A moment of reckoning: the need for a strong and global cybersecurity response

blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/

December 18, 2020

The final weeks of a challenging year have proven even more difficult with the recent exposure of the world's latest serious nation-state cyberattack. This latest cyber-assault is effectively an attack on the United States and its government and other critical institutions, including security firms. It illuminates the ways the cybersecurity landscape continues to evolve and become even more dangerous. As much as anything, this attack provides a moment of reckoning. It requires that we look with clear eyes at the growing threats we face and commit to more effective and collaborative leadership by the government and the tech sector in the United States to spearhead a strong and coordinated global cybersecurity response.

The evolving threats

The past 12 months have produced a watershed year with evolving cybersecurity threats on three eye-opening fronts.

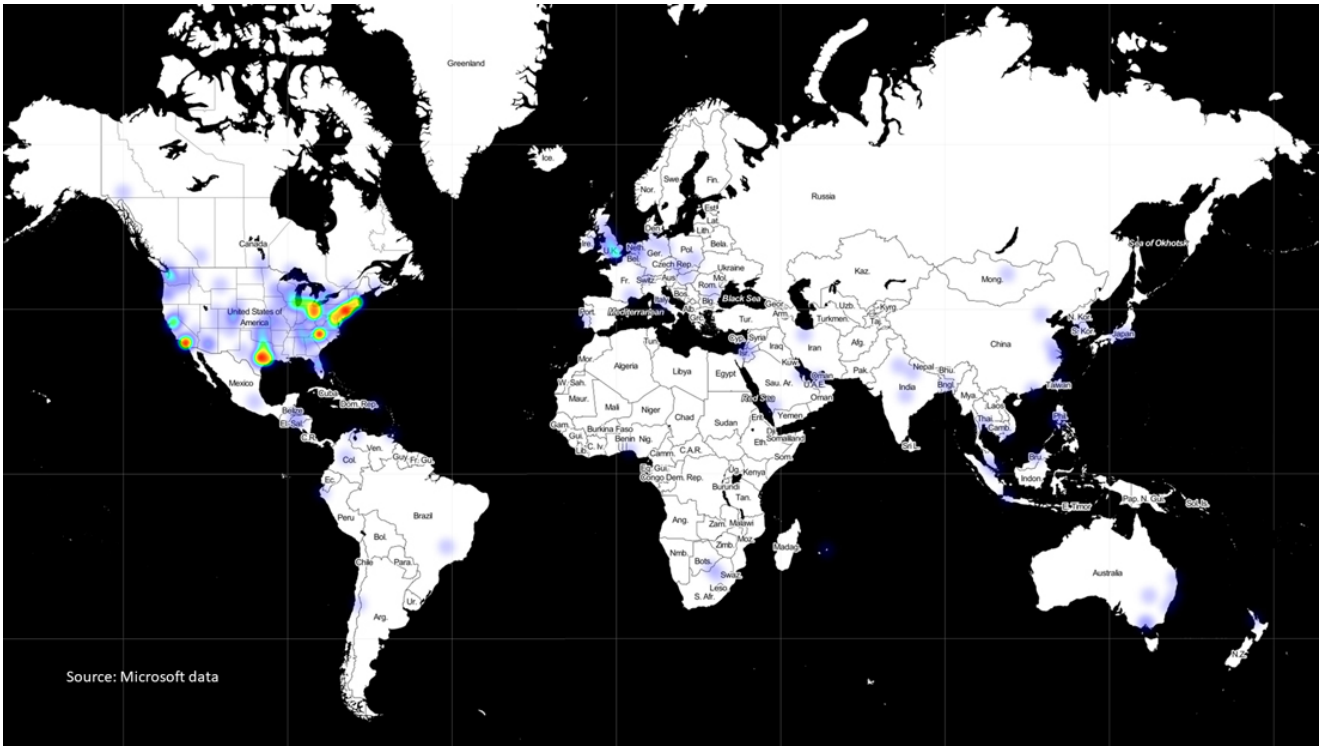
The *first* is the continuing rise in the determination and sophistication of nation-state attacks. In the past week this has again burst into the headlines with the story of an attack on the firm FireEye using malware inserted into network management software provided to customers by the tech company SolarWinds. This has already led to subsequent news

