Orange
Cyberdefense

Winds of change

Underlying causes and implications of the SolarWinds attack

Table of Contents

Introduction: SolarWinds was inevitable

Chasing the storm

The SolarWinds incident is set to dominate the cybersecurity weather for many months to come. Indeed, it will likely be remembered as a pivotal moment in the short history of our industry. The typhoon that everyone will remember. Much of the discussion will focus on what the perpetrators did, and what the victims did not do. Many suggestions for improvement will be made, and hopefully many significant changes will result .

SolarWinds did not come out of the blue, however, and should not be regarded as such. SolarWinds is the inevitable consequence of a powerful set of systemic factors that collectively produce a climate that is inherently volatile but can still be predicted. While forecasts for a specific day may fail, the general tendency is driven by known forces and systems.

This volatile context currently strongly favours the attacker over the defender. That is not going to change unless the systemic drivers that create it are dealt with. In this case that means confronting and addressing some factors (like a massive investment by governments into computer hacking capabilities) and accepting and adapting to others (like the strong ties of interdependence that lie at the heart of cyberspace, the business ecosystem and indeed society in general).

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Co-author: Wicus Ross
Senior Security Researcher
Orange Cyberdefense

Be prepared for nasty weather

As in our battle with climate change, addressing these systemic factors is bound to be a slow and difficult process, which leaves us to deal with the daily reality of poorly built systems, growing security debt, a cunning and motivated adversary and a never-ending series of new vulnerabilities, threats and general shifts in the landscape.

Resilience in the face of such a volatile environment requires us to achieve a tenuous balance between agility and consistency. We must be able to rapidly detect, understand and respond to relevant changes in our space, but to do so repeatedly and consistently via institutionalised processes that nevertheless do not themselves become impediments to speed or responsiveness.

This goal is captured in the notion of intelligence-led security. Mimicking the process pioneered by the US Airforce military strategist John Boyd, we seek to continuously Observe, Orient, Decide and Act (OODA[1]) more quickly and reliably than our adversary.

Background

We published our first security bulletin on the so-called SolarWinds attack on 14 December. The SolarWinds Orion Platform is a unified system to monitor, analyse and manage IT infrastructure remotely.

This software is used by a wide variety of companies, including prominent US Telco's, banks, and major US government institutions.

Attackers, dubbed UNC2452 by FireEye, managed to breach SolarWinds sometime around September 2019[2]. They cleverly managed to insert a backdoor, labelled SUNBURST, into the SolarWinds Orion Platform software via the dynamic software build process, thereby infecting several versions of the software that were made available to SolarWinds customers via official, digitally signed, updates. According to CrowdStrike[3], who are investigating the breach, this was achieved by a specific malware component dubbed 'SUNSPOT'.

SUNSPOT is the malware used to insert the SUNBURST backdoor into software builds of the SolarWinds Orion product. It monitors running processes for those involved in compilation of the Orion product and replaces one of the source files to include the SUNBURST backdoor code.

A third malware payload is called 'Teardrop' [4]. This is employed during post exploitation and is delivered by Sunburst. Teardrop is used to drop a Cobalt Strike Beacon, which allows it to communicate to the common commercial Command and Control system of the same name. It was not known at the time how SolarWinds themselves were breached, and details have not yet emerged at this time.

The Sunburst backdoor is sophisticated in that it hides in a trusted component that is signed with a legitimate SolarWinds code signing certificate. The backdoor resides in a trusted process that is used for IT system administration, thus blending in nicely. SUNBURST will remain dormant on initial infection anywhere between 12 to 14 days before it starts its activities.

The attackers use SUNBURST for initial access with the intent to steal credentials and to gain secure remote access to the compromised environment. The attackers used remote secure access with the stolen credentials to propagate through the network.

The SUNBURST backdoor, which uses steganography to hide any communication, can temporarily replace legitimate utilities with malicious versions, use a domain generated algorithm (DGA) for the C2 hostnames they wish to contact and can detect the presence of anti-malware that will cause it to become dormant or stop any activity when it detects these "blocklist" items.

Other vectors (apart from the software backdoor) may also have been used by the attackers and are currently being investigated.

The SolarWinds story has been unfolding continuously since it first broke, with several high-profile government agencies and corporations (including Microsoft) confirming that they were breached via the backdoor in the SolarWinds software.

Victims so far include the US Treasury, and the US NTIA, the US Department of Energy and the US nuclear weapons agency.

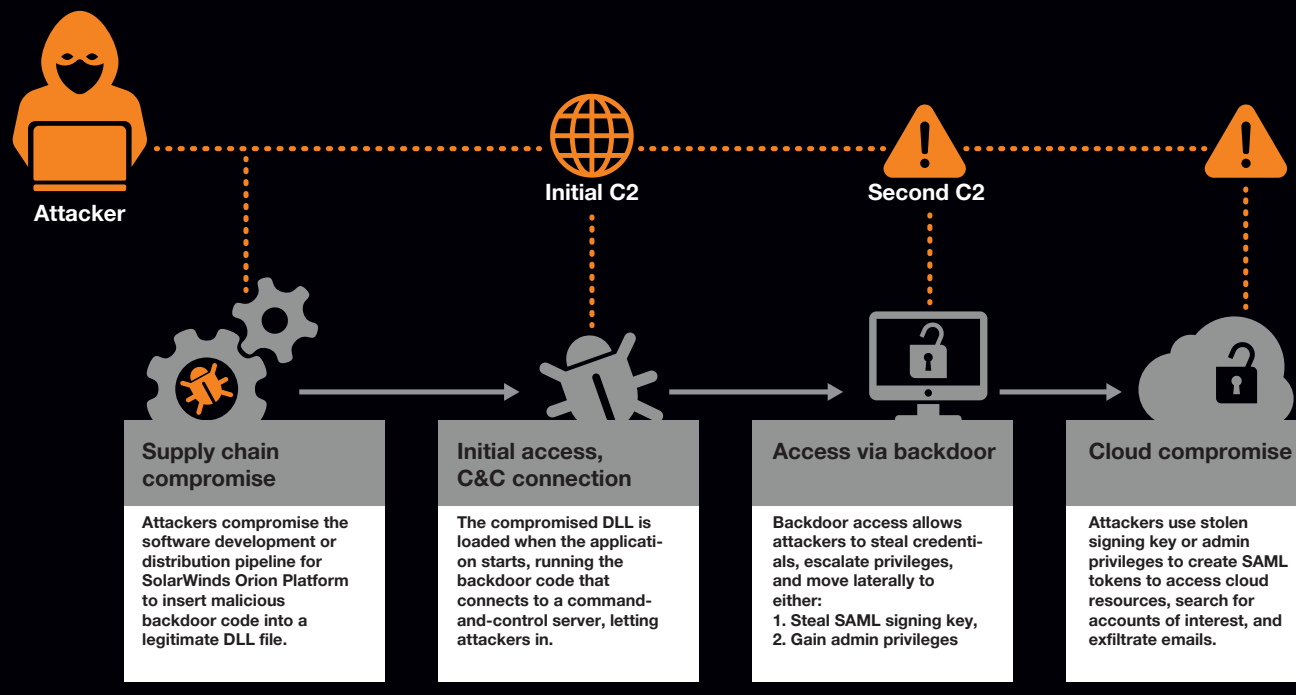
Microsoft was also a victim and has revealed additional details regarding the attack it suffered. The company reported that it detected unusual activity with a small number of accounts. Further investigations made it clear that attackers used these accounts to view source code in several source code repositories. According to Microsoft, no code was altered as the accounts had only read-only privileges.

Microsoft maintains that the attackers viewing source code doesn't mean elevation of risk because its threat model assumes that attackers have knowledge of the source code. Microsoft has not disclosed which of its products were affected or for how long hackers were inside its network.

In an unrelated incident, which we reported on December 31st, attackers, believed to be separate from the supply chain attack first announced by FireEye, managed to exploit a vulnerability in SolarWinds Orion to install a web shell. The governments of Mongolia and Vietnam also suffered supply chain attacks. These were unrelated to the SolarWinds supply chain attack.

Solorigate attack

High-level sophisticated supply chain compromise



Impact

As many as 18,000 businesses and government agencies were potentially impacted via SolarWinds. Though the actual number will be much smaller than that, it is now believed to have affected upward of 250 federal agencies and businesses[5]. In data published by Microsoft they report that, from a list of 40 of their customers who were impacted by the attack, only a small proportion were government agencies, and almost half were private IT-related businesses[6]. Indeed, the SolarWinds attack has been described as one of the most catastrophic cybersecurity incidents in recent history[7].

Various government and private-sector analysts have attributed this attack to a Russian Foreign Intelligence Services known as SVR. This allegation is widely supported and appears to have merit but cannot be confirmed at this time.

One shouldn't use the word 'unprecedented' blithely, but as the details of this incident unfold, and scope and scale become apparent, we can honestly claim that this SolarWinds represents another definitive 'turning point' in the young history of cybersecurity. It's not our intention to deliberate on the political and financial implications of the attack on its numerous and various victims here. There are other voices more qualified to do so than us. Instead, we want to draw your attention to a less apparent, but nonetheless critical couple of victims of this attack – integrity and trust.

A threat to Integrity

As many in the cybersecurity space will know, the widely accepted "CIA" security model consists of confidentiality, integrity and availability. Confidentiality here is linked to the threat of data theft, while availability could be seen in context of the DDoS and ransomware attacks increasingly submerging IT teams around the world. Integrity hasn't quite had the same press as the first two concepts, yet it plays a vital role in any effective security strategy and is increasingly the goal of nation-on-nation cyber-attacks. It therefore warrants some consideration in this context.

It is widely believed that as early as 2009[8], nation state-backed hackers developed the Stuxnet[9] worm with the goal of slowing disrupting and down Iran's nuclear programme.

It was done by targeting not just the centrifuges at the Natanz facility but also the telemetry systems used by engineers to manage and troubleshoot systems. By infecting the integrity of the telemetry systems, the attackers made it incredibly difficult to determine the root cause of the problem.

The exploitation of vulnerabilities in the supply chain could have even more severe repercussions.

A report Chatham House published in 2018[10] claimed that cyber-attacks on nuclear systems could undermine integrity, "leading to increased uncertainty in decision-making" and potentially even the inadvertent use of nuclear weapons. If the likes of US government leaker Daniel Ellsberg[11] are to be believed, even the slightest failure of integrity of nuclear weapons control systems could and probably would have genuinely catastrophic consequences for the entire planet, making this a risk that cannot be ignored, no matter how improbable we may consider it to be.

