SUNBURST (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 20:09:04 UTC

FireEye describes SUNBURST as a trojanized SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that communicates via HTTP to third party servers. After an initial dormant period of up to two weeks, it uses a DGA to generate specific subdomains for a set C&C domain. The backdoor retrieves and executes commands, that include the ability to transfer files, execute files, profile the system, reboot the machine, and disable system services. The C2 traffic to the malicious domains is designed to mimic normal SolarWinds API communications: Orion Improvement Program (OIP) protocol. The backdoor uses multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers. Multiple trojanzied updates were digitally signed from March - May 2020 and posted to the SolarWinds updates website.

2023-04-13 · · CERT.PL ·
CERT Polska and SKW warn against the activities of Russian spies
BOOMBOX EnvyScout SUNBURST 2022-09-10 · cocomelonc
Malware development: persistence - part 10. Using Image File Execution Options. Simple C++ example.
SUNBURST 2022-07-31 · BushidoToken Blog · BushidoToken
Space Invaders: Cyber Threats That Are Out Of This World
Poison Ivy Raindrop SUNBURST TEARDROP WastedLocker 2022-07-18 · Palo Alto Networks Unit 42 · Unit 42
Solar Phoenix
SUNBURST TEARDROP UNC2452 2022-06-18 · R136a1 · Dominik Reichel
Using dotnetfile to get a Sunburst timeline for intelligence gathering
SUNBURST 2022-04-27 · Mandiant · Mandiant
Assembling the Russian Nesting Doll: UNC2452 Merged into APT29
Cobalt Strike Raindrop SUNBURST TEARDROP 2021-12-29 · Palo Alto Networks Unit 42 · Daiping Liu, Jielong Xu, Wanjin Li, Zhanhao Chen
Strategically Aged Domain Detection: Capture APT Attacks With DNS Traffic Trends
Chrysaor SUNBURST 2021-09-02 · Bleeping Computer · Sergiu Gatlan
Autodesk reveals it was targeted by Russian SolarWinds hackers
SUNBURST 2021-07-27 · Gigamon · Joe Slowik
Ghosts on the Wire: Expanding Conceptions of Network Anomalies
SUNBURST 2021-07-13 · YouTube (Matt Soseman) · Matt Soseman
Solarwinds and SUNBURST attacks compromised my lab!
Cobalt Strike Raindrop SUNBURST TEARDROP 2021-06-12 · YouTube (BSidesBoulder) · Kaspersky, Kurt Baumgartner
Same and Different - sesame street level attribution
Kazuar SUNBURST 2021-06-01 · SANS · Jake Williams, Kevin Haley
A Contrarian View on SolarWinds
Cobalt Strike Raindrop SUNBURST TEARDROP 2021-05-31 · Wired · Andy Greenberg
Hacker Lexicon: What Is a Supply Chain Attack?

EternalPetya SUNBURST 2021-05-14 · CISA · US-CERT

Analysis Report (AR21-134A): Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise

SUNBURST 2021-05-08 · The Record · Catalin Cimpanu

SolarWinds says fewer than 100 customers were impacted by supply chain attack

SUNBURST 2021-05-07 · SolarWinds · Solarwind

An Investigative Update of the Cyberattack

SUNBURST 2021-04-22 · RiskIQ · RiskIQ

SolarWinds: Advancing the Story

SUNBURST 2021-04-15 · European Council · Council of the European Union

Declaration by the High Representative on behalf of the European Union expressing solidarity with the United States on the impact of the SolarWinds cyber operation

SUNBURST 2021-04-15 · North Atlantic Treaty Organization · NATO

North Atlantic Council Statement following the announcement by the United States of actions with regard to Russia

SUNBURST 2021-04-15 · Ministry of Foreign Affairs Republic of Poland · Ministry of Foreign Affairs Republic of Poland

Statement on Solar Winds Orion cyberattacks

SUNBURST 2021-04-15 · Ministry of foreign affairs of the Republic of Latvia · Ministry of foreign affairs of the Republic of Latvia

Latvia’s statement following the announcement by the United States of actions to respond to the Russian Federation’s destabilizing activities (Deadlink)

SUNBURST 2021-03-18 · Github (cisagov) · CISA

CISA Hunt and Incident Response Program (CHIRP)

