SOLARWINDS SECURITY INCIDENT REVIEW & WHAT TO DO NEXT TO PROTECT YOUR PLATFORM

Thursday 7th January 2020

CONNECT WITH US

Prosperon Networks

Blogs: https://www.prosperon.co.uk/blog

LinkedIn: https://www.linkedin.com/company/826099

Twitter: https://twitter.com/Prosperon

YouTube: https://www.youtube.com/user/ProsperonNetworksLtd

Mark Roberts, Technical Director, Prosperon Networks

LinkedIn: https://www.linkedin.com/in/mark-roberts-3347762

THWACK: https://thwack.solarwinds.com/people/m_roberts

Mon Dulay, Sales Manager, Prosperon Networks

LinkedIn: https://www.linkedin.com/in/mon-dulay

AGENDA

- Introduction to Webinar & Prosperon Network Overview
- Sunburst and Supernova Security Vulnerabilities
- Current situation
- Actions to perform and decide upon
- Question & Answer Session
- Resources Available

PROSPERON AT GLANCE

Partner for 15 Years

First UK Partner

Over 800 Days PS

800 Support Cases pa

8 SCP Engineers

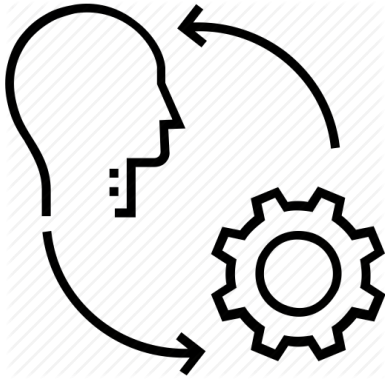
Security Cleared

Technical Excellence Award

THWACK MVP

PROFESSIONAL SERVICES

Consultancy



Implementation

System Integration

Training

Support

Health Checks

POLL: 1

HAVE YOU UPGRADED YOUR ORION PLATFORM YET?

SOLARWINDS – SUNBURST OVERVIEW

- FireEye a CyberSecurity company announced on 13th Dec 2020 they had identified a vulnerability in their installation of SolarWinds Orion
- A ‘Supply Chain’ vulnerability existed whereby signed files had malicious code within them, which could be used to allow malicious actor to execute commands on affected systems
- SolarWinds.Orion.Core.BusinessLayer.dll is the file affected and had code added that makes an HTTP call home, masquerading its traffic as part of the Orion Improvement Program protocol
- A very clever design
  - Hiding itself within genuine application protocols
  - Authentic digitally signed files
  - System checks to determine if it is ‘safe’ to make the call home
  - Domain Generation Algorithm (DGA) hash which includes source domain data
- No indication of automated malicious activity, but a call to Command & Control (C2) domain (<DGA>.appsync-api.<region>.avscmcloud.com)
  - Microsoft took swift ownership of this domain, which enabled identification of compromised organisations

SOLARWINDS – SUPERNOVA OVERVIEW

- An additional vulnerability was detected as part of the investigations into Sunburst
- Currently not felt to be connected to the Sunburst vulnerability and therefore from a second threat source
- This malware is an unsigned file ‘App_Web_logoimagehandler.ashx.b6031896.dll’, which is placed in the IIS “Inetpub\SolarWinds\bin folder” providing a method of remote code execution as a ‘webshell’ method, a known common attack vector
- This file is NOT implanted as part of the SolarWinds Orion application, instead would have to come from another source yet to be determined
- Designed to hide itself within legitimate Orion code, replacing original file with file which includes the malicious backdoor code, exposing a web API to receive commands from Command & Control source
- Designed to run fully in memory to reduce any fingerprint or forensic tracing

AFFECTED ORION VERSIONS

Orion Platform Version	Known Affected by SUNBURST?	Known Vulnerable to SUPERNOVA?	Recommended Action
2020.2.1 HF 2	NO	NO	No action needed
2020.2.1 & 2020.2.1 HF 1	NO	YES	Upgrade to 2020.2.1 HF 2
2020.2 & 2020.2 HF1	YES	YES	Upgrade to 2020.2.1 HF 2
2019.4 HF 6	NO	NO	No action needed
2019.4 HF 5	YES	YES	Upgrade to 2019.4 HF 6 (or upgrade to 2020.2.1 HF 2)
2019.4 HF 4 2019.4 HF 3 2019.4 HF 2 2019.4 HF 1 2019.4	NO	YES	Upgrade to 2019.4 HF 6 (or upgrade to 2020.2.1 HF 2)
2019.2 HF 3	NO	YES	Upgrade to 2020.2.1 HF 2 (or apply 2019.2 HF 3 Security Patch)
2019.2 HF 2 2019.2 HF 1 2019.2	NO	YES	Upgrade to 2020.2.1 HF 2 (or upgrade to 2019.2 HF 3 AND apply 2019.2 HF 3 Security Patch)
2018.4 2018.2	NO	YES	Upgrade to 2020.2.1 HF2 (or ensure you are running 2018.4 HF3 AND apply the 2018.4 HF3 Security Patch)
All prior versions	NO	YES	Upgrade to 2020.2.1 HF 2, apply temporary mitigation script, or discontinue use