Integrity is hinged on credible, accurate, and trustworthy information and systems. If you damage that, you create significant problems. Attacks on the integrity in cyberspace often support the policy and political agendas cyber campaigns seek to achieve. The US and Israel found a way to do it at Natanz, and it's one of the significant impacts of the SolarWinds attacks.

As the list of victims grows, and fears of additional vulnerabilities, supply chain paths and attack vectors emerge, the US government (and much of the private sector) will at this stage be sucked into a paralysing vortex of fear, uncertainty and doubt (FUD). Given the success of the known aspects of the attack, and its longevity and persistence despite a heightened level of awareness over the 2020 US election period, no US government agency or commercial SolarWinds customer will at this time feel any confidence that they have escaped the hackers' reach. As one cannot prove a 'negative' (that they have not been hacked) decision makers are forced to accept that they have been compromised or face living with the uncertainty indefinitely. The only real choice, which was the only real choice presented to the engineers at Natanz, is to burn everything down and start again.

Oh, that we were a fly on the wall in the rooms where these decisions are being made. We're not, and we don't have the information these decision makers may have access to, but the 'contagious' effect of an attack on integrity can be clearly seen. It doesn't matter whether a given government agency or SolarWinds customer have discovered indicators of attack. The very fact of their 'interconnectedness' with SolarWinds or with the other agencies that have been attacked is enough to sow the seeds of doubt and force down the same damaging set of decisions being faced by the known victims.

Integrity is concerned with ensuring that information and systems are credible, accurate and trustworthy. Without it, you have a problem.

Some are arguing that the SolarWinds attacks are more of an 'intelligence' operation then 'warfare' operations and therefore should get classified amongst the myriad of such operations that are standard fair for governments on all sides; thus don't really warrant any kind of specific response.

The victim is Trust

This is an oversimplification, however. Regardless the motivation of the attackers, or the direct or indirect benefits accrued to them by the attack, the real victim breaches like this… is Trust.

Trust is the product of resilience, which in turn is the result of an effective and consistent implementation of the CIA triad. When we fail at any element of the CIA triad, and thus fail to assure the resilience of our information systems, there is a breach of trust.

Trust is not just the philosophical goal of information security; it is the concrete and essential infrastructure that any free and prosperous society requires to operate.

Trust in healthy societies defines the relationships between peoples and their governments, allows us to race down motorways at dangerous speeds and enables banks to profit by holding our hard-earned savings for us. Without trust, nothing works. Information systems are no exception; businesses and people need to believe that they can trust the technologies and systems they depend on. Without such trust, information technology would be effectively useless to us and modern society as we know it would collapse.

(Mis)trust is contagious

To explore the real impact of a cybersecurity failure like SolarWinds, we introduce the idea of risk 'contagion'[12]: a situation where a shock in an economy or region spreads out and affects others.

Consider a hypothetical scenario from the automotive industry.

Let's say a car is in an accident. It could be because of driver error, a mechanical failure, or just plain bad luck. There is loss, but the drivers knew the risk and (though the impact to the driver may be devastating) the impact of that accident on the transport network, business, the economy or society overall is negligible.

Now let's say a few cars across the country are in independent accidents. At first those accidents seem unrelated. Accidents happen all the time after all. But then we learn that the cars involved in those accidents all had something in common: The accidents were caused by a weakness in the cars' chassis, which caused a failure. In our hypothetical example, steel manufacturers haven't been monitored closely enough, which lead to shortcuts in production and weaker steel, resulting in a weaker vehicle chassis and eventually an accident. The incidents aren't independent; they're related. However, it gets worse, because this realisation creates a contagion effect. As the problem was in the steel, it becomes very hard to objectively isolate the problem or its impact. There may be a dozen or more vehicle manufacturers using this particular steel producer for any number of years.

This makes it incredibly difficult to determine how many cars have been affected, or which models need to be recalled. Cars have been sold and resold, so the individual owners are hard to reach, and their vehicles are hard to track down.

People will become nervous to drive potentially affected cars so car sales slow - almost to a standstill - across multiple manufacturers. Enormous amounts of money are spent on the investigations and recall process and there are fines and penalties, civil and class-action lawsuits.

Car sales grind to a halt.

Eventually it emerges that some of the quality controls had become lax and worse - that managers and board members potentially knew that there might have been problems and ignored them. Investors sense trouble in the auto industry and start dropping shares in a fire sale, not just for specific manufactures but for all of them, and the business that support them. Workers are let go as factories and sales grind to a halt, effecting entire sectors of the economy across the world, even causing recession in certain regions and countries.

Investors can't see where the contagion will stop, whether it be manufacturing, materials, insurance, financial institutions, or beyond. Taking no chances, they rush to get out of the markets, selling shares for whatever they can get and causing the markets to collapse even further. More businesses fail, more jobs are lost, economies shrink even further.

Eventually, in this hypothetical example, we find ourselves in a global recession that costs the economy billions and takes decades to recover from.

Information malaise

It all sounds a bit dramatic, but there's a powerful real-world example of contagion in action in the 2008 global financial crisis, where the risk was shared across many businesses in a way that ultimately impacted a wide range of sectors. When the housing bubble burst, it created a 'contagion effect' that brought the entire system crashing down[13].

When considering the impact of the SolarWinds attack the question we face is whether we are dealing with an incident that is unfortunate, but limited in its broader impact, or whether is the potential for a contagion. If so, what is the potential impact on us?

In 2014 the Centre for Risk Studies at Cambridge University ran a study[14], in which they developed a detailed risk scenario describing a slow burning cyberattack on a fictional software developer that has global consequences. The improbable but plausible scenario is based on a variety of real (but smaller) cases.

Called the Sybil Logic Bomb Project[15], the scenario describes a malicious insider who modifies the source code in a regular upgrade of the Sybil (the company is fictional) database software. The 'bomb' is designed to slowly corrupt data by introducing small errors in the systems — errors so small that they are not noticeable at first. Because the Sybil software is a popular database used by many companies, the bomb gets distributed into the information systems of companies around the world within a few weeks. Imperceptibly, the virus damages and undermines business systems over a period of several years.

Eventually the full extent of the damage is uncovered, but only after a period of up to 15 months. As the full, horrifying extent of the damage becomes apparent, people's faith in the information technology systems in both the private and public sector is shaken, leading to what the researchers call "information malaise". Based on the scenario, the total losses to global GDP output over a five-year period range from $4.5 trillion to, in the most extreme scenario, $15 trillion.

This is comparable to estimates that the 2008 GFC cost the world economy somewhere in the region of $ 20 trillion.

To trust something, we need to trust everything

Forget SolarWinds for a moment and take yourself back a few years. The wave of high-profile ransomware incidents of previous years showed us just how blind we can be to potential threats that we unwittingly expose a business to.

The NotPetya ransomware was particularly significant because it was initially introduced into most organisations through a compromised accounting software vendor – a classic form of 'supply chain' attack, eventually costing the global economy US$ 10 billion worldwide[16].

Similarly, the CCleaner tool, used for years by many privileged system users, was compromised with malicious code. During the same period, there were allegations of a prominent Russian anti-virus firm's involvement in government spying. These examples serve to illustrate that threats are increasingly being introduced by software and systems that serve us somewhere in the supply chain beyond the direct control of the corporation itself.

More recently we learnt from the Spectre and Meltdown attacks that many CPUs used in servers, desktops, notebooks and mobile devices are vulnerable to exploits that can leak sensitive information. What's worse was that these vulnerabilities were baked into the hardware. To completely mitigate this risk, a solution would be to replace the hardware, which could be very costly. Popular software vendors and affected hardware vendors rushed to publish solutions to these complex problems.

The likelihood of a catastrophic cyber event on the scale of Sybil Logic bomb is considered improbable (1% chance of occurrence within a given year) but plausible. We don't know if SolarWinds is the Sybil Logic Bomb we've been fearing, but it comes pretty close. At the very least it should serve as a sobering reminder of just how interconnected IT systems (and industries in general) really are, and how a failure in one domain directly and meaningfully impacts the ecosystem as a whole.

To review a more detailed examination of the contagion effect in security, the Sybil Logic Bomb project and the exacerbating issue of 'Security Debt' please take a moment to watch a presentation we delivered at the 44Con conference in London (under our previous brand – 'SecureData')[17].

How we got here

Threats are driven by forces

We believe the SolarWinds attacks is the inevitable consequence of a series of systemic drivers that we have commented on frequently in the past (for instance in our World 2020 talk). Indeed, there is nothing in our analysis here that we have not discussed in detail in the various papers and presentations in which we share our work.

The SolarWinds compromise occurred in an unwieldly and chaotic threat landscape that is created when three forces collide. These include:

Structural forces

Structural forces include the systemic forces that are the enablers or constraints that shape the threat and our ability to respond. These factors are woven into our contexts and environments and have a fundamental impact on the shape the threat takes and our ability to respond to that threat. For example, structural forces can include not having proper cyber law enforcement or regulatory controls in place.

