SECURITY INSTITUTE

SolarWinds Breach

December 2020

SolarWinds Eight-Part Security Series
By: Bill Alderson

COMPREHENSIVE PAPER

SolarWinds Supply Chain Attack, notwithstanding nation-state criminal involvement, a global blame game continues – but are we denying reality? It seems we did not lock our own doors with FBI, CIA, and NSA, themselves culpable for losing their Red-Team hacking tools criminals now use against the world. Opinions aside, startling facts remain.

Bill Alderson solved security denial of service attacks against the US Stock market, led the team bringing back online the Pentagon at 9/11, solved numerous network meltdowns affecting F-500 companies, optimized biometric Intelligence applications, deploying with US military to Iraq and Afghanistan 6 times, certified 3,500 vendor-independent Network Forensic Security Professionals. Forty years' experience analyzing network packets, securing US government and American corporations provides the background to offer this analysis.

CONTENTS

SolarWinds Breach Eight-Part Series

Part 1

Anatomy of a Massive Data Breach - Eleven Steps Evading Prevention and Detection

SolarWinds Eight-Part Security Series By: Bill Alderson   © 2021 All Rights Reserved

Security INSTITUTE

SolarWinds SW Orion breach compromised private, proprietary, confidential and trade secret data of countless private and government organizations.

Some have taken comfort in the idea SolarWinds monitoring software does not "hold" PHI or high value data. While some monitoring products use a docile, low security "ping" test, Orion's deep internal monitoring requires **all-access security credentials** to firewalls, SQL servers, workstations, and routers. While it may not hold the data, **it does hold access**.

Do we understand the anatomy of how this attack occurred and how it might have been prevented? In this eight-part series, offering cogent packet analysis to the actual exfiltration host, we uncover the Who, What, When, Where, and Why of the SolarWinds breach. Considering ways the attack may have been prevented, we offer ways secretly remaining Trojan components might be detected, protected against, and rooted out of compromised networks over time.

SolarWinds breach attack was through an update of SolarWind's Orion Improvement Program OIP. Inserting rogue code into the software update established backdoor paths into SolarWinds customers who subscribed to the optional OIP eco-system, designed to improve software using customer shared metrics.

Rogue code perfectly timed went undetected and hid inside a Software Improvement Program SIP package update. Popular with vendors and customers, SIPs appeal to the altruist in all of us to click "participate anonymously to help" improve the software. Orion's SIP was the chosen delivery vehicle, successfully infecting thousands. While SIPs may improve overall services, they allow people with no "need to know" and who are potentially out to do harm "see" and pull data from inside an organization resulting in significant compromise. I will never click that "known compromise" box again. Maybe the industry should consider phasing out SIPs.

SECURITY INSTITUTE

Occurrence	SolarWinds Breach Steps
1	Attack Dll code named SolarWinds.Orion.Core. Businesslayer.dll undetected insertion.
2	The covertly names Dll is considered a valid compilation object into the update.
3	The Dll is made available for Internet download.
4	Available online to be pushed or pulled to the SW Server through its Internet access.
5	Smartly waits two weeks to avoid incoming detection mechanisms.
6	Code mechanisms to hide backdoor capabilities by sandbox detection.
7	Checked for Antivirus on the host.
8	Starts gathering information for exfiltration to awaiting criminals.
9	Code communicates to command-and-control C2 criminal server outside on the internet at DNS address avsvmcloud.com making data available to the criminals.
10	Outside criminals are now informed allowing greater enduring remote access compromise.
11	External criminals are enabled to conduct a hands-on-attack.
Access	Downloads additional compromise tools to use automated methods to surveil enterprise.
Access	Skilled attacker/s start going through the network, identifying vital systems from which to gather data, maintaining quiet control until discovered.

Fig 1 Diagram Depicting Eleven Breach Steps

The anatomy of the SolarWinds attack is outlined in the Eleven Steps below and depicted in Figures 1 and 2.

1. A .dll file placed in an update within the SIP at just the right place and at the right time.

2. The .dll compiled as digitally signed authentic code but only after lying dormant for two weeks.

3. The newly compiled update is pushed to a vital SW Server to the SolarWinds domain.

4. Clients, eager to keep their systems up to date, now download and install the Solar Winds update allowing the compromising code into their servers and individual computers.

5. The code sits dormant preventing immediate discovery and potential removal.

6. Does it live in sandbox?

7. Does it live in an anti-virus push?

8. Once executed, the code begins to gather data to be pulled off the target systems.

9. Once gathered, the data is prepared for exfiltration.

10. A message that data is readied for gathering is transmitted back to "hacker".

11. The gate is now open, and the data is free to be accessed. The same person who embedded the code has a pathway into the server just as they were authorized users.
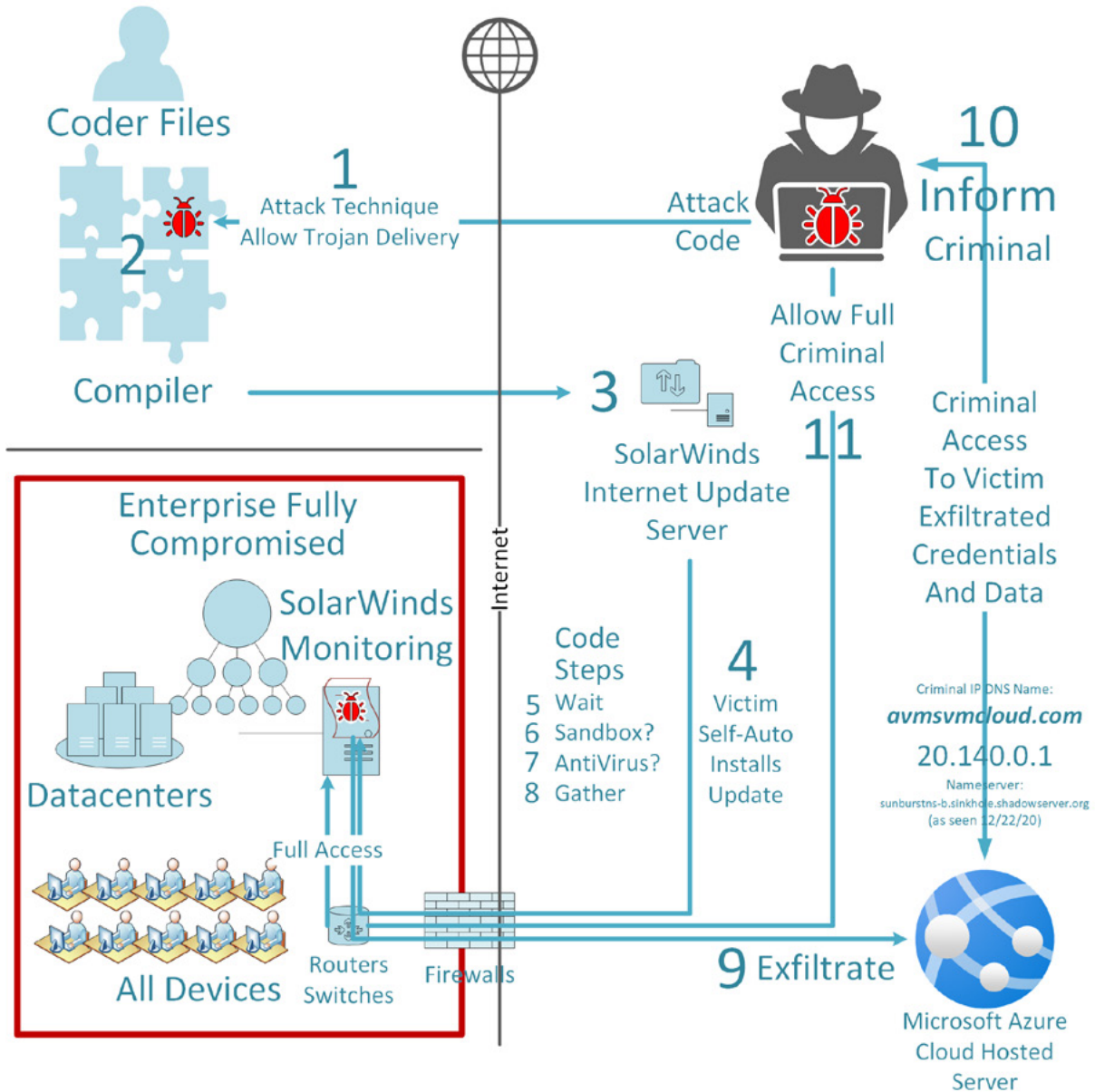
SECURITY INSTITUTE

SolarWinds 11 Breach Steps

Coder Files

1 Attack Technique
Allow Trojan Delivery

2

Compiler

Attack
Code

10
Inform
Criminal

**Allow Full
Criminal
Access**

Criminal
Access
To Victim
Exfiltrated
Credentials
And Data

3

**SolarWinds
Internet Update
Server**

11

Criminal IP DNS Name:
avmsvmcloud.com
20.140.0.1
Nameserver:
sunburstns-b.sinkhole.shadowserver.org
(as seen 12/22/20)

**Enterprise Fully
Compromised**

**SolarWinds
Monitoring**

Code
Steps
5 Wait
6 Sandbox?
7 AntiVirus?
8 Gather

4

**Victim
Self-Auto
Installs
Update**

Datacenters

Full Access

All Devices

Routers
Switches

Firewalls

9 Exfiltrate

**Microsoft Azure
Cloud Hosted
Server**

Internet

Fig 2 *Numbered List of Evading Attack Steps*

Criminals covertly placed Trojan Dll Code among files which compile into a software update package. Expanding on this high-level step by step summary, the trojan was either pushed or pulled from the Internet to SolarWind's customer-victim server, waiting patiently to begin its attack.

Once installed on customer-victim's server, smart attacker code waits two weeks, performs checks for antivirus or if contained in a "Security Sandbox" ensuring DNS resolution to the legitimate address of the host: **API.SolarWinds.com**. If it were in a sandbox, the DNS test might not resolve to the API server and the Trojan stops not risking detection. For this reason, air gapped SolarWinds Servers on government networks without Internet access may not fall prey to this attack but proves the same attack method could also affect government classified environments. As security risks are themselves classified information, no report is expected on how many classified networks were affected. Some 4000 lines of code garnered SolarWind's global admin access privilege allowing attackers to connect, gather, and configure anything.

