



Cybersecurity Update 2021

Jenny Jeffers
Jennan Enterprises

Michael Morrissey
Morrissey Consultants

2020 – Year of the Biggest US Hack

- The SolarWinds Orion data breach, among other attacks
- What it was, how it worked and who was affected
- Why this matters to receivers and troubled companies
- Our obligation to protect Company data – what to do now?

SolarWinds Attack

- On December 11 , 2020 the U.S. government and the company SolarWinds disclosed a breach of their Orion Platform
- A sophisticated and likely nation-state-based attacker.
- SolarWinds Orion is commonly used network management software used to manage complex switched and routed IT/OT architectures.
- 30,000 companies use Orion. Approximately 18,000 downloaded infected updates.
- Congressional investigation underway

US Government Targets

- Treasury Department
- Departments of Energy and Commerce
- Department of Homeland Security
- The Pentagon
- State Department
- National Institutes of Health
- National Nuclear Security Administration

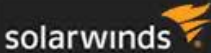
James Comer - House Committee on Oversight and Reform 2/26/2021

Chairwoman Carolyn B. Maloney

13:06 / 5:02:55



Solar Winds Management Console



HOME
NETWORK

NPM Summary
Network Top 10
Wireless
Overview
VSANs
UCS
Fibre Channel
EnergyWise
NOC View
Capacity


NPM Summary

All Nodes managed by NPM MANAGE NODES HELP

GROUPED BY REGION

- APAC
- EMEA
- North America
- 3Com
- American Power Conversion Corp.
- APC NetBotz
- Aruba Networks Inc
- Avaya Communication
- Cisco
- Compatible Systems Corp.
- Debian
- Dell Computer Corporation
- Extreme Networks
- F5 Labs, Inc.
- FlowPoint Corporation
- Foundry Networks, Inc.
- HP
- IBM
- Juniper Networks, Inc.
- Juniper Networks/NetScreen
- Linksys
- Linux
- Multi-Tech Systems, Inc.
- net-snmp
- Northern Telecom
- Palo Alto Networks
- Ruckus Wireless Inc
- Samsung Group
- Symbol Technologies, Inc.
- Synoptics
- U.S. Robotics, Inc.
- Unknown
- VMware Inc.
- Windows
- ZyXEL Communications Corp.
- South America

Worldwide Map of Orion Nodes HELP

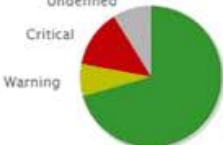


Map Data by OpenStreetMap. Tiles by MapQuest

Interfaces with High Percent Utilization HELP

INTERFACE	RECEIVE	TRANSMIT
LAB-CLUSTER-01.lab.tex		
WAN Miniport (SSTP) - Local Area Connection*	94%	96%
Router3.lab.local		
FastEthernet0/0 - Fa0/0	94%	96%
NPM_Cisco_FibreChannel		
vsan1 - IPFC interface - vsan1	63%	100%
fc1/7	63%	91%
fc1/10	62%	91%
Internet Gateway 3725		
Ethernet1 - WAN (NetFlow)	85%	65%
NPM_Cisco_FibreChannel		
fc1/14	63%	76%
fc1/9	64%	71%
fc1/13	62%	73%
fc1/12	62%	72%
fc1/5	65%	67%
fc1/3	62%	67%
fc1/4	67%	62%
fc1/8	62%	67%
fc1/11	62%	67%
sup-fc0	62%	67%
fc1/19	73%	54%
fc1/17	12%	100%
Comet 23		
Generic Marvell Yukon Chipset based Gigabit Ethernet Controller	13%	87%
NPM_Cisco_FibreChannel		
fc1/6	6%	79%
fc1/20	11%	74%
Bas-HP5400		
A1	72%	12%
NPM_Cisco_FibreChannel		

Hardware Health Overview HELP



Node Count: 68

48 Up 5 Warning

9 Critical 6 Undefined

Active Alerts (48) ALL ACTIVE ALERTS HELP

ALL UNACKNOWLEDGED ALERTS

ALERT NAME	MESSAGE	TRIGGERING OBJECT	ACTIVE TIME
Alert me when an application goes down	Alert me when an application goes down	Microsoft IIS	1d 2h 6m
High Transmit Percent Utilization	High Transmit Percent Utilization	Ethernet1 - WAN (NetFlow)	1d 4h 50m