SUNBURST 2021-03-18 · CISA · US-CERT

Alert (AA21-077A): Detecting Post-Compromise Threat Activity Using the CHIRP IOC Detection Tool

SUNBURST 2021-03-17 · CISA · US-CERT

SolarWinds and Active Directory/M365 Compromise: Detecting Advanced Persistent Threat Activity from Known Tactics, Techniques, and Procedures (Dead Link)

SUNBURST 2021-03-16 · Mimecast · Mimecast

Incident Report

SUNBURST 2021-03-10 · US-CERT · CISA

Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise

SUNBURST 2021-03-08 · Youtube (SANS Digital Forensics and Incident Response) · Adam Pennington, Jen Burns, Katie Nickels

STAR Webcast: Making sense of SolarWinds through the lens of MITRE ATT&CK(R)

Cobalt Strike SUNBURST TEARDROP 2021-03-04 · Microsoft · Andrea Lelli, Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center (MSTIC), Ramin Nafisi

GoldMax, GoldFinder, and Sibot: Analyzing NOBELIUM’s layered persistence

SUNBURST TEARDROP UNC2452 2021-03-01 · Microsoft · Microsoft

Detect and defend against the recent nation-state cyber attack

SUNBURST 2021-02-28 · PWC UK · PWC UK

Cyber Threats 2020: A Year in Retrospect

elf.wellmess FlowerPower PowGoop 8.t Dropper Agent.BTZ Agent Tesla Appleseed Ave Maria Bankshot BazarBackdoor BLINDINGCAN Chinoxy Conti Cotx RAT Crimson RAT DUSTMAN Emotet FriedEx

FunnyDream Hakbit Mailto Maze METALJACK Nefilim Oblique RAT Pay2Key PlugX QakBot REvil Ryuk StoneDrill StrongPity SUNBURST SUPERNOVA TrickBot TurlaRPC Turla SilentMoon WastedLocker WellMess Winnti ZeroCleare APT10 APT23 APT27 APT31 APT41 BlackTech BRONZE EDGEWOOD Inception Framework MUSTANG PANDA Red Charon Red Nue Sea Turtle Tonto Team 2021-02-26 · YouTube (Oversight Committee) · Oversight Committee

Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and Ongoing Campaign

SUNBURST 2021-02-25 · BrightTALK (FireEye) · Andrew Rector, Mandiant, Matt Bromiley

Light in the Dark: Hunting for SUNBURST

SUNBURST 2021-02-25 · Microsoft · Microsoft Identity Security Team

Microsoft open sources CodeQL queries used to hunt for Solorigate activity

SUNBURST 2021-02-25 · Microsoft · Microsoft

CodeQL queries to hunt for Solorigate activity

SUNBURST 2021-02-24 · Bleeping Computer · Sergiu Gatlan

NASA and the FAA were also breached by the SolarWinds hackers

SUNBURST 2021-02-23 · CrowdStrike · CrowdStrike

2021 Global Threat Report

RansomEXX Amadey Anchor Avaddon BazarBackdoor Clop Cobalt Strike Conti Cutwail DanaBot DarkSide DoppelPaymer Dridex Egregor Emotet Hakbit IcedID JSOutProx KerrDown LockBit Mailto Maze MedusaLocker Mespinoza Mount Locker NedDnLoader Nemty Pay2Key PlugX Pushdo PwndLocker PyXie QakBot Quasar RAT RagnarLocker Ragnarok RansomEXX REvil Ryuk Sekhmet ShadowPad SmokeLoader Snake SUNBURST SunCrypt TEARDROP TrickBot WastedLocker Winnti Zloader Evilnum OUTLAW SPIDER RIDDLE SPIDER SOLAR SPIDER VIKING SPIDER 2021-02-19 · THE NEW STACK · Dror Alon, Lior Sonntag

Behind the Scenes of the SunBurst Attack

SUNBURST 2021-02-17 · YouTube (The White House) · Anne Neuberger

Update on Investigaton on Solarwinds supply chain attack from the Deputy National Security Advisor

SUNBURST 2021-02-17 · Netresec · Erik Hjelmvik

Targeting Process for the SolarWinds Backdoor

SUNBURST 2021-02-17 · apirro · Ariel Levy

Detect and prevent the SolarWinds build-time code injection attack

SUNBURST 2021-02-16 · Accenture · Alexandrea Berninger

Hard lessons learned: Threat intel takeaways from the community response to Solarigate

