech_lead_pos3*

United States Senate: US Senatoren verlangen Antworten bezüglich der SolarWinds Cyberattacke.

Link: *https://www.moran.senate.gov/public/_cache/files/e/d/ed2078ad-8f58-460a-ab54-5ffe570bfd23/9E2CFEA30538117FF470015E-BAD88368.12.15.2020---letter-to-cisa-and-fbi-re-solarwinds---final-signed.pdf*

16.12.2020:

CRN Magazine: SolarWinds teilt mit, dass sie die kompromittierten Zertifikate für ihre MSP Tools zurückziehen werden und Kunden diese erneut signieren müssen.

Link: *https://www.crn.com/news/managed-services/solarwinds-msp-to-revoke-digital-certificates-for-tools-issue-new-ones-as-breach-fallout-continues*

KrebsonSecurity: Sicherheitsexperten finden Kill Switch

Link: *https://krebsonsecurity.com/2020/12/malicious-domain-in-solarwinds-hack-turned-into-killswitch/*

New York Times: Tom Bossert, früherer Homeland Security-Berater unter Präsident Trump, spricht in einem Artikel der New York Times über die Tragweite des Vorfalls.

DHS-CISA: Das Federal Buero of Investigation der Vereinigten Staaten (FBI) untersucht die Bedrohungslage und sammelt Informationen, um die Verantwortlichen zuordnen und verfolgen zu können.

Link: *https://www.cisa.gov/news/2020/12/16/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure*

CNBC/Washington Post: Mediale Spekulationen über potentiellen Insiderhandel (Aktienhandel zwei Tage vor offizieller Bekanntgabe)
Link: *https://www.cnbc.com/2020/12/16/solarwinds-hack-triggers-23percent-stock-haircut-this-week-so-far.html; https://www.washingtonpost.com/technology/2020/12/15/solarwinds-russia-breach-stock-trades/#*

17.12.2020:

Microsoft: Microsoft findet eine Kompromittierung bei 40 der Kunden, wovon ca. 44 % in den Bereichen IT-Service Provider, Software oder Technologie zu finden sind.

Link: *https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/?source=content_type%3Areact%7Cfirst_level_url%3Anews%7Csection%3Amain_content%7Cbutton%3Abody_link*

POLITICO: Bekanntwerden, dass die National Nuclear Security Administration (diese unterhält den US Atomwaffenvorrat) auch zu den angegriffenen Zielen gehört.
Link: *https://www.politico.com/news/2020/12/17/nuclear-agency-hacked-officials-inform-congress-447855*

Microsoft: Microsoft bestätigt maliziöse Binaries in ihrer Umgebung und, dass diese isoliert und entfernt wurden.
Link: *https://twitter.com/fxshaw/status/1339728948104581120?source=content_type%3Areact%7Cfirst_level_url%3Anews%7Csection%3Amain_content%7Cbutton%3Abody_link*

Seeking Alpha: SolarWinds gibt Statement bezüglich Insiderhandelsspekulationen in der Washington Post vom 15.12.2020 zu.
Link: *https://seekingalpha.com/filing/5276758*

The Hill: President-elect Joe Biden gibt Statement bezüglich des weiteren Vorgehens zum Umgang mit dem Angriff nach dessen Amtseinführung.
Link: *https://thehill.com/policy/cybersecurity/530706-biden-vows-to-make-cybersecurity-imperative-following-massive-hack*

18.12.2020

SentinelOne: In dem SentinelLabs Blog bestätigt James Haughom, dass für Firmen, die SentinelOne im Einsatz haben, nie eine Gefahr bestanden hat. Die Kunden sind nicht nur sicher aufgrund der Detektionsfähigkeit von SentinelOne, sondern auch weil SUNBURST sich eigenständig sofort beendet, wenn der geladene SentinelOne Treiber auf einem System vorgefunden wird.

Link: *https://labs.sentinelone.com/solarwinds-sunburst-backdoor-inside-the-stealthy-apt-campaign/*

19.12.2020:

Wall Street Journal: Mike Pompeo macht Russland für den Angriff verantwortlich.

Link: *https://www.wsj.com/articles/pompeo-blames-russia-for-solarwinds-hack-11608391515*

Bloomberg: Recorded Future identifiziert 198 Unternehmen, die über die SolarWinds Backdoor kompromittiert wurden.

Link: *https://www.bloomberg.com/news/articles/2020-12-19/at-least-200-victims-identified-in-suspected-russian-hacking*

21.12.2020:

CNBC: In einem CNBC Interview teilt Treasury Secretary Steven Munich mit, dass im U.S. Treasury Department keine Anzeichen für einen Einbruch in klassifizierte Systeme nachgewiesen werden konnten.

Link: *https://www.channele2e.com/technology/security/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details/*

Wall Street Journal: Es werden mindestens 24 Unternehmen identifiziert (von Technologie über Krankenhaus bis hin zu Universitäten), die das kompromittierte Update eingespielt hatten. Hierzu gehören unter anderem namenhafte Hersteller wie beispielsweise Cisco Systems, Intel, Nvidea, Deloitte, VMware und Belkin. Ob die Angreifer weitere Schritte ausgeführt haben, ist derzeit nicht bekannt.

Link: *https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402?mod=tech_lead_pos1*

22.12.2020:

AP News: Einen Tag nach dem Interview mit Steven Munich wird bekannt, dass einige E-Mail-Accounts der U.S. Treasury Departments kompromittiert wurden.

Link: *https://apnews.com/article/technology-politics-ron-wyden-russia-hacking-572ac201e8f365cf6ec218b478742aa0*

23.12.2020:

Crowdstrike: Fehlgeschlagener Einbruchsversuch in die CrowdStrike Azure-Umgebung.

Link: *https://www.crowdstrike.com/blog/crowdstrike-launches-free-tool-to-identify-and-help-mitigate-risks-in-azure-active-directory/*

GitHUB: CrowdStrike veröffentlicht freies Tool zur Risikoidentifizierung in Azure-Umgebungen.

Link: https://github.com/CrowdStrike/CRT

24.12.2020:

SolarWinds: Veröffentlichung Statement und Patch bezüglich der SUPERNOVE Malware

Link: https://investors.solarwinds.com/news/news-details/2020/SolarWinds-Releases-Updates-to-Address-Vulnerability-Related-to-SUPERNOVA-Malware/default.aspx

30.12.2020:

DHS-CISA: Das CISA aktualisiert seine Emergency Directive 21-01 (Pflicht-Update der SolarWinds Orion-Plattform auf Version 2020.2.1HF2).