Exfiltration to an attacker- chosen Microsoft Azure Cloud Server with a disarming DNS hostname: amsvmcloud.com, using common HTTP/S Put or Posts commands placed information on the criminal's server. Web links called (Universal Resource Locators) URLs were derived from unique enterprise names to evade obvious detection over suspicious terms as keylogger or backdoor. Automatic exfiltration was enabled through open Internet access from SolarWinds Orion providing awaiting criminals the information to carry out deeper hands-on surveillance activities inside the enterprise or the victim's cloud environments.

Burrowing deeper, criminals create security certificates as if the owner, authorizing themselves to build an Advanced Persistent Threat APT without detection. The DLL code, covertly named **SolarWinds.Orion. Core.Businesslayer.dll** prepared for outside criminals to operate unfettered in thousands of SolarWinds customer-victim networks.

Apparently, even advanced tools looking for Indicators of Compromise (IoC) failed to detect or alarm on the activity. Ironically, Fireye, a leading security software and services company, happened upon the SolarWinds attack while looking for their own recently stolen Red-Team tools (tools used to simulate hacking to discover security holes in customer networks). Fireye's stolen tools are like those used to break into domestic and foreign systems which were exposed to criminals by the FBI, NSA, and CIA in recent years. Now criminals and nation-states have expert tools developed by billion-dollar US government agencies.
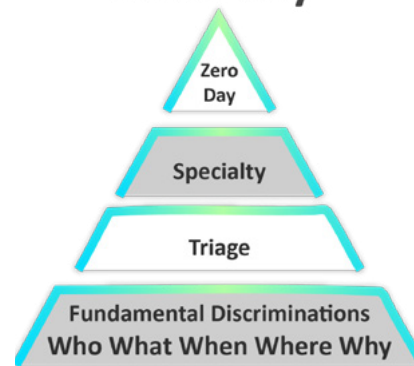
Security Analysis Hierarchy

Fig 3 *Hierarchical Security Priority Pyramid*

Criminal success has risen to perhaps impotent acceptance that hacker-criminals are omniscient, omnipotent, and omnipresent (God-like) - something the author rejects offering an alternative view.

This eight-part series explores security best practices letting you decide what fundamental analysis might have prevented or detected the attack. Join a detailed examination of the eleven steps and techniques that successfully evaded the mental discipline, capacity and immense capitalization of American government and business security. Consider the security hierarchy pyramid in Figure 3 suggesting fundamentals first, leading to triage, and more esoteric specialties as zero-day discovery at top. Hierarchical security steps and priorities, examined throughout the series, suggest that basic security fundamentals may have prevented the SolarWinds Orion breach.

Figure 4 Introduces 5 W's findings which are covered in Articles 4 and 6.

SolarWinds Breach 5 W's

Who	Criminals using IP DNS Name: avmsvmcloud.com Microsoft Cloud Server IP 20.140.0.1 Nameserver: sunburst-ns-b.sinkhole.shadowserverorg (as seen 12/22/20).
What	Ongoing access to intellectual property, finance, commerce, and defense information.
When	Trojan placed, waiting two weeks, criminals enter.
Where	Inside SolarWinds Orion Owning Victims Entire Enterprise.
Why	Surveillance to exfiltrate ongoing vital information gaining defense and economic opportunity over the United States.

SECURITY INSTITUTE

Bill@SecurityInstitute.com
11400 Concordia University
Austin TX 78726
SecurityInstitute.com

Fig 4

Who What When Where Why Findings

Part 2 _____

Danger of Direct Internet Updates

Protecting Vital Servers Holding All-access Credentials

CEO's and organization leaders might reconsider dependence on certified-by-brand security solutions responsible for protecting and managing Vital Servers without assurances that Internet access has been "air gapped".

Disastrous consequences have resulted from breaches in networks where this type of air-gap security was not in place. Many continue to suffer ongoing catastrophic effects of the 2015 Office of Personnel and Management OPM's leaking intimate details of clearance holders and their family members. Most organizations consider firewalls high security and have little experience with air-gap security concepts. Mammoth security vendors, through market-capitalization, and *certified-by-brand* loyalty protections, have convinced the market that their products are near impervious – with exception only to

"nation-state" actors. Thought **Omniscient, Omnipotent,** and **Omnipresent**, many falsely maintain foreign hackers cannot be stopped - minimizing accountability. Brand certified employees consider me out of my mind to suggest air-gap-like controls for Vital Servers. Vendors intrinsically suggest wide-open Internet for the convenience of automatic direct updates. CEO's and organization leaders might consider how *certified-by-brand security* foxes may be guarding the henhouse leaving Internet access wide open to Vital Servers.

Updating Vital Servers via automatic Internet updates is akin to having your coffee maker automatically add cream and sugar because the manufacturer thinks it will make your life easier. Just because something can be done, does not mean it should be. Greater scrutiny vetting Internet access may pay security dividends. Both Microsoft and Linux O/S auto update as a matter of common practice, however small security conscious organizations use Microsoft's free Windows Security Update Server WSUS internally for all O/S updates, preventing all devices from updating on the Internet automatically.

DATA
PROTECTION

SECURITY INSTITUTE

Windows has a purchase version named System Control Update Center SCCM that updates Windows and other O/S versions. SolarWinds also offers an internal network patch manager product we do not yet know if impacted. Each of these options provides a "gap" between your Vital Server and over 4 billion devices on the Internet.

Regardless how a SolarWinds customer-victim was updated, the Trojan DLL requires Internet access to be successful. Internet hosts: api.solarwinds.com and amsvmcloud.com were allowed access the Internet. In the future, should SolarWinds servers be minimally air-gapped from the Internet to prevent breaches?

Reasons Internet Access May Have Allowed SolarWinds Attack

1 Victims would not have been able to directly download the update, automatically or otherwise. If an internal Update Server was used, increased scrutiny may have prevented placement on an internal hardened Update Server.

2 Criminals may have used a backchannel from SolarWinds Internet Update to reach back into the Coder's compiler files allowing Trojan code to be placed. Simply reversing direction, the Coder used to place a file on the Internet for download might have been the path for reverse insertion.

3 Trojan code may have failed its DNS lookup Sandbox test to Api.solarwinds.com. A Vital Server should not have access to External Internet DNS, it should resolve to an internal DNS server maintained to include mission critical records and exclude known risky Internet-wide DNS records which may have stopped access to the amsvmcloud.com criminal DNS entry. Notice the DNS Nameserver's name.

4 If the Sandbox test included a communications access check to reach api.solarwinds.com before launching attack, it would have failed.

5 Exfiltration to the Internet Hosted Microsoft Azure Server avmsvmcloud.com would have failed preventing the Attacker from getting or using information gathered from the inside altogether.

Fig 1 *Reasons Internet Access May Have Allowed SolarWinds Attack*

Without Internet access the SolarWinds server breach would have failed.

1. Victims would not have been able to directly download the update, automatically or otherwise. If an internal Update Server was used, increased scrutiny may have occurred before placement on an internal hardened Update Server.

2. Criminals may have used a backchannel from SolarWinds Internet Update to reach back into the Coder's compiler files allowing Trojan code to be placed. Simply reversing direction, the Coder used to place a file on the Internet for download might have been the path for reverse insertion.

3. Trojan code may have failed its DNS lookup Sandbox test to Api.solarwinds. com. A Vital Server should not have access to External Internet DNS, it should resolve to an internal DNS server maintained to include mission critical records and exclude Internet-wide DNS records which may have stopped access to the amsvmcloud.com criminal DNS entry.

4. If the Sandbox test included a communications access check to reach api.solarwinds.com before launching it would have failed.

5. Exfiltration to the Internet Hosted Microsoft Azure Server avmsvmcloud. com would have failed preventing the Attacker from getting or using information gathered from the inside altogether.

Commercial organizations cannot fully air-gap their networks, yet applying some concepts would have foiled the breach.

Mission critical systems with global admin privilege might find more secure authenticated distribution methods beyond automatic updates. As mentioned,

## Vital Server   Internet
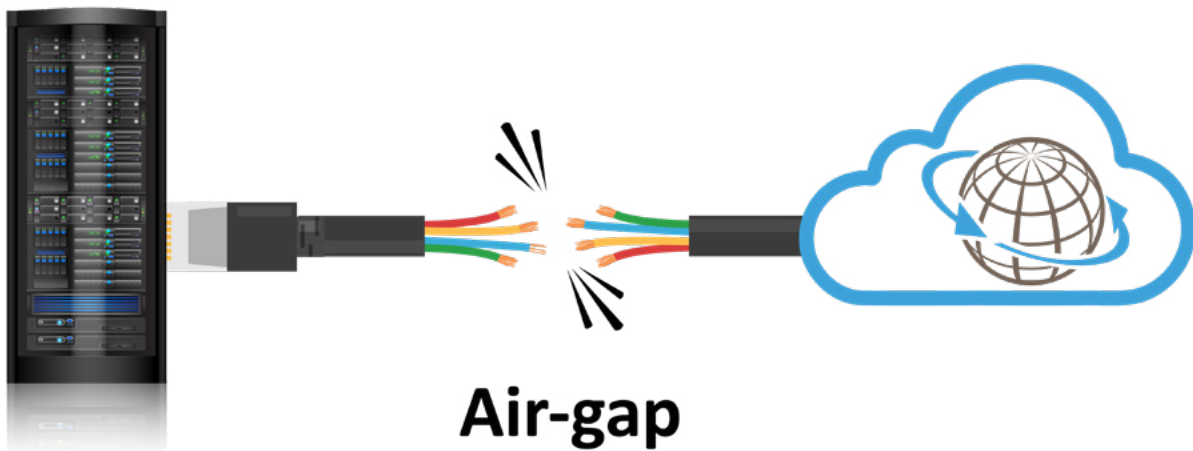
Air-gap

Fig 2 *Air-Gap Concept Illustration*

enterprise solutions exist to update private network servers internally – avoiding direct Internet updates. An internal update server solution may not have prevented this breach, but a wise best practice with small inconvenience to stop vital server access to the Internet.

