2020 SolarWinds Hack

- Name: Aravinth TM
- Registration Number: 19BCE7415

Recently a supply chain attack trojanized SolarWinds Orion softare to target organisations around the world. Victims include several US Government organisations and several Fortune 500 companies. This was possible due to a gross lack of security procedures within SolarWinds to secure software distribution pipelines.

About SolarWinds Orion Software suite

SolarWinds Orion Software is a non-free, proprietary network performance monitoring tool for Windows platform that has the following capabilities:

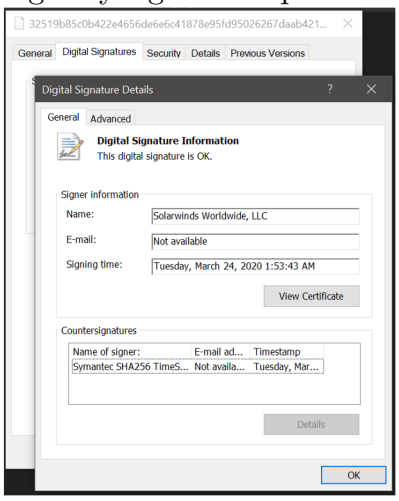
- Performance monitor
- Traffic analyzer
- Configuration manager
- User device tracker
- Server performance monitor

It is a software that runs with top privileges.

Discovery

On December 8. 2020, FireEye an Independent security team conducted an audit on it's own infrastructure, supposedly to contain a breach that they were experiencing.

They discovered that `SolarWinds.Orion.Core.BusinessLayer.dll`, a SolarWinds digitally-signed component of Orion Software suite contained a trojan horse.



Infection:

Attackers infiltrated SolarWinds's build system and planted the malware which would further be distributed to all their customers. This typical of supply chain attack. The infected SolarWinds software was then distributed via their website. Update package `CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp (02af7cec58b9a5da1c542b5a32151ba1)` was the first update that contained `SolarWinds.Orion.Core` a malicious software plugin. All updates from March 2020 and June 2020 contained this malicious plugin.

Authorized system administers download and install updates to SolarWinds Orion software that span large networks.

Characteristics

- It has a HTTP based backdoor that communicated with third-party servers. The malware has code execution capabilities - It contacts C2(command and Control) to retrieve "Jobs" to run on victim machine.
- The malware remains dormant for a period of two weeks and attempts to query `CNAME` of a subdomain of `avsvmcloud dot com`. The result is an other domain name which points to a C2. A full list of C2 domains was published by FireEye here.
- The malicious traffic is masqueraded as Orion Improvement Program protocol, a SolarWinds proprietary protocol to collect telemetry on the product.
- All reconnaissance results are stored with legitimate plugin configuration files toe evade detections

Victims

Solar winds stated that 33,0000 of their 300,000 customers use Orion. Some of the notable organisations are listed below:

SolarWinds' Customers

SolarWinds' comprehensive products and services are used by more than 300,000 customers worldwide, inclu
military, Fortune 500 companies, government agencies, and education institutions. Our customer list includes:

- More than 425 of the US Fortune 500
- All ten of the top ten US telecommunications companies
- All five branches of the US Military
- The US Pentagon, State Department, NASA, NSA, Postal Service, NOAA, Department of Justice, and the C
  the President of the United States
- All five of the top five US accounting firms
- Hundreds of universities and colleges worldwide

Partial customer listing:

Acxiom
Ameritrade
AT&T
Bellsouth Telecommunications
Best Western Intl.
Blue Cross Blue Shield
Booz Allen Hamilton
Boston Consulting
Cable & Wireless
Cablecom Media AG
Cablevision
CBS
Charter Communications
Cisco
CitiFinancial
City of Nashville
City of Tampa
Clemson University
Comcast Cable
Credit Suisse
Dow Chemical
EMC Corporation
Ericsson
Ernst and Young
Faurecia
Federal Express
Federal Reserve Bank
General Dynamics
Gillette Deutschland GmbH
GTE
H&R Block
Harvard University
Hertz Corporation
ING Direct
IntelSat
J.D. Byrider
Johns Hopkins University
Kennedy Space Center
Kodak
Korea Telecom
Leggett and Platt
Level 3 Communications
Liz Claiborne
Lockheed Martin
Lucent
MasterCard
McDonald's Restaurants
Microsoft
National Park Service
NCR
NEC
Nestle
New York Power Authority
New York Times
Sabre
Saks
San Francisco Intl. Airport
Siemens
Smart City Networks
Smith Barney
Smithsonian Institute
Sparkasse Hagen
Sprint
St. John's University
Staples
Subaru
Supervalu
Swisscom AG
Symantec
Telecom Italia
Telenor
Texaco
The CDC
The Economist
Time Warner Cable
U.S. Air Force
University of Alaska
University of Kansas
University of Oklahoma
US Dept. Of Defense
US Postal Service

Prevention

1. Freely publish source code: A network monitoring tool can listen in on all network chatter so it requires top privileges. No non-free, proprietary program should be top privileges. If sources were freely published, several actors along the supply chain would validate and audit changes before publishing it further downstream. This is typical of how free software organisations like GNU/Linux Distributions and BSD variants function.

2. Reproducible builds: Supply chain attacks are becoming increasingly popular. A supply chain compromise could lead to compromise of all parties that use that software. The best way to prevent against these types of attacks is offering reproducible builds. Doing so would enable everyone that has access to source code to independently compile and verify the signatures of officially distributed binaries.

3. Securing build environments: build environment security is critical. When an organisation doesn't have enough resources to monitor their build environment, they should consider outsourcing software build pipelines to commercially available solutions. These solutions have dedicated teams that monitor their infrastructure round the clock to protect against intrusions. In an increasingly cloud-favouring climate, the is the appropriate way to distribute software.

Investigation

SolarWinds claims that Russian government sponsored hackers were responsible for planting the malware.

Karspersky said that the malware has characteristics that resemble Kazur, which is believed to be created by an Estonian intelligence group called Turla, which has links to Russian federal security service, FSB.

The Russian government has denied involvement.

References:

1. Wikipedia article: https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach#Conclusions_by_investigators
2. FireEye Report: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
3. Kerbs on Security reports: https://krebsonsecurity.com/tag/solarwinds-breach/