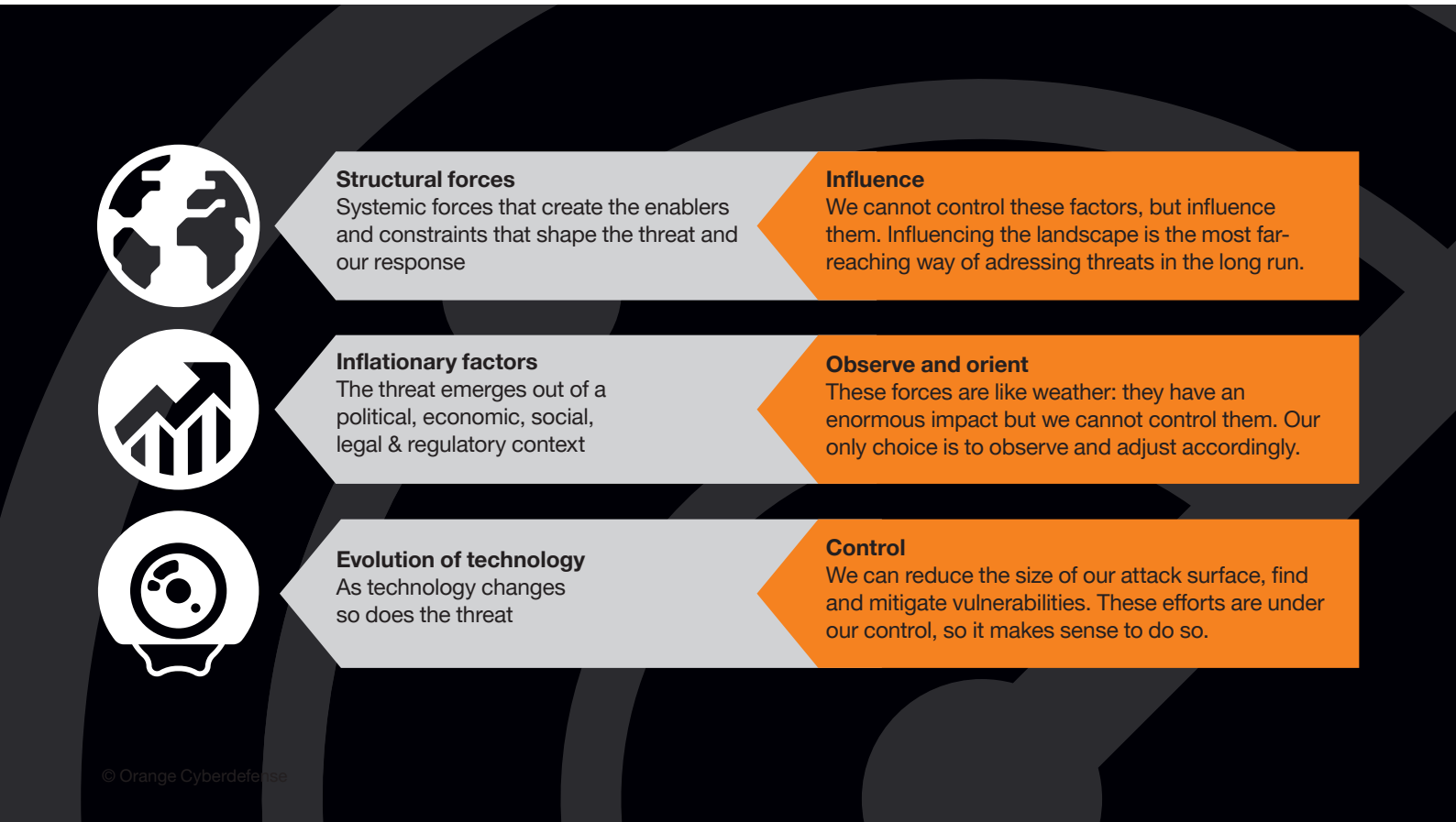
Businesses looking to cover themselves to avoid penalties, using security approaches that are not in the best interest of clients or broader society. Structural forces tend to be beyond our direct sphere of influence and there is little we can do to control them on a day-to-day basis.

Inflationary factors

Inflationary factors bloat the landscape. Examples include the unregulated use of hacking techniques and tools by governments underpinned by huge budgets which don't support wider society, the arrival of 5G and IoT which will dramatically exacerbate the problem of finding and preventing attacks and the emergence of cryptocurrencies, which makes it easier for cybercriminals to operate under the radar and run ransomware attacks. Again, these factors are large and beyond our control, although we can influence them by engaging with government, policy makers and regulators.

Technology

Finally, technology itself. As technology advances and changes so do threats. The more technology increases the more the attack surface grows. In addition, new technology never fully replaces old technology, so there are still always inherent security issues in legacy technology to deal with. Neither can security technology magic away the security issue. Security vendor SonicWall, for example, recently issued an urgent security notice about threat actors exploiting a zero-day vulnerability in their own VPN products to perform attacks on SonicWall's internal systems. Indeed, attacks against security technologies are a notable trend now.



Factors leading up to Solorigate

SolarWinds was the consequence of several diverse factors that have colluded over years to create a context in which a compromise of this kind was all but inevitable. We will highlight four primary factors in this report:

1. **Government investments in computer hacking capabilities.** Government demand for cyber capabilities that support its national and international political objectives drives the creation of an offensive cyber operations ecosystem that operates off budgets that have no parallel in the civilian realm.
2. **IT Interdependence.** IT systems and the businesses that use them do not operate in isolation. Security risk cannot be assessed for a single business in isolation, and the impact of a breach or compromise is never restricted to the primary target alone.
3. **Accumulated security debt.** Developers and IT teams continually compromise on the security of their software and systems. In the quest to ship fast, bugs and other imperfections are introduced into code & architectures with a vague intention to patch or rectify in future. Many businesses – either unconsciously or through intellectually dishonestly – have been taking on security debt at an irresponsible rate and hiding it from stakeholders, such as their customers, regulators and the wider public. The problem has been growing both silently and exponentially, and the results are only made visible when significant breaches occur in the public eye.
4. **Supply Chain Risk.** The interaction between various hardware and software components and their human users across an organization leads to an explosion in security risk. The supply chain also presents hackers with a force multiplier for their efforts. By compromising just one key system at the right place in the supply chain an entire ecosystem can be simultaneously targeted. This creates an irresistible target for sufficiently resourced and motivated attackers.

We discuss each of these contributing factors in the section below.

Government investments in computer hacking capabilities

A major contributor to the SolarWinds compromise is government spending on offensive cybersecurity. We are confronted with a far-reaching trend that is likely to shape the world in a very significant way over the next decade. Government demand for cyber capabilities that support its national and international political objectives drives the creation of an offensive cyber operations ecosystem that operates off budgets that have no parallel in the civilian realm.

SolarWinds and their customers are the direct victims of a highly professional and resourced government hacking operation. It's too soon to speculate on who the perpetrator was, but several governments would be willing and able to execute such an attack including the 'usual suspects' of Russia, China, North Korea and Iran. Of course, western countries like the USA, the UK, Israel and several European players would also be capable of such an operation, if the tables were turned. There is no doubt that, at given time, several countries are actively engaged in computer hacking operations of one kind or another around the world.

The obvious and direct consequences of these government hacking operations are clear to see in SolarWinds. This is only the proverbial 'tip of the iceberg', however.

The evolution of such capabilities starts by developing the required skills and then grows to tools and ultimately exploits and zero-day exploits, eventually producing thousands of government-trained, well equipped and battle-tested cyber 'warriors'.

As these government employees inevitably reach the end of their tenures and retire to civilian jobs, they join defense-related businesses within the cyber-military complex with a remarkable level of skill and experience and a completely different perspective on what can and should be accomplished in digital conflict. Eventually all these elements will find their way into the civilian ecosystem, where the impact they have is bound to be highly disruptive.

The scope and scale of government-funded initiatives have the potential to totally invert everything we hold to be 'true' in our industry.

It's not only human capabilities that government programs are producing however, its technology also. Governments across the world have taken an offensive step in proactively researching and developing vulnerabilities and exploits, covertly infecting machines in key strategic locations and industries, and conducting reconnaissance against Critical National Infrastructure (CNI).

In one example from the USA, the National Security Agency's work came back to bite it. It appeared that Russian intelligence had discovered and then leaked some of these exploits, one of which, EternalBlue, was used to spread the notorious WannaCry ransomware, which cost various private sector victims millions in damages.

This investment in computer hacking tools, skills and operations continues amongst dozens of countries, despite the obviously damaging implications for information security.

We're living in an extraordinary time. We're continuing to see a steady escalation in the intensity and complexity of nation-on-nation cyber campaigns. A nascent geo-political conflict between global players in cyberspace is now affecting innumerable private sector businesses, organisations and individuals around the world. As we witness conflicts between nation states in cyberspace, it's worth noting that they are occurring on the Internet – a stage that all of us share.

In the eyes of government agencies and armies world-wide, cyberspace is a confrontation space, like the real world, where they want to defend their short term interest but also to be in the best position if a higher intensity confrontation is declared.

IT interdependence

Considering the several supply chain attacks discussed this month, we want to draw your attention to the systemic issue of 'Interdependence', which we have touched on before but bares mentioning again.

The term 'Interdependence' refers to a threat, vulnerability or incident emerging from the inter-dependence businesses have on each other and how that impacts their security individually. A simple example of this would be supply chain vulnerabilities and attacks, attacks against MSSPs & attacks against shared (e.g. Open Source) code bases or systems (e.g. DNS or domain registrars). It also describes risk, attacks or compromises being spread from one organization to another (e.g. Maersk and notPeta or Marriott).

Supply-chain attacks are one example of how the systemic reality of interdependence in IT affects the threat landscape. We simply cannot afford to think of our own security as isolated or separate from the security of our technology product or service providers, or from the myriad of other business entities or government agencies we share technology with.

This goes far beyond simple vendor supply risk. The business environment is a highly networked ecosystem, linked in several different ways by a complex mesh of homogenous technologies that either directly, or indirectly connect them.

As the Cambridge Sybil Logic Bomb analysis (referenced above) powerfully illustrates, 'interconnectedness' goes far beyond simply network connections. A shared dependency on core technologies, vendors, protocols or core Internet systems like DNS or CDNs bind businesses together just as tightly as fibre links and IP networks. Businesses in turn also bind together the suppliers who depend on them, the industries they belong to, the countries they operate in and, eventually, the entire global economy.

Risk, vulnerabilities, threats, security debt and the impact of security failures are shared across business in the broader ecosystem.

Businesses are also in an interdependent relationship with their consumer customers. We observed in a recent blog post[18] that "between 60% and 80% of US Social Security Numbers have already been compromised. For a key item of personal identification to be so thoroughly undermined is a devastating setback for the autonomy, safety and privacy of the individuals involved".

In the same post[19] on our site we've previously argued:

"When businesses are breached and data is lost and used in identify theft, when accountants in Baltimore can't file tax returns and when faith is lost in election results because of hacking, email dumps and misinformation campaigns, the real victims are the people who depend on those systems to live their lives. Everybody is talking about the Equifax share price and how their CISO was fired, but almost nobody talks about Aunty May, whose private information was stolen and will never be returned to her."

The fundamental systemic reality of interdependence has two major implications: The first is that the chain of security is only as strong as its weakest link. In the SolarWinds case that weakest link happens to be a software product supplier. The second implication is that the impact of a security breach is never limited to the initial victim. There are always externalities[20]. When we as businesses asses the risk of a security failure, we need to also start considering the secondary and tertiary impact that compromise could have on the wider ecosystem.