Link: https://cyber.dhs.gov/ed/21-01/#supplemental-guidance

31.12.2020:

New York Times: Microsoft teilt mit, dass russische Hacker Einblick in Teile des Source Codes von Microsoft Software erhalten haben, jedoch diesen nicht verändern konnten.

Link: https://www.nytimes.com/2020/12/31/technology/microsoft-russia-hack.html

05.01.2021:

The Hill: U.S. Geheimdienste beschuldigen offiziell Russland, mit den jüngsten Angriffen in Verbindung zu stehen (FBI, ODNI, NSA und CISA).

Link: https://thehill.com/policy/cybersecurity/532756-us-intel-agencies-blame-russia-for-massive-solarwinds-hack

SentinelOne: Der Hersteller der gleichnamigen Autonomous AI Endpoint Security Platform veröffentlicht ein freies Tool, das prüft, ob eine Infektion erfolgreich ausgeführt worden wäre, oder ob sich die Infektion eigenständig deaktiviert hätte.
Link: https://github.com/SentineLabs/SolarWinds_Countermeasures

06.01.2021:

NewYorkTimes: Ein möglicher Eintrittspunkt für die Kompromittierung von SolarWinds war die Software JetBrains TeamCity (aktuell noch nicht endgültig bestätigt).

Link: https://www.nytimes.com/2021/01/06/us/politics/russia-cyber-hack.html

DHS-CISA: CISA erweitert die Emergency Directive 21-01 um v3 der Supplemental Guidance (Mitigate SolarWinds Orion Code Compromise).

Link: https://www.nytimes.com/2021/01/06/us/politics/russia-cyber-hack.html

SolarWinds: Der frühere CEO Kevin Thompson wird das Unternehmen für Untersuchungen möglicher Verstöße und anderer Angelegenheiten bis zum 01.Juni 2021 unterstützen.

Link: https://www.sec.gov/Archives/edgar/data/1739942/000173994221000005/0001739942-21-000005-index.htm

11.01.2021:

Crowdstrike: CrowdStrike findet die initiale Kompromittierung der Build-Prozesse.

Link: https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

Hinweis: Die hier aufgeführten Meldungen beinhalten nur Informationen aus Erstquellen und von großen Medienhäusern mit Quellen-Verifizierungen bis Januar. Es gibt zusätzlich viele weitere spekulative Meldungen, die hier nicht eingeflossen sind.

SUNBURST Supply Chain Attack

Gerade in Zeiten, in denen die meisten Unternehmen bereits von Multi-Stage- und Multi-Vektor-Angriffen gehört haben und sich durch neue Technologien – kombiniert mit einem internen oder externen Security Operation Center (SOC) und Security Incident Response Team (SIRT) – schützen, erhöht sich der Aufwand für Angreifer, um in ein Unternehmen zu gelangen.

Bereits seit längerer Zeit ist es beispielsweise in der Autoindustrie allgemein üblich, die Zulieferer einzelner Komponenten zu reglementieren und Sicherheitsvorgaben zu machen, um die Qualität der einzelnen Teile sicherzustellen und geistiges Eigentum (z.B. Baupläne) zu schützen. Doch wie viele Unternehmen sind in der Lage, solche Vorgaben für jede eingesetzte Software zu machen, zumal nicht jedes Unternehmen ein entsprechendes Umsatzvolumen bei den Herstellern erreicht.

Im folgenden Ablauf der Kompromittierung (nach aktuellem Kenntnisstand) ist zu erkennen, welche Mühe sich die Angreifer gegeben haben, um möglichst unentdeckt zu bleiben. Im Fall SUNBURST wurde der Source Code das erste Mal am 26.10.2020 verändert, damit zum Zeitpunkt der Aktivierung keine größeren Veränderungen in der Größe des Codes erfolgen und dadurch potenziell auffallen.

06.08.2019	• Früheste aufgezeichnete Domänen-Registrierung
04.09.2019	• Angreifer gelangen in das Netz von SolarWinds
12.09.2019	• Erste Modifikation des SolarWinds Orion Source Codes und Testlauf
04.11.2019	• Ende des Testlaufs
06.12.2019	• Übernahme der DGA Domain avsvmcloud[.]com durch die Angreifer
20.02.2020 - x	• SUNBURST Kompilierung und Verteilung
04.06.2020	• Die Angreifer entfernen die Malware von den SolarWinds Build VMs
08.12.2020	• FireEye Report über den Einbruch und die Entwendung von RED Team Tools
13.12.2020	• FireEye Report über SolarWinds Kompromittierung
13.12.2020	• SolarWinds Security Advisory
14.12.2020	• Die C&C Domänen-Inhaberschaft wird an Microsoft übertragen (+ Transformation in Killswitch)
15.12.2020	• SolarWinds veröffentlicht einen Fix für die Orion Software

Hinweis: Die hier aufgeführten Schritte der Angreifer basieren auf aktuellem offiziell kommuniziertem Kenntnisstand und können sich im Laufe der Zeit noch erweitern oder verändern.

Supply Chain Attack – keine Neuheit

Eigentlich ist das Thema Supply Chain Attack nicht wirklich neu, es wurde sogar bereits im Dezember 2013 in einem MITRE Technical Report beschrieben (MTR140021).

Link: https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf

Ein Blick in die Vergangenheit zeigt, dass der Fall SUNBURST bei weitem nicht der erste Angriff dieser Art ist. Folgendes ist nur ein kleiner Auszug von Supply Chain Attacks aus der Vergangenheit:

Dezember 2013	Target Corporation	Einer der größten Discounter in den USA wird durch HVAC Zulieferer Fazio Mechanical Services kompromittiert
September 2015	XcodeGhost	Verteilung einer modifizierten Variante von Xcode, die beim kompilieren von MacOS- oder IOS-Applikationen weiteren Code injiziert hat
März 2016	KeRanger	Kompromittierung eines beliebten BitTorrent Clients
Juni 2017	NotPetya	Kompromittierung einer beliebten Finanzsoft-ware aus der Ukraine (MEDoc)
September 2017	CCleaner	Kompromittierung des beliebten Freeware Tools CCleaner von Avast
Anfang 2018	WordPress	Infizierung vieler WordPress Plugins
Juli 2018	PDF Editor	Kompromittierung eines Installers für einen PDF Editor, wodurch zusätzlich ein CryptoMiner installiert wurde
Vor Februar 2019	Pro Selfie Beauty Camera, Selfie Beauty Camera Pro, und Pretty Beauty Camera – 2019	Kompromittierung von drei beliebten Selfie Apps im Google Play Store
2016 bis April 2019	Exodus	Eine Android Spyware Made in Italy in mehreren Apps
September 2019	CCleaner	Erneute Kompromittierung der Software CCleaner

SUNBURST (Aka Solorigate)

Intro

Im Rahmen des SUNBURST APT, zu deren Opfern selbst prominente Unternehmen wie Microsoft und FireEye gehören, wurden zahlreiche, erstklassige Analyseberichte[1] veröffentlicht. FireEye selbst hat einen signifikanten Beitrag zur Analyse[2] und Aufklärung dieses Angriffs geleistet. Diese Berichte dienen als Referenz für fast alle Veröffentlichungen in diesem Kontext.

