RAPID7

2021 Technology Industry Cyber Threat Landscape Report

Cyber Threat Landscape

Coming off a global pandemic that dispersed the workplace and further drove cloud and third-party services adoption, technology companies are faced with never-before-seen challenges. For most, there is no "new normal" but rather the ongoing progression of a hybrid network environment where physical and virtual assets operate in tandem. This blurred line of demarcation has not gone unnoticed by threat actors.

Regulatory bodies are also taking notice of the cyber threat landscape, particularly within the technology company supply chain. Technology companies must be prepared to show solid proof of compliance with specific mandates, as well as a significantly enhanced effort to follow cybersecurity best practices. When this has not been the case, as in several recent third-party exploits, precedent-setting rulings and fines have been the result.

This report gathers the latest information on threats to the technology industry and the valuable data traversing its systems. Read on to learn:

- How the SolarWinds supply chain attack impacted regulatory activity
- Why China's APT groups are a significant threat vector
- What MSPs must do to protect the technology companies they serve
- How intellectual property and other confidential business information gets leaked
- Where to look for holes in BYOD and remote workforce processes

The Threat Landscape of the Technology Industry

The technology industry is a top target for both cybercriminals and state-sponsored cyber espionage groups. Attacks on technology companies can affect organizations in other industries, as well as individual consumers, because so many organizations and individuals rely on them. Network breaches of technology companies often facilitate third-party and supply chain attacks on organizations in other industries that use their products or services. Furthermore, data breaches at technology companies often expose consumers' personal information. Technology companies may also be more vulnerable to attack during and after the COVID-19 pandemic due to their often higher proportions of remote workers.

One of the most important use cases for attacks on technology companies is to enable third-party compromises of their enterprise customers via software updates, trusted access, or other supply chain or infrastructure channels. The recent SolarWinds supply chain attack campaign is merely the most high-profile and high-impact example of such attacks; both criminals and state-sponsored actors have been conducting these campaigns for years. Technology companies also have intellectual property or other confidential business information, such as source code, that both criminals and state-sponsored actors seek for financial or economic reasons, or to enable further attacks.

In addition to the above, technology companies are useful as sources of bulk customer data, such as the personally identifiable information (PII) of individual consumers, for both criminals and state-sponsored actors. The recent disclosures of massive amounts of PII scraped from Facebook and LinkedIn are perhaps among the largest examples of the value of technology companies as sources of such data.

Despite the attribution of the SolarWinds campaign to state-sponsored Russian actors, Chinese cyber espionage groups – specifically, APT10, APT17, and APT41 – have historically been the most significant practitioners of supply chain attacks, both in general and via compromised technology companies in particular. China's huge economy and global market share give it significant advantages in conducting supply chain attacks. In many of these cases, however, it is unclear if or how this advantage might or might not have enabled or facilitated supply chain attacks via breaches of technology companies outside mainland China. Indeed, technology companies in Taiwan, which mainland China views as both a renegade province and a major economic competitor, appear to be a significant target in attacks on the technology industry in general, including supply chain attacks.

The SolarWinds campaign brought extended regulatory focus onto the global supply chain, as it exposed the growing liability associated with the data flow between the integrated network of businesses and technology. In February, an executive order on securing the supply chain was issued in the US to ensure cybersecurity checks and balances are conducted on risk to the supply chain.

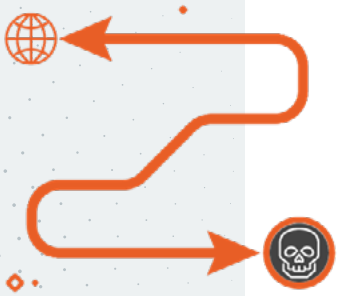
Third-Party and Supply Chain Attacks on Business-to-Business (B2B) Customers

The SolarWinds campaign was the most severe example of a type of third-party attack that had been happening long before that campaign came to light. Threat actors often use compromises of technology companies to infect those companies' customers, such as via software updates or trusted remote access to customer devices or networks. The advantage of this strategy is that it enables attackers to dramatically increase the scale of their operations, infecting numerous customers via a compromise of just one technology company. The trusted or privileged access that many service providers have to customers' networks, such as via specialized software or tools with which to maintain or administer customer infrastructure, can also facilitate intrusions into networks that might otherwise be harder to breach. Compromised software updates, **as in the case of SolarWinds**, also provide a way to evade detection by disguising or bundling malicious code with legitimate software.