Accumulated security debt

What we notice when we critically examine our security posture in light of incidents like SolarWinds and other new threats is how much 'security debt' we've been saddled with. "Security debt" is a concept that emerged from software development[21] that reflects the implied cost of additional rework caused by choosing an easy solution in the short term instead of using a better approach that would take longer. This kind of debt is rife in security. When the Internet was still new and promised to enable radical new business concepts many companies rushed blindly to 'get online' in one way or another.

There was no appreciation of real security threats at the time and security was neglected or ignored. We started to accumulate security debt and it's been adding up for three decades now. Some of the debt is easy to see, but much of it is hidden deep in the architectures, legacy code, 3rd party libraries and dependencies and even the fundamental economic principles that some business models are based on.

These interdependencies are so complex and intertwined that it may be beyond the abilities of the average corporate to fully determine what they are.

Think of the potential impact of this debt as a kin to what happened in the financial markets with the Global Financial Crisis in 2008. The GFC really began with something called 'Collaterized Debt Obligations' (CDO) in 2007. CDOs are a form of derivative in which the value of the instrument is derived from the value of other assets, often high-yield junk bonds, mortgage-backed securities[22], credit-default swaps and other high-risk, high-yield products.

"CDOs are complex instruments; so much so that normal people could hardly understand them. Debt owned by one business is resold to another, broken up, bundled and resold again and on and on. Eventually no-one could reasonably determine where the original debt lay or how risky it was and so when the bottom started to fall out of the domestic property market in 2008 the assets at the core of CDOs were going under and the mathematical models that were supposed to protect investors didn't work.

There was more debt and more risk than the business model could tolerate and the whole thing, literally, collapsed. Eventually, the fallout spread to the point that bond insurance companies had their credit ratings lowered; state regulators forced a change in how debt is rated, and some of the bigger players in the debt markets reduced their stakes in the business or exited the game entirely".

Could a similar thing happen because of poor risk assessment and accumulated security debt in modern digital businesses? Could it be that the whole IT industry is borrowing security time at a rate that we'll never be able to repay, and that the debt is so broken up, bundled and resold that no-one could ever accurately determine what theirs really is? Could it be that we just need one major incident for the bottom to fall out and regulators to step in, reducing appetite, increasing costs and effectively driving many businesses under? It's true to say that we haven't seen anything close this yet, and it's too soon to say whether SolarWinds will prove to be such an event, but it would serve us well to learn from other domains and in this case the similarities are disconcerting.

It's almost as if we are stuck in a kind of debt trap. We need technology to meet our daily business objectives, yet when a flaw in our solution stack is exploited, we are forced to react. Failing to address the accumulated 'security debt' puts stress on the very business it is supposed to empower. What's worse is that we are in this position because vendors and service providers we chose to partner with, have themselves made poor decisions and thus accumulated debt.

This 'security debt' is inherited when we buy and use their products. We are now forced to spend effort in ways that we did not plan to. This hidden cost, this compound interest, has reached a climax and someone must surely pay the toll.

SolarWinds and their customers now know exactly how that feels.

Renowned security analyst Bruce Schneier shared some strong opinions on the topic in a recent blog post[23], which we believe support our own arguments about the systemic causes of the breach:

"The fundamental problem is one of economic incentives. The market rewards quick development of products. It rewards new features. It rewards spying on customers and users: collecting and selling individual data. The market does not reward security, safety or transparency. It doesn't reward reliability past a bare minimum, and it doesn't reward resilience at all.

This is what happened at SolarWinds. A New York Times report[24] noted the company ignored basic security practices. It moved software development to Eastern Europe, where Russia has more influence and could potentially subvert programmers, because it's cheaper.

Short-term profit was seemingly prioritized over product security.

Companies have the right to make decisions like this. The real question is why the US government bought such shoddy software for its critical networks".

The risk introduced by security debt incurred within our supply chain must play a role in our Threat Models and in our procurement processes, with all the implications that thinking unfortunately brings with it.

To review a more detailed examination of the contagion effect in security and the exacerbating issue of 'security debt' please take a moment to watch a presentation we delivered at the 44Con conference in London (under our previous brand – 'SecureData')[25].

The pressure's been building

The systemic factors described in this report that contributed to this event occurring should be familiar to readers who've followed our research. An ongoing research
initiative called 'World Watch', which we operate within Orange Cyberdefense, allows us to monitor and track these systemic issues on a continual basis.

The World Watch service works to collect, analyze, prioritize, contextualize and summarize global, geographical and vertical threat and vulnerability intelligence to provide actionable security intelligence relevant to our business and our customers.

World Watch publishes between 30 and 50 bulletins (called 'Signals') each month regarding significant vulnerabilities, threats, breaches or security developments that should be noted and responded to by our customers or internal teams.

In the process of triaging and processing these Signals our analysts also organize and tag them with set of meta-data markers that allow us to track trends, patterns or significant anomalies that emerge.

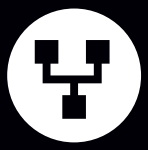
The resultant dataset provides a unique perspective on the significant events that have been shaping our industry and allows us to develop a high level view of emerging security landscape – the forces that are driving it, the technologies that are shaping it, the trends that are likely to result and the winners and losers that emerge.

The observations in this section are gleaned from the slight but nevertheless insightful dataset that the World Watch service provides us...

We highlight two systemic drivers, covered in our 'State of the Threat' model, and the resulting threat of supply chain attacks, in the graphic below.

Government cyber operations

Involves work or investment by governments, state-sponsored or supported hackers, state-developed tools or capabilities, or their associated contractors.



Cyber interdependence

A threat, vulnerability or incident emerging from the inter-dependence businesses have on each other. A simple example of this would be supply chain vulnerabilities and attacks, attacks against MSSPs & attacks against shared (e.g. Open Source) code bases or systems (e.g. DNS or domain registrars). Incidents involving risk, attacks or compromises being spread from one organization to another (e.g. Maersk and notPetya or the Marriott breach would also fall into this category.

Security debt

Security debt accumulates deep in the architectures, legacy code, 3rd party libraries and dependencies and even the fundamental economic principles that some business models are based on.

Supply Chain Attacks

The notion that the 'supply chain' is a growing new threat vector. 'Supply chain' would include software supply chain (including full applications, Open Source tools or common modules, service providers, contractors and other suppliers.

The hypothesis is that it makes sense for hackers to target the supply chain because it's often the 'weak' link in the chain, but also because a single carefully-selected supply chain compromise (e.g. a commonly used package or system) could allow for a high number of downstream compromises.

Context: World Watch

All the World Watch Signals we publish are also tagged with markers for significant global security trends we track in our efforts to better understand the security landscape. In this paper we focus on the geopolitical impact of government computer hacking, the structural challenge of 'IT interdependence', and the resulting threat of supply chain attacks. We consider the significance of these two systemic drivers in our statistics.

As the two charts to the right illustrate, both 'government hacking' and 'interdependence' – two of the leading systemic contributors to the SolarWinds incident – feature very prominently in our Signals.

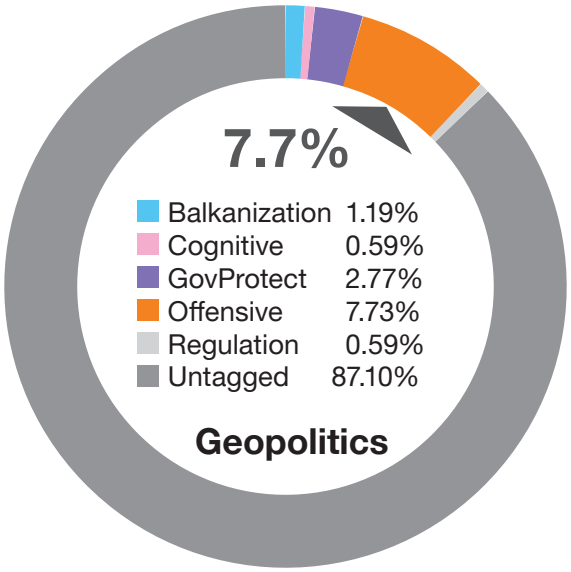
Indeed, each of these is the dominant factor in its respective category – 'Geopolitics' and 'Structural Forces'. As we've argued for years now, these factors have been shaping the threat landscape in significant ways for some time.

Since there is no sign of either of them abating in any way, incidents like SolarWinds have been almost inevitable. SolarWinds isn't the only incident of this type in recent years (think Wannacry and notPetya) and, unless significant changes occur within government and the private sector, we can expect them to happen again.

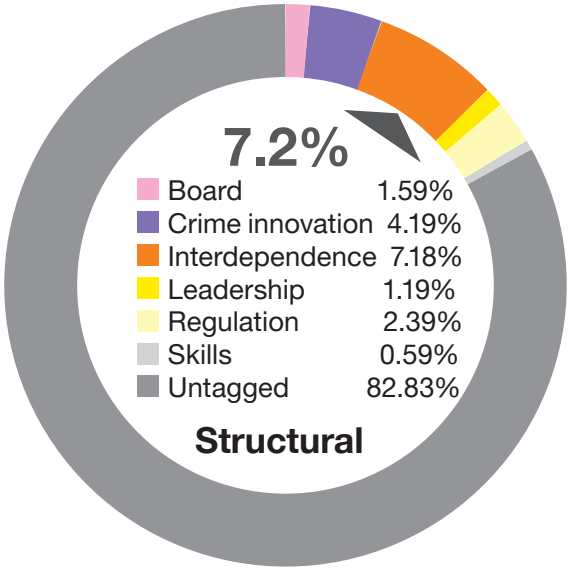
A third contributing factor – the collective build-up of 'security debt' - is discussed in the YouTube link we shared earlier[26] and in a paper we previously published on the topic[27].

Through our State of the Threat model, supply chain attacks are one the of the threat classes that we predict will emerge. Government hacking and supply chain attacks featured less frequently in the 2nd and 3rd quarters, where COVID-19 and ransomware attacks dominated the landscape, but supply chain attacks increased again in the 4th quarter.