reports of penetration into multiple parts of the U.S. Government. We should all be prepared for stories about additional victims in the public sector and other enterprises and organizations. As FireEye CEO Kevin Mandia stated after disclosing the recent attack, “We are witnessing an attack by a nation with top-tier offensive capabilities.”

As Microsoft cybersecurity experts assist in the response, we have reached the same conclusion. The attack unfortunately represents a broad and successful espionage-based assault on both the confidential information of the U.S. Government and the tech tools used by firms to protect them. The attack is ongoing and is being actively investigated and addressed by cybersecurity teams in the public and private sectors, including Microsoft. As our teams act as first responders to these attacks, these ongoing investigations reveal an attack that is remarkable for its scope, sophistication and impact.

There are broader ramifications as well, which are even more disconcerting. First, while governments have spied on each other for centuries, the recent attackers used a technique that has put at risk the technology supply chain for the broader economy. As SolarWinds has reported, the attackers installed their malware into an upgrade of the company’s Orion product that may have been installed by more than 17,000 customers.

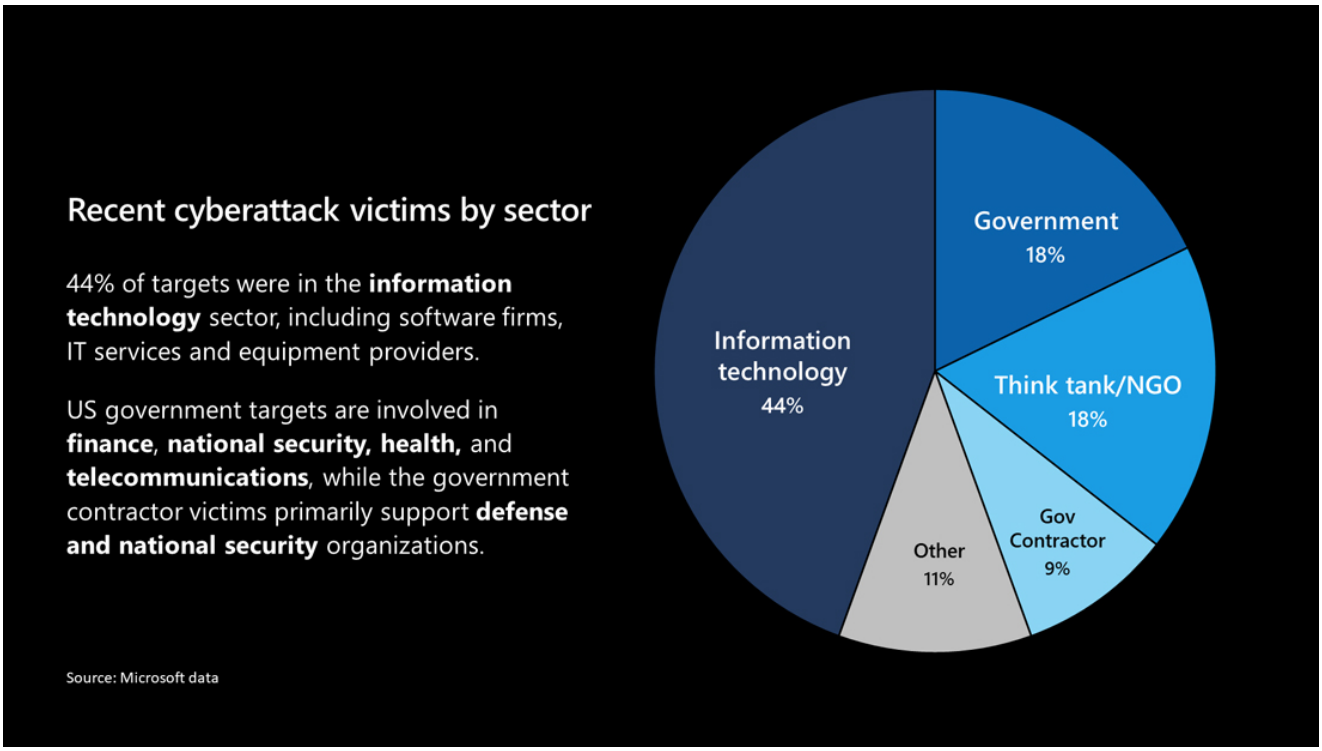
The nature of the initial phase of the attack and the breadth of supply chain vulnerability is illustrated clearly in the map below, which is based on telemetry from Microsoft’s Defender Anti-Virus software. This identifies customers who use Defender and who installed versions of SolarWinds’ Orion software containing the attackers’ malware. As this makes clear, this aspect of the attack created a supply chain vulnerability of nearly global importance, reaching many major national capitals outside Russia. This also illustrates the heightened level of vulnerability in the United States.