SOLARWINDS – APPLICATIONS NOT AFFECTED

8Man

Access Rights Manager (ARM)

AppOptics

Backup Document

Backup Profiler

Backup Server

Backup Workstation

CatTools

Dameware Mini Remote Control

Dameware Patch Manager

Dameware Remote Everywhere

Dameware Remote Manager

Database Performance Analyzer (DPA)

Database Performance Monitor (DPM)

DNSstuff

Engineer's Toolset

Engineer's Web Toolset

FailOver Engine

Firewall Security Monitor

Identity Monitor

ipMonitor

Kiwi CatTools

Kiwi Log Viewer

Kiwi Syslog Server

LANSurveyor

Librato

Log & Event Manager (LEM)

Log and Event Manager Workstation Edition

Loggly

Mobile Admin

Network Topology Mapper (NTM)

Papertrail

Patch Manager

Pingdom

Pingdom Server Monitor

Security Event Manager (SEM)

Security Event Manager Workstation Edition

Server Profiler

Service Desk

Serv-U FTP Server

Serv-U Gateway

Serv-U MFT Server

Storage Manager

Storage Profiler

Threat Monitor

Virtualization Profiler

Web Help Desk

SQL Sentry

DB Sentry

V Sentry

Win Sentry

BI Sentry

SentryOne Document

SentryOne Test

Task Factory

DBA xPress

Plan Explorer

APS Sentry

DW Sentry

SQL Sentry Essentials

SentryOne Monitor

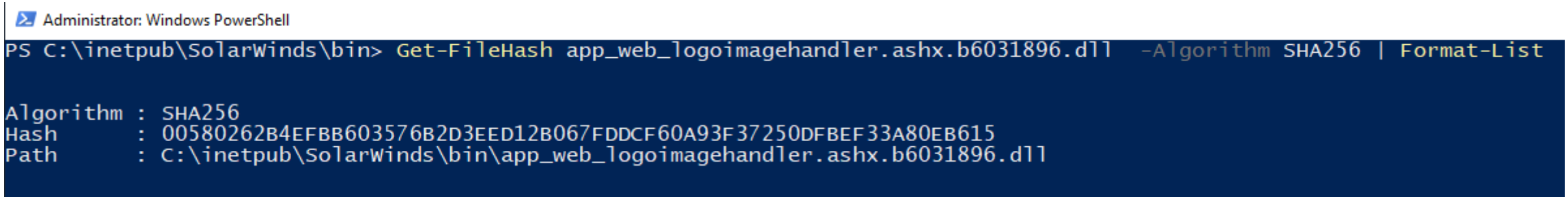
BI xPress

INDICATORS OF COMPROMISE - SUNBURST

- Check the hash (SHA256 of the files to identify if you have any malicious versions of the file SolarWinds.Orion.Core.BusinessLayer.dll
  - From 2019.4 HF 5: 32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
  - From 2020.2: ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
  - 019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
  - ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c
  - c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77
  - dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b
  - eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed
- SolarWinds have a script to automate this process
  - https://tinyurl.com/yyp3r552
- Review traffic logs to known IOC domains
  - deftsecurity[.]com
  - avsvmcloud[.]com
  - digitalcollege[.]org
  - freescanonline[.]com
  - globalnetworkissues[.]com
  - kubecloud[.]com
  - lcomputers[.]com
  - seobundlekit[.]com
  - solartrackingsystem[.]net
  - thedoccloud[.]com
  - virtualwebdata[.]com
  - webcodez[.]com
  - 13.59.205.66
  - 18.217.225.111
  - 18.220.219.143
  - 196.203.11.89
  - 3.16.81.254
  - 3.87.182.149
  - 3.87.182.149
  - 34.219.234.134
  - 54.193.127.66
  - 54.215.192.52

INDICATORS OF COMPROMISE - SUPERNOVA

- Check the hash (SHA256) of the app_web_logoimagehandler.ashx.b6031896.dll file
  - C15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71



- SolarWinds SUPERNOVA validation script
  - PowerShell script to confirm that you do not have vulnerable files
  - https://support.solarwinds.com/SuccessCenter/s/article/Use-a-script-to-verify-that-the-Supernova-patch-was-applied-to-all-Orion-web-servers?language=en_US

ACTIONS TO TAKE

- Identify if you are running an affected version
- Review your infrastructure for the IoC's
  - Review network Traffic logs, proxy logs, web traffic logs for communication to any of the C2 domains
  - Review lateral movement: new account logins to key infrastructure, privilege account escalation, new high-level accounts created
- Plan your immediate Orion patch/upgrade response
- Plan your long term Orion patch/upgrade response
- Change the password on all Service Accounts Orion uses to monitor and manage your infrastructure
  - NPM/SAM/IPAM credentials
  - NCM SSH/Telnet credentials
  - VMan credentials