SUNBURST TEARDROP 2021-02-16 · FireEye · Andrew Rector, Matt Bromiley, Robert Wallace

Light in the Dark: Hunting for SUNBURST

SUNBURST 2021-02-08 · US-CERT · US-CERT

Malware Analysis Report (AR21-039A): SUNBURST

SUNBURST 2021-01-29 · Aon · Alex Parsons, Carly Battaile, Partha Alwar

Cloudy with a Chance of Persistent Email Access

SUNBURST 2021-01-28 · Check Point · Lior Sonntag

Deep into the SunBurst Attack

SUNBURST 2021-01-28 · YouTube (Microsoft Security Community) · Microsoft

Microsoft 365 Defender webinar: Protect, Detect, and Respond to Solorigate using M365 Defender

SUNBURST 2021-01-26 · Kaspersky Labs · Kaspersky Lab ICS CERT

SunBurst industrial victims

SUNBURST 2021-01-26 · Bleeping Computer · Sergiu Gatlan

Mimecast links security breach to SolarWinds hackers

SUNBURST 2021-01-26 · Mimecast · Mimecast Contributing Writer

Important Security Update

SUNBURST 2021-01-26 · Fidelis · Chris Kubic

Ongoing Analysis of SolarWinds Impacts

SUNBURST 2021-01-25 · Netresec · Erik Hjelmvik

Twenty-three SUNBURST Targets Identified

SUNBURST 2021-01-25 · ZenGo · Tal Be'ery

Ungilded Secrets: A New Paradigm for Key Security

SUNBURST 2021-01-24 · Medium vrieshd · VriesHD

Finding SUNBURST victims and targets by using passive DNS, OSINT

SUNBURST 2021-01-22 · Symantec · Threat Hunter Team

SolarWinds: How Sunburst Sends Data Back to the Attackers

SUNBURST 2021-01-22 · DomainTools · Joe Slowik

Change in Perspective on the Utility of SUNBURST-related Network Indicators

SUNBURST 2021-01-21 · NetbyteSEC · Fareed Fauzi

Solarwinds Attack: Sunburst's DLL Technical Analysis

SUNBURST 2021-01-20 · Microsoft · Microsoft 365 Defender Research Team, Microsoft Cyber Defense Operations Center (CDOC), Microsoft Threat Intelligence Center (MSTIC)

Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop

Cobalt Strike SUNBURST TEARDROP 2021-01-19 · Github (fireeye) · FireEye

Mandiant Azure AD Investigator: Focusing on UNC2452 TTPs

SUNBURST 2021-01-18 · Symantec · Threat Hunter Team

Raindrop: New Malware Discovered in SolarWinds Investigation

Cobalt Strike Raindrop SUNBURST TEARDROP 2021-01-17 · a12d404 · Markus Piéton

Backdooring MSBuild

SUNBURST 2021-01-15 · Symantec · Threat Hunter Team

SolarWinds: Insights into Attacker Command and Control Process

SUNBURST 2021-01-14 · Microsoft · Microsoft 365 Defender Team

Increasing resilience against Solorigate and other sophisticated attacks with Microsoft Defender

SUNBURST 2021-01-14 · DomainTools · Joe Slowik

The Devil’s in the Details: SUNBURST Attribution

SUNBURST 2021-01-12 · BrightTALK (FireEye) · Ben Read, John Hultquist

UNC2452: What We Know So Far

Cobalt Strike SUNBURST TEARDROP 2021-01-11 · Kaspersky Labs · Costin Raiu, Georgy Kucherin, Igor Kuznetsov

Sunburst backdoor – code overlaps with Kazuar

Kazuar SUNBURST 2021-01-11 · SolarWinds · Sudhakar Ramakrishna

New Findings From Our Investigation of SUNBURST

Cobalt Strike SUNBURST TEARDROP 2021-01-11 · CrowdStrike · CrowdStrike Intelligence Team

SUNSPOT: An Implant in the Build Process

SUNBURST 2021-01-11 · Netresec · Erik Hjelmvik

Robust Indicators of Compromise for SUNBURST

SUNBURST 2021-01-08 · US-CERT · US-CERT

Alert (AA21-008A): Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments

SUNBURST SUPERNOVA 2021-01-08 · splunk · James Brodsky, John Stoner, Lily Lee, Marcus LaFerrera, Ryan Kovar

