SECURITY INSTITUTE

SolarWinds Breach

December 2020

SolarWinds Eight-Part Security Series
By: Bill Alderson

PART 1/8

Part 1

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

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.

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.

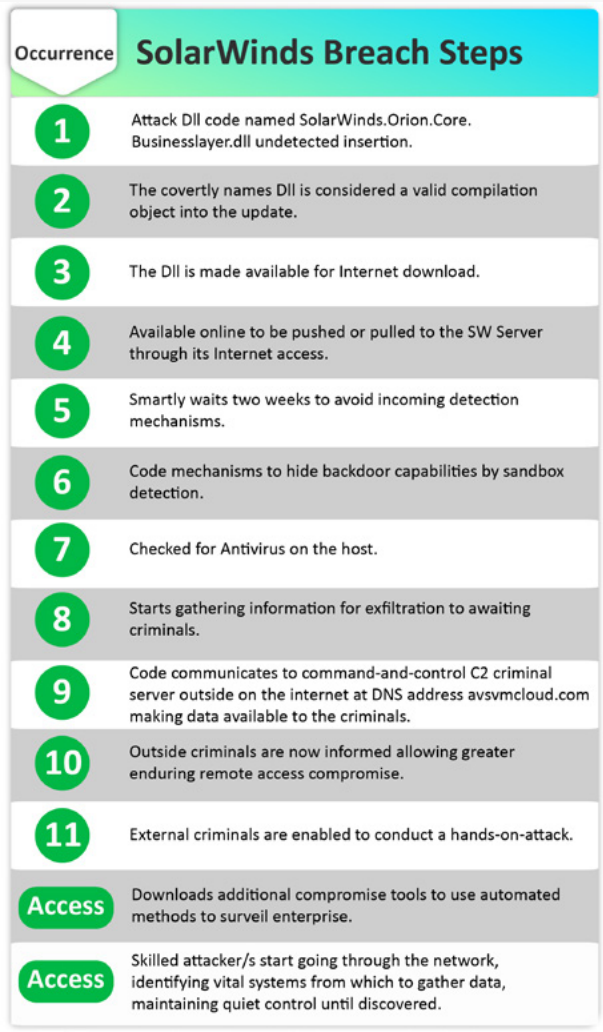

Fig 1 Diagram Depicting Eleven Breach Steps

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.