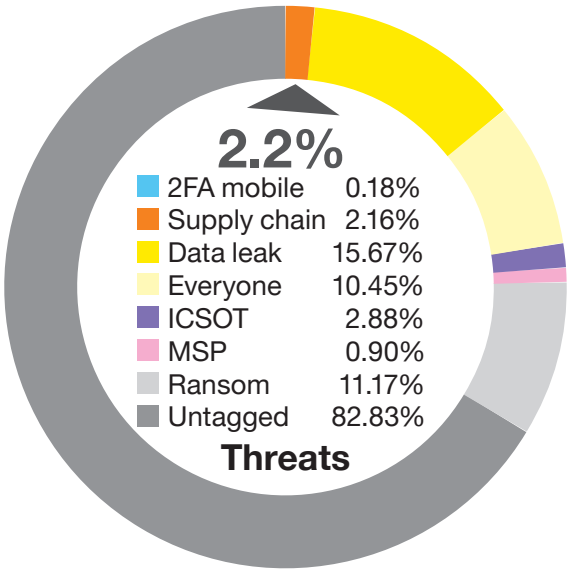
Breaches from direct state-sponsored attacks remain by far the exception rather than the rule. From a dataset of 127 significant publicly reported breaches our team has analysed, only 5 could be clearly attributed to state-backed actors. Despite the systemic significance of government hacking therefore, actual breaches by state-backed hackers are rarely reported in public.



Almost 8% of all Signals published involve government hacking in some way



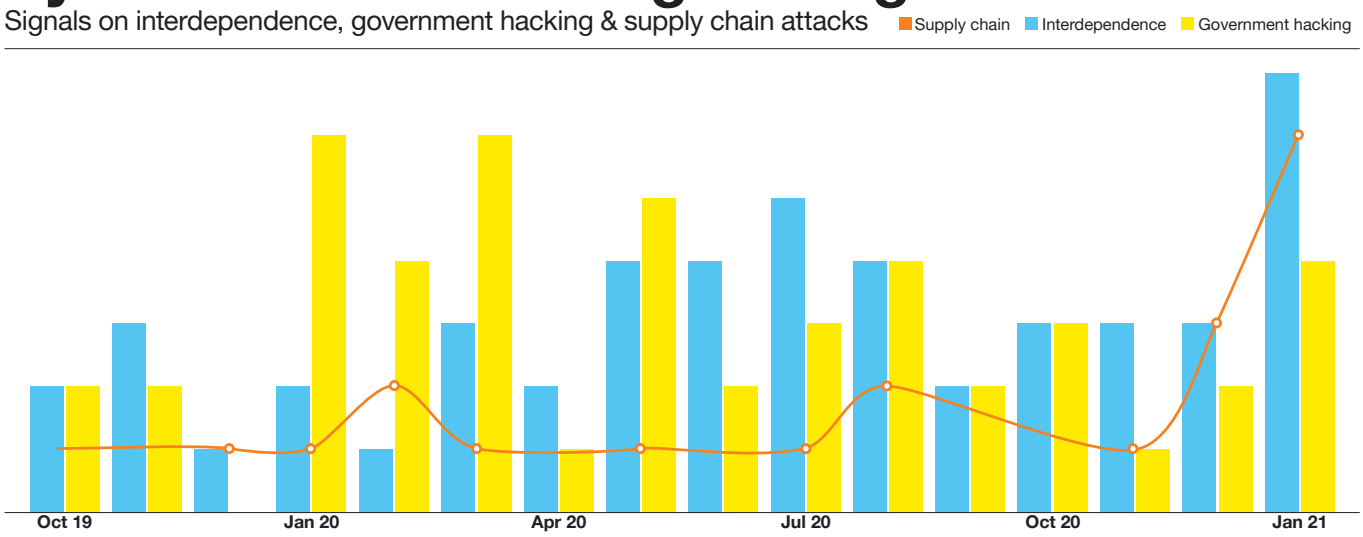
Over 7% of ALL Signals published discuss the issue of cyber interdependence in some way



Supply chain attacks emerge as a result of consistent systemic drivers

Systemic issues driving Solorigate

Signals on interdependence, government hacking & supply chain attacks



'Interdependence' featured more often as the year progressed and in the last quarter, we recorded 50% more cases reflecting this theme than in the first quarter. The systemic issue of 'interdependence' also features much more frequently in our Signals than the resulting threat of supply chain attacks, which is to be expected.

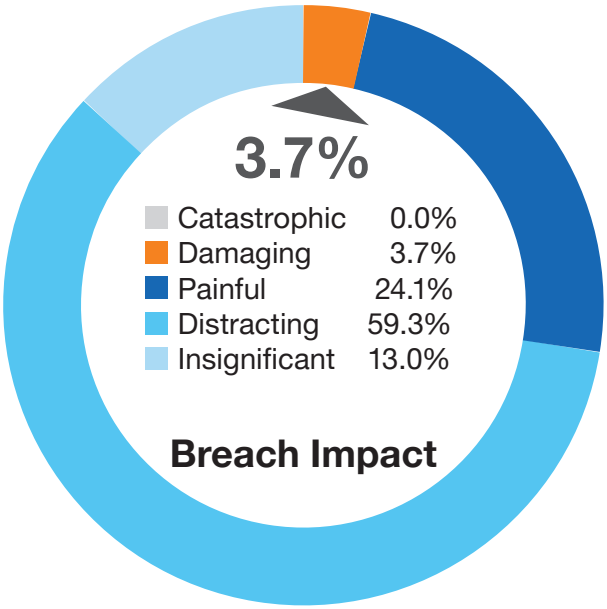
By their very nature, supply chain attacks provide the attacker with vast scope and scale, even if they take more resources and time to perpetrate. The frequency of these attacks is therefore not as important as their impact, which the notPetya and SolarWinds incidents have shown as can be very severe indeed.

Given the persistence of the systemic forces that enable these attacks, we anticipate that they will increase in both frequency and impact.

What to expect next

We're too far removed from the core of this incident to predict with any certainty what will come of it. In fact, at this stage so much is being learned daily that even those closest to the case couldn't be sure. Of course, that needn't stop us from speculating!

Its highly likely that SolarWinds will face all kinds of legal, regulatory and civil sanctions. The nature and the impact of these will vary. There's no doubt that there will significant costs to the company from fines, reparations and lawsuits, but our data suggest that most corporate victims experience the impact of a breach as merely 'distracting'. As the chart shows, less than 4% of the victims in 108 breaches we analysed for this attribute experienced the consequence as really 'damaging. None were 'catastrophic'



As we suggest earlier in this report, the real cost of this breach will be in the form of the Fear, Uncertainty and Doubt that it sows amongst the vast number of potential victims. A myriad of US agencies and private corporations will need to conduct wide-ranging investigations to assure themselves that they have not been breached. As this process unfolds more victims, more attack vectors and more technical details will continue to emerge, probably well into 2021.

There will also be a political fall-out. To what extent the USA currently has the time or energy to exert itself politically is not clear at present, but eventually intelligence and law enforcement agencies from the US and her allies will develop a case against a probable perpetrator. They will eventually identify the operators and seek (symbolic) indictments against some of the individuals involved.

There will probably be other forms of political response also. In the past we've seen the US leverage sanctions, object publicly at the UN and other forums, evict diplomats (usually those suspected of being spies) and perhaps exert pressure via high-level diplomatic talks (which appeared to be quite effective for President Obama after the Office of Personnel Management was compromised by China between Nov 2013 and April 2015[28]).

Theoretically the USA also has the option of retaliation via a 'kinetic' response of some form. The US has argued that it withholds the right to respond to cyber-attacks with physical force, but there is no public record that this has never happened before. Could this be the first time?

While there is no way of knowing, it is also safe to assume that the USA will retaliate in cyberspace with a combination of visible and covert attacks.

The purpose of the visible attacks is signalling. That is, to demonstrate to the suspected adversary and the world at large that the US can, and will, retaliate in kind. Covert operations to properly establish a meaningful beachhead within its adversary's key systems would serve as a deterrent to future hostile behaviour, provided the adversary is convinced the US would truly be willing to exercise that option.

Under a new administration, the USA will seek to examine and improve its own cyber readiness, having already commited to making cybersecurity a top priority[29]. According to a recent article by the Brookings Institute[30]:

"Members from both parties requested information about the SolarWinds attack from the FBI, CISA, ODNI, and DHS and stated intentions to work on bipartisan cybersecurity legislation in 2021. The latter could also tie into negotiations over comprehensive federal privacy legislation, as many privacy bills in the 116th Congress would require companies to implement "reasonable" cybersecurity measures (most notably, the SAFE DATA Act and COPRA). Other areas of congressional focus may include strengthening the Department of Homeland Security's EINSTEIN program, continuing to fund and implement CISA's Continuous Diagnostics and Mitigation program, and facilitating the recruitment and retention of IT personnel in the federal government".

Indeed, on the very last day of his tenure, President Trump's administration issued an Executive Order[31] on "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities" to " address the use of United States Infrastructure as a Service (IaaS) products by foreign malicious cyber actors".

The order calls for three actions by 'cloud service' providers, namely to verify the identity of persons obtaining an IaaS account and to maintain records of those transactions, to limit certain foreign actors' access and to establish more robust cooperation providers, including the increase in voluntary information sharing.

While it appears that the impetus for this order precedes the SolarWinds attack, it will no doubt gain momentum due the 'crisis' the US now finds itself in. New initiatives will follow under the Biden administration, though its not clear what priority they will really enjoy given the other burning issues the new administration faces.

In the civilian domain the SolarWinds incident will be a significant shot in the arm for the security industry and for CISOs wrestling to get their message across. Rightfully so. We hope and believe that our customers, and businesses worldwide, will learn a sobering lesson from what befell SolarWinds and take those lessons to heart. SolarWinds will feature in an endless series of PowerPoint decks offering advice on how not to be 'the next SolarWinds'. Much of this guidance will be snake oil, but some of it will not. There are well understood and readily accessible technical controls that can be put in place to reduce the risk of being the next SolarWinds, or collateral damage from the next SolarWinds. We at Orange Cyberdefense would of course also be very happy to discuss these with you, and we do believe we can truly be of help.

More of the same

A senior colleague at Orange Cyberdefense has often counselled that it's very hard to know what's going to change, but it's not very hard to guess what's not going to change.

SolarWinds will no-doubt trigger a fresh look at the more complex issues like supply chain security, and hopefully even a deeper consideration of the question of security debt and risk contagion. Unless there are catastrophic repercussions for SolarWinds or a notable response by regulators, however, we have our doubts that the risk calculations for most businesses will fundamentally change. That is until the next big incident happens. We regretfully predict it inevitably will.

In the meantime, there is no doubt that the USA, her allies and her adversaries will continue (or even escalate) their investments in offensive security research, capabilities development and operations. Cyber espionage will continue to present an attractive option for intelligence communities worldwide and with time we will probably see more shows of cyber force – large scale Denial of Service, compromise of critical infrastructure and possibly even attacks that cost a human life.