For example, the Chinese APT17 conducted at least two supply chain attacks via compromised software from technology companies to deliver ShadowPad malware in 2017. In the first campaign, APT17 **infected enterprise networks via compromised versions of software from Netsarang,** which specializes in server management and security connectivity software. Later that year, APT17 also **used compromised versions of the CCleaner computer optimization software to infect targets** – specifically, users at other technology companies.

Attackers also seek access to technology companies' source code in order to facilitate further attacks. In the case of the SolarWinds campaign, Microsoft indicated that the **attackers had gained access to some of its Azure, Intune, and Exchange source code.** This exposure of source code could have enabled the attackers to analyze the source code for vulnerabilities that researchers and other attackers have not yet identified. APT17's **"Operation Aurora" campaign that targeted Google, Adobe, and other technology companies** went further in targeting those companies' source code management systems, which would have enabled the attackers to alter source code so as to enable supply chain compromises.

The code signing certificates of software companies are another valuable target within the technology industry, particularly for state-sponsored threat actors **such as the Chinese APT41**. They can add stolen code signing certificates to their malware payloads in order to increase their ability to evade detection, as the malware will appear to have come from the legitimate issuer of the compromised certificate. The use of stolen code signing certificates is more typical of state-sponsored cyber espionage groups, which generally go to greater lengths than criminals to prevent the detection and attribution of their attacks.



Managed service providers (MSPs) are another popular infection vector for third-party attacks. Chinese cyber espionage groups pioneered this strategy of targeting MSPs and have been among its most prolific practitioners. Indeed, the Chinese APT10, also known as Stone Panda, MenuPass, POTASSIUM, RedLeaves, and Red Apollo, **specializes in the use of compromised MSPs as an attack vector** against MSP customers in other industries. The group also **targeted cloud service providers in its "Cloud Hopper" campaign.** The impact of APT10, which has been active since 2006, and its attacks were such that **the U.S. Department of Justice indicted APT10 members** in 2018.

Compromised MSPs have also become a popular vector for ransomware attacks on their enterprise customers. **Operators of the GandCrab ransomware family became early adopters of this strategy** in early 2019, and operators of other ransomware families subsequently followed suit. Third-party attacks via MSPs or other technology companies are especially productive for ransomware operators because the success of their business model depends in part on the number of victims that they infect. Only a fraction of ransomware victims pay ransoms, so increasing the number of infected victims increases the number of ransom payments that ransom operators can collect. Ransomware operators typically infect the customers of compromised MSPs via specialized tools that provide the trusted access to customer networks that they use in order to provide their services.

Breaches of other specialized technology companies can enable attacks on their B2B customers, as well as the business-to-consumer (B2C) customers of those enterprises. For example, breaches of domain registrars can enable DNS hijacking attacks, such as those of the Iranian cyber espionage campaign "**DNSpionage**." In this 2017-2019 campaign, the attackers **gained access to the infrastructure of domain registrars** via compromised credentials. They used that unauthorized access to redirect traffic for enterprise customers' domains to infrastructure under the attackers' control, which they disguised as that of the targeted customers. The attackers used that infrastructure to compromise the credentials of users logging into what they mistakenly believed to be their organizations' real infrastructure.

The widespread use of third-party payment form code on e-commerce websites has made the technology companies that provide such code targets for operators of digital payment card skimmers. Digital payment card skimmers are the software equivalent (often in the form of scripts) of the hardware payment card skimmers that criminals historically installed in ATM and point-of-sale (PoS) card slots to collect payment card details. Digital skimmers perform a similar function virtually, collecting and transmitting the payment card details of customers who enter them into an e-commerce website or the online payment forms of businesses. Many websites use third-party code for their payment forms, making the companies that develop and provide such code **desirable targets for criminals to inject their skimmer scripts** into them, in another type of supply chain attack.