A Golden SAML Journey: SolarWinds Continued

SUNBURST 2021-01-07 · Symantec · Threat Hunter Team

SolarWinds: How a Rare DGA Helped Attacker Communications Fly Under the Radar

SUNBURST 2021-01-07 · TRUESEC · Sebastian Olsson

Avoiding supply-chain attacks similar to SolarWinds Orion’s (SUNBURST)

SUNBURST 2021-01-06 · Department of Justice · Department of Justice

Department of Justice Statement on Solarwinds Update

SUNBURST 2021-01-06 · Github (SentinelLabs) · SentinelLabs

SolarWinds_Countermeasures

SUNBURST 2021-01-06 · MITRE · MITRE ATT&CK

ATT&CK Navigator layer for UNC2452

SUNBURST 2021-01-06 · CISA · US-CERT

Supply Chain Compromise

SUNBURST 2021-01-05 · · Sangfor · Clairvoyance Safety Laboratory

Red team's perspective on the TTPs in Sunburst's backdoor

SUNBURST 2021-01-05 · CISA, FBI, NSA, ODNI

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)

SUNBURST 2021-01-04 · Netresec · Erik Hjelmvik

Finding Targeted SUNBURST Victims with pDNS

SUNBURST 2021-01-01 · DomainTools · Joe Slowik

Conceptualizing a Continuum of Cyber Threat Attribution

CHINACHOPPER SUNBURST 2021-01-01 · Mandiant · Mandiant

M-TRENDS 2021

Cobalt Strike SUNBURST 2021-01-01 · Symantec · Symantec Threat Hunter Team

Supply Chain Attacks:Cyber Criminals Target the Weakest Link

Cobalt Strike Raindrop SUNBURST TEARDROP 2020-12-31 · Microsoft · MSRC Team

Microsoft Internal Solorigate Investigation Update

SUNBURST 2020-12-31 · IronNet · IronNet

SolarWinds/SUNBURST: Behavioral analytics and Collective Defense in action

SUNBURST 2020-12-30 · Recorded Future · John Wetzel

SOLARWINDS ATTRIBUTION: Are We Getting Ahead of Ourselves? An Analysis of UNC2452 Attribution

SUNBURST 2020-12-29 · Netresec · Erik Hjelmvik

Extracting Security Products from SUNBURST DNS Beacons

SUNBURST 2020-12-29 · CyberArk · Shaked Reiner

Golden SAML Revisited: The Solorigate Connection

SUNBURST 2020-12-28 · Microsoft · Microsoft 365 Defender Team

Using Microsoft 365 Defender to protect against Solorigate

SUNBURST TEARDROP 2020-12-25 · Comae · Matt Suiche

SUNBURST & Memory Analysis

SUNBURST 2020-12-24 · FireEye · Jay Smith, Stephen Eckels, William Ballenthin

SUNBURST Additional Technical Details

SUNBURST 2020-12-23 · · Qianxin · Qi AnXin CERT

从Solarwinds供应链攻击（金链熊）看APT行动中的隐蔽作战

SUNBURST 2020-12-23 · Palo Alto Networks Unit 42 · Unit 42

A Timeline Perspective of the SolarStorm Supply-Chain Attack

SUNBURST TEARDROP 2020-12-23 · CrowdStrike · Michael Sentonas

CrowdStrike Launches Free Tool to Identify and Help Mitigate Risks in Azure Active Directory

SUNBURST 2020-12-23 · Prevasio · Sergei Shevchenko

DNS Tunneling In The SolarWinds Supply Chain Attack

SUNBURST 2020-12-22 · Checkpoint · Check Point Research

SUNBURST, TEARDROP and the NetSec New Normal

SUNBURST TEARDROP 2020-12-22 · Symantec · Threat Hunter Team

SolarWinds Attacks: Stealthy Attackers Attempted To Evade Detection

SUNBURST 2020-12-22 · Microsoft · Alex Weinert

Azure AD workbook to help you assess Solorigate risk

SUNBURST 2020-12-22 · Medium mitre-attack · Adam Pennington, Matt Malone

Identifying UNC2452-Related Techniques for ATT&CK

SUNBURST TEARDROP UNC2452 2020-12-22 · Youtube (Colin Hardy) · Colin Hardy

SUNBURST SolarWinds RECON - Malware Reverse Engineering, OSINT and Identifying Victims