The installation of this malware created an opportunity for the attackers to follow up and pick and choose from among these customers the organizations they wanted to further attack, which it appears they did in a narrower and more focused fashion. While investigations (and the attacks themselves) continue, Microsoft has identified and has been working this week to notify more than 40 customers that the attackers targeted more precisely and compromised through additional and sophisticated measures.

While roughly 80% of these customers are located in the United States, this work so far has also identified victims in seven additional countries. This includes Canada and Mexico in North America; Belgium, Spain and the United Kingdom in Europe; and Israel and the UAE in the Middle East. It's certain that the number and location of victims will keep growing.

Additional analysis sheds added light on the breadth of these attacks. The initial list of victims includes not only government agencies, but security and other technology firms as well as non-governmental organizations, as shown in the chart below.



It's critical that we step back and assess the significance of these attacks in their full context. This is not "espionage as usual," even in the digital age. Instead, it represents an act of recklessness that created a serious technological vulnerability for the United States and the world. In effect, this is not just an attack on specific targets, but on the trust and reliability of the world's critical infrastructure in order to advance one nation's intelligence agency. While the most recent attack appears to reflect a particular focus on the United States and many other democracies, it also provides a powerful reminder that people in virtually every country are at risk and need protection irrespective of the governments they live under.

As we have now seen repeatedly, Silicon Valley is not the only home of ingenious software developers. Russian engineers in 2016 identified weaknesses in password protection and social media platforms, hacked their way into American political campaigns, and used disinformation to sow divisions among the electorate. They repeated the exercise in the 2017 French presidential campaign. As tracked by Microsoft's Threat Intelligence Center and Digital Crimes Unit, these techniques have impacted victims in more than 70 countries, including most of the world's democracies. The most recent attack reflects an unfortunate but similarly ingenious capability to identify weaknesses in cybersecurity protection and exploit them.

These types of sophisticated nation-state attacks are increasingly being compounded by another technology trend, which is the opportunity to augment human capabilities with artificial intelligence (AI). One of the more chilling developments this year has been what appears to be new steps to use AI to weaponize large stolen datasets about individuals and spread targeted disinformation using text messages and encrypted messaging apps. We should all assume that, like the sophisticated attacks from Russia, this too will become a permanent part of the threat landscape.

Thankfully, there is a limited number of governments that can invest in the talent needed to attack with this level of sophistication. In our first Microsoft Digital Defense Report, released in September, we reviewed our assessment of 14 nation-state groups involved in cybersecurity attacks. Eleven of the 14 are in only three countries.