Malvertising, or malicious advertising, can affect any business that advertises itself on external websites or has external advertisements on its own website, as well as online advertising companies themselves. Malvertising historically served as an important attack vector, particularly for criminal campaigns delivering payloads of commodity malware, such as banking Trojans, loaders for second-stage payloads, or ransomware. The significance of malvertising has declined in conjunction with the decline of exploit kits, to whose landing pages malvertising campaigns historically redirected victims in order to infect their devices. Malvertising campaigns can nonetheless still achieve a variety of other malicious objectives, such as social engineering prompts to install disguised malware or to become the target of a tech support call scam. While malvertising attackers often purchase their own online advertisements via legitimate channels, they can also **compromise the infrastructure of online advertising companies** in order to inject malicious code into others' legitimate advertisements.

The Theft of Intellectual Property and Other Confidential Business Information

Intellectual property is a common target for attacks on enterprise networks, including those of technology companies. The most typical form of intellectual property for attackers to steal from a technology company is the source code of its software. Criminals can sell compromised source code in dark web forums and marketplaces for profit. State-sponsored threat actors, particularly those in China, may also seek source code or other intellectual property from their foreign competitors for the benefit of their own businesses, particularly Chinese state-owned enterprises. The Chinese **APT41 has stolen the source code of foreign video game companies,** but it is possible in this case that the actors did so for their own criminal financial gain on the side, rather than on behalf of the Chinese government. Competitors, whether state-owned or private, may also use compromises of technology companies to collect competitive intelligence with which to outmaneuver competitors in the marketplace.

Hardware manufacturers can also become targets of intellectual property theft. For example, the Chinese cyber espionage group "Chimera" **targeted competing Taiwanese semiconductor manufacturers** in "Operation Skeleton Key" in order to steal their intellectual property. Taiwan is not only a breakaway province in the eyes of the mainland Chinese government, but also a market leader in the semiconductor business and thus a valuable target for mainland Chinese competitors.

The rise of data disclosure as an additional layer of extortion in ransomware attacks on enterprise networks poses the added risk of exposing technology companies' intellectual property. This risk can become a reality not only in ransomware attacks on the companies themselves, but also in ransomware attacks on manufacturers, suppliers, vendors, and other third parties. For example, in April 2021, operators of the REvil ransomware family claimed to have **breached Taiwan-based Quanta Computer,** a supplier for Apple. The attackers timed their initial disclosure of what they described as Apple intellectual property, such as Macbook schematics, to coincide with an Apple product launch in order to maximize the potential business and reputational impact of the disclosure. Quanta confirmed that it had experienced an incident but provided few details beyond its refusal to pay ransom. The attackers sought payment from Apple itself, threatening to disclose more Apple intellectual property.

DDoS

Online gaming and entertainment companies are particularly desirable targets for distributed denial of service (DDoS) attacks due to the vulnerability of their businesses to disruptions in service. These companies may experience widespread customer complaints and dissatisfaction, and perhaps lose revenue, if and when their services go offline due to a DDoS attack. Attackers can use that pressure to coerce targets into making extortion payments. Additionally, gaming companies in particular can be targets of attackers with non-financial motivations, such as cheating against competing players by knocking them offline, or protesting the rules or other features of an online game.

Similarly, streaming services for video or audio entertainment content can become targets of DDoS attacks due to the lower tolerance of their business model and customers for downtime. One such streaming service became a target of an unusually large attack for 13 days in spring 2019, using over 402,000 infected devices, possibly from the Mirai Internet of Things (IoT) botnet. The attackers tried to disguise their attack as legitimate traffic with a User Agent string from the company's app.

Data is becoming increasingly valuable, and its use across integrated business networks more diverse. Over time, the liability associated with using data has grown substantially as new data privacy legislation has been created and existing mandates enhanced. This is happening in an effort to define the boundaries of use as well as the responsibilities of those who use personal data for business, including the practitioners and technologies that collect and process it.