Zur Beschreibung von Cyberangriffen und deren Gliederung in Phasen/Taktiken existieren diverse Modelle, beispielsweise die klassische Cyber Kill Chain von Lockheed Martin[3] oder das ATT&CK Framework [4] von MITRE. Diese Modelle unterstützen dabei, zusätzliche Informationen pro Angriffsphase zu erlangen, um vor allem die Detektion zu erhöhen und eine umfassende Analyse zu ermöglichen. Die Informationen, die aus der jeweiligen Untersuchung stammen, enthalten häufig auch Indikatoren, sogenannte IoCs, die Details zum Angriff beschreiben und unterschiedlicher Art sein können.

Indikator-Typ	Beschreibung	Beispiel
Atomic	Eindeutige Daten zu Aktivitäten, die nicht weiter heruntergebrochen werden können	IP-Adresse Prozess-Name
Computed	Berechnete Werte	MD5 File-Hash
Behavioral	Kombination aus Indikatoren und eine Beschreibung, wie ein Angreifer diese verwendet	TTPs

Tabelle: Arten von Indikatoren

Die Indikatoren selbst werden durch den Angreifer bestimmt. Die Art der Indikatoren beeinflusst den sogenannten „Course of Action“, also die Vorgehensweise im Umgang mit den Indikatoren.

Course of Action	Beschreibung	Beispiel
Discover	Rückwärtsgerichteter, historischer Blick in bestehende Daten (Logs, Netflows etc.)	SIEM-Suche während der Incident-Analyse
Detect	Vorwärtsgerichtet, Erkennung von Indikatoren in der Zukunft	SIEM Use Case IDS-Signatur Blacklists

Tabelle: Course of Action Matrix

[1] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[2] https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html

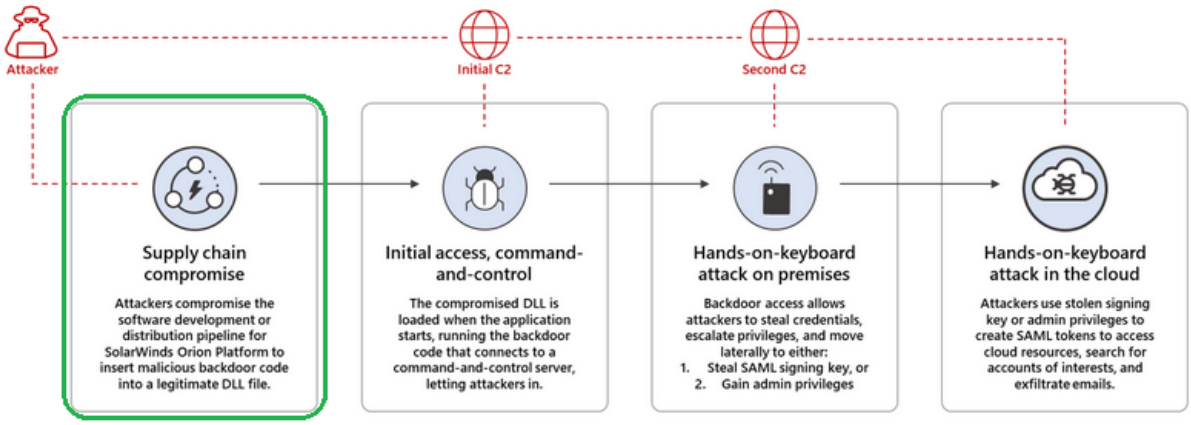
[3] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[4] https://attack.mitre.org/matrices/enterprise/windows/

Das folgende Kapitel soll keine Rezitation bestehender Analysten-Berichte sein. Vielmehr stellt es einen Versuch dar, mögliche Detektions- und Reaktionsmöglichkeiten im Kontext einer Supply Chain-Attacke im Allgemeinen sowie am Beispiel SUNBURST im Speziellen aufzuzeigen.

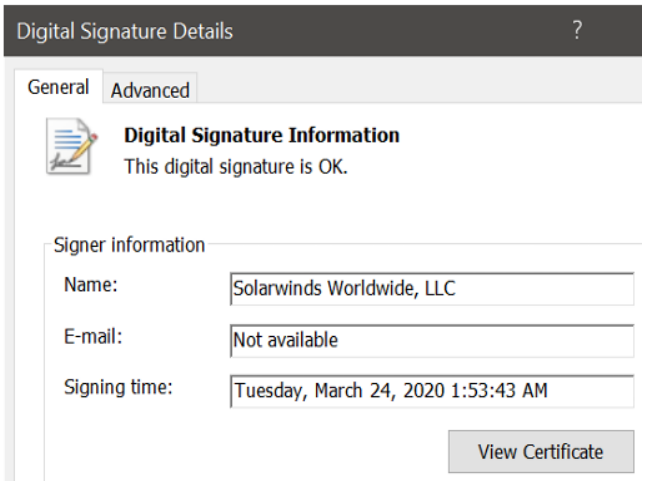
SUNBURST: Initiale Infektion der SolarWinds Software durch Backdoor

Die initiale Infektion erfolgte über ein Software-Update der SolarWinds Orion-Plattform.