SolarWinds offers Premises, Internet, and Cloud Monitoring solutions in one or separated packages. Having all three monitoring domains in one system means full compromise of all monitored domains. Another concept of air-gapping is to separate monitoring tools by Premises, Internet, or Cloud domains as a suggested alternative in Figure 3. Separating monitoring domains removes compromise one – compromise all risk. This is often accomplished intrinsically by using the best of breed tool for the environment monitored. SolarWinds started as a router, switch, firewall tool and grew into a one solution to include Vital Servers like Microsoft SQL Servers. Organic monitoring growth may have insulated some SolarWinds customers from full compromise if they had not yet bought into the single solution for all monitoring. A small insulation to stop one breach from taking all access credentials from one environment as was the case in this SolarWinds Breach.

Preventing Servers from unnecessary direct Internet access and separating monitoring systems makes good sense to distribute security.

Directional Security Perspectives next up in the series provides insightful ways to think about which connection directions matter most offering a simple way to think about security.
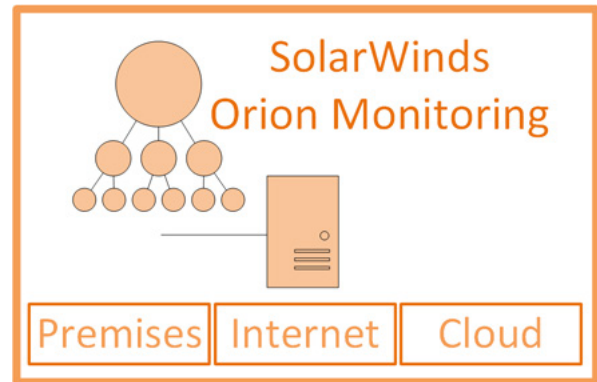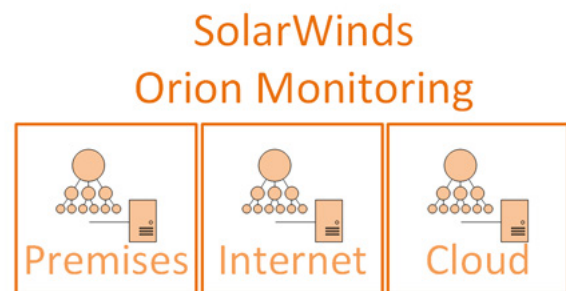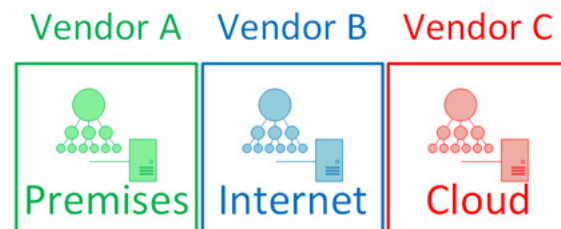
Fig 3   *Monitoring System Air-Gap Separated Monitoring Domains*

Part 3

Four Communications Perspectives of a Vital Server

Multiple Directional Security Perspectives Explained

Multiple directional attacks from public to private and private to public were used to complete the SolarWinds attack successfully. Understanding directional perspectives of security might require some understanding and visual reinforcements. Figure 1 Depicts IP Addresses by usage using Red as most concerning in any direction. Figure 2 provides a visual of Directional Perspectives using an organization's network: Incoming, Outgoing, Internal and External. Figure 3 provides narrative definitions to each perspective. A quick glance will help understand the many SolarWinds attack vectors used to evade and compromise.

Internet Protocol IP Address Range Definition and Usage Chart

A, B, or C Public Internet Addresses Can Be Used By Anyone –
Considered Dangerous To Communicate with Unaware.

Class	Usage	IP Address Range
A	Public Internet	1.000.000.000 - 126.255.255.255
A	Host Loopback	127.000.000.000 - 127.255.255.255
B	Public Internet	128.000.000.000 - 191.255.255.255
C	Public Internet	192.000.000.000 - 223.255.255.255
A RFC 1918	Private Internal	10.000.000.000 - 10.255.255.255
B RFC 1918	Private Internal	172.016.000.000 - 172.031.255.255
C RFC 1918	Private Internal	192.168.000.000 - 192.168.255.255
D	Multicast	224.000.000.000 - 239.255.255.255
Other	Experimental	240.000.000.000 +
Broadcast	All As Defined	255.255.255.255

Fig 1 Depicts IP Addresses
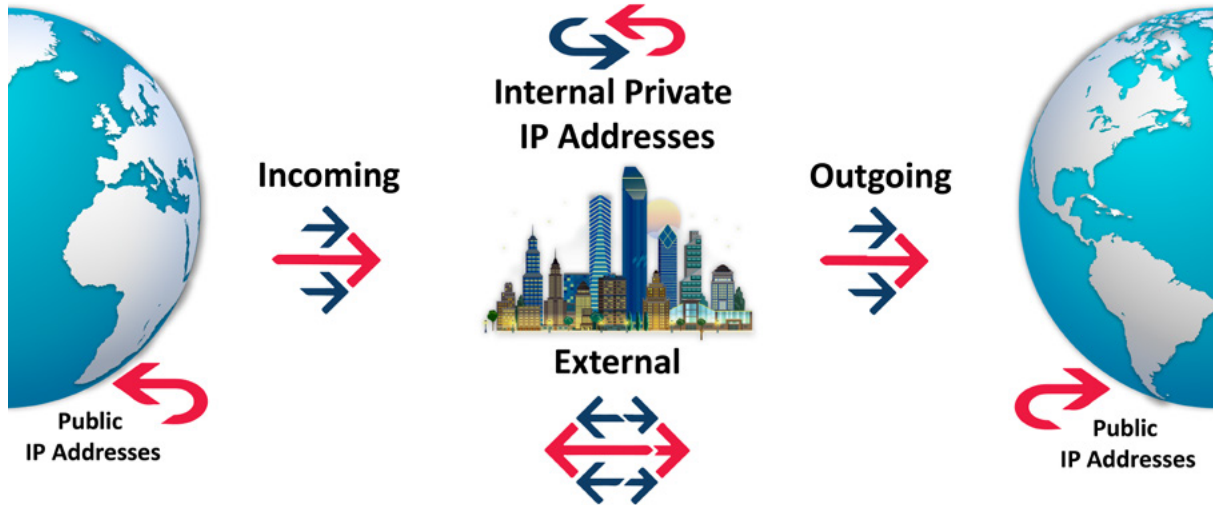
The Four Security Perspectives

Fig 2 *Visual of Directional Perspectives*

Fig 3 *The Four Security Perspectives*

SolarWinds attack used multiple directional attacks.

1. Public Criminal to Private SW Victim allowed placing the Trojan Code

2. Private SolarWinds pushing Trojan Code Update to SolarWinds Public Internet Update Server

3. Private SW Victims directly accessing Public Domain Name Service DNS Internet Servers instead of hardened filtered Private DNS Servers to acquire DNS Address on the Internet checking for: api.solarwinds.com IP Address.

4. Private Victims SolarWinds server DNS Address query for avmsvmcloud.com from a questionable DNS Nameserver: sunburst-ns-b.sinkhole.shadowserver.org (as observed 12/20/2020) may have been avoided by better DNS Security filtering.

5. Private Inside SW Server access to any Internet IP Address without whitelist or distance limits.

6. Private Inside SW Server access to any internal device without IP or Port whitelist or packet distance limitation.

Directional Perspective drives security decision vetting priority. Security perspectives are illustrated and described in several ways to speed understanding. Study the directional characteristics and stated priorities. WHO starts (begins or initiates) a connection from WHERE starts the security vetting process. Protocol and log analysis of TCP/IP sessions allow determination of the initiating or responding side of any conversation to know with confidence the initiating party. We vet sessions initiated from public Internet visitors more carefully than from a device inside a network. An Internet location provides some diligence toward keeping a Private Network, private
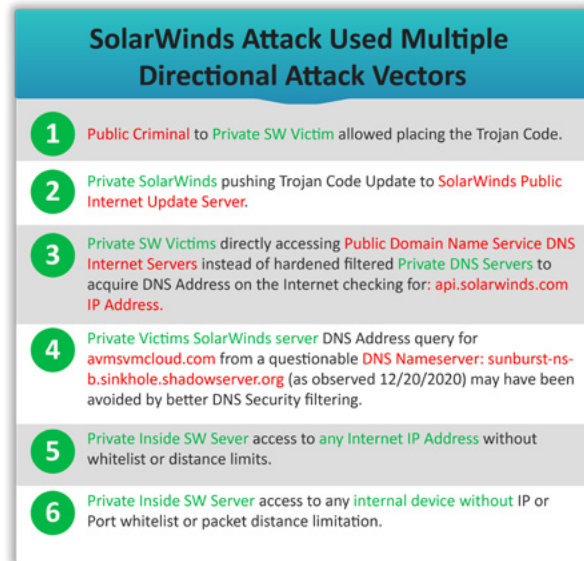

Fig 4 *SolarWinds attack used multiple directional attacks.*

by knowing where the initiator resides on the Internet. Although not perfect, Internet location has pretty good definition because each country received network numbers allocated by country. The Internet uses Reverse-Path-Forwarding which in simple terms means it will not let a wrong imposter address inappropriately route across the network. In other words, Coca Cola cannot send a packet that was assigned to Pepsi, or one from China be sent from India keeping some propriety to network number location. There are many reliable Internet IP Address location lookup services both free and paid. There are also services that report on IP Address Fraud Scores and security risk related value added insights. Many large organizations use IP lookups to vet allowed traffic. Gathering security score metrics about traffic is gaining popularity at large enterprises but seems out of reach to mid or small networks unless it is essential to their mission.