SUNBURST 2020-12-22 · FBI · FBI

PIN Number 20201222-001: Advanced Persistent Threat Actors Leverage SolarWinds Vulnerabilities

SUNBURST 2020-12-22 · Zscaler · Zscaler

The Hitchhiker’s Guide to SolarWinds Incident Response

SUNBURST 2020-12-22 · Prevasio · Sergei Shevchenko

Sunburst Backdoor, Part III: DGA & Security Software (Broken Link)

SUNBURST 2020-12-21 · SophosLabs Uncut · SophosLabs Threat Research

How SunBurst malware does defense evasion

SUNBURST UNC2452 2020-12-21 · Microsoft · Alex Weinert

Understanding "Solorigate"'s Identity IOCs - for Identity Vendors and their customers.

SUNBURST 2020-12-21 · McAfee · Arnab Roy, Mo Cashman

How A Device to Cloud Architecture Defends Against the SolarWinds Supply Chain Compromise

SUNBURST 2020-12-21 · Microsoft · MSRC Team

Solorigate Resource Center

SUNBURST TEARDROP 2020-12-21 · IronNet · Peter Rydzynski

SolarWinds/SUNBURST: DGA or DNS Tunneling?

SUNBURST 2020-12-21 · Fortinet · Udi Yavo

What We Have Learned So Far about the “Sunburst”/SolarWinds Hack

Cobalt Strike SUNBURST TEARDROP 2020-12-20 · Medium Asuna Amawaka · Asuna Amawaka

A Look into SUNBURST's DGA

SUNBURST 2020-12-20 · Twitter (@TychoTithonus) · Royce Williams

SolarWinds/SunBurst FNV-1a-XOR hashes found in analysis

SUNBURST 2020-12-19 · Bleeping Computer · Lawrence Abrams

The SolarWinds cyberattack: The hack, the victims, and what we know

SUNBURST 2020-12-18 · Cloudflare · Jesse Kipp, Nick Blazier

A quirk in the SUNBURST DGA algorithm

SUNBURST 2020-12-18 · DomainTools · Joe Slowik

Continuous Eruption: Further Analysis of the SolarWinds Supply Chain Incident

SUNBURST 2020-12-18 · Kaspersky Labs · Costin Raiu, Igor Kuznetsov

Sunburst: connecting the dots in the DNS requests

SUNBURST 2020-12-18 · Elastic · Camilla Montonen, Justin Ibarra

Combining supervised and unsupervised machine learning for DGA detection

SUNBURST 2020-12-18 · ThreatConnect · ThreatConnect

Tracking Sunburst-Related Activity with ThreatConnect Dashboards

SUNBURST 2020-12-18 · Microsoft · Microsoft 365 Defender Research Team, Microsoft Threat Intelligence Center (MSTIC)

Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers

SUNBURST SUPERNOVA TEARDROP UNC2452 2020-12-18 · Sentinel LABS · James Haughom

SolarWinds SUNBURST Backdoor: Inside the APT Campaign

SUNBURST 2020-12-18 · IBM · Gladys Koskas

SUNBURST indicator detection in QRadar

SUNBURST 2020-12-17 · US-CERT · US-CERT

Alert (AA20-352A): Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations

SUNBURST 2020-12-17 · Microsoft · Brad Smith

A moment of reckoning: the need for a strong and global cybersecurity response

SUNBURST 2020-12-17 · Twitter (@megabeets_) · Itay Cohen

Tweet on SUNBURST malware discussing some of its evasion techniques

SUNBURST 2020-12-17 · McAfee · Cedric Cochin, Christiaan Beek, Raj Samani

Additional Analysis into the SUNBURST Backdoor

SUNBURST 2020-12-17 · Youtube (Colin Hardy) · Colin Hardy

SUNBURST SolarWinds Malware - Tools, Tactics and Methods to get you started with Reverse Engineering