Bildquelle: *https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/*

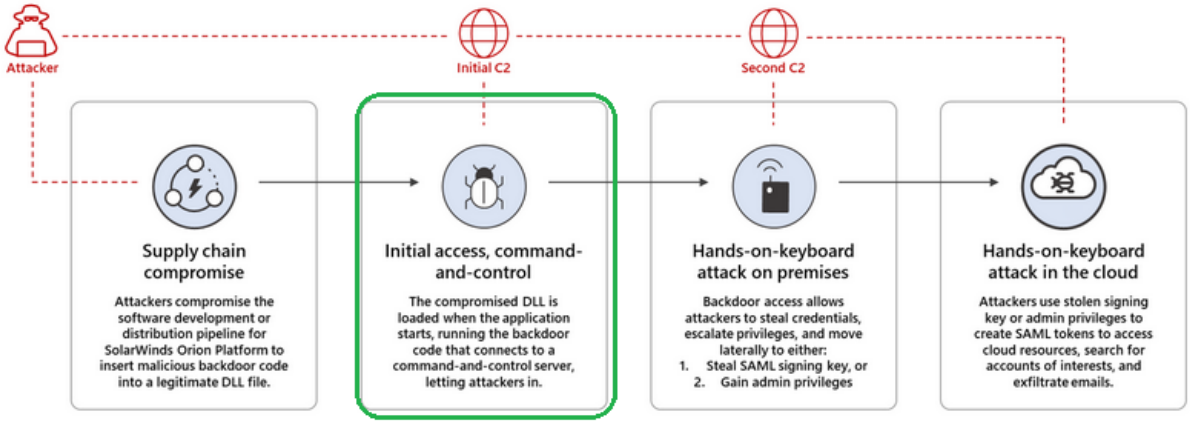
Eine Besonderheit ist die digitale Code-Signatur. Aktuell wird davon ausgegangen, dass der Software-Build-Prozess von SolarWinds kompromittiert wurde. Gesicherte Informationen vom Hersteller SolarWinds, wie die Backdoor in das Software-Update gelangen konnte, liegen bis dato noch nicht vor. CrowdStrike beschreibt[5] hingegen eine Malware namens Sunspot, die offenbar als Implantat in die Build-Umgebung von SolarWinds platziert wurde, um die Backdoor in die Orion-Plattform zu integrieren.



Häufig wird in dem Kontext über eine SolarWinds Schwachstelle gesprochen, vielmehr handelt es sich hierbei jedoch um eine Malware bzw. Backdoor in der **SolarWinds.Orion.Core.BusinessLayer.dll**, einer zentralen Programmbibliothek, die über ein Software-Update-Paket (**SolarWinds-Core-v2019.4.5220-Hotfix5.msp**) auf die betroffenen Systeme gelangte.

[5] https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

Nach dem Update wird die .Net Anwendung **SolarWinds.BusinessLayerHost.exe** ausgeführt, um Plug-Ins zu laden, unter anderem die Backdoor.



Bildunterschrift: Backdoor wird geladen

Die Backdoor führt daraufhin zunächst diverse „Anti-Analysis“-Überprüfungen durch, um eine Erkennung zu vermeiden oder das Ausführen unter bestimmten Bedingungen zu beenden. Ein Auszug:

Überprüfung	Beschreibung
File System-Zeitstempel: Erstellung des Assembly und aktuelles Datum > 12 Tage	Software seit mind. 12-14 Tagen installiert Nicht in Testumgebungen erkannt werden, kein verdächtiges Verhalten offenbaren
Ist das System AD joined?	Fokus auf Domainen-Maschinen AD Accounts für Lateral Movement
Befindet sich der Domänen-Name auf der Blacklist?	Best. AD-Domänen werden ausgenommen (vermutlich SolarWinds eigene AD Domains)
Aktive Security Tools ermitteln	Prozesse gegen eine Blacklist vergleichen Services über Registry deaktivieren
Internet-Verbindung prüfen/IP-Adresse ermitteln	Hat das System eine Internet-Verbindung? Befindet sich das System auf einer Blacklist von IP Ranges (z.B. Microsoft) – stoppen

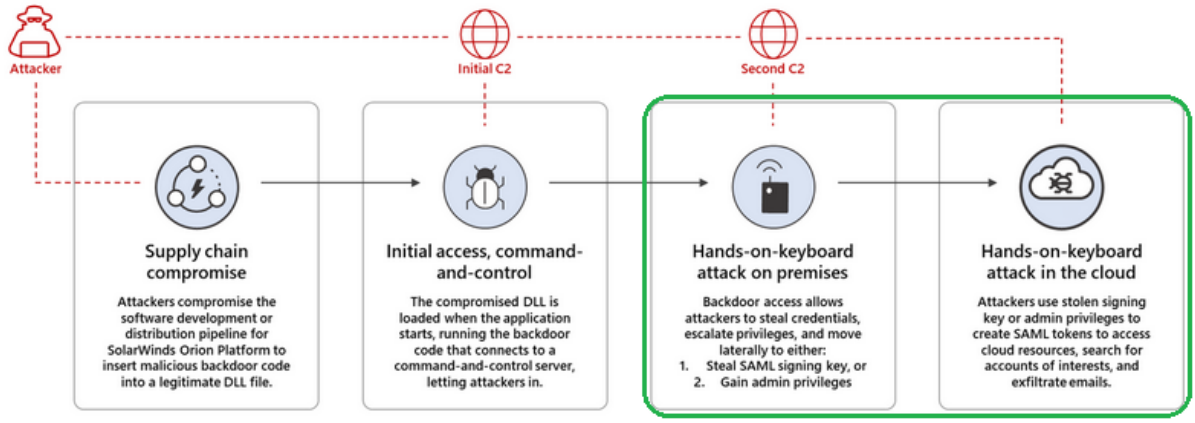
Erst dann generiert das Plug-in zufällige Domains über einen Domain Generation Algorithmus (diese enthalten verschleiert die AD-Domain des Opfer-Systems) und kontaktiert den DNS-Server, der sich unter Kontrolle des Angreifers befindet. Dieser decodiert die Informationen aus der Domain und entscheidet, ob das Opfer ein relevantes Ziel ist oder nicht. Über verschiedene Betriebsmodi kann ein kompromittiertes System zunächst auch inaktiv geschaltet werden.

Betriebsmodus	Beschreibung	Aktionen
Truncate	Deaktiviert via Kill Switch	Opfer kein relevantes Ziel
New	Passiver Modus	DNS für Status-Infos und C2 Beaconing Je nach A-Record-Antwort ermittelt SUNBURST den Betriebsmodus (Hard Coded-Liste von IP Ranges pro Betriebsmodus)
Append	Aktiver Modus	HTTP für C2, um Kommandos zu empfangen Prozesse erstellen/stoppen, Dateien lesen/schreiben, Registry Operationen, Sicherheits-Tools deaktivieren HTTP Responses via Steganographie verschleiert

Post Compromise Activity

Teardrop: Hands-on-Operationen der Angreifer

Wurde die Opfer-Domain vom Angreifer als interessantes Angriffsziel ausgewählt, beginnt Phase 2.