Product Security Issues

"Internet of Things" (IoT) devices are popular targets for criminal malware operations, particularly those involving botnets that criminals use for DDoS or brute force attacks, or other malicious purposes. These devices frequently do not receive the same level of security support and hygiene as desktops, laptops, or mobile phones, making them easier and thus more desirable targets for criminal botnet operators. Users frequently leave them vulnerable to compromise by failing to change easily guessed default passwords or update old, vulnerable, and exploitable firmware. The most common negative impact of a compromised IoT device is increased bandwidth consumption from attackers' use of the device for DDoS or brute forcing. Compromised IoT devices can nonetheless serve as initial points of access from which attackers can move laterally into a wider network. For example, a **breach of a North American casino's network** began with the compromise of an IoT device that monitored the temperature, hygiene, and food supply of a fish tank.

Pre-installed and automated update utilities can mitigate the unfortunate tendency of many users to fail to update their devices. Attackers can, however, use pre-installed and automated update utilities in supply chain attacks to deliver malware in ways that increase their ability to evade detection. For example, in early 2019, it emerged that the Chinese APT41 had used a **malicious version of the ASUS Live Update utility** on computers from Taiwan-based ASUS to infect ASUS computer users. APT41 signed those malicious payloads with compromised code signing certificates in order to increase its ability to evade detection, as that group has done in other attacks.

Compromising the PII, Other Data, and Accounts of Business-to-Consumer (B2C) Customers

The recent disclosure of massive amounts of PII from scraping attacks on **Facebook** and **LinkedIn** highlighted the degree to which compromises and vulnerabilities can expose consumer data. In the case of the Facebook and LinkedIn data dumps, the exposure of users' phone numbers and email addresses provides an abundance of targets for spam and phishing campaigns. Attackers could use publicly visible information on the associated Facebook and LinkedIn profiles to craft social engineering lures to which targets are more likely to respond. Those Facebook and LinkedIn profiles could also provide personal details that attackers could use in attempts to compromise users' email addresses in password reset attacks by providing answers to their security questions. The combination of phone numbers and email addresses from these leaks may also facilitate SIM swapping attacks against SMS-based 2FA users by revealing which phone numbers to target in an attack on a given user. The leak of LinkedIn data poses a particular risk to enterprises because attackers could target employees' personal accounts and devices in attempts to gain access to their employers' infrastructure. Gaining access to enterprise infrastructure via employees' personal accounts and devices has become a more viable strategy in the wake of the COVID-19 pandemic and the shift to remote work, often from personal devices.

The Facebook and LinkedIn breaches could have significant impact even though they did not include more sensitive data points, such as passwords, payment card details, dates of birth (DOBs), and (for US users) Social Security numbers (SSNs). User data breaches at technology companies that include these more sensitive data points can have significant impact by enabling account takeovers, payment card fraud, and identity theft. DOBs and SSNs are prized PII data points among fraudsters because their potential to enable identity theft makes them a lucrative investment in the longer term.

Organizations in non-technology industries, such as **healthcare** and **telecommunications,** are usually better sources of DOBs or SSNs than technology companies, although some technology companies may collect customer DOBs for age verification or other purposes. Most users of a technology company's products and services will, however, have passwords paired with email addresses that they used to register their accounts. Technology companies that charge for their products and services may also store payment card details, which are a top commodity in underground criminal marketplaces.

Customer data breaches at technology companies can be and often are productive sources of credential combinations that enable further attacks on consumer accounts on other websites and services. Criminals circulate lists of pairs of email addresses and passwords for use in credential stuffing attacks, in which they try those same credential pairs on other websites and services. These attacks exploit the unfortunate tendency of many users to use the same combination of email addresses and passwords across multiple websites. Even if only a small percentage of affected users reuse their passwords, the often large numbers of affected users can yield a significant return on investment (ROI) for credential stuffing attackers. Automated credential stuffing tools make this strategy efficient and cost effective.

Consumers' compromised email and social media accounts are also useful for phishing attacks on other users. These attacks may be more likely to succeed if they come from compromised legitimate accounts, rather than accounts that threat actors created themselves for the purpose of attacks. The contacts of the legitimate owners of compromised accounts may be more likely to open any malicious links or attachments that they believe to have come from the legitimate owners. The older age and the legitimate history of compromised accounts may also subject them to less scrutiny from the security teams of the technology companies that provide these services than new accounts that attackers create.