Consider massive data losses containing credential theft sold on the dark web, those credentials (maybe yours) are used against us everyday from far away simple hackers letting us know our accounts are compromised. More advanced criminals cloak their locations using Anonymous VPNs, Proxies or taking over accounts belonging to others they compromised to use to compromise others. Not all criminals are smart. Assuming all criminals are omniscient, omnipresent and omnipotent is a significant mistake, missing signals both amateurs or professionals might make disclosing their nefarious intentions – just this week we heard the Nashville Christmas explosion perpetrator's girlfriend reported his building explosives in his RV over a year ago, and police even saw and reported the RV with suspicious wires - a mistake not to get a search warrant to follow up. My point: criminals are not god like. Knowing statistics about WHERE connections are initiated provides the beginning of intelligent judgement on WHO we allow into a Private Network. WHERE session initiation originates becomes important to Defense or Military networks. Learning sessions are initiating from Iran, North Korea, or Syria creates due concern. COVID-19 required millions immediately begin work from home through remote access VPN's. A favorite pandemic hack has become the theft and sale of VPN credentials on the dark web allowing common criminals around the world to enter Private Networks. One indication is mapping WHERE VPN connections are initiated. Most IT personnel know WHERE VPN users should be initiated nearby their offices. Viewing a map of VPN originating locations opens eyes without advanced security skills. In this article, I will limit discussion to Incoming and Outgoing concepts of Security Perspectives. Outgoing controls are most important for Vital Servers. There are many products that

control user web browsing. SolarWinds breach sounds the alarm loudly to vet connections more diligently. Increased concern of what Vital Servers can reach is at a fever pitch. Mentioned earlier, solutions exist so Vital Servers and internal devices do not need to get updates off the Internet. Even if manual download is required, it is a wise choice to discontinue automatic Internet Updates for all servers using an alternative in-house update server – for all devices ideally. Four Directional Security Perspectives has gained popularity for good reason – it is easy to understand and organize security decisions.

Conversation on Security Perspectives

Any can be reduced by breaking it into logical elements. IP Address Directional Security Perspective Convention:

Refer to Figure 1. Public Internet devices are forced to use a Public Internet Address. Failing to do so, ensure packets cannot be delivered through the network of Internet routers. Internet routers will only route the Public Address space. The Internet specifically will not route a packet with a Private RFC-1918 IP Address. The IP Address Class and Use Table provides Public and Private Address Utilization for TCP/IP Networks. Simply, any IP Address beginning with dotted decimal 10.x.x.x or 172.16.x.x – 172.31.x.x or 192.168.x.x cannot ride the Public Internet.

This can be studied in the IP Address table. Any Red to any Green, Danger! Any Green to any Red, Danger! The IP Address Table included other address types for completeness and full understanding. Focus on Red Public to Green Private to gain basic concern concepts.

The Directional Perspectives helps understand the security concerns of communicating directionally. Some directions are more sensitive, basic numbered priorities provide directional sensitivity priority.

Starting with the conversation initiator's motivation to converse is the first task. The second is the other side or peer of the conversation. Why does IP Address A wish to initiate a conversation with B. Consider A is on the Public Internet and B Inside a Private controlled access network. The most important perspective is from the Internet into a Private Network controlling what is received from the Internet.

Firewall settings control this perspective unless a Private Address holder uses a Public Address on the outside of a Firewall or Load Balancer to purposely allow data from an External Address mapping to an inside Private Address. We term the External Address a Virtual IP VIP used to get to a Private IP not reachable from the Public Address. VIPs are created on the External side on the Public Internet to receive traffic destined for Internal Vital Servers. External Addresses on the Firewall or VPN device allow any Public Internet device to send to the External address. Firewalls examine the source address IP and Port number, often performing a more advanced vetting using a DNS reverse lookup to make sure it belongs to the appropriate domain before considering allowing it to access the internal server. If the Firewall settings agree and checks are affirmed, the Firewall will map the external device to access the Internal Server for the TCP/UDP Ports allowed and let the conversation operate bidirectionally. Many other DNS security validations can be performed to ensure an IP is assigned to the organization you are allowing entrance. DNS security has become a significant business for good reason. DNS Addresses can be spoofed to trick users to connect to B0A (using a zero instead of an O) getting their username and password to use after someone tries and fails... Start with these Directional Security Perspectives exhibits – and remember Red External Public Internet to anything is a high priority decision to vet session peers carefully.

Now that you understand allowing a Public Red IP Address in to access a Private Green IP Address is the highest number priority, you are ready to Vet connections. The 5 W's Who What When Where and Why help us Vet security access. This is the next topic to be covered. As you can see, the SolarWinds attack involved many access directions between Public and Private Addresses in both directions allowing the breach to occur. Can you see how allowing directional communications from the SolarWinds Vital server enabled the attack success?

Part 4 _____

Vital Server Communication Vetting 5 W's

SECURITY INSTITUTE

Allowing or Denying Vital Server Communications

A quick read of Figure 1 provides context and the basis for this narrative. SolarWinds Breach Security Research Findings in Figure 1 show benefits of 5W's Vital Server Session Vetting. A careful reading of

Vetting Vital Servers carefully on a regular basis provides a baseline for Vetting Internet access limits and alarming on suspicious behavior. Sensory visualization of communication sessions on an Interactive World Map allows non-expert data owners to see where their data is moving, helping security experts better know what is abnormal for Vital Server data travel limits. One security person cannot be expected to Vet 500 Vital Servers without platform, application, and data owner observations.

The 5 W's of Security Analysis

Process | **Question** | **Across The Four Perspectives**

1 Who? Both Communicating Pair IP, DNS, Reverse DNS, ASN,

2 What? Application Ports, Anonymous Proxy, TOR, GDPR

3 When? Day, Time, Frequency of Occurrence

4 Where? GeoIP Location, Building, Floor, Cubical, Row, Column, Rack

5 Why? Reason to Allow or Deny Communications

Fig 1 *The 5 W Descriptions*

Vetting anonymous communications to Vital Servers require collaboration from data owners and even user observation. In future, users, and system managers, will daily be able to see where their DNS Name and IP Address travels on data travel maps, allowing their input, spreading security manpower from one security person responsible for 10,000 IP's to distributing security responsibility hierarchically from End User – Manager - Data Owner - Platform – Business Application Owner to Security Firewall controls where data travel policies are controlled. SolarWinds Breach should end the carefree days of allowing anonymous communications sessions without prior allowance and vetting.

The example on the next page were from 38 actual example packet captured sessions using the same exact URL's to the same Microsoft Server avmsvmcloud.

com used by the criminals. DNS packet captures showed the DNS lookups going to non-SolarWinds DNS Nameservers sunburst-ns-b.sinkhole.shadowserver.org with a tip off to the nefarious nature of the criminal objectives. Client and Server TCP Flags indicate proper 3-Way SYN SYN ACK were present. A common SYN attack might only indicate a lone "S" for SYNs flooding the network. Session recording, mapping, and research for every session on a network are shown making quick work of session vetting. Manual research requires minutes each to find the data provided by one click on a map dot popping up security research for a suspect session. IP Addresses and DNS info can be researched one by one using WhatismyIP.com or MXToolbox and other internet tools. The patented mapping and research tool are from HOPZERO founded by the author.

SECURITY INSTITUTE

Actual SolarWinds Breach Exfiltration Host 5 W's Security Research Provided from Tool at Right.

Who:
Criminals using IP DNS Name: avmsvmcloud.com
Microsoft Cloud Hosted Server IP Address 20.140.0.1
Autonomous System Number ASN: 8070,
ASN Name: Microsoft-Corp-Msn-ASN
Criminal Nameserver: sunburst-ns-b.sinkhole.shadowserver.org

What:
Data Exfiltration on HTTPS TCP Port 443
Client Server Bytes C-Bytes 43429 S-Bytes 32076 (example session)
TCP Sessions: 38 Slow speed 1927 – 2609 bps
Risk Scores: Disabled for this test
Criminal ongoing access to intellectual property, finance, commerce, and defense information

When:
Trojan placed, waited two weeks, gather credential data
Exfiltration Date: Dec 23, 2020 at 9:12:04PM CST (example)
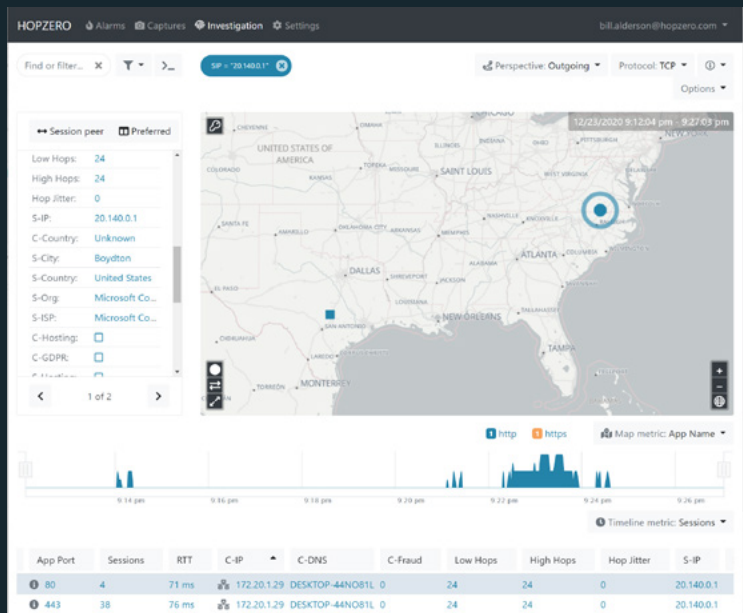
Where:
Server Responder Microsoft Azure Datacenter Boydton VA
Client Request Inside SolarWinds-Victims Entire Enterprise
(Example: Austin Texas, Steiner Ranch, St. Address Redacted)
Distance: 24 Network Router Hops away, no Hop Jitter
Round Trip Time RTT: 76ms

Why:
Surveillance to exfiltrate ongoing vital information gaining defense and economic opportunity over the United States

Security Research Tool

Duration:	133171
S-AS:	8070
S-ASOrg:	MICROSOFT-CORP-M$
S-Type:	business
C-bps:	2609
S-bps:	1927
C-Bytes:	43429
S-Bytes:	32076
Data:	☑
App Name:	https
App Port:	ⓘ 443
Sessions:	38
RTT:	76
C-IP:	172.20.1.29
C-DNS:	DESKTOP-44NO81L
C-Fraud:	0
Low Hops:	24
High Hops:	24
Hop Jitter:	0
S-IP:	20.140.0.1
S-City:	Boydton
S-Country:	United States
S-Org:	Microsoft Corporation
S-ISP:	Microsoft Corporation
C-Hosting:	☐
C-GDPR:	☐
S-Hosting:	☐
S-EU:	☐
C-AnonVPN:	☐
C-LegitProxy:	☐
C-PublicProxy:	☐
C-TOR:	☐
Risk Score:	0
Client Flags:	U A P R S F
Server Flags:	U A P R S F

Who:

Who includes DNS names and IP addresses, with associated ownership for each communicating pair.