We believe this kind of activity will continue, to the detriment of cyberspace security in general, even as well-meaning policy makers and diplomats struggle to secure meaningless agreements on cyber norms intended to govern that kind of activity.

As a compelling article on Lawfare[32] argues: "This approach is deeply flawed in both principle and practice. Part of the problem arises from the conflation of two related but distinct concepts: that of cybersecurity on the one hand, and cyber power on the other. There are links between the two, of course. But they are two different things, serving two quite distinct purposes".

As we argued earlier in this paper, the key systemic factors that contributed to this incident show little sign of abating. Government investment in offensive cyber capabilities is just as likely to increase than decrease as a result of SolarWinds, and interdependence is a fundamental structural reality that needs to be calculated in, not managed out.

The COVID-19 pandemic has taught us how closely-knit our societies and economies are, and how spectacularly a catastrophe in one area spills over to the other. In responding to the crisis, we are learning to appreciate the impact that our behaviour has on the whole of society, and not just on us as individuals, families and businesses. This is an essential lesson for the security community also. When we consider when, where and how much to invest in security, we must think beyond the single-dimensional risk we are addressing for our business and consider the impact of the secondary and tertiary effects on the broader economy when breaches and compromises happen. We need to recognize that what's bad for society generally, is bad for us as businesses also.

Our hope is that the SolarWinds incident will serve as another reminder of how interdependent we are as citizens of the new digital world, and encourage the development of a more wholistic form of risk assessment that not only considers the risk posed to us by third parties, but also the risk our own failures may pose to our suppliers, customers and society as a whole.

The accumulation of security debt is also unlikely to slow. As Bruce Schneier eloquently argues in the quote we shared above, as long as short-term profit is prioritized over security, risk assessment equations are unlikely to change, and debt will continue to build until the whole house of cards comes crashing down.

A final systemic factor that is likely to continue shaping the security landscape, for better or for worse, is the role played by cyber insurance[33]. In light of the increasing number of attacks and growing impact of incidents, business increasingly seek to cover their residual risk with cyber insurance policies.

Whilst still in its infancy, this approach promises to remove much of the uncertainty and angst from the issue of information security and reduced the problem to a simple one of risk appetite and budget, which is appealing to business. Such businesses will seek to identify the pertinent legislation, regulation and best practice guidelines that permit them to make the smallest possible investments in cybersecurity whilst still complying with the minimum requirements laid down by governments and the insurance industry.

The first meaningful iteration of such regulation for our customers appears to be the EU GDPR. With its thoughtful expression and mature execution, the legislation promises to shape the future of Information Security in Europe and the UK for the next few years to come. Emerging Californian Data Protection legislation seems likely to have a similar impact in the U.S.A and collectively these regulations are certain to impact corporate spending, strategy and behaviour in a significant way.

How exactly behaviours will change, and whether those behaviours are ultimately good for security and society at large, remains to be seen. One possible dark side to severe compliance penalties is that they incentivise compliance, rather than a genuine reduction in security debt and the associated risk. Another risk is the possibility of extortion rackets, in which companies are breached and then forced to pay a moderate bribe rather than face potentially stiffer GDPR fines and the negative backlash of public disclosure, a notable trend we are already starting to observe.

Winds of change

The systemic context from the SolarWinds incident emerge seems unlikely to change significantly in the short term, except for the likely increase of a significant geopolitical force that we have not discussed here yet, namely cyber balkanisation.

As governments battle it out in cyber-space and the attacks become more advanced and impactful, the question of cyber balkanisation starts to emerge - - the splintering of the world into politically aligned camps that all run the same hardware and software that is developed and controlled by the technology superpowers. This has been previously demonstrated by the drama around a prominent Russian AV company and its deployment within US government sites[34]. The US government's concern about the integrity of security software produced in Russia was perhaps a little exaggerated but prescient, nevertheless. This "balkanisation" of cyberspace takes many forms but seems immediately obvious in the recent focus of the US government on improving the integrity of its supply chain. Foreign technology providers from China and Russia are just the first to find themselves in the firing line, but they certainly won't be the last.

The long-term implications of such balkanisation could be game-changing: As other governments take America's lead and start rejecting first security software, then sensitive apps, infrastructure and eventually entire Operating Systems on the grounds of National Security, this may lead to a level of balkanisation not seen in the world since the cold war.

The global, borderless internet that a generation has envisaged is growing less and less global and borderless by the day. In fact, it's becoming increasingly defined by geopolitical lines. Smaller countries don't have their own security vendors and can't afford to build their own OS stacks. All nations capable of providing such a stack are also involved in offensive operations however, so the smaller nation is thus forced to choose the lesser of the evils: aligning itself with the cyber super power it distrusts the least and accepting that it can no longer engage the others for fear of being compromised. They will be forced to align with one major power or the other, gradually consolidating into camps until just a few major blocks remain. Because running software controlled by a single nation-state is effectively a form of voluntary compromise by that nation-state, the smaller country then also loses its autonomy and becomes fundamentally beholden to its technology master, no longer able to escape.

How this will impact on enterprise security remains to be seen, but this must surely be significant. What happens to your own credibility as a smaller nation when the integrity of your systems is effectively built on compromised systems? One click and your national sovereignty is washed away. Allying with a superpower could be the only way forward to maintaining that all-important integrity in key systems. It might be a kind of digital feudalism, but it could be the least bad option for smaller nations facing these threats and it further exacerbates the growing threat of global balkanisation.

As the world's superpowers move to occupy strategic territory in cyberspace by exploiting vulnerable systems the companies and countries caught in the middle will have to decide on which side to stake their allegiance. In this rapidly fragmenting world, technology and cyber capability will increasingly define the prosperity of nations.

Balkanisation appears to be the direct and natural consequence of a logical and inevitable concern about supply chain security. By noting that SolarWinds chose to outsource their software development to Eastern Europe, the saga is already putting the question of software origin and "indigenous or semi-indigenous software"[35] on the agenda. These are existing discussions, and logical in the current context, but they may well have far-reaching implications for technology, geopolitics and the notion of a free and open internet that connects and empowers all who use it.

We wrote some early thoughts on this for a NATO conference some years ago (under a previous brand – SensePost)[36].

How we should respond

Never has the realm of computer security been more followed in the mainstream, nor indeed has it ever played such a significant role in the day-to-day life of the average man on the street. The changes sweeping our domain today have far-reaching implications, not only for security but also for society.

As we've endeavoured to illustrate in this report, the SolarWinds incident is not about specific technical failures of the victims or the specific Tactics, Techniques and Procedures (TTPs) deployed by the attackers. It's about understanding and countering a powerful set of deeply rooted systemic factors that collectively create a context in which incidents like this are all but inevitable and appear likely to escalate. So many of these issues are being driven and shaped by factors not directly under our control. As an industry we need to start fighting these problems at the root. This begins with government policy, regulations and practices.

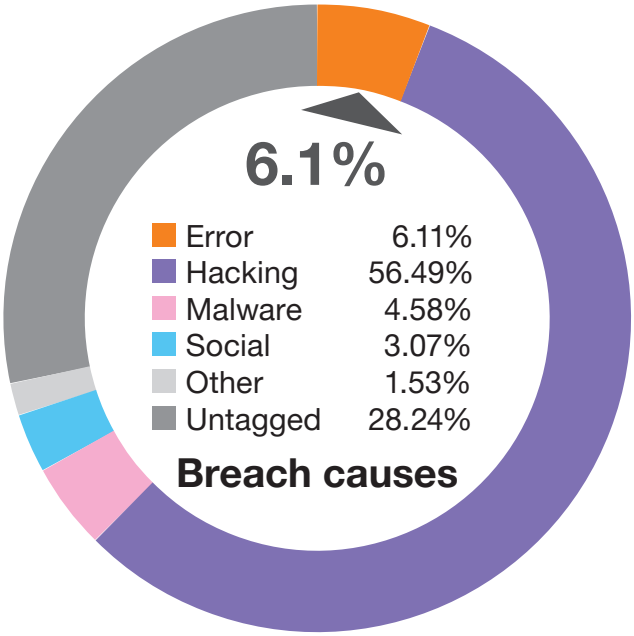
Questions of free trade and free speech, questions of the government's place on the civilian Internet, questions about the ethics and morality of military and the police using and even building hacking tools, questions of responsibility and accountability for the cost (and hidden costs) of breaches, and the extent that these should be insured against, international geopolitics and the like.

For complex questions like these there is no single place for the proverbial buck to stop. Multiple diverse role players - many of which are not adversely impacted by cyber issues, and some of which even benefit from the on-
going state of uncertainty and risk – need to step forward to consider and address the problems. With little or no incentive to do so, however, these key players are likely to stay silent and so fundamental issues are likely to persist unquestioned.

The cost of all of this is shared by numerous (mostly) nameless victims and each individual incident is often too small to warrant the kind of outcry and response that would be required to affect any kind of meaningful change.

The weakest link

Security starts with a trustworthy software and hardware supply chain. We've been collectively reminded. The risk introduced by our supply chain must now play a role in our Threat Models and in our procurement processes, with all the implications (to hardware, software, networks and everything in between).



Cloudy with a chance of rain

The analysis we've seen so far suggests that a breach of the SolarWinds Orion platform also indicates a breach of various cloud systems, because Orion holds credentials such as Domain Admin, AWS, and Azure Cloud API keys. We believe that such credentials gleaned by attackers were used to pivot from their on-premises network environments into their various cloud environments.

There is no simple silver bullet for the new set of security risks that the complexity of cloud migration introduces. 'Cloud' solves many security problems for our customers, but it also introduces some new ones, most of them linked to the challenges that security teams have in understanding what exposures cloud environments introduce.

In a study we conducted of 131 publicly reported breaches, the fundamental cause identified for 6% of breaches was 'error'. This may not seem like much, but its higher than the number attributed to malware or social engineering in our dataset.

Cloud exacerbates the risks in other ways also. A recent advisory released by the US National Security Agency (NSA) states[37]: "While careful cloud adoption can enhance an organization's security posture, cloud services can introduce risks that organizations should understand and address both during the procurement process and while operating in the cloud". The paper is thorough and very much worth the read.

Per an article on SC Magazine[38] "As cloud and cloud-integrated systems are deployed, they frequently connect to each other via service accounts, API integrations, OAuth tokens, etc. And these connections are cloud-to-cloud, not mediated by internal networks. This means that many of the tools security teams may be using to monitor their clouds (e.g. CASBs) will not have visibility into activity."

