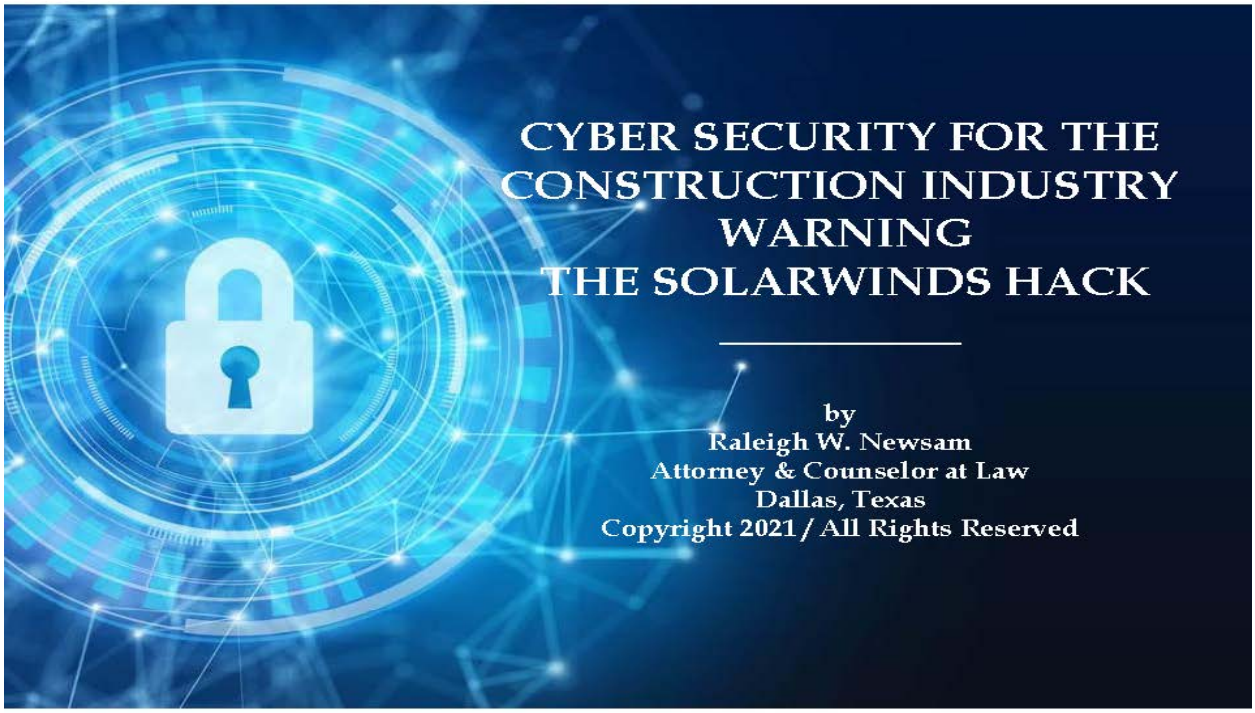

The SolarWinds Hack Is A Massive Cyber Breach — Trust, But Verify

"**Trust, But Verify**," in Russian, "***Doveryay, No Proveryay***" was the phrase used by President Ronald Reagan many times in his negotiations with Soviet General Secretary Mikhail Gorbachev between 1984 and 1987. President Reagan learned the phrase from one of his advisors, Suzanne Massie, an American scholar of Russian history. She taught President Reagan the phrase, a Russian proverb, advising him that "the Russians like to talk in proverbs." President Reagan quickly adopted the phrase as his own, and used it frequently in his negotiations with the Soviets over the Intermediate-Range Nuclear Forces (INF) Treaty.

The SolarWinds Hack — Cyber Attack and Cyber Espionage

President Reagan's use of the Russian proverb "Trust, But Verify," provides a useful jumping off place to discuss what has become known as the SolarWinds cyber attack. From what we now know, the United States has suffered a massive Russian cyber attack or, as others have characterized it, Russian cyber espionage. Either way, the cyber attack and/or cyber espionage likely originated from Russia, one of the four major state sponsors of cyber terrorism. According to the latest information available, the cyber attack began sometime before March 2020. Initial indications are that hackers employed by the Russian SVR — formerly known as the KGB — launched the attack by hacking into SolarWinds via a backdoor into an Orion software update. The likely culprit is the Russian government group APT29, also known as Cozy Bear.

The SolarWinds Hack — Supply-Chain Attack

Which begs the question: What is SolarWinds and why does this matter? SolarWinds is an American company that has developed software applications that helps businesses manage their networks, and information technology systems. Its Orion product is currently used by over 300,000 public and private sector customers worldwide. The cyber event is called a supply-chain attack because it has targeted a supplier to businesses rather than the businesses itself. In that way, a supply-chain attack is a more effective weapon because it targets hundreds or thousands of end users or customers. Much like a multiple independently targetable reentry vehicle, or MIRV

ballistic missile, a supply-chain attack is capable of hitting many different targets from the same hack. In effect, the cyber terrorists transformed a routine software update from a reputable and trustworthy company into a MIRV ballistic missile.