Public Internet Who Includes:

Microsoft Azure Cloud Server, IP Address, Autonomous System Numbers ASN's are different networks within the internet, each named by who owns that part of the Internet, each one having its own IP address ranges the ASN originates and routes across the Internet to other ASN's before reaching the destination ASN.

Internet Reverse DNS names bring context to Who your vital server is communicating, representing the host name and the Internet Domain for an IP Address session peer.

Private Internal Who Includes:

Internal Device Name and RFC 1918 IP Address and Internal Reverse DNS name/s,

Internal names often provide a type such as SQL Server or Computer name or User's ID.

IP Addresses and names:

Are assigned automatically by a DHCP (Dynamic Host Configuration Protocol) Server automatically or assigned permanently called a Static IP Address. Dynamic addresses can change requiring a record of which machine/user was using an address on a date or time.

What:

Application Port, directional data volume statistics, speed in bps, measured latency round trip time RTT, number of routers between (HOP distance)

When:

Date, time, interval, recurrence, days, nights, after hours, weekends, holidays to avoid detection.

Day of week, hour of day, weekends, month end, quarter end, yearend.

When is important to resolve Who at that time was in control of the IP Address or DNS Name.

Session duration length in seconds.

Where:

Knowing locations of both sides of sessions provides timely risk information. Visualizing application users by location opens a whole new understanding to location-based security risks. Seeing where users are communicating by application both internal and offer powerful visibility.

Application	Port Number
HTTP	80
HTTPS	443
Oracle SQL	1525
Microsoft SQL	1433

Fig 2 Ports Are WHAT Is Being Sent

Being able to see where one or a group of users are located provides enhances security awareness.

Internet Addresses: Paid GeoIP services provide accurate map location and important insights.

Internal RFC 1918 IP Address: Internal GeoIP for multi-site networks is even most important providing mapping of internal users or servers to know what devices might be compromised.

Vetting user access to a known criminal on the Internet requires finding your own user fast and getting an idea of where Internal users of a high security application under attack provides rapid useful information.

In addition to location are IP attributes such as an Anonymous VPN, Private or Public Proxy, TOR Node, and if the connection creates legal requirements as from California or an EU GDPR nation. Advanced security database lookup on IP Fraud / Risk and added Calculated Risk Scores provide key security metrics to Vet access to Vital Servers.

Why:

The purpose of the first 4 W's is to answer the final Why leading to allowing or denying the connection regardless of The Four Directional Perspectives: Incoming, Outgoing, Internal or External traffic.

Consider **Who**	in the Why: Communicating with a device from a known bad location is elementary.
Consider **What**	application port provides sensitivity context.
Consider **When**	should make sense to timing elements.
Consider **Where**	allows a simple logical decision of where such data may be safe.
Consider **Why**	by putting all findings together to allow or deny the traffic.

5 W Example Allow - Deny Decisions:

We choose to **allow** a **Who**: IP of SQL Server communicate between **Who**: Middleware server **Where**: in the Datacenter using **What**: Oracle Port 1525 **When**: 24 Hours as developer application flow diagram specifies.

We choose to **deny** a **Who**: IP SolarWinds Server **Where**: in the Datacenter to a **Who**: DNS **amsvmcloud.com** resolving to **20.140.0.1** a Microsoft Hosted Server by DNS Nameserver: **sunburst-ns-b.sinkhole. shadowserver.org** across **What**: Port HTTPs 443 or HTTP 80 **When**: anytime, **Why**: because it is a bogus DNS Name, resolved by a bogus DNS Nameserver to a Paid Microsoft Hosting Service IP Address.

Do you have the Who: What: When: Where: to answer Why: a Vital Server is allowed to communicate?

SECURITY INSTITUTE

Part 5

Software Improvement Program – An Inside Job?

SECURITY INSTITUTE

How Did Attackers Get Intimate Information?

SolarWinds attack required obscure private intimate knowledge combined with more accessible information domains and skilled execution. Figure 1 offers potentials for how information could have been exposed to enable the SolarWinds attack. Articles 1, 6 mentions steps and the topic of how the attack happened. This article focuses on how information thought to be near impossible to know became available to the attackers. Simple logic defies that a foreign nation-state without assistance from those holding intimate information could have carried out the entire attack.

Programmers today change jobs often, do related side freelance jobs allowing access to intimate information such as Software Improvement Programs. Although not privy to SolarWinds development security, their outsourcing policy or control policies, the industry often discloses internal information in the process of development. Requests for Quotation RFQ and Development Specifications can expose some key intimate details to potentially insecure resources.

Some Inside Job Considerations

1 Impossible to Know Intimate Information

File names of compiling file components.
File directory names.
Network location of files.
Server name where files located.
Security credentials to access and add files.
Internal SolarWinds compiling steps and resultant file package destinations.
Where files are moved along the steps to SolarWinds Update Server on Internet.
SolarWinds Internal Processes Updates Utilize.

2 Commonly Available Information

Standard Microsoft or Dev Kit compiling file default locations
Software Improvement Program Dev Products and Service Companies
Standard File directory names
Previous SolarWinds Update directory and filenames

3 Intimate Information Found or Guessed

Previous undiscovered SolarWinds breaches.
Previous unreported SolarWinds breaches.
Included in SolarWinds RFQ for OIP/SIP Developers.
Microsoft Developer Training Documentation and Examples Names

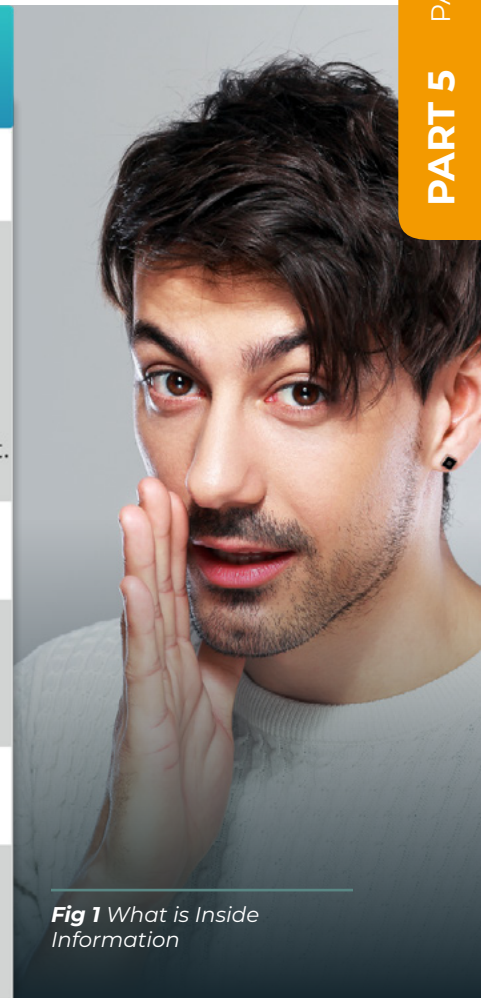*Fig 1* *What is Inside Information*

SECURITY INSTITUTE

Surmising that SolarWinds did not always have an Orion Improvement Program for customers to participate, at some time it decided to benefit from Software Improvement Program SIP gaining customer assistance from their information. It is plausible that another company had a SIP program that was developed by a company offering a dev kit for SIP's, or perhaps even a full-service development offering. That SIP company would have intimate knowledge of how to perform some parts of this attack. Programmers offering freelance services may also help someone as SolarWinds or others build out the SIP system using a formula used previously. Merely guessing that may suggest how a foreign nation-state might gain assistance to pull off a sophisticated multidisciplined attack requiring intimate information to carry out a sophisticated supply chain coordinated attack.

Where did attackers get intimate information required to carry out the attack without detection?

1. **Impossible to Know Intimate information includes:**
   - File names of compiling file components.
   - File directory names.
   - Network location of files.
   - Server name where files located.
   - Security credentials to access and add files.
   - Internal SolarWinds compiling steps and resultant file package destinations.
   - Where files are moved along the steps to SolarWinds Update Server on Internet.
   - SolarWinds Internal Processes Updates Utilize.

2. **More available information:**
   - Standard compiling file default locations
   - Standard File directory names
   - Previous SolarWinds Update directory and filenames

3. **Ways Intimate information may have been guessed or found:**
   - Previous undiscovered SolarWinds breaches.
   - Previous unreported SolarWinds breaches.
   - Employees, contractors, companies receiving development SolarWinds RFQ for OIP/SIP Developers.
   - Microsoft Developer Training Documentation and Examples names used.

SECURITY INSTITUTE

Criminals Create Authentic Certificates Reusing Keys & Tokens

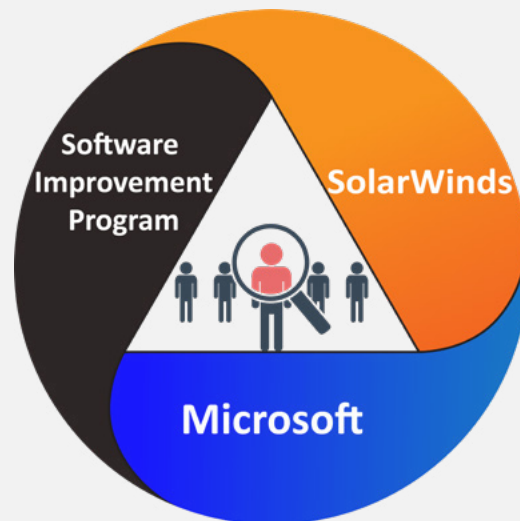**Fig 2** *Criminal create their own certificates*

Fig 3 *Who Could Provide Inside Job Information*

Figure 2 visualizes how attackers created their own certificates and used credential keys and certificates to build an Advanced Persistent Threat APT. Not only could they gather credentials but create their own as if they were the customer-victim building greater and deeper access.