SUNBURST 2020-12-17 · TRUESEC · Fabio Viggiani

The SolarWinds Orion SUNBURST supply-chain Attack

SUNBURST 2020-12-17 · Netresec · Erik Hjelmvik

Reassembling Victim Domain Fragments from SUNBURST DNS

SUNBURST 2020-12-17 · TrustedSec · Trustedsec

SolarWinds Backdoor (Sunburst) Incident Response Playbook

SUNBURST 2020-12-17 · splunk · John Stoner

Onboarding Threat Indicators into Splunk Enterprise Security: SolarWinds Continued

SUNBURST 2020-12-17 · Prevasio · Sergei Shevchenko

Sunburst Backdoor, Part II: DGA & The List of Victims

SUNBURST 2020-12-16 · Github (RedDrip7) · RedDrip7

A script to decode SUNBURST DGA domain

SUNBURST 2020-12-16 · ReversingLabs · Tomislav Pericin

SunBurst: the next level of stealth SolarWinds compromise exploited through sophistication and patience

SUNBURST 2020-12-16 · Intel 471 · Intel 471

Intel471's full statement on their knowledge of SolarWinds and the cybercriminal underground

SUNBURST 2020-12-16 · Twitter (@0xrb) · R. Bansal

List of domain infrastructure including DGA domain used by UNC2452

SUNBURST 2020-12-16 · Twitter (@FireEye) · FireEye

Tweet on SUNBURST from FireEye detailing some additional information

SUNBURST 2020-12-16 · · Qianxin · Red Raindrop Team

中招目标首次披露：SolarWinds供应链攻击相关域名生成算法可破解！

SUNBURST 2020-12-16 · Microsoft · Shain Wray

SolarWinds Post-Compromise Hunting with Azure Sentinel

SUNBURST 2020-12-16 · Bleeping Computer · Lawrence Abrams

FireEye, Microsoft create kill switch for SolarWinds backdoor

SUNBURST 2020-12-16 · Cloudflare · Jesse Kipp, Malavika Balachandran Tadeusz

Trend data on the SolarWinds Orion compromise

SUNBURST 2020-12-16 · Twitter @cybercdh) · Colin Hardy

Tweet on 3 key actions SUNBURST performs as soon as it's invoked

SUNBURST 2020-12-16 · Cyborg Security · Josh Meltzer

SUNBURST: SolarWinds Supply-Chain Attack

SUNBURST 2020-12-16 · Pastebin · Anonymous

Paste of subdomain & DGA domain names used in SolarWinds attack

SUNBURST UNC2452 2020-12-15 · Corelight · John Gamble

Finding SUNBURST Backdoor with Zeek Logs & Corelight

SUNBURST 2020-12-15 · Github (sophos-cybersecurity) · Sophos Cyber Security Team

solarwinds-threathunt

Cobalt Strike SUNBURST 2020-12-15 · PICUS Security · Süleyman Özarslan

Tactics, Techniques, and Procedures (TTPs) Used in the SolarWinds Breach

Cobalt Strike SUNBURST 2020-12-15 · Twitter @cybercdh) · Colin Hardy

Tweet on CyberChef recipe to extract and decode strings from #SolarWinds malware binaries.

SUNBURST 2020-12-15 · Twitter @cybercdh) · Colin Hardy

Tweet on some more capabilties of SUNBURST backdoor

SUNBURST 2020-12-15 · · 360 Threat Intelligence Center · Advanced Threat Institute

Operation Falling Eagle-the secret of the most influential supply chain attack in history

SUNBURST 2020-12-15 · Cyborg Security · Austin Jackson

Threat Hunt Deep Dives: SolarWinds Supply Chain Compromise (Solorigate / SUNBURST Backdoor)

SUNBURST 2020-12-15 · Prevasio · Sergei Shevchenko

Sunburst Backdoor: A Deeper Look Into The SolarWinds' Supply Chain Malware (Broken link)

SUNBURST 2020-12-14 · Twitter (@KimZetter) · Kim Zetter

Tweet thread on microsoft report on Solarwind supply chain attack by UNC2452

SUNBURST 2020-12-14 · Cado Security · Christopher Doman

Responding to Solarigate

SUNBURST 2020-12-14 · Twitter (@ItsReallyNick) · Nick Carr

Tweet on summarizing post-compromise actvity of UNC2452

SUNBURST 2020-12-14 · Twitter (@lordx64) · Taha Karim

Tweet on a one liner to decrypt SUNBURST backdoor

SUNBURST 2020-12-14 · Olaf Hartong

FireEye Sunburst KQL Detections

SUNBURST 2020-12-14 · splunk · Ryan Kovar

Using Splunk to Detect Sunburst Backdoor

SUNBURST 2020-12-14 · DomainTools · Joe Slowik

Unraveling Network Infrastructure Linked to the SolarWinds Hack

SUNBURST 2020-12-14 · Volexity · Damien Cash, Matthew Meltzer, Sean Koessel, Steven Adair, Thomas Lancaster, Volexity Threat Research