The SolarWinds Hack— The Targets, The Damage, The Recovery Cost

According to SolarWinds, its customers include more than 425 of the Fortune 500 companies, the White House, all five branches of the U.S. military, the State Department, the Pentagon, the Commerce Department, the Justice Department, the Treasury Department, the top five U.S. accounting firms, the top ten U.S. telecommunication companies, and hundreds of universities and colleges. In its SEC filing, SolarWinds claimed that "fewer than 18,000" of its customers installed the malicious update. As one observer noted, that's another way of saying more than 17,000 did.

The SolarWinds hack was an attack against the critical cyber infrastructure of the United States. Functioning critical infrastructure industries are essential for the security of our country. These industries include telecommunications, energy, financial, food and agriculture, manufacturing, transportation, and yes, construction. As we've learned during the Covid-19 pandemic, each of these critical infrastructure sectors are essential to a resilient economy.

Although the extent of the SolarWinds is still not fully understood, initial estimates put the recovery cost at roughly $100 billion. The government agencies and businesses will likely spend that amount or possibly more to contain and repair the damage from the SolarWinds hack. Finding and eliminating or compartmentalizing the advanced persistent threat

The SolarWinds Hack — Four Malware Strains and Counting

As of January 19, 2021, cyber security firm Symantec had identified a fourth malware strain that was deployed during the SolarWinds supply chain attack. So far, the four are Sunspot, Sunburst, Teardrop, and now Raindrop. There may be more to come, a few more or many more.

The Solar Winds Hack — Why Should Construction Firms Be Concerned?

Because the SolarWinds hack is a Supply-Chain Attack, we still do not know the total number of companies and government agencies affected. With upwards of 18,000 companies that may have downloaded the trojan, the likelihood that construction industry firms may have been downstream or second-order victims is more likely than not. What steps should construction industry firms take to protect themselves against possible attack vectors posed by the SolarWinds hack?

- ***Detection, Response and Containment — Execute an Effective Incidence Response Plan***. Do not rely on finding Indicators of Compromise (IOCs). IOCs may or may not be present. There's a good chance any virus may have become dormant. All construction industry firms should assume they've been compromised. As discussed in the attached COVID-19 Alert 2, implementing all 4 Steps of an Incidence Response Plan should be repeated on a regular basis to detect and, if necessary to respond to a cyber attack.
- ***Compartmentalize***: All IT systems running SolarWinds should be compartmentalized and, if necessary, quarantined until the full scope of the SolarWinds attack is better understood.
- ***Install Updated Orion Version***: All SolarWinds customers should immediately install the updated version of Orion that removes the backdoor code and changes the credentials for all users.
- ***Tracking the Advanced Persistent Threat of the SolarWinds Supply-Chain Attack (APT29)***: The Cybersecurity and Infrastructure Security Agency (CISA) has established a webpage for tracking the APT cyber activity - see CISA Alert (AA20-352A) https://us-cert.cisa.gov/ncas/alerts/aa20-352a with technical details for mitigating the cyber attack.
- ***Tactics, Techniques and Procedures —Trust, But Verify***: All construction industry firms must become more vigilant in managing supply-chain risk. The risk mitigation strategy must now incorporate vigorous controls with all third-party vendors, even those considered trustworthy and reliable. Companies can no longer trust anyone, even their security vendor.

To recap, this was a Supply-Chain Attack. And the attack vectors and list of victims has continued to grow. Technology vendors including Microsoft, Intel, Nvidia, VMare, Belkin, and the cyber security firm FireEye, likely allowed the compromised SolarWinds Orion update inside their perimeter defenses. According to cyber security firm TrueSec, IT powerhouse Cisco and accounting giant Deloitte were likely infected by the SolarWinds Orion update. According to cyber security firm Prevasio, telecommunications mega-firm Ciena, software and professional services NCR, German multinational software firm SAP, the world's largest semiconductor chip manufacturer, Intel, and software development firm Digital Sense, are on the list of organizations which may have downloaded the infected trojan. Hospitals, financial institutions, power companies, educational institutions, and local governments are on the list. Federal government agencies victims include the Departments of State, Defense, Commerce, Energy, Homeland Security, and the Treasury.

The SolarWinds hack is not a one-off event. From this point forward, we will do business in a rapidly evolving and far more dangerous cyber landscape. All organizations will now have to confront a new reality of cyber threats and cyber risks. More state sponsors of cyber terrorism will follow in the footsteps of APT29. ***Trust, But Verify***.