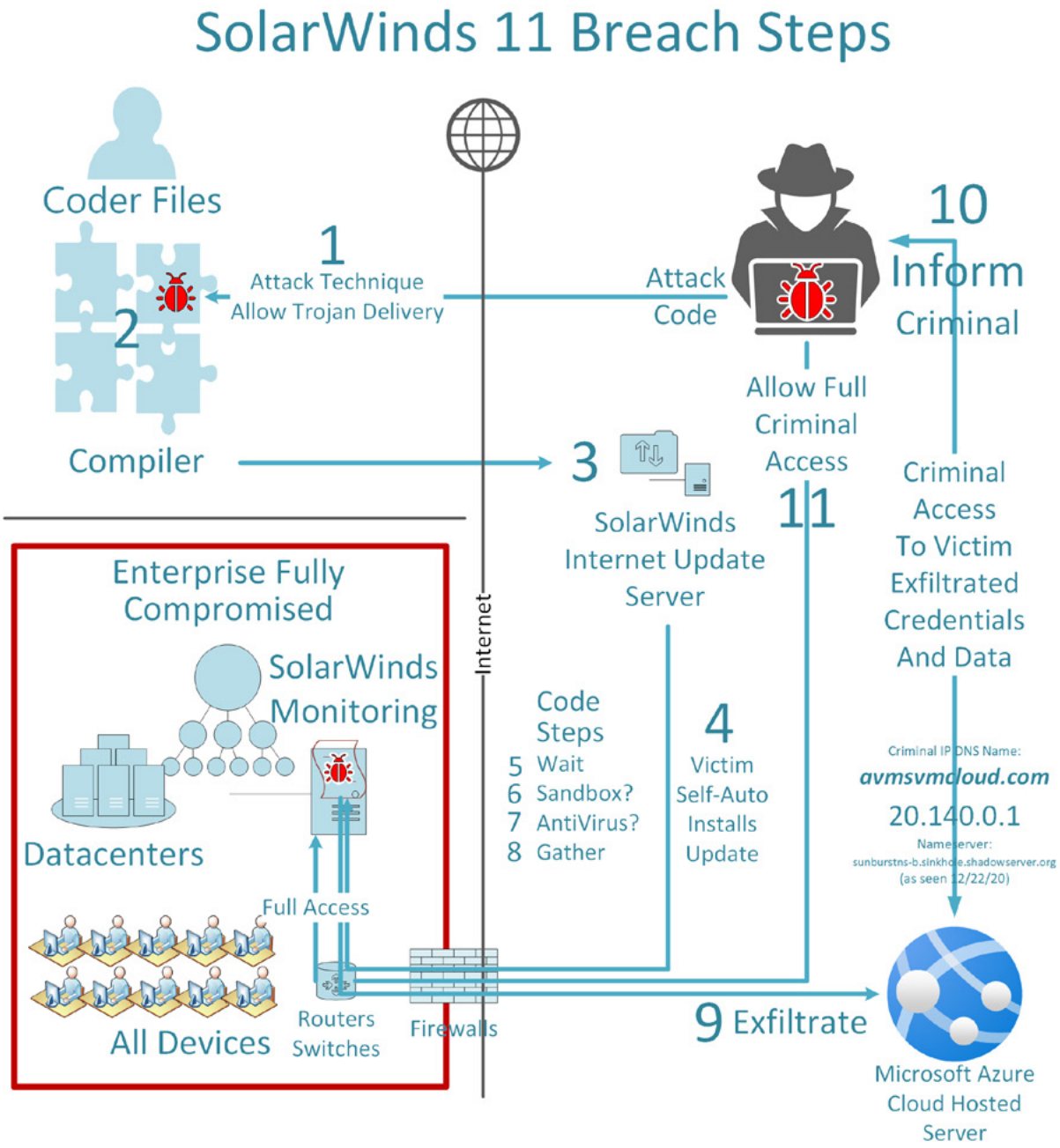

Fig 2 Numbered List of Evading Attack Steps

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.

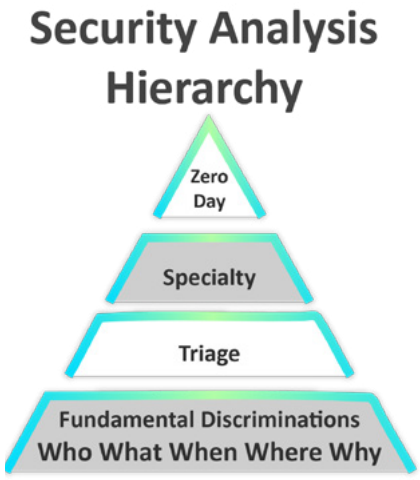

Fig 3 Hierarchical Security Priority Pyramid

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.

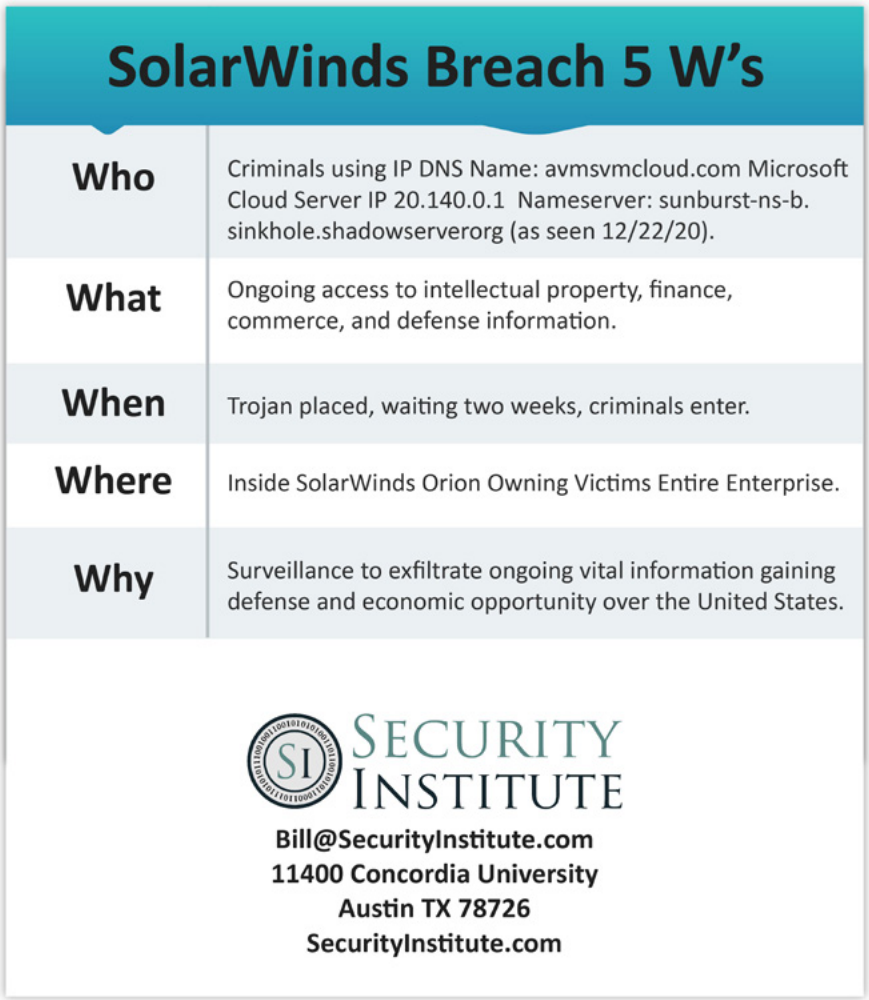

Fig 4

Who What When Where Why Findings

SECURITY INSTITUTE

SolarWinds Breach

December 2020

SolarWinds Breach Eight-Part Series

1. **Anatomy of a Massive Breach**
2. Vital Server Direct Internet Updates
3. Four Communications Perspectives of a Vital Server
4. Basic 5 W Vetting of Vital Server Communications
5. Software Improvement Program – An Inside Job?
6. Vetting and Exterminating Entrenched Criminals
7. Opinion: Breach Diagram - Color Indicating Responsible Party
8. Preventing Data Breach Through DataTravel Limits

The full analysis is available at the Socurity Institute.
CLICK HERE TO DOWNLOAD

SecurityInstitute.com/SolarWinds

Inquire@SecurityInstitute.com
11400 Concordia University Dr,
Austin, TX 78726