All this is changing because of a *second* evolving threat, namely the growing privatization of cybersecurity attacks through a new generation of private companies, akin to 21st-century mercenaries. This phenomenon has reached the point where it has acquired its own acronym – PSOAs, for private sector offensive actors. Unfortunately, this is not an acronym that will make the world a better place.

One illustrative company in this new sector is the NSO Group, based in Israel and now involved in U.S. litigation. NSO created and sold to governments an app called Pegasus, which could be installed on a device simply by calling the device via WhatsApp; the device's owner did not even have to answer. According to WhatsApp, NSO used Pegasus to access more than 1,400 mobile devices, including those belonging to journalists and human rights activists.

NSO represents the increasing confluence between sophisticated private-sector technology and nation-state attackers. Citizen Lab, a research laboratory at the University of Toronto, has identified more than 100 abuse cases regarding NSO alone. But it is hardly alone. Other companies are increasingly rumored to be joining in what has become a new $12 billion global technology market.

This represents a growing option for nation-states to either build or buy the tools needed for sophisticated cyberattacks. And if there has been one constant in the world of software over the past five decades, it is that money is always more plentiful than talent. An industry segment that aids offensive cyberattacks spells bad news on two fronts. First, it adds even more capability to the leading nation-state attackers, and second, it generates cyberattack proliferation to other governments that have the money but not the people to create their own weapons. In short, it adds another significant element to the cybersecurity threat landscape.

There is a *third* and final sobering development worth noting from what has obviously been a challenging year. This comes from the intersection between cyberattacks and COVID-19 itself.

One might have hoped that a pandemic that cut short millions of lives might at least have received a pass from the world's cyberattacks. But that was not the case. After a brief lull in March, cyberattackers took aim at hospitals and public health authorities, from local governments to the World Health Organization (WHO). As humanity raced to develop vaccines, Microsoft security teams detected three nation-state actors targeting seven prominent companies directly involved in researching vaccines and treatments for Covid-19. A crisis always seems to bring out the best and worst in people, so perhaps we should not be surprised that this global crisis was no exception.

Put together, however, these three trends point to a cybersecurity landscape that is even more daunting than when the year began. The most determined nation-state attackers are becoming more sophisticated. Risks are both growing and spreading to other governments through new private sector companies that aid and abet nation state attackers. And nothing, not even a pandemic, is off limits to these attackers.

We live in a more dangerous world, and it requires a stronger and more coordinated response.

A more effective strategy as we enter a new year

Put simply, we need a more effective national and global strategy to protect against cyberattacks. It will need multiple parts, but perhaps most important, it must start with the recognition that governments and the tech sector will need to act together.

The new year creates an opportunity to turn a page on recent American unilateralism and focus on the collective action that is indispensable to cybersecurity protection. The United States did not win World War II, the Cold War or even its own independence by fighting alone. In a world where authoritarian countries are launching cyberattacks against the world's democracies, it is more important than ever for democratic governments to work together – sharing information and best practices, and coordinating not just on cybersecurity protection but on defensive measures and responses.

Unlike attacks from the past, cybersecurity threats also require a unique level of collaboration between the public and private sectors. Today's technology infrastructure, from data centers to fiberoptic cables, is most often owned and operated by private companies. These represent not only much of the infrastructure that needs to be secured but the surface area where new cyberattacks typically are first spotted. For this reason, effective cyber-defense requires not just a coalition of the world's democracies, but a coalition with leading tech companies.

To be successful, this coalition will need to do three things more effectively in the future:

***First*, we need to take a major step forward in the sharing and analysis of threat intelligence.** In a new year that will mark the 20th anniversary of 9/11, we should remember one of the lessons from the tragic day that the 9/11 Commission called "a shock but not a surprise." A recurring theme of the commission's findings was the inability across government agencies to build collective knowledge by connecting data points together. The commission therefore focused its first recommendation on "unifying strategic intelligence" and moving from the "need to know" to the "need to share."