Figure 3 identifies potential identification of suspects that knew Microsoft, SolarWinds and Software Improvement together as likely candidates for helping the catalyst perpetrator which could be a nation-state or sophisticated well resourced criminal group.

In addition to understanding this attack are potential Trojan attacks hand placed by the group or continue to be placed due to continued access. The next article addresses Vetting and Exterminating Entrenched Criminals speaking to continually ferreting out these and other such interlopers.

Part 6 _____

Vetting and Exterminating Entrenched Criminals

Security Perspectives 5 W Extreme Vetting Vital Servers

Extreme Vetting adds to basic security fundamentals already discussed in Article 3 Directional Security Perspectives and 4 Vital Server Host 5 W Vetting.

This article assumes criminals have fully embedded and there are no assurances additional Trojans were not planted while the system was fully owned. It is very difficult to assure a customer that their network is free of active criminals.

The RX for Extreme Vetting is as follows:

1. Record and log all network communication session forever - good, bad, denied, or suspicious malformed session attempts. Unlike server generated and collected logs, logging of sessions as actually occur provides a central collection point that cannot be erased and are permanently stored.

2. Look for suspicious incomplete and partial TCP/IP communications session attempts.

3. Regularly spot check persistent continued communication attempts occurring on the outside of the Firewall that now may be denied by changes after the attack, this shows continued attempts criminals were previously successful accessing data from. These old attempts show continued attempt history and if followed to the 5 W's may uncover information about the criminal's method of operation MO and what they may expect will work given a hidden Trojan attack vector come to life after some period.

4. Use tools that identify the running program executable responsible for spawning each network session. This shows what program initiates each TCP/IP communications session, providing traceability for each session back to the program responsible. Even docile connections to common locations can contain covert exfiltration of data. If an attacker left a Trojan called exfilattack. exe or even something less suspiciously named, it uses anonymous SSL encryption to hide the payload from easy examination.

5. From a server owned by your organization, most encrypted sessions can be decrypted by using your private encryption certificate to do so. This allows secondary analysis and inspection of suspicious encrypted sessions.

6. Impossible to decrypt are sessions to devices you do not own, that use an external (or criminal) owned private certificate to encrypt the session. In such case, you are blind except trusting the 5 W's for the destination server to Vet the session. The SolarWinds exfiltration was to a Microsoft Server giving false confidence as the destination of the exfiltration. In that case the private certificate was owned by the criminal not allowing decryption, so not accounting for what information was exfiltrated.

It is a time-consuming process to record all network sessions, considered a daunting "boil the ocean" task. We will discuss tools more specifically in Article 8 that can accommodate session recording.

The same Five W's: Who, What, When, Where and Why discussed in article 4 performed for all sessions, with filters for partial, malformed or incomplete connections broken down by critical application ports provide faster work at Extreme Vetting.

Extreme Vetting Discovers Embedded Criminals

1 Record and log all network communication sessions forever - good, bad, denied, or suspicious malformed session attempts.

2 Look for suspicious incomplete and partial TCP/IP communications session attempts

3 Spot check communication attempts on the outside of the Firewall that may persist even after attack firewall changes made to deny entry. Continued attempts may uncover information about the criminal's method of operation MO and their expectation of a hidden Trojan attack vector come to life

4 Use tools with features that identify the running program executable responsible for spawning each network session. Microsoft's NetMon shows what program initiates each TCP/IP communications session, providing traceability for each session back to the program responsible. Even docile connections to common locations can covertly exfiltrate data. If an attacker left a Trojan called exfilattack.exe or even something less suspiciously named, it uses anonymous SSL encryption to hide the payload from easy examination.

5 A server owned by your organization encrypted sessions can be decrypted by using your private encryption certificate in analyzer and other tools, allowing secondary analysis and inspection of suspicious encrypted sessions

6 Criminal server encrypted sessions are impossible to decrypt. These sessions use criminally owned private certificates to encrypt the session which you do not have access. Such sessions should be Extreme Vetted with 5 W's for potential criminal ownership or fraudulent behavior. SolarWinds exfiltration was to a Microsoft Server offering false confidence. In that case the private certificate was owned by the criminal not allowing decryption, so not accounting for what information was exfiltrated. It was the DNS Nameserver's own DNS hostname that tipped off criminal ownership.

Four Communications Perspectives and 5 W's Against Bulk Sessions

Recording volume Vital Server traffic sessions on the wire is a consolidated location to see all traffic, not just one server's log (which hackers often modify covering their tracks). Some devices do not provide logs and some communications never go through a firewall to be recorded. Recording the wire provides a central place to monitor traffic. Ports help describe vital data movement by what type of data. Perspectives importantly describe What side initiates a session – vitally important to know if an unknown outsider on the Internet starts the connection to ensure maximum vetting occurs on sessions started on the public Internet. The four perspectives described, become critical to understanding and applying high volume session traffic or over longer periods, addressing directional security perspective answering the "Who" we allow our vital servers to converse. Remember SolarWinds criminal session activity using the Mission Critical Vetting Form? Finding Microsoft Azure avsvmcloud.com Outgoing Direction uncovering the nefarious motivation of the Criminals? Here we will describe the same process to Vet bulk sessions.

TCP Connection Status Indicators

| ID	Ports/Apps	TCP Connection Type	Packet Error	Capture Error	Notes
1	Admin	Good	No	No	Admin Ports 22,23 3389 (other Remote Control)
2	Database	Good	No	No	Database Ports 1433, 1521, 50000,5432, 3306, 6379, 11211
3	Email	Good	No	No	Email Ports 110,995, 25, 587, 465, 143
4	File Access	Good	No	No	Email Ports 110,995, 25, 587, 465, 143
5	EP Mapper	Good	No	No	File Access Ports 111, 1110, 2049, 4045, 139, 445
6	Any	Failed Sync attack wo ack	Yes	No	
7	Any	Failed Sync attack w ack	Yes	No	
8	Any	Failed Connection	No	Maybe	Failed Conns ToClientFlagsAck = false
9	Any	Failed Sync	Yes	No	Ack Attack
10	Any	Succesful with/without data	No	No	
11	Any	Successful with Data	Yes	No	Contains Data = true
12	Any	Successful without Data	No	No	Contains Data = false
13	Any	Suspicious	Yes	No	TCP Flags Ack=true Data = false
14	Any	Unidirectional	No	Yes	Not Bidirectionally Captured
15	Any	Unidirectional	No	Yes	Alternate Path not Captured
16	Any	VN Tagged	No	Yes	Captured Virtual Network Tags
17	Any	802. 1q Tagged	No	Yes	Captured VLAN Tags
18	Any	Ether-channel	No	Yes	Missing Mac Address Channels
19	Any	Full Data Captured	No	Data	Use Snap-Len Limit

SECURITY INSTITUTE
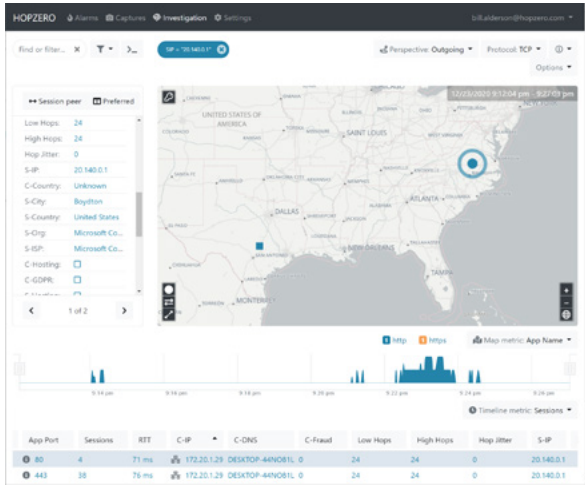
Fig 1 (Left) *Individual Session Vetting*
Fig 2 (Below) *Bulk Session Vetting Filters*
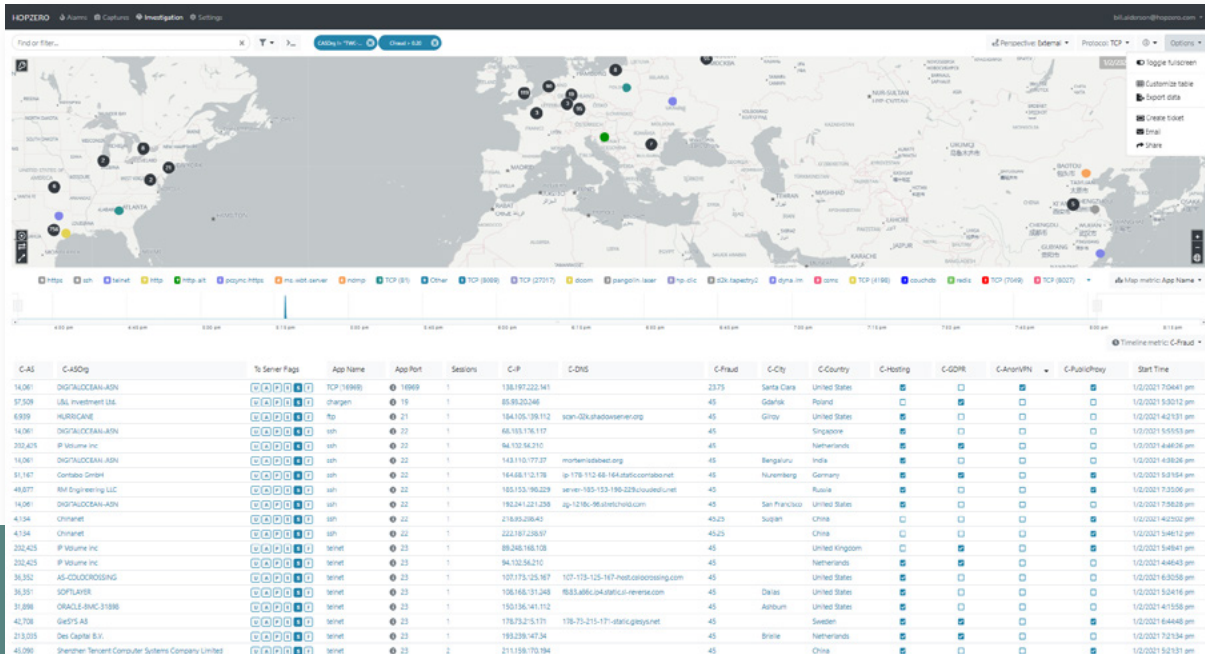
The 5 W's Who, What, When, Where, and Why in list format:

Figure 2 shows a large view of incoming session attempts from around the world on the map and below a listing of some of the 5 W's limited by this article's ability to display. Figure 1 provides a smaller view of similar outgoing vetting to the actual Microsoft server criminals used for exfiltration.