In Phase 2 wird eine weitere Malware (Codename Teardrop) nachgeladen. Über diese Malware werden vom Angreifer interaktive „Hands-on"-Operationen auf dem Opfersystem ausgeführt. Für die Reconnaissance und das Abziehen von Credentials wird ein weiteres Script (Codename CosmicGale) eingesetzt.

Bei Teardrop handelt es sich um einen „In Memory Dropper", also Malware, die direkt in den Arbeitsspeicher geladen und dort ausgeführt wird, ohne vorher auf Disk geschrieben worden zu sein. Mit diesem Mechanismus lassen sich klassische File System-Filtertreiber von AV-Lösungen umgehen. Teardrop verteilt im weiteren Verlauf eine Cobalt Strike-Variante. Für die weiteren Phasen des Angriffs setzen die Angreifer auf „Altbewährtes", wie die folgende Tabelle verdeutlicht.

Ein Auszug:

Stage / Taktik	Technik
Execution	PowerShell | CMD
Persistence	PowerShell | WMI | Rundll32
Credential Access	PowerShell (Get-PassHashes) – CosmicGale
Lateral Movement	Remote Scheduled Task, PowerShell
Command and Control	Cobalt Strike Custom C2 Protocol
Exfiltration	Verschlüsseltes File mit Credentials – CosmicGale
Impact	Logs löschen – CosmicGale

```
rule APT_Dropper_Win64_TEARDROP_2
{
    meta:
        author = "FireEye"
        description = "This rule is intended match specific sequences of opcode found within TEARDROP, including those that decode the embedded
    strings:
        $loc_4218FE24A5 = { 48 89 C8 45 0F B6 4C 0A 30 }
        $loc_4218FE36CA = { 48 C1 E0 04 83 C3 01 48 01 E8 8B 48 28 8B 50 30 44 8B 40 2C 48 01 F1 4C 01 FA }
        $loc_4218FE2747 = { C6 05 ?? ?? ?? ?? 6A C6 05 ?? ?? ?? ?? 70 C6 05 ?? ?? ?? ?? 65 C6 05 ?? ?? ?? ?? 67 }
        $loc_5551D725A0 = { 48 89 C8 45 0F B6 4C 0A 30 48 89 CE 44 89 CF 48 F7 E3 48 C1 EA 05 48 8D 04 92 48 8D 04 42 48 C1 E0 04 48 29 C6 }
        $loc_5551D726F6 = { 53 4F 46 54 57 41 52 45 ?? ?? ?? ?? 66 74 5C 43 ?? ?? ?? ?? 00 }
    condition:
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and any of them
}
```

Bildunterschrift: YARA Rule zur Erkennung spezifischer Code-Sequenzen von Teardrop
Quelle: https://github.com/fireeye/sunburst_countermeasures/tree/main/rules/TEARDROP/yara

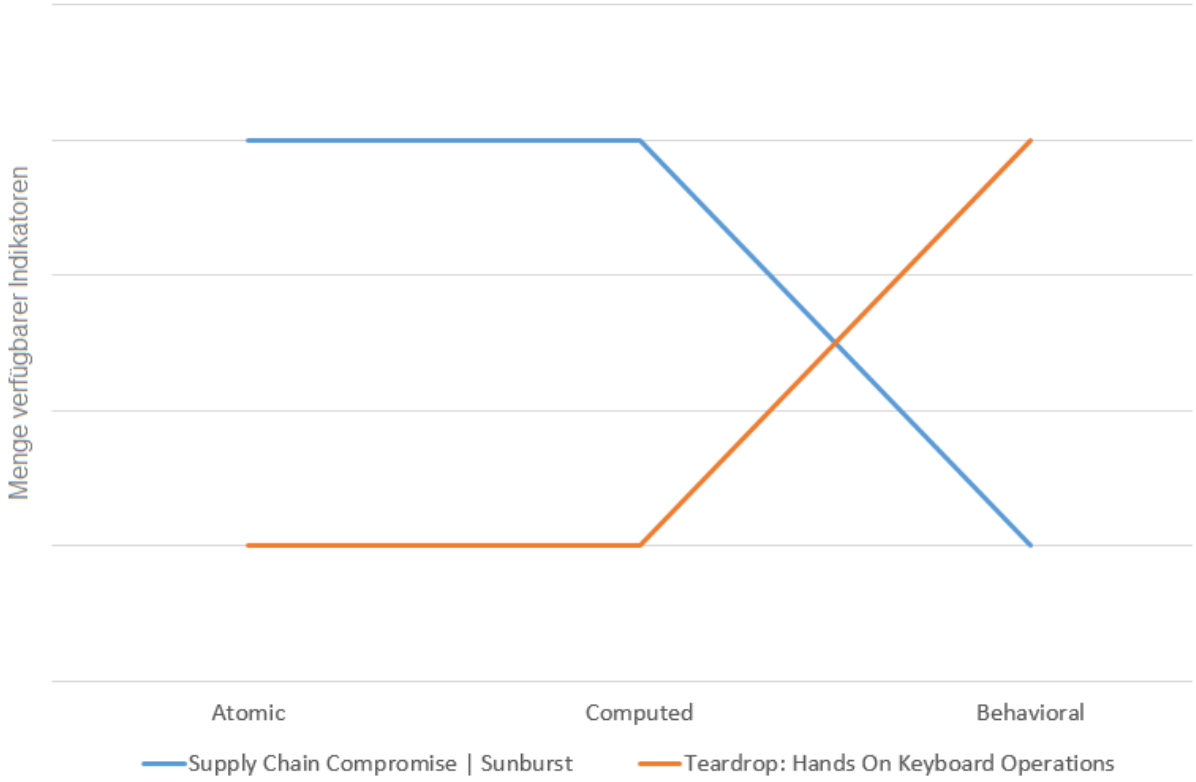
Detection Opportunity

Discovery vs. Detect

Die in den initialen Phasen „Supply Chain Compromise“ und „Initial Access“ verwendeten Techniken, Prozeduren und Tools waren vollständig auf diese Angriffskampagne maßgeschneidert und sehr spezifisch. Kompromittierte Build-Prozesse des Software-Herstellers, valide Code-Signaturen, diverse ausgeklügelte Anti-Analyse-Techniken und Betriebs-Modi ermöglichten es den Angreifern, über längere Zeit unerkannt zu bleiben. Die im Nachhinein veröffentlichten Indikatoren aus diesen frühen Phasen des Angriffs zeigen, dass es sich quantitativ vor allem um Atomic und Computed IoCs handelt.