High Errors & Discards Today HELP

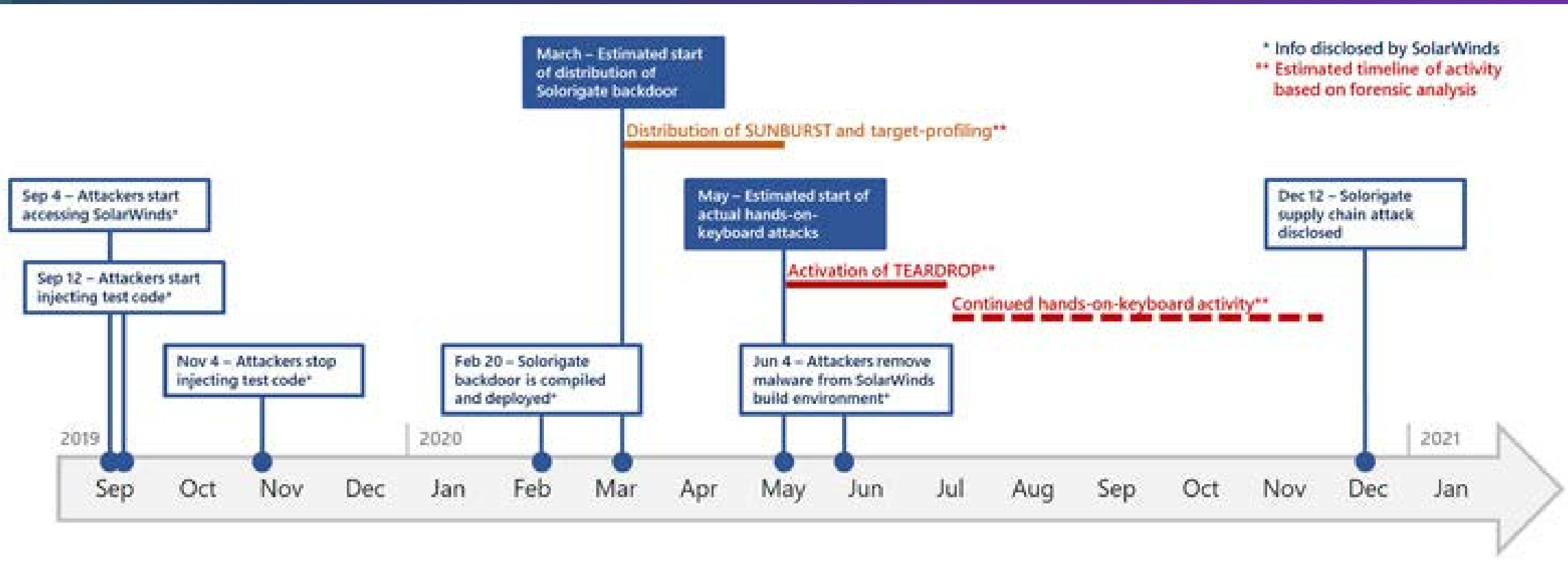
INTERFACES WITH ERRORS+DISCARDS GREATER THAN 10000 TODAY

NODE	INTERFACE	RECEIVE ERRORS	RECEIVE DISCARDS	TRANSMIT ERRORS	TRANSMIT DISCARDS
Perm_Tex-Mds9120-76-76	fc1/5	0 errors	0 discards	5,582,170,112 errors	5,808,010 discards

How They Got In

- Attacked SolarWinds and other software vendors.
- Hackers breached a system that SolarWinds uses to put together updates to its Orion product, per SEC filing on 12/14/20.
- Carefully matched the update files with files created in situ.
- “Trojanized” the updates to create a backdoor to the customer environments and installed various tools to gain administrative access.
- The malware remained dormant for 12–14 days before attempting to communicate with one or more of several command-and-control servers (C2s).
- C2s at Amazon AWS, GoDaddy and others allowed traffic to go undetected.

