The Sunburst hack was massive and devastating – 5 observations from a cybersecurity expert

December 30 2020, by Paulo Shakarian

Some of the exposed organizations, like Microsoft, made limited use of the SolarWinds software, which appears to have contained the damage they suffered. Credit: Raimond Spekking, CC BY-SA

So much remains unknown about what is now being called the Sunburst hack, the cyberattack against U.S. government agencies and

corporations. U.S. officials widely believe that Russian state-sponsored hackers are responsible.

The attack gave the perpetrators access to numerous key American business and government organizations. The immediate effects will be difficult to judge, and a complete accounting of the damage is unlikely. However, the nature of the affected organizations alone makes it clear that this is perhaps the most consequential cyberattack against the U.S. to date.

An act of cyberwar is usually not like a bomb, which causes immediate, well-understood damage. Rather, it is more like a cancer—it's slow to detect, difficult to eradicate, and it causes ongoing and significant damage over a long period of time. Here are five points that cybersecurity experts—the oncologists in the cancer analogy—can make with what's known so far.

1. The victims were tough nuts to crack

From top-tier cybersecurity firm FireEye to the U.S. Treasury, Microsoft, Intel and many other organizations, the victims of the attack are for the most part firms with comprehensive cybersecurity practices. The list of organizations that use the compromised software includes firms like MasterCard, Lockheed Martin and PricewaterhouseCoopers. SolarWinds estimates about 18,000 firms were affected.

As CEO of cybersecurity firm Cyber Reconnaissance Inc. and an associate professor of computer science at Arizona State University, I have met security professionals from many of the targeted organizations. Many of the organizations have world-class cybersecurity teams. These are some of the hardest targets to hit in corporate America. The victims of Sunburst were specifically targeted, likely with a primary focus on intelligence gathering.

2. This was almost certainly the work of a nation—not criminals

Criminal hackers focus on near-term financial gain. They use techniques like ransomware to extort money from their victims, steal financial information, and harvest computing resources for activities like sending spam emails or mining for cryptocurrency.

Criminal hackers exploit well-known security vulnerabilities that, had the victims been more thorough in their security, could have been prevented. The hackers typically target organizations with weaker security, like health care systems, universities and municipal governments. University networks are notoriously decentralized, difficult to secure, and often underfund cybersecurity. Medical systems tend to use specialty medical devices that run older, vulnerable software that is difficult to upgrade.

Hackers associated with national governments, on the other hand, have entirely different motives. They look for long-term access to critical infrastructure, gather intelligence and develop the means to disable certain industries. They also steal intellectual property—especially intellectual property that is expensive to develop in fields like high technology, medicine, defense and agriculture.

The sheer amount of effort to infiltrate one of the Sunburst victim firms is also a telling sign that this was not a mere criminal hack. For example, a firm like FireEye is an inherently bad target for a criminal attacker. It has fewer than 4,000 employees yet has computer security on par with the world's top defense and financial businesses.

3. The attack exploited trusted third-party software

The hackers gained access by slipping their malware into software updates of SolarWinds' Orion software, which is widely used to manage large organizational networks. The Sunburst attack relied on a trusted relationship between the targeted organization and SolarWinds. When users of Orion updated their systems in the spring of 2020, they unwittingly invited a Trojan horse into their computer networks.

Aside from a report about lax security at SolarWinds, very little is known about how the hackers gained initial access to SolarWinds. However, the Russians have used the tactic of compromising a third-party software update process before, in 2017. This was during the infamous NotPetya attack, which was considered the most financially damaging cyberattack in history.

4. The extent of the damage is unknown

It will take time to uncover the extent of the damage. The investigation is complicated because the attackers gained access to most of the victims in the spring of 2020, which gave the hackers time to expand and hide their access and control of the victims' systems. For example, some experts believe that a vulnerability in VMWare, software that is widely used in corporate networks, was also used to gain access to the victims' systems, though the company denies it.

I expect the damage to be spread unevenly among the victims. This will depend on various factors such as how extensively the organization used the SolarWinds software, how segmented its networks are, and the nature of their software maintenance cycle. For example, Microsoft reportedly had limited deployments of Orion, so the attack had limited impact on their systems.

In contrast, the bounty the hackers stole from FireEye included penetration testing tools, which were used to test the defenses of high-

end FireEye clients. The theft of these tools was likely prized by hackers to both increase their capabilities in future attacks as well as gain insights into what FireEye clients are protecting against.

5. The fallout could include real-world harm

There is a very thin, often nonexistent line between gathering information and causing real-world harm. What may start as spying or espionage can easily escalate into warfare.

The presence of malware on a computer system that gives the attacker greater user privileges is dangerous. Hackers can use control of a computer system to destroy computer systems, as was the case in the Iranian cyberattacks against Saudi Aramco in 2012, and harm physical infrastructure, as was the case Stuxnet attack against Iranian nuclear facilities in 2010.

Further, real harm can be done to individuals with information alone. For example, the Chinese breach of Equifax in 2017 has put detailed financial and personal information about millions of Americans in the hands of one of the U.S.'s greatest strategic competitors.

No one knows the full extent of the Sunburst attack, but the scope is large and the victims represent important pillars of the U.S. government, economy and critical infrastructure. Information stolen from those systems and malware the hackers have likely left on them can be used for follow-on attacks. I believe it is likely that the Sunburst attack will result in harm to Americans.

Provided by The Conversation