Sobald Phase 2 erreicht wird, in der die Angreifer in einen interaktiven Hands-on-Modus wechseln, verschiebt sich die Verteilung hin zu Behavioral IoCs, also eher der Beschreibung von Angreifer TTPs (in Form von MITRE ATT&CK-Techniken), da der Angreifer über den In-Memory Trojaner eigene Kommandos und Operationen spezifisch pro Opfer ausführt.

Die folgende Darstellung soll dies verdeutlichen:



Bildunterschrift: Verteilung Indikatortypen pro Phase

Discovery

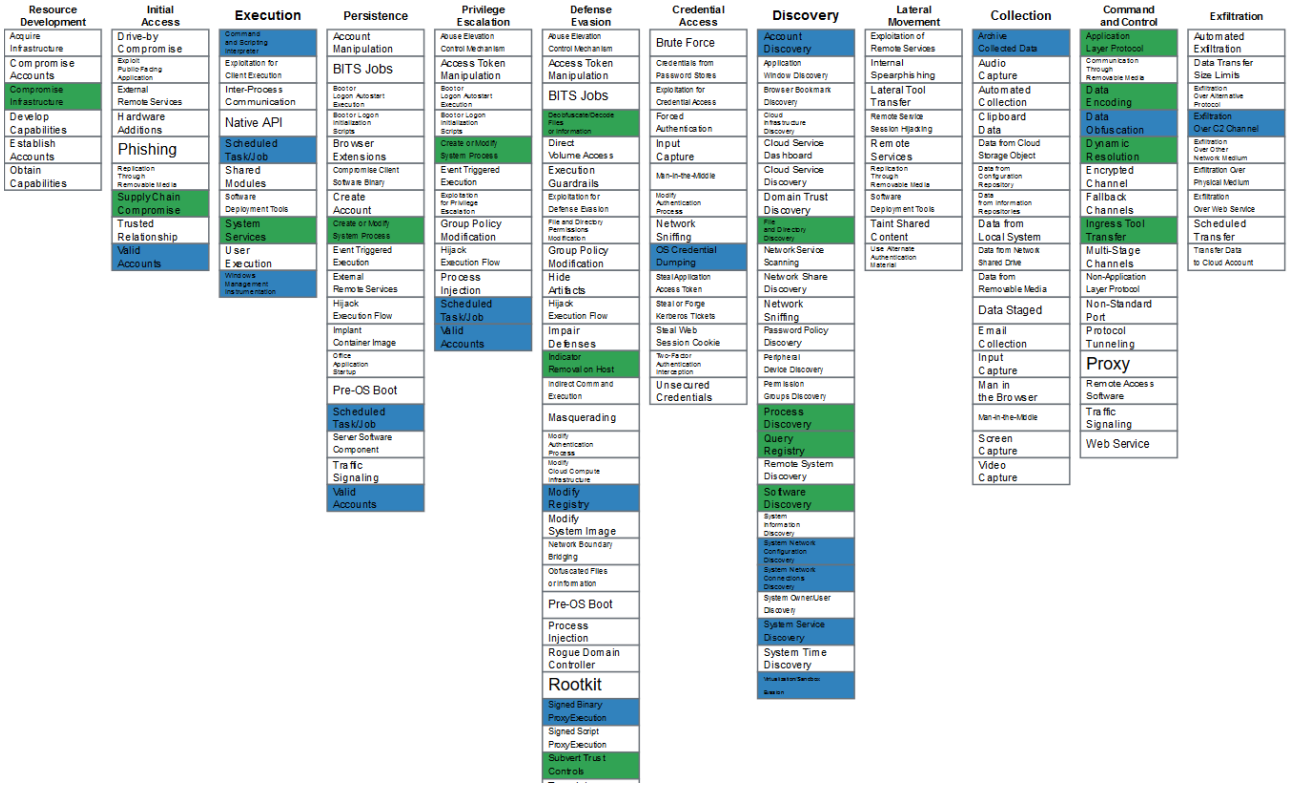
Angreifer(-Gruppen) in komplexen Supply Chain-Attacken, wie auch in diesem Fall, sind definitiv „OPSEC aware“. Das bedeutet, sie werden Maßnahmen treffen, um die eigene Operation und die verwendeten Techniken, Taktiken und Prozesse so lange wie möglich geheim zu halten. Insbesondere Atomic und Computed IoCs werden regelmäßig verändert und sind von kurzer Lebensdauer. Sie stellen daher den größten Mehrwert für die Discovery, also die rückblickende Betrachtung, Analyse und das Threat Hunting innerhalb eines Incidents, dar. In der Scoping Phase eines Incidents kann mithilfe dieser Indikatoren eingeordnet werden, ob und inwieweit eine Infektion fortgeschritten ist.

Im Fall SUNBURST bezog sich das beispielsweise darauf, ob im Proxy initiale Command and Control-Kommunikation zum Intermediate C2 Server festgestellt wurde (falls ja = Backdoor vorhanden) und in welchem Betriebsmodus sich die Backdoor befindet (DNS A-Record Response auswerten).

Detect

Atomic und Computed IoCs werden zur Detektion primär in Form von Blocklisten oder Lookup-Listen für SIEM Use Cases genutzt. Behavioral IoCs sind wesentlicher Input bei der Angriffsvektor-Modellierung (**Threat Modelling**). Angriffsvektor-Modellierung stellt (unabhängig vom gewählten Ansatz) im Wesentlichen einen systematischen Prozess dar, um potentielle Bedrohungen für ein definiertes System/einen Service anzunehmen und die Ausnutzbarkeit von Schwachstellen zu antizipieren. Die klassische Lockheed Martin Cyber Kill Chain ist hierfür nur eingeschränkt geeignet, da sie zum Mapping von Angreifertechniken nicht holistisch genug ist und eher ein Phasenmodell darstellt, dem es an angemessener Detailtiefe mangelt. Hierfür bietet sich vor allem das MITRE ATT&CK Framework an, eine bzw. die Wissensdatenbank aktueller „Real-world"-Angreifertechniken und Taktiken, das genau diese Detailtiefe und Taxonomie bietet.

Die folgende Darstellung zeigt die veröffentlichten Behavioral IoCs im SUNBURST APT anhand der zugeordneten MITRE-Techniken:



Bildunterschrift: FireEye SolarWinds APT Report | Weitere SolarWinds APT Reports

Diese veröffentlichten TTPs in Form von Behavioral IoCs können dabei helfen, die eigene Detektionsfähigkeiten hinsichtlich genau dieser Angreifertechniken zu testen.