The piece goes on to argue (better than we could!) that businesses need to "understand the interconnectedness of their IaaS and SaaS cloud services and recognize that breaches like the SolarWinds one may not be limited to a single service or vendor by virtue of this interconnectedness. Security teams need to also understand what access to data and capabilities service accounts, tokens, and integrations have in other clouds. If a breach results in the compromise of integration accounts, those integration accounts may be used to exfiltrate data or create residency on other, totally unrelated services like a customer database or a version control system."

The focus for businesses that are on a cloud 'journey', as most now are, is to effectively enforce least privilege, and control the trust policies of all roles so they don't allow unintentional access for third party roles or identities.

Its further important to ensure that any cloud services are protected at a network level as far as possible so that direct access to APIs and other endpoints from the Internet are kept to an absolute minimum.

Tactical response

What should our readers be doing at a practical, tactical level to avoid incidents like this?

We will allow others, closer to the heart of the incident, to inform us on the details of the vulnerabilities, exploits and general vectors the SolarWinds actors leveraged. The compromises and mistakes made by the various victims will also emerge with time and prove very educational.

We believe it to be a mistake, however, to focus too closely on the specific details of the SolarWinds attack. Instead we need to recognise that the security landscape is deeply fluid and dynamic, reshaping itself rapidly and continuously, and position ourselves to perceive and respond to it appropriately. Businesses need to appreciate they are going to be targeted simply because they are on the field. There is a very real degree of unpredictability in what, when and how compromises happen, and businesses need a plan for it.

We should not be distracted by the identity of the attacker, or the speculation about state-backed adversaries. Ransomware attacks, botnets, crypto miners and the like, all follow the same 'opportunistic' philosophy in which no target is too small or insignificant.

Indeed, despite the intense focus currently on SolarWinds, ransomware and extortion attacks remain the primary threat most of our customers will face.

This is why it's crucial for a new way of thinking, moving away from naïve but convenient rules-based security practices towards an agile, intelligence-based line of thinking.

Although this reality can be both disorienting and unsettling for CISOs, there are things we can do to adapt and thrive. Consider this three-point plan:

1. **Be purposeful.** These systemic changes in the landscape are forcing security teams to think hard about their role in the organisation. More and more security is becoming about enablement. Not only do we need to enable the business to thrive be providing secure and resilient platforms, but we also now need to enable technology teams within the business to take ownership of the security of their own networks, platforms and code.
2. **Be ready.** As the landscape changes around us and the adversary becomes more capable and more brazen, we have to prepare for a reality in which security is in a state of constant 'engagement'. The world won't stop changing and the bad guys won't stop hacking. Not only must be we comfortable with change, but also with attack and compromise, which are almost an inevitability. 'Readiness' means planning, process, platform, people and practice. As the boxer Mike Tyson once famously said: "Everyone has a plan until they get punched in the face". We need to prepare to deal with attack, compromise and breach, but we'll really only be ready once we've practiced attack detection and response in real-world environments.
3. **Be agile.** The key to taking back control is to understand your own environment and reorient efforts around changing business and technology trends. Eschew scattergun investments in the same breadth of tools that peers are buying, and simply hoping for the best. Instead, develop processes to look at where the organisation is most exposed, model the relevant threats, and decide which controls, tools, policies and processes are needed to address them.

The hard truth is that there is no 'simple' model for security, no checklist, no framework and shopping list of technologies that cover off all your risks. You see there is no end-goal in security. No bar to be reached. There's external set of compliance standards that guarantee security. Criminals, governments and other hackers are going to continue to apply themselves to developing new tools and techniques.

We are engaged with an adversary who has intent, is determined, resourceful and agile.

We similarly need to commit to engaging in an active way with creative and innovative responses that leverage our own inherent home-field advantages to keep on their toes.

No two organisations are the same. But it's likely that many are already experiencing the trends we've outlined in this paper. CISOs are faced with overwhelming odds. Control might seem like it's slipping out of their hands as new trends emerge, and skills gaps hamper efforts to tackle growing complexity and threats. But by remaining focused on agility and the bigger strategic picture, as well as seeking expert third-party help where appropriate, we can chart a course through the storm.

The threat of hackers needs to be countered on every front – consistently and relentlessly. Each phase of the kill-chain that the attacker must go through to achieve a full compromise presents the defender with opportunities for prevention, detection and response. We need to relentlessly seek to identify, understand and exploit these opportunities within our own systems in order to slow or thwart the attacker's progress. Whilst attacker's work is necessarily forced into becoming more and more complex, ours needs to become simpler, with an intense focus on simply getting the universally understood basics right… more often than not.

While we seek to mature as a community, to understand and counter the systemic factors that are setting us up for failure, our focus needs to be on the agile, active and intelligence-led application of the basics. Get the basics right. Solve the fundamental problems of authentication, privilege management, malware, egress filtering, web application security and threat detection. Develop an honest and thorough threat model. Know your footprint. Partner with real specialists. Consider insurance for the rest.

Strategic response

As computer security professionals, we need to urgently note and acknowledge the role that systemic issues like government policy are playing in shaping our industry and the digital world. These are issues that go far beyond the scope of our day jobs as defenders of our own corporate digital assets, to the general functioning and welfare of cyberspace in general.

As the 'security community', we understand the fundamentals of enterprise security. We're just learning the basics of communicating in the board room and talking the language of business. Now a new challenge is at hand and we're going to have to come face-to-face with truly 'advanced' technical threats, buoyed by powerful systemic drivers, and learn the language of legislatures, courtrooms, media, military, intelligence and the political domain.

For those of us who can master these new skills, this is a once-in-a-lifetime opportunity to tangibly impact the world.

There is an urgent need for cybersecurity professionals to be able to participate in discussions and decisions at levels far beyond our current comfort zone. We need to move past technical one-upmanship and finger pointing and rapidly evolve to incorporate ideas and practices from the domains of teaching, philosophy, science, engineering, medicine and diplomacy.

There are six distinct phases in what we believe is the required maturity curve for CISOs and cybersecurity professionals:

1. **Performance:** Master the theory and practice of information security.
2. **Process:** Capture the practice in the form of clear and repeatable processes that can be delegated to others.
3. **People:** Focus on enabling others through education and mentoring to also master security fundamentals and practice.
4. **Purpose:** Understand the why of cybersecurity - the fundamental goals it has of enabling business, government and healthy life in the modern world.
5. **Principle:** Understand and explain how security can and should contribute to the fundamental goals of society.
6. **Policy:** Interact with regulators, executives and other leaders in society to create and influence the policies that will ultimately shape the world we live in for many years to come

If the security industry truly wants to make an impact on the escalating crisis of cyber crime we need to urgently accelerate our own personal and collective journeys to maturity. We need to move beyond our traditional fixation with technical solutions and our narrow understanding of cyber risk as a business issue. We need to think, speak and act to earn a place in the discussions about values, principles and policies that may be able to fundamentally shift the fundamental systemic context and shift the underlying odds back in favour of the defender at the front lines.

Intelligence-led security in action

The Orange Cyberdefense response

At Orange Cyberdefense we implement a philosophy of 'intelligence-led Security' to ensure that we remain aware of significant events like SolarWinds and agile enough to provide our customers with the appropriate response when new threats and vulnerabilities emerge.

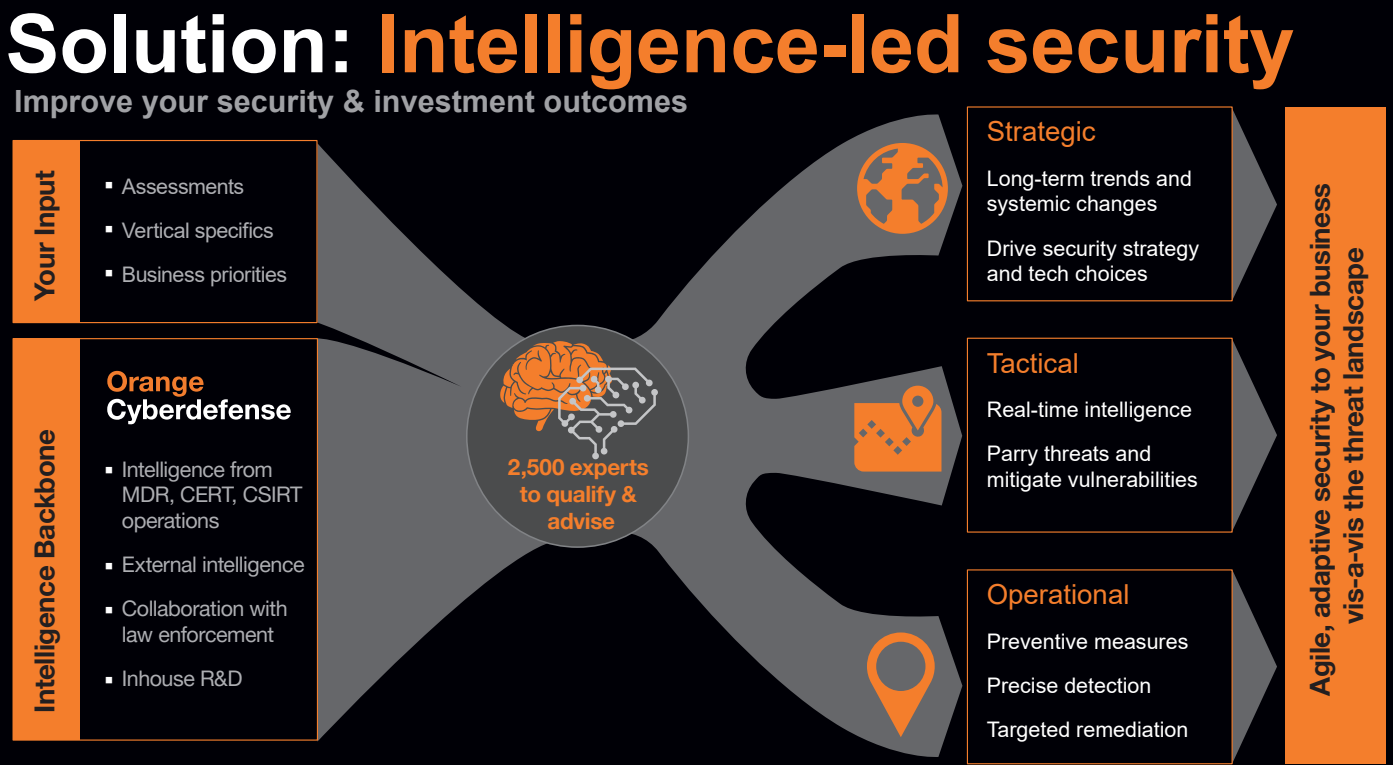
Intelligence-led security is the collection and analysis of both internal (operational) and external (landscape) data in order to understand continuously changing risks so that limited security resources can be appropriately invested where they will have the most impact.