PATCH OR UPGRADE

Patch

- If your version has a patch available, this is quickest security fix method.
- Instructions provided in patch Zip file on replacing files, settings etc.
- Each server must have the correct patching applied

Upgrade

- An application upgrade will deal with vulnerability resolution and provide enhancements, new features, performance benefits
- Depending on version level and modules and scale, it can take as little as 30 minutes to perform the actual upgrade
- If on version 11.x (2016.1) or below a multi step upgrade is necessary and likely recommendation to migrate to new servers for OS upgrade etc.
- Opportunity to review architecture; topology, use of cloud for hosting platform

OPTION 1 – INPLACE UPGRADE

NO COMPROMISE EXPOSURE

- Review version upgrade path
  - Orion Web Console (2019.x +) Settings > My Deployment > Upgrades
  - Support Portal > Upgrade Advisor
- Capture essential information
  - Server details; Name, IP, Local Admin login
  - SQL Server; location and account details - default username is SolarWindsOrionDatabaseUser
- Backups!
  - VM Snapshot (or whatever quick restore method you have)
  - SQL Database backups (Orion, Netflow, Log)
- Upgrade method – Centralised through Orion Web UI or Offline
  - Allow Internet access to specific URL's for centralised upgrade to download necessary files

OPTION 2 – REPLACE APPLICATION SERVERS

RISK AVERSE

- Removes risk of compromise being placed on the server for later usage
- Essentially the same as previous option, but fresh Application servers provided
- Keep the SQL database, within the Configuration Wizard process connect to the existing Orion database(s)
- ALL configuration and historic data remains
- Installation performed on the servers directly
  - Primary first then Additional Polling Engines and Additional Web Servers
- Use same Hostname or IP Address
  - Changes in DB necessary if you change the Hostnames of any Orion role servers
- Still very quick to implement
  - Example 5 Application server topology can be installed in a single day

OPTION 3 – COMPLETE REBUILD

TOTAL RISK AVERSE

- Slash and Burn approach with new servers and a blank Orion configuration and loss of all historic data
- Can be mitigated by reviewing the database, so an option felt can be avoided
  - Tools that were monitoring for any schema changes
  - Manual review of areas of the DB that could be used to re-execute malicious code; Alerting Engine, Stored Procedures, SAM script based monitors, NCM scripts
- Configuration can be exported from old platform, to expedite rebuild and bring same definition back
  - Alerts, Reports, SAM templates, UnDP templates, Views (via a script), Groups & dependencies (via a script)
  - However, this negates the reason for starting afresh

UPDATE SECURITY POSTURE

How does this incident change how you do things within Orion and ANY solution which has privileges to perform administrator level tasks

- Whitelisted access to the Internet from any Orion role server
  - https://thwack.solarwinds.com/t5/NPM-Documents/Orion-URLs-for-Firewall-Whitelisting/tac-p/614090
  - Create within your new monitoring procedure change request for adding to whitelist e.g. onboarding new SAS solution to allow monitoring of that platform
- Least Minimum Privileges
  - Reduce to lowest level possible, whilst maintaining function permissions Orion user accounts have for collecting data
  - Windows WMI protocol Read Only account vs Domain Administrator – can be painful to configure but is perfectly feasible
- Does the use of the SolarWinds Orion agent for polling increase your security position?

UPDATE SECURITY POSTURE

- Enable end-point protection on Orion servers, removing previous guidance on file/folder exclusions
  - Except MDF/LDF SQL files
  - Closely monitor performance impact of removal of such exclusions
  - **NOTE**: Some AV solutions are incorrectly identifying the updated safe files
  - SolarWinds are expected to update their advice in this area
- Central and capable event log monitoring - Are you capturing all of the data you need for forensic analysis?
  - Windows Event Logs, including AD audit events
  - Authentication system logs; AD, Radius, TACACS
  - Application logs
  - Network device logs (Syslog/SNMP Traps)
- Is your forensic source data being kept long enough to go back to point in time such a vulnerability was deployed

POLL: 2

Will YOU BE REVIEWING HOW YOU MONITOR YOUR INFRASTRUCTURE DUE TO THIS SECURITY INCIDENT?

Q&A SESSION

Prosperon networks | solarwinds

DO YOU HAVE ANY QUESTIONS?

PLEASE POST IN THE GOTOWEBINAR ASK A QUESTION PANEL

FURTHER READING & RESOURCES

- Core SolarWinds Security Advisory
  - https://www.solarwinds.com/securityadvisory
- Prosperon Blog Posts on incident
  - https://prosperon.co.uk/insights/applying-solarwinds-orion-remediation-to-vulnerability/
  - https://prosperon.co.uk/insights/solarwinds-security-alert/
- FireEye Blog Post
  - https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
- SolarWinds Upgrade Guides
  - https://documentation.solarwinds.com/en/Success_Center/orionplatform/content/orion_platform_installation_guide.htm
  - https://documentation.solarwinds.com/en/Success_Center/orionplatform/content/orion_platform_migration_guide.htm
- Collated list of links on this incident
  - https://github.com/eanmeyer/SolarwindsVulnerablityInfo