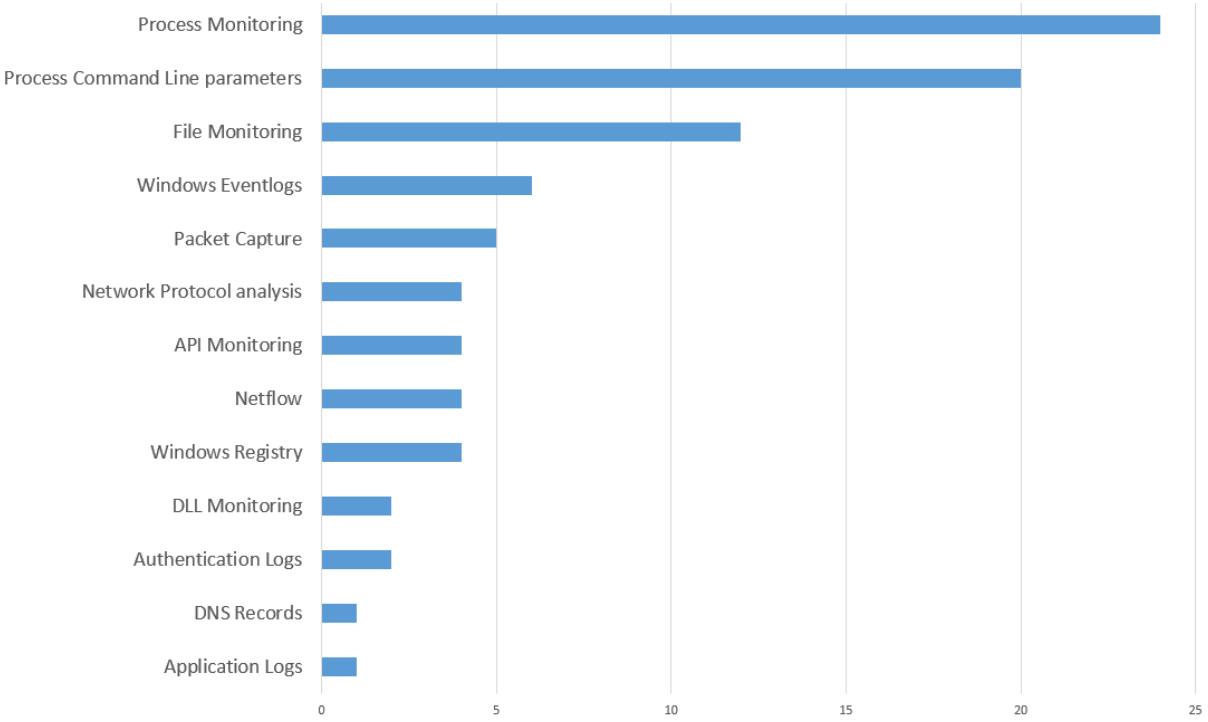
Bei den sogenannten Red-Team Automation Frameworks (RTA), wie Atomic[6] von Red Canary, handelt es sich um eine Sammlung an Open Source-Tests, die Angreifertechniken simulieren, um beispielsweise eigene Detektions-Mechanismen und Regeln (z.B. SIEM Use Cases der Lösungen) hinsichtlich dieser Techniken zu testen und zu optimieren. Auch für das **Threat Hunting** und die Erstellung von Use Cases (SIEM, EDR) sind Behavioral IoCs ein fundamentaler Input und das MITRE ATT&CK Framework ein ebenso wichtiges Hilfsmittel. Es unterstützt zunächst dabei, die für eine Technik relevanten Daten und -quellen zu ermitteln.

[6] https://github.com/redcanaryco/atomic-red-team

ID: T1059.001
Sub-technique of: T1059
Tactic: Execution
Platforms: Windows
Permissions Required: Administrator, User
Data Sources: DLL monitoring, File monitoring, Loaded DLLs, PowerShell logs, Process command-line parameters, Process monitoring, Windows event logs
Supports Remote: Yes
Contributors: Praetorian
Version: 1.0
Created: 09 March 2020
Last Modified: 24 June 2020

Bildunterschrift: Beispiel: T1059.001: Command and Scripting Interpreter: PowerShell

Bei Betrachtung der am häufigsten benötigten Datenquellen aller im Kontext dieser Angriffskampagne veröffentlichten MITRE-Techniken, ergibt sich folgendes Bild:



Für die Erkennung einer überwiegenden Mehrheit der verwendeten Techniken werden Logs vom Windows Endpoint benötigt, insbesondere im Bereich File- und Process-Monitoring sowie beim Process-Commandline-Monitoring. Diese Informationen können entweder durch moderne EDR-Lösungen oder durch Sysmon (Microsoft Sysinternals) protokolliert werden und lassen sich idealerweise in einem zentralen Data Lake oder SIEM zur zentralen Auswertung speichern.

Mitigation

Folgende Maßnahmen gelten als Best Practices und sind auch in Supply Chain-Attacken relevant.

Allgemein	
Internet-Zugriff für Applikationen	Zugriff so granular wie möglich (IPs, Domains)
Netzwerk-Segmentierung	Firewall-Regeln, kontinuierliche Überwachung auf Anomalien in Kommunikationsbeziehungen
Log Management	Zentrales Speichern relevanter Log-Daten
Multifaktor-Authentifizierung	v.a. für VPN-Zugriff, Zugriff auf Cloud-Anwendungen
Least Privilege-Prinzip	Nur für den jeweiligen Zweck notwendige Zugriffe und Berechtigungen gewähren

Insbesondere im Kontext von Windows Betriebssystemen und Active Directory gibt es zahlreiche empfohlene Maßnahmen, die einen Angriff zumindest erschweren sollen.