Our 'World Watch' Service works on behalf of the customer to collect, analyse and summarise global threat and vulnerability news to provide actionable security intelligence relevant to our business and our customers. The World Watch 'Signals' are produced by a dedicated Security Research Unit.

The World Watch process continuously collects security intelligence from diverse internal and open sources then processes it to produce actionable security bulletins, called Signals, that can be delivered to CISOs and Security Managers when they need them, how they need them.

A key element our World Watch process is that the actionable intelligence we collect is synthesised and communicated to our operational teams in a consistent, efficient and timely manner to ensure that the appropriate actions can be taken on behalf of the customers we support.

We can see this principle in action in the diagram below. This process worked as planned in the SolarWinds instance, and we take the liberty of sharing examples of the different kinds of interactions we've had with our customers around this issue on the following pages.



Example: SolarWinds

Vulnerability Management

At 10:34 GMT on December 14th our research teams logged a ticket with our Managed Vulnerability Scanning teams to advise them of the SolarWinds breach and initiate a scan for any instances of the affected SolarWinds software amongst the customers we support.

DESCRIPTION

Description
Our Ref: SIG-7658

Description:
This Signal relates to SIG-7594, which is the FireEye breach. In this Signal we cover the notification that SolarWinds was used in the supply chain compromise affecting FireEye and possibly many more.

Managed Vulnerability Scanning:
Please scan for any hosts that run the SolarWinds Orion Platform. The affected versions are listed in the SolarWinds advisory in the Read more section below.

Read More:
https://www.solarwinds.com/securityadvisory
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
https://github.com/fireeye/sunburst_countermeasures

Via our processes and the data on our customers' systems that we have in hand, we were able to quickly conduct a search for potentially impacted systems.

Three impacted customers in the retail, manufacturing and financial industries were identified and notified, resulting in internal investigations and appropriate remediating actions being taken.

Threat Hunting

At the same time, on December 14th, we logged a similar ticket with our Threat Hunting teams:

DESCRIPTION

Description
Our Ref: SIG-7658

Description:
This Signal relates to SIG-7594, which is the FireEye breach. In this Signal we cover the notification that SolarWinds was used in the supply chain compromise affecting FireEye and possibly many more.

Managed Thread Detection:
Please find attached IOC for domains and file hashes.

Recommended Actions:* Review DNS logs or proxy logs for any evidence of hostnames matching the attached domain name list.
* The SUNBURST backdoor uses DGA for subdomain names. See if we have any detections for those. Examples are included in the dga hosts attachment.
* The hashes attachments are for SHA1 and MD5 hashes. If possible, use these to detected possible instances of compromised SolarWinds hosts. We will be asking the MVS team to perform scans for SolarWinds to detect any MVS customer that might be affected.
* Look at the Github link shared in the Read More section below. See if it is possible to create detections based on these and add them to our existing set of detections.

Read More:
https://www.solarwinds.com/securityadvisory
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
https://github.com/fireeye/sunburst_countermeasures

We have standardised processes in places to respond to such so-called MTC (Major Threat Crises). These processes are launched in response to relevant threat intelligence in order to coordinate our internal and external communications, share technical information between operational teams and conduct threat hunts and investigations across customer systems and data.

The goal of our threat hunters was to perform the hunt for relevant system indicators, and especially to identify the malicious DLL. We also performed hunting for relevant network IOC and TTPs.

On the very day the process was initiated – December 14th – at a customer in the luxury goods industry, a falsified Orion DLL (SolarWinds.orion.core.businesslayer.dll) was detected.

It had been present since September 2020.

The file discovered on a production server in the USA by means of its fingerprint and quarantined.

DNS resolution logs were also recovered, which made it possible to conclude that the machine had probably not contacted any known C&C. A check of the connection logs was also performed to verify that no connection attempts were made.

To allow forensics, a full snapshot of the VM was carried out immediately, then the machine was isolated from the network. Finally, despite the lack of proof of post-exploitation, the customer decided to replace the machine.

Security Operations

Intelligence also impacts the platform management services we provide via our Security Operations Centers, in this case instigating the cautionary step of blocking access to the known SUNBURST Command and Control servers:

DESCRIPTION

Description
this is a precautionary change tp a block rule for the solarwinds server on the PAs? which is facing towards internet.

Please implement the changes in below firewalls,

Created by:

Summary Notes
Hello Team,

Change has been completed as requested. Please test and advise us.

Kind regards,

Safety restored!

Conclusion

The security landscape is ever-changing and adversarial. There is no ultimate 'bar' to reach and no 'out of hours' respite to enjoy. New threats, vulnerabilities and risks will emerge continuously, and thus active engagement with a persistent adversary is essential. This volatile context requires us to remain vigilant, prepared, and agile. We accomplish this through the diligent implementation of a philosophy of 'intelligence-led security'.

'Intelligence' in this context doesn't refer to data or 'Indicators of Compromise'. Rather it describes the ability to comprehend the entire operating environment and continuously re-orient our platforms, people, and processes to adapt to new realities that keep emerging. By deeply entrenching this philosophy into the core of how we operate in security, we position ourselves to learn quickly, adapt, and respond as appropriate when we face fresh challenges.

Successful cybersecurity today therefore requires us to strike a fine balance between two prerogatives that will often be in tension with one another: Firstly a state of perpetual agility in which we continuously discern shifts in our environment and adjust our own approach accordingly, both at a tactical and a strategic level.

Secondly, we need to move doggedly toward understanding, adjusting to, or impacting the underlying systemic factors that are shaping the volatile asymmetric reality we're forced to contend with.

Literature & Sources

Sources

[1] hhttps://en.wikipedia.org/wiki/OODA_loop

[2] https://orangematter.SolarWinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

[3] https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

[4] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-SolarWinds-supply-chain-compromises-with-sunburst-backdoor.htm

[5] https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html

[6] https://www.zdnet.com/article/microsoft-says-it-identified-40-victims-of-the-SolarWinds-hack/

[7] https://fortune.com/2020/12/16/gao-SolarWinds-government-tech-security/

[8] https://www.vice.com/en/article/ezp58m/the-history-of-stuxnet-the-worlds-first-true-cyberweapon-5886b74d80d84e45e7bd22ee

[9] https://en.wikipedia.org/wiki/Stuxnet

[10] https://www.chathamhouse.org/publication/cybersecurity-nuclear-weapons-systems-threats-vulnerabilities-and-consequences

[11] https://www.nytimes.com/2017/12/28/books/review/daniel-ellsberg-the-doomsday-machine.html

[12] https://www.investopedia.com/terms/c/contagion.asp

[13] ttp://www.brainstormmag.co.za/business/14549-the-contagion-effect

[14] https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-sybil-logic-bomb-cyber-catastrophe-stress-test.pdf

[15] https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-sybil-logic-bomb-cyber-catastrophe-stress-test.pdf

[16] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[17] https://www.youtube.com/watch?v=4Use1n8zGmM

[18] https://orangecyberdefense.com/uk/blog/cyberdefense/the-human-element-in-cybersecurity/

[19] https://orangecyberdefense.com/uk/blog/cyberdefense/the-human-element-in-cybersecurity/

[20] https://en.wikipedia.org/wiki/Externality

[21] https://en.wikipedia.org/wiki/Software_development

[22] https://www.thebalance.com/mortgage-backed-securities-types-how-they-work-3305947

[23] https://www.schneier.com/blog/archives/2021/01/russias-SolarWinds-attack-and-software-security.html

[24] https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html

[25] https://www.youtube.com/watch?v=4Use1n8zGmM

[26] https://www.youtube.com/watch?v=4Use1n8zGmM

[27] https://orangecyberdefense.com/global/wp-content/uploads/sites/12/2020/04/Orange_Cyber_Before_the_bubble_bursts_Whitepaper.pdf

[28] https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

[29] https://www.csoonline.com/article/3603519/SolarWinds-hack-is-quickly-reshaping-congress-s-cybersecurity-agenda.html

[30] https://www.brookings.edu/blog/techtank/2021/01/11/after-the-SolarWinds-hack-the-biden-administration-must-address-russian-cybersecurity-threats/

[31] https://www.whitehouse.gov/presidential-actions/executive-order-taking-additional-steps-address-national-emergency-respect-significant-malicious-cyber-enabled-activities/

[32] https://www.lawfareblog.com/cyber-deterrence-brexit-analogy

[33] https://hbr.org/2020/10/does-your-cyber-insurance-cover-a-state-sponsored-attack

[34] https://www.zdnet.com/article/dhs-issues-directive-to-pull-government-use-of-kaspersky-lab-software/

[35] https://taosecurity.blogspot.com/2017/03/five-reasons-i-want-china-running-its.html

[36] https://sensepost.com/blog/2011/from-the-international-conference-on-cyber-conflict/

[37] https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

[38] https://www.scmagazine.com/home/security-news/cloud-security/SolarWinds-hack-poses-risk-to-cloud-services-api-keys-and-iam-identities/

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Our organization retains a 25+ year track record in information security, 250+ researchers and analysts 17 SOCs, 11 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries. We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Orange Cyberdefense has built close partnerships with numerous industry-leading technology vendors.

We wrap elite cybersecurity talent, unique technologies and robust processes into an easy-to-consume, end-to-end managed services portfolio.

At Orange Cyberdefense we embed security into Orange Business Services solutions for multinationals worldwide. We believe strongly that technology alone is not a solution. It is the expertise and experience of our people that enable our deep understanding of the landscape in which we operate. Their competence, passion and motivation to progress and develop in an industry that is evolving so rapidly.

We are proud of our in-house research team and proprietary threat intelligence thanks to which we enable our customers to focus on what matters most, and actively contribute to the cybersecurity community. Our experts regularly publish white papers, articles and tools on cybersecurity which are widely recognized and used throughout the industry and featured at global conferences, including Infosec, RSA, 44Con, BlackHat and DefCon.

www.orangecyberdefense.com
Twitter: @OrangeCyberDef