Interactive filtering by IPs, Application Ports, Fraud Score, or any combination by Boolean operators on labels "contains" or number range or values. Like high risk "scores > 20" and domains "containing Microsoft" and "China". The filtered list of session characteristics can contain "only good sessions with Data" or malformed session attempts without an "Ack". Export to CSV allows other tool ingestion like Splunk or another session risk assessment tool or report.

SECURITY INSTITUTE

Mission Critical Session Vetting Form

Client (Initiator) IP A	10.10.10.1 SolarWinds.local		Server (Responder) IP B	20.140.0.1 avsvmcloud.com	
Directional Priority	5W's Who	What	When	Where	Why
Incoming No					
Incoming Yes	Azure Hosted NOT SolarWinds Owned	80/443 Orion Improvement Program	Anytime 24x7	Boydton VA Microsoft Hosting	OIP FAIL TO VET Not SolarWinds Azure!

URL's *https://3mu76044hgf7shjf.appsync-api.eu-west-1.avsvmcloud.com /swip/upd/Orion.Wireless.xml
*https://3mu76044hgf7shjf.appsync-api.us-east-2.avsvmcloud.com /pki/crl/492-ca.crl
*https://3mu76044hgf7shjf.appsync-api.us-east-1.avsvmcloud.com/fonts/woff/6047-freefont-ExtraBold.woff2

Internal No					
External No					

Using a sortable, filterable list of session vetting provides fast Vetting of thousands of sessions to discover and exterminate criminals dwelling inside a network. Controlling capability through limiting how far data may travel will be discussed in Article 8. Limiting how far data may travel is accomplished by learning how far you want certain data to travel and then setting packet travel limits to prevent data exfiltration, alarming on denied session attempts.

SECURITY INSTITUTE

Part 7 _____

Who is responsible for the SolarWinds Breach

SECURITY INSTITUTE

Opinions about potential responsibilities and impacts.

With a breach this massive and complex, there are multiple points of failure. In this article, we will look at those points of failure at the various steps in the process of the breach and how the responsible parties (bolded below) may well have thwarted this attack using some of the same basic security fundamentals already discussed. Follow Figure 1 providing a numbered, color coded diagram of steps and potential faults that allowed the attack's success.

1. **SolarWinds allowed hacker code** to be inserted directly into the compile update files being prepared for customers.

   SolarWinds allowed criminal access to incoming Internet to place files, or coders was Phished to bring the files in to be placed. Incoming Internet allowed DLL file to get placed just as criminal desired.

2. **SolarWinds neglected to Vet files** to be compiled into a customer update.

   SolarWinds Failed to recognize rogue code file lacking appropriate File Controls

3. **SolarWinds placed update files containing Trojan** on Internet Update Server. Perhaps this process reversed by criminal inserted files on programmer computers. This process may have included an automatic update process. Direct Internet Automatic Updates might be dangerous to customers.

4. **Customer-Victim manually or automatically downloads update file** introducing Trojan into their network lacking proper vetting of updates prior to download directly to production systems.

5. **Criminal program code lays dormant for two weeks to avoid detection**. After two weeks, code starts by checking for Internet access. Without Internet access for exfiltration this attack cannot succeed.

6. **Customer -Victim allows internet access and Code** confirms reach to Internet api.SolarWinds.com

7. **Customer-Victim has no AntiVirus** in place that Criminal knew would detect this attack.

8. **Criminal code gathers information and credential**s for Exfiltration

9. **Customer-Victim failed to Vet external domain allowing SolarWinds**, a Vital Server unfettered Internet. Code exfiltrates to avmsvmcloud.com.

10. **Criminal Code on Microsoft Azure** server likely notifies criminals of a new victim.

11. **Customer -Victim has allowed criminal to have full control from Internet Criminals**. Criminals are able to create their own certificates enabling an Advanced Persistent Threat APT
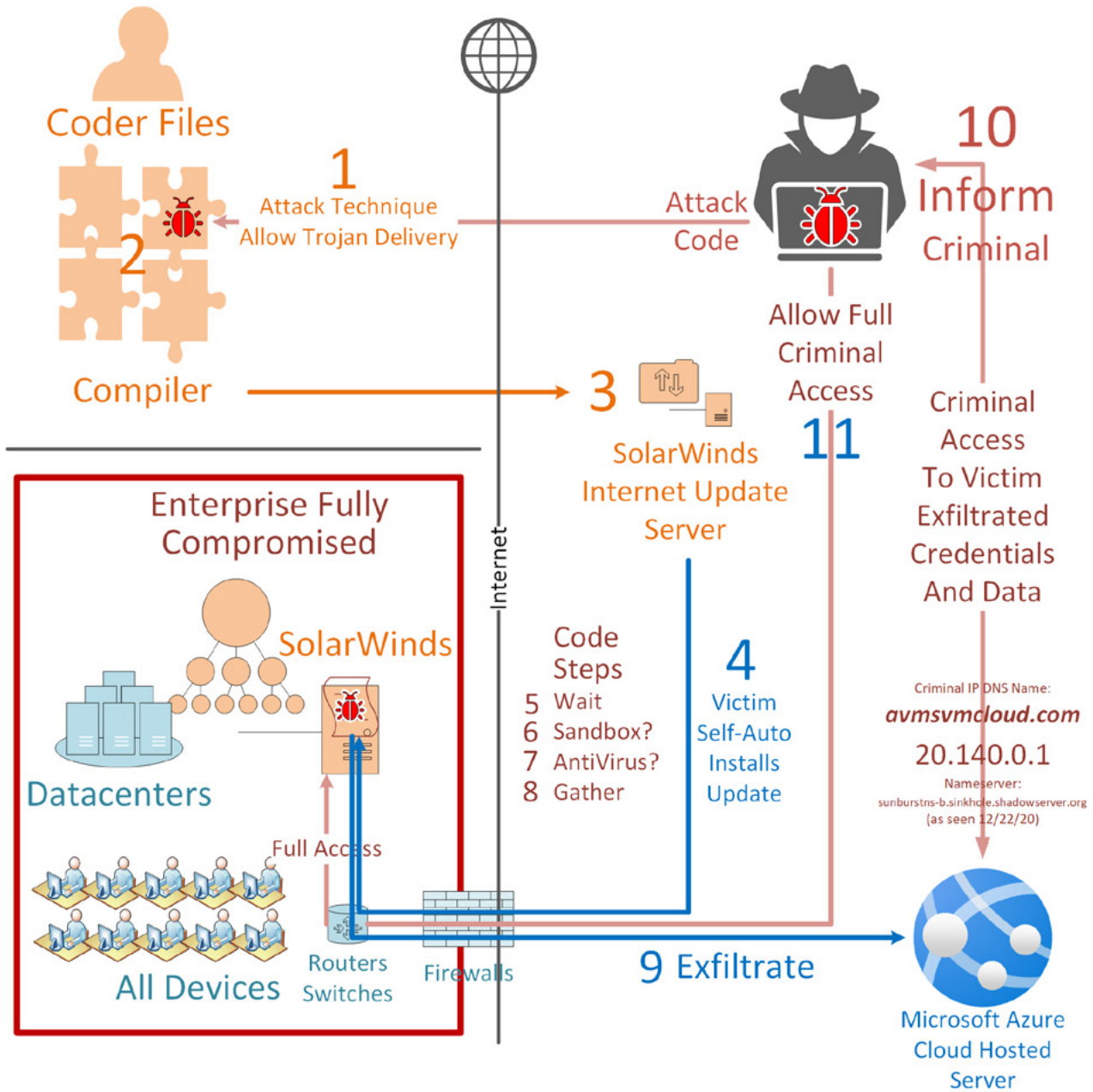
Fig 1 Numbered List of Evading Attack Steps

Step	Responsible Party	What Happened	Reason	Impact
1	SolarWinds	Inserted Dll code named: SolarWinds.Orion.Core.Businesslayer.dll	Failed to Vet Incoming	Criminals insert Trojan
2	SolarWinds	Dll considered valid compilation object into the update	Failed to Control Critical Files	Compiled DLL signed
3	SolarWinds	Dll is made available for Internet download	Available for Auto update	Update by Customer
4	Customer-Victim	Update push or pull to the SolarWinds Server through Internet access	Vital Server direct on Internet	Updates not vetted on Vital server
5	Criminal	Criminal	Avoid detection mechanisms	Dll Continues
6	Customer-Victim	Code test Internet access for backdoor capabilities sandbox detection	Trojan impotent without Internet Access	Internet access green lights the DLL
7	Admin	Checked for antivirus on host	Avoids AV Detection	Avoids Detection
8	SolarWinds Customer-Victim	Gathers information for exfiltration to awaiting criminals	No Isolation by SolarWinds or customer	Premises Internet and Cloud all compromised
9	Customer-Victim	Internet DNS address avsvmcloud.com making data available to criminals	No limits Direct Internet Server to non-SolarWinds domain.	Exfiltration of Vital Data
10	Customer-Victim	Criminals informed - enduring remote access compromise	Allows Outgoing Access to Bad Server	Places Vital Data on Bad Server
11	Customer-Victim	External criminals are enabled to conduct hands-on attack	Vital Server Direct on Internet	Extends Criminal Access

Fig 2 *table of Responsible Party reasons and impacts*

Figure 2 provides a table of Responsible Party reasons and impacts for consideration.