Dark Halo Leverages SolarWinds Compromise to Breach Organizations

SUNBURST 2020-12-14 · Palo Alto Networks Unit 42 · Unit 42

Threat Brief: SolarStorm and SUNBURST Customer Coverage

Cobalt Strike SUNBURST 2020-12-14 · Sophos · Ross McKerchar

Incident response playbook for responding to SolarWinds Orion compromise

SUNBURST 2020-12-14 · TrustedSec · Nick Gilberti, Tyler Hudak

SolarWinds Orion and UNC2452 – Summary and Recommendations

SUNBURST 2020-12-14 · Youtube (Ali Hadi) · Ali Hadi

Learning about .NET Malware by Going Over the SUNBURST SolarWinds Backdoor

SUNBURST 2020-12-14 · Cisco Talos · Nick Biasini

Threat Advisory: SolarWinds supply chain attack

SUNBURST TEARDROP 2020-12-14 · Symantec · Threat Hunter Team

Sunburst: Supply Chain Attack Targets SolarWinds Users

SUNBURST TEARDROP 2020-12-14 · Solarwind · Solarwind

Security Advisory on SolarWinds Supply chain attack

SUNBURST SUPERNOVA 2020-12-14 · Solarwind · Solarwind

Security Advisory on SolarWinds Supply chain attack FAQ

SUNBURST SUPERNOVA 2020-12-13 · VX-Underground

Directory: /samples/Exotic/UNC2452/SolarWinds Breach/

SUNBURST 2020-12-13 · Microsoft · Microsoft Security Intelligence

Trojan:MSIL/Solorigate.B!dha

SUNBURST 2020-12-13 · CISA · CISA

Active Exploitation of SolarWinds Software

SUNBURST 2020-12-13 · Github (fireeye) · FireEye

SUNBURST Countermeasures

SUNBURST SUPERNOVA TEARDROP UNC2452 2020-12-13 · FireEye · Alex Berry, Alex Pennino, Alyssa Rahman,

Andrew Archer, Andrew Rector, Andrew Thompson, Barry Vengerik, Ben Read, Ben Withnell, Chris DiGiamo, Christopher Glyer, Dan Perez, Dileep Jallepalli, Doug Bienstock, Eric Scales, Evan Reese, Fred House, Glenn Edwards, Ian Ahl, Isif Ibrahima, Jay Smith, John Gorman, John Hultquist, Jon Leathery, Lennard Galang, Marcin Siedlarz, Matt Dunwoody, Matthew McWhirt, Michael Sikorski, Microsoft, Mike Burns, Nalani Fraiser, Nick Bennett, Nick Carr, Nick Hornick, Nick Richard, Nicole Oppenheim, Omer Baig, Ramin Nafisi, Sarah Jones, Scott Runnels, Stephen Eckels, Steve Miller, Steve Stone, William Ballenthin

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

SUNBURST SUPERNOVA TEARDROP UNC2452 2020-12-08 · Securonix · Den Iyzvyk, Oleg Kolesnikov

Detecting SolarWinds/SUNBURST/ECLIPSER Supply Chain Attacks

SUNBURST 2020-12-01 · FireEye · FireEye

Solarwinds Breach Resource Center

SUNBURST 2020-01-22 · Thomas Barabosch

The malware analyst’s guide to PE timestamps

Azorult Gozi IcedID ISFB LOLSnif SUNBURST TEARDROP

▶ [TLP:WHITE] win_sunburst_w0 (20201215 | This rule is looking for portions of the SUNBURST backdoor that are vital to how it functions. The first signature fnv_xor matches a magic byte xor that the sample performs on process, service, and driver names/paths. SUNBURST is a backdoor that has the ability to spawn and kill processes, write and delete files, set and create registry keys, gather system information, and disable a set of forensic analysis tools and services.)