If there is an initial question for the incoming Biden-Harris Administration and America's allies, it is this: Is the sharing of cybersecurity threat intelligence today better or worse than it was for terrorist threats before 9/11?

In the wake of this most recent attack, perhaps no company has done more work than Microsoft to support agencies across the federal government. As much as we appreciate the commitment and professionalism of so many dedicated public servants, it is apparent to us that the current state of information-sharing across the government is far from where it needs to be. It too often seems that federal agencies currently fail to act in a coordinated way or in accordance with a clearly defined national cybersecurity strategy. While parts of the federal government have been quick to seek input, information sharing with first responders in a position to act has been limited. During a cyber incident of national significance, we need to do more to prioritize the information-sharing and collaboration needed for swift and effective action. In many respects, we risk as a nation losing sight of some of the most important lessons identified by the 9/11 Commission.

One indicator of the current situation is reflected in the federal government's insistence on restricting through its contracts our ability to let even one part of the federal government know what other part has been attacked. Instead of encouraging a "need to share," this turns information sharing into a breach of contract. It literally has turned the 9/11 Commission's recommendations upside down.

It will be critical for the incoming Biden-Harris Administration to move quickly and decisively to address this situation. One ready-made opportunity is to establish a national cybersecurity director as recommended by the Solarium Commission and provided for in the National Defense Authorization Act.

Effective progress will also require a second realization that goes beyond anything the 9/11 Commission needed to confront. Cybersecurity threat intelligence exists in even more disconnected silos than more traditional information about national security threats. This is because it is spread not only among different agencies and governments but across multiple private sector companies as well. Even within a large company like Microsoft, we have learned that it is critical for our Threat Intelligence Center to aggregate and analyze data from across our data centers and services. And when there is a major threat, we need to share information and collective assessments with other tech companies.

Recent years have brought several important steps to better share cybersecurity information, and we greatly appreciate the dedication and support of many key people across the U.S. government. But we still lack a formal and cohesive national strategy for the sharing of cybersecurity threat intelligence between the public and private sectors. While there need to be important safeguards to protect government secrets and private citizens' privacy, the time has come for a more systemic and innovative approach to the sharing and analysis of threat intelligence with those best positioned to act.

***Second*, we need to strengthen international rules to put reckless nation-state behavior out of bounds and ensure that domestic laws thwart the rise of the cyberattack ecosystem.** While the world has important international norms and laws to address nation-state attacks, we continue to believe it is important to fill in gaps and continue to develop clear and binding legal obligations for cyberspace.

This should build on the lessons of 2020 and prioritize key and specific areas. For example, it should include the continued development of rules to expressly forbid the type of broad and reckless activity used against SolarWinds and its customers, which tampered with legitimate software and threatened the stability of a broader software supply chain. The international community has been moving in this direction, building on a 2015 report by a United Nations Group of Governmental Experts that received broad UN endorsement last year, as well as multi-stakeholder support by the Global Commission on the Stability of Cyberspace (GCSC). The U.S. government and its allies need to make crystal clear their views that this type of supply chain attack falls outside the bounds of international law.

We need similar strong and effective endorsements of rules that put attacks on health care institutions and vaccine providers off limits. (The recently convened Oxford Process has done important work to highlight the protections existing international law affords in this context.) And international rules should include stronger protections of democratic and electoral processes, as reflected in the principles of the Paris Call for Trust and Security in Cyberspace, which now has more than 1,000 signatories – the largest multi-stakeholder group ever assembled in support of an international cybersecurity-focused agreement.

In addition, governments should take new and concerted steps to thwart the rise of private sector offensive actors. As described above, these companies in effect have created a new ecosystem to support offensive nation-state attacks. The sooner governments take action to

put this ecosystem out of business, the better.