SolarWinds and their customers (victims) had several points at which some basic security practices may have stopped this attack or minimized its impact.

Bottom line, the United States government users of SolarWinds and the United States capitalist companies using solarwinds.com or SolarWinds code have been fully breached and do not even know what the hackers may or may not have planted as landmines in their infrastructure and are ill-equipped to find the fundamentals. Extreme bulk session vetting is for all these organizations to root out and find and identify and exterminate any current or future malicious code that begins trying to communicate out to the internet again. Using log files on computers to Vet the presence of Criminals may be thwarted by criminals deleting log entries of their activity. Recording session traffic at a network Tap or switch span offers a reliable, central place for thousands of device sessions to be collected and Extreme Vetted.

SECURITY INSTITUTE

Part 8

Preventing Data Breach Through DataTravel Limits

SECURITY INSTITUTE

DataTravel Limits – A New Vital Server Security Layer

After analyzing the SolarWinds breach, capturing actual packets to the very amsvmcloud.com, performing Directional Perspective and 5 W analysis, learning how and why it happened, the various points of failure and responsibility for each of those failures, we close this series with something completely new to consider. Evident from this, and many other news-worthy data breaches (not to mention the ones we never hear about because they are not considered important enough or classified) the current tools, methods and techniques of cyber security are failing.

In this article we will look at a new method of breach prevention using Data Travel Limits. With 40 years of network troubleshooting and packet analysis it was clear that a new approach based on basic security fundamentals was needed. Internet routers have been kept safe by limiting how far their packets may travel, ensuring only Adjacent routers can receive route updates. It is this same method that data travel security is based. Attempts to keep hackers out of networks and servers have failed again and again. It is time to protect Vital Data by keeping it from walking out the door. This is the quintessential message that has been put forth for four years finally resulting in Utility Patent US 10,673,881 B2 Granted June 2, 2020. Developed "for such a time as this".

The premise is simple. First you learn what distance your vital server is communicating to now. This can be accomplished through vetting of vital server communication sessions as shown in article four using visualization tools. Using this tool to identify a safe perimeter for data travel, you can utilize Data Travel Limits by setting the default HOP value to ensure that data does not go outside of that perimeter. Even if a bad actor breaches your firewall and tries to exfiltrate data, when the HOP decrements by one as traversing through each router reaches ZERO, the packet is discarded and never reaches the waiting criminal.

Using Data Travel tools to record all communication sessions on the wire, improving on individual security log collection requirements and creates an alarm that triggers any time data attempts to go beyond the established safe perimeter. Once an alarm points to a session, Microsoft NetMon exposes the executable code, malware, virus or Trojan trying to communicate beyond the established limit. Tools such as NetMon can be used to trace the session back to the originating IP for full vetting using the Who, What, When, Where, and Why to assess the appropriateness of the communication. This information, combined with the geo location of your RFC 1918 internal address gives you rapid means of assessing any exfiltration attempt, such as your SQL
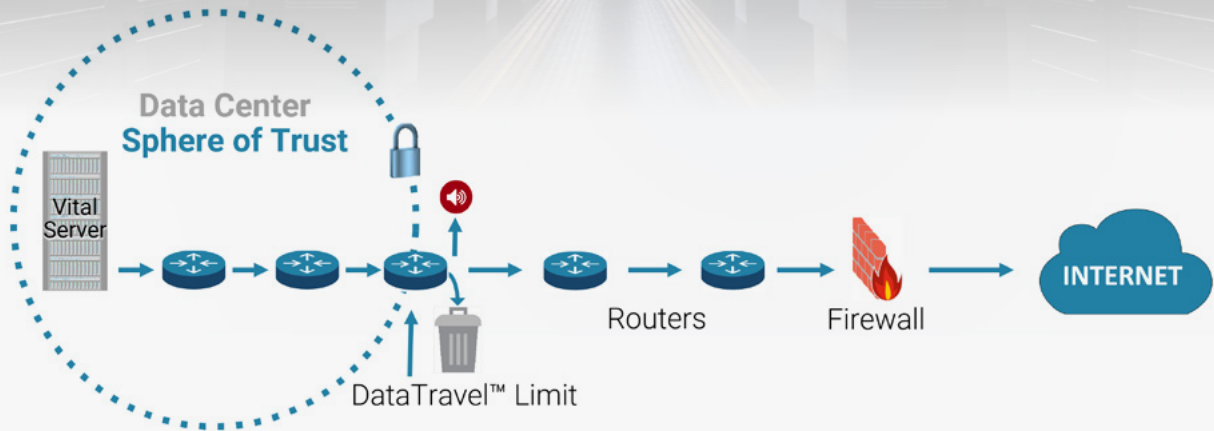
Security INSTITUTE

Fig 1 *How hop starvation keeps data inside a Sphere of Trust*

server attempting to send data to China or Russia, and allows you to catch the machine that has been phished in the process. This same method catches ransomware movement attempts between servers placed to encrypt your data and hold it hostage for ransom payment.

While it sounds very basic, the result is powerful. Data does not leave a Vital Server's appropriate Sphere of Trust, i.e., your data center or organization once Data Travel Limits are in place. Following these steps, to learn the distance metric, apply Travel Distance Limits, and vet sessions by alarms, keeping your Vital Server data safe and allow you to catch those attempting exfiltration. Pretty simple, patented, and ready to Vet vital communication

sessions, stop data compromise, uncover and eradicate hackers dwelling in your environment.

When an organization finds itself in crisis due to a breach, an immediate capture of packet headers without data can be taken to investigate and map device location on the Internet and internal RFC 1918 addresses by Extreme Vetting to exterminate hands-on criminals and Trojan malware and virus code dwelling inside your servers and network. Figures 1 shows how hop starvation keeps data inside a Sphere of Trust and Figure 2 illustrates how Phish and Ransomware are caught when setting distance limits on vital servers. Figure 3 lists the simple steps to Record, Vet and Prevent Data Compromise.
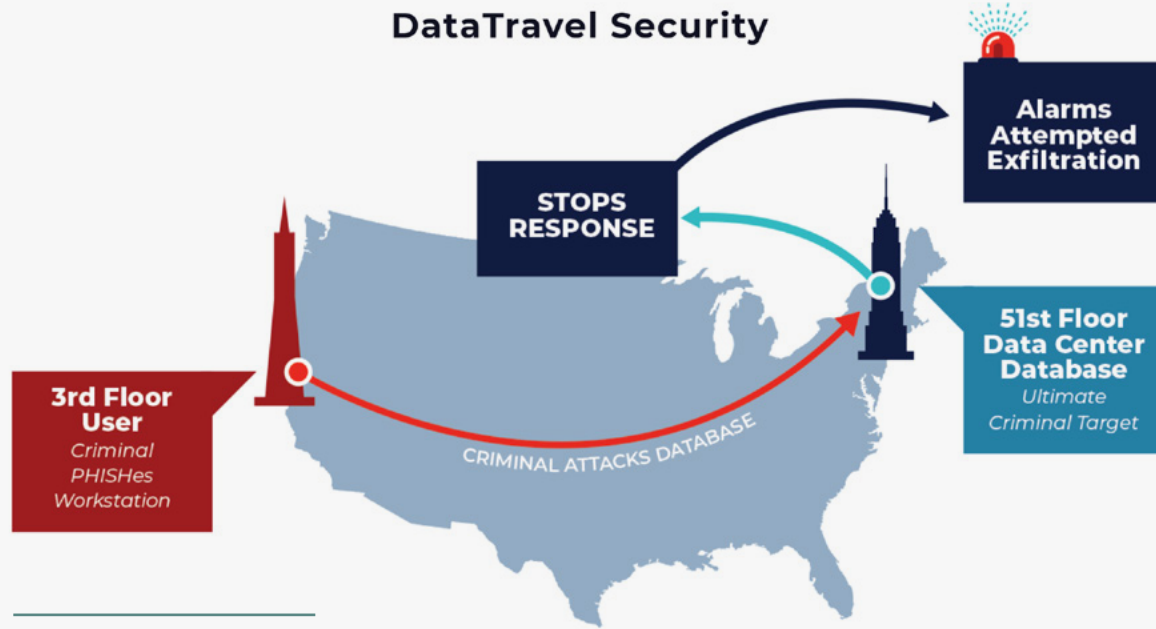
DataTravel Security

Alarms Attempted Exfiltration

STOPS RESPONSE

3rd Floor User
Criminal PHISHes Workstation

51st Floor Data Center Database
Ultimate Criminal Target

CRIMINAL ATTACKS DATABASE

Fig 2 *How Phish and Ransomware are caught*

DataTravel Limit Technology Steps

1	Learn Distance Metrics
2	Apply Distance Limit
3	Monitor Communication Sessions
4	Alarm on Attempts to Escape Safe Perimeter
5	Catch Phish and Ransomware
5	Exterminate Dwelling Criminals

Fig 3 *Lists the simple steps to Record, Vet and Prevent Data Compromise*

SECURITY
INSTITUTE

SolarWinds Breach

December 2020

Author

Bill Alderson solved security denial of service attacks against the US Stock market, led the team bringing back online the Pentagon at 9/11, solved numerous network meltdowns affecting F-500 companies, optimized biometric Intelligence applications, deploying with US military to Iraq and Afghanistan 6 times, certified 3,500 vendor-independent Network Forensic Security Professionals. Forty years' experience analyzing network packets, securing US government and American corporations provides the background to offer this analysis.

SecurityInstitute.com/SolarWinds

Inquire@SecurityInstitute.com

11400 Concordia University Dr, Austin, TX 78726