Highly Sophisticated Stealth Attack



Finding and Stealing the Data

- Orion connected to customers' Office 365 accounts as a trusted 3rd-party app
- Attackers were able to access emails and other confidential documents.
- Disabling the compromised Orion software would no longer be sufficient to sever the attackers' access
- Having accessed data of interest, they encrypted and exfiltrated it –over hidden transport channels.
- As new (Zero Day) malware, the attackers were able to evade detection by Einstein, a national cybersecurity system operated by DHS

Commercial/Financial Targets?

- Most Fortune 500 Companies used Orion software, as did tech firms.
- Source Code stolen from Microsoft Azure, Exchange, VMWare, others

January 5, 2021 - Cyber Unified Coordination Group (includes the FBI, CISA, and Office of the Director of National Intelligence with support from NSA):

- Attackers were likely Russian in origin
- The attack was an *intelligence-gathering effort*



THREAT ENVIRONMENT REMAINS

- Malicious acts by highly trained attackers
- Ransomware
- Intrusion and data theft
- Denial/interruption of service
- Reputation at Risk
- Others?

The Dark Marketplace 2021

1 Services



2 Distribution



3 Monetization



Source:
CrowdStrike
Cybersecurity
Report 2021

So What?

Why does this concern receivers and supervisors?

- If every government and business entity has been hacked, is anyone liable?
- Risks of intrusion are higher than ever
- Liability persists regardless of the challenges to protect data
- Security will cost more than ever
- IT resources are scarce in troubled companies

Follow Best Practices*

Recommendations remain the same:

- Assess Risks
- Inventory Data
- Protect the Data
- Protect the Network
- Protect Employees--and train them!

*Clearly, SolarWinds is responsible to some extent. It is owned by VC firms known for cutting costs. Management was warned of weak security in Orion applications.

One of many weaknesses was an FTP password of "Solarwinds123".

During Congressional testimony SolarWinds management blamed an intern for the [weak password] error

SolarWinds Homepage Today (sans apology)

solarwinds 

Security Advisory: In order to help ensure the security of your environment, SolarWinds asks all customers to upgrade/update their software within the **next 3 days** (by March 8, 2021). More information is available in your [Customer Portal](#), and in our [Security Advisory](#) and [New Digital Code-Signing Certificate pages](#).

Monitor any application and any server, anywhere.

Server & Application Monitor

Best Practice: ASSESS RISKS

- **CONSIDER A 3RD PARTY ASSESSMENT**
- **INCIDENT RESPONSE PLANS** – Complete? Current?
- **OUTSOURCING AND VENDOR MANAGEMENT**
 - Where is the data?
 - Clouds – are they safe?
 - Managed Service Providers – are they good?
 - SOCs and Vendor Attestations

Best Practice: DATA INVENTORY

Where is the sensitive or valuable data?

(Do archival records need to be online?)

- Actuarial Data – it's valuable too
- Policyholder data
- Claims data
- HR – Employee data
- Backups – what kind and where are they? Encrypted?

Best Practice: ASSESS LOGICAL SECURITY

- “Zero Trust Mentality” - Microsoft
- Password policies stated and enforced
- Multi-factor authentication -- Mandatory
- Lock it down – partition the data
- Disable old accounts

Best Practice: Restrict Sensitive Data

- ROLE BASED ACCESS – WHO AND WHY
- PASSWORD POLICIES
- ISOLATE SENSITIVE DATA (or move it offline)
- CONTINUOUS MONITORING – now easier in cloud environments like O365

Best Practice: Systems Review

- Network diagrams
- Server and pc inventory
- Firewalls – up to date?
- IPS/IDS – mandatory now
- Remote access – patched?



Best Practice: Incident Response Plan

- What constitutes a security event?
- Steps to identify and assess a breach
- Seek professional help before hand
- Cyberinsurance ?
- Notification – new laws coming
- Repair and learn

Best Practice: Encrypt Sensitive Data

- "AT REST" ENCRYPTION
- SERVERS
- LAPTOPS
- PORTABLE STORAGE DEVICES
- DATA IN TRANSIT
- CLOUD REPOSITORIES (turn it on)

Best Practice: IT Budget Review

- Is there a budget process in place?
- What security gaps must be filled?
- Outsourcing for security?
- Find the money or accept the risk
- Timeline?



Case Study Discussion

What we have seen lately....



Questions & Comments ?

Jenny Jeffers
Jennañ Enterprises, LLC

Michael Morrissey
Morrissey Consultants, LLC

Thank You.