An early opportunity for the Biden-Harris Administration will come in an appellate judicial case involving the NSO Group itself. NSO has appealed a lower court finding that it is not immune from claims that it violated the U.S. Computer Fraud and Abuse Act by accessing mobile devices without permission. Its argument is that it is immune from U.S. law because it is acting on behalf of a foreign government customer and hence shares that government's legal immunity. NSO's proposed recipe would make a bad problem even worse, which is why Microsoft is joining with other companies in opposing this interpretation. The Biden/Harris Administration should weigh in with a similar view.

NSO's legal approach, while disconcerting, does the world a service by highlighting the path needed to thwart this new cyberattack ecosystem. It's to ensure that domestic laws clearly and strongly prohibit companies from helping governments engage in unlawful and offensive cyberattacks and investors from knowingly financing them.

Consider the analogy to other forms of societally harmful activity, like human trafficking, narcotics or terrorism itself. Governments not only take strong steps to prohibit the illegal activity itself – such as engaging in drug trafficking – but also ensure that airlines don't transport the drugs and investors don't finance the activity.

A similar approach is needed to deter private sector offensive actors. We need steps to ensure, for example, that American and other investors don't knowingly fuel the growth of this type of illegal activity. And the United States should proactively pursue discussions with other countries that are giving rise to these companies, including Israel, which has a strong cybersecurity ecosystem that can be drawn into dangerous support of authoritarian regimes.

***Finally*, we need stronger steps to hold nation-states accountable for cyberattacks.** Governments and private companies have taken stronger steps in recent years to hold nation-states publicly accountable for cyberattacks. We need to build on this course and continue to press forward with it, with governments ensuring that there are greater real-world consequences for these attacks to promote stability and discourage conflict.

The world's democracies took important steps in 2017 and 2018, led by the United States. With public statements about WannaCry and NotPetya, multiple governments attributed these attacks publicly to the North Korean and Russian governments, respectively. These types of coordinated public attributions have become an important tool to respond to nation-state attacks. The United States followed with stronger deterrent steps to protect the 2018 mid-term elections, and an even more concerted effort to successfully deter foreign tampering with voting in the 2020 Presidential elections.

In the private sector, circumstances have also changed dramatically since the early days in 2016 when we at Microsoft took legal action to thwart Russian cyberattacks on American political campaigns but were reluctant to speak publicly about it. In the years since,

companies such as Microsoft, Google, Facebook and Twitter have all acted and spoken directly and publicly when responding to nation-state cyberattacks. Moreover, a coalition of more than 145 global technology companies have signed on to the Cybersecurity Tech Accord – committing themselves to upholding four principles of responsible behavior to promote peace and security online, including opposing cyberattacks against innocent civilians and enterprises.

The coming months will present a critical test, not only for the United States but for other leading democracies and technology companies. The weeks ahead will provide mounting and we believe indisputable evidence about the source of these recent attacks. It will become even clearer that they reflect not just the latest technology applied to traditional espionage, but a reckless and broad endangerment of the digital supply chain and our most important economic, civic and political institutions. It is the type of international assault that requires the type of collective response that shows that serious violations have consequences.

If there is a common lesson from the past few years, it's the importance of combining ongoing learning with new innovations, greater collaboration, and constant courage. For four centuries, the people of the world have relied on governments to protect them from foreign threats. But digital technology has created a world where governments cannot take effective action alone. The defense of democracy requires that governments and technology companies work together in new and important ways – to share information, strengthen defenses and respond to attacks. As we put 2020 behind us, the new year provides a new opportunity to move forward on all these fronts.

Editor's note: 12/17/2020, 7:50pm PT

Following news reports about the impact on Microsoft of the SolarWinds issue, the company issued the following statement:

"Like other SolarWinds customers, we have been actively looking for indicators of this actor and can confirm that we detected malicious SolarWinds binaries in our environment, which we isolated and removed. We have not found evidence of access to production services or customer data. Our investigations, which are ongoing, have found absolutely no indications that our systems were used to attack others."

Tags: COVID-19, cyberattacks, cybersecurity, Defending Democracy Program, ElectionGuard