Windows	
Microsoft ASR- (Attack Surface Reduction) Regeln verwenden[7]	verhindern Aktionen, die häufig von Malware missbraucht werden
Administratoren in die Gruppe "Protected Users"[8]	Pass-the-Hash-Angriffe auf Anmeldeinformationen von Administratoren erschweren
Service Accounts	granulare Berechtigungen auf bestimmte Dienste (keine lokalen Admin-Rechte für Service Accounts)
LAPS einsetzen[9]	kein einheitliches Passwort für lokale Administratoren, sondern pro Gerät ein zufälliges, in der Domäne verwaltetes Passwort
User-Berechtigungen	Benutzer sollten keine lokalen Administratoren sein
Authentifizierung lokaler Admins	keine Authentifizierung lokaler Admins über das Netzwerk erlauben
SeDebug-Berechtigung	keine SeDebug-Berechtigung für lokale Admins (nur bei Bedarf), diese wird von Credential Dumping Tools wie Mimikatz benötigt
Credential Guard verwenden[10]	virtualisierte Sicherheit für Anmeldeinformationen
Remote Credential Guard verwenden[11]	Anmeldeinformationen über RDP schützen

[7] https://docs.microsoft.com/de-de/windows/security/threat-protection/microsoft-defender-atp/enable-attack-surface-reduction

[8] https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/manage/how-to-configure-protected-accounts#BKMK_AddtoProtectedUsers

[9] https://support.microsoft.com/de-de/help/3062591/microsoft-security-advisory-local-administrator-password-solution-laps

[10] https://docs.microsoft.com/de-de/windows/security/identity-protection/credential-guard/credential-guard-how-it-works

[11] https://docs.microsoft.com/de-de/windows/security/identity-protection/remote-credential-guard

FAZIT

Während sich initiale Malware-Infektionen (z.B. durch schadhafte E-Mail-Anhänge) in klassischen Cybercrime-Kampagnen mittlerweile relativ zuverlässig erkennen oder sogar verhindern lassen (Sandboxen, EDR), stellen gezielte und komplexe Angriffe eine besondere Herausforderung dar. Der SolarWinds APT in seiner enormen Komplexität zeigt, dass derartige Angriffe vor allem in der Phase des initialen Zugriffs kaum verhindert werden können. Ziel sollte es also sein, zumindest eine Ausbreitung und Folgeaktivitäten des Angreifers nicht unerkannt bleiben zu lassen und in der Lage zu sein, Fragen nach dem Ausmaß des Angriffs zu beantworten und entsprechende Maßnahmen abzuleiten.

Das vorige Kapitel stellt diverse Korrelationen her. Welche technischen Voraussetzungen sind notwendig, um relevante Angreifertechniken zu erkennen, wie beeinflusst die Art der verfügbaren Informationen mögliche Vorgehensweisen von Analysten usw. Diese Korrelationen unterstreichen das Paradigma von „People, Process, Technology“ vor allem im Cyber Defense-Kontext. Eine erfolgreiche Cyberabwehr-Strategie ist nur durch ein Zusammenspiel aufeinander abgestimmter technischer Lösungen, Experten und entsprechender Response-Prozesse möglich. Diese Erkenntnis ist nicht neu. Unternehmen sind sich der Gefahren zwar zum Teil bewusst, scheuen aber oftmals die hohen Investitionen in Sicherheitstechnologie und qualifiziertes Personal. Wenn eigene IT-Abteilungen den SOC-Betrieb neben den Kerntätigkeiten übernehmen sollen, ohne über die dafür notwendigen Ressourcen zu verfügen, kann dies schnell zum Risiko werden.

Managed Security Services, wie die Controlware Managed Cyber Defense Services, sind eine gute Alternative. Sie ermöglichen – abhängig vom individuell gewählten Leistungsumfang – die Erkennung von Cybergefahren, Schwachstellen und Anomalien durch unterschiedliche Risiko-Erkennungsmodule in Verbindung mit Dienstleistungen zur Analyse, Bewertung und Priorisierung von Security Incidents. Besonderer Schwerpunkt ist unter anderem die ständige Beobachtung der weltweiten aktuellen Bedrohungslage, um Angriffsmuster zu verstehen und die Detektions-Mechanismen kontinuierlich darauf anzupassen.

Glossar

APT: Advanced Persistent Threat beschreibt einen ausgefeilten Angriff

CA: Certificate Authority, eine unabhängige Instanz, die die Gültigkeit von Zertifikaten bestätigt

EDR: Endpoint Detection und Response

Red Team: Eine Gruppe, die sanktionierte Angriffsübungen durchführt

Blue Team: Eine Gruppe (meist SOC/CERT), die versucht, die vom Red Team durchgeführten Angriffe abzuwehren

SOC: Security Operation Center

CERT: Computer Emergency Response Team

SIRT: Security Incident Response Team

CISA: Cybersecurity and Infrastructure Security Agency, Teil der DHS, US-amerikanische Bundesbehörde

MSP: Managed Service Provider

Kill Switch: Eine Funktion in einer Software, die die eigentliche Ausführung unterbricht

DHS: Department of Homeland Security, US-amerikanische Bundesbehörde

FBI: Federal Buero of Investigation, US-amerikanische Bundesbehörde

Backdoor: Geheime Funktion in Software, die das unbemerkte Eindringen in ein Unternehmen ermöglicht

Nation State Actor: Staatlicher Akteur, im Zusammenhang mit der Cybersicherheit, meist ein Geheimdienst.

XCode: Apple IDE

IDE: Integrated Development Environment

Threat Actor: Ausführende Person hinter einem Angriff, wird meist im Kontext von APTs verwendet

MITRE: Die MITRE Corporation ist eine NGO, die unter anderem das MITRE ATT&CK Framework pflegt und bereitstellt

MITRE ATT&CK Framework: Globale Knowledge Base, in der die Taktiken und Techniken von Angreifern beschrieben sind

TTP: Tools Tactics and Procedures, beschreibt die genutzten Tools, Taktiken und Vorgehensweisen bei komplexen Angriffen

Cyber Kill Chain: Ablaufdiagramm komplexer Angriffe, das initial durch Lockheed Martin entwickelt wurde

IOC: Indicator of Compromise, Daten (URLs, Ips, Hashes), die bei einem Angriff erkannt wurden und standardisiert beschrieben werden

SIEM: Security Incident Event Management

IDS: Intrusion Detecion Response System, siehe Suricata oder Snort

Supply Chain: Englisch für Zulieferer/Lieferkette

Command and Control (C2): Die Kommunikation von einem infizierten System mit dem Angreifer oder zur Steuerung und zum Nachladen weiterer Angriffs-Tools

AD: Microsoft Active Directory

DNS: Domain Name System

Quellen

Zitat Nakasone
https://www.defenseone.com/threats/2020/11/big-2020-election-hack-never-came-heres-why/169806/
Zitat SEC Report
https://d18rn0p25nwr6d.cloudfront.net/CIK-0001739942/57108215-4458-4dd8-a5bf-55bd5e34d451.pdf