State-sponsored cyber espionage groups that target citizens of their own countries, such as those of Iran and China, may target the technology services and platforms that their domestic cyber espionage targets use in order to monitor them. For example, a 2011 compromise of the Dutch certificate authority DigiNotar **enabled Iranian cyber espionage actors to compromise the Gmail accounts of 300,000 Iranian users.** The attackers fabricated SSL certificates that they used to compromise targeted users' credentials in man-in-the-middle (MITM) attacks when they logged into Gmail. Iranian actors have also **spoofed and compromised VPN and proxy software** that Iranian dissidents use to evade pervasive Internet surveillance and censorship in order to infect such users with disguised or bundled malware.

The Risks of a Remote Workforce

Technology companies may be more vulnerable than others to a broader shift in the threat landscape as a result of the COVID-19 pandemic. The rise of remote work in the wake of the pandemic has made many organizations more vulnerable by transforming their attack surfaces in ways that are advantageous to attackers. Technology companies are more likely to embrace remote work and often have higher proportions of remote employees, increasing their exposure to these heightened risks.

The home routers that remote employees use to access the internet are an often-neglected point of initial access for attackers. Many home router users fail to change their default passwords, which are typically easy for attackers to guess. Furthermore, many home users do not update the firmware on their routers. Old firmware versions leave these routers vulnerable to exploitation if vulnerabilities in those firmware versions have emerged since the last updates.

Compromised home routers are popular targets for incorporation into DDoS botnets. There are nonetheless many other malicious uses for compromised routers that can have more significant impacts on the employers of remote workers. Attackers can infect connected endpoints with malware, collect network traffic via packet capture (PCAP), or conduct DNS hijacking attacks. Malware infections of devices from which remote employees work can of course compromise enterprise accounts and data. PCAP of remote employees' unencrypted network traffic can also expose enterprise data. DNS attacks can compromise enterprise credentials if attackers redirect traffic meant for the enterprise's domain to their own infrastructure. DNS attackers can capture user credentials with their malicious infrastructure when users try to log into what they mistakenly believe to be their employer's legitimate infrastructure.

"Bring Your Own Device" (BYOD) policies often go hand-in-hand with remote work. BYOD can also increase cyber risk if BYOD devices do not receive the same level of security hygiene and support as enterprise-issued devices. Any such devices that do not have regularly updated endpoint security software or receive regular patches for software vulnerabilities are at much greater risk of compromise. The lack of network security monitoring for many BYOD devices may also enable attackers to gain and expand their access undetected.

The remote access services and software that many remote employees use to access enterprise infrastructure from home are attractive targets for attackers. Furthermore, the unfamiliarity of some of these services and software to some newly remote employees may increase the risk of misconfigurations or other user errors that create opportunities for attackers to compromise them. Virtual Private Networks (VPNs) can protect network traffic but can also be vulnerable to attack via misconfigurations or unpatched software vulnerabilities. Remote Desktop Protocol (RDP) was a popular target before the pandemic, particularly for targeted ransomware attacks on enterprise networks, and often via brute force attacks on RDP credentials. Increased use of RDP by remote employees during the pandemic has thus given attackers more opportunities to pursue this already popular attack vector.

The rise of the remote workforce during the pandemic has fueled a massive increase in the use of videoconferencing software, such as Zoom, and other software that enables communication between employees in different locations. This trend significantly expands the exploitable attack surface simply by forcing communications between employees into an electronic form that cyber attackers can compromise, which might not have been the case if employees were communicating in person. The chat and messaging features of such software also provide another avenue for attackers to send malicious links and files to targeted employees. Attackers can eavesdrop on communications via compromised accounts or by impersonating legitimate users. The phenomenon of "Zoom bombing," in which mischievous intruders disrupt Zoom calls with offensive or otherwise inappropriate content, has received significant media coverage. More subtle but also more alarming from an information security perspective is the risk of intruders using the same techniques for stealthy eavesdropping, rather than obvious disruption. Zoom's use of Chinese infrastructure for encryption keys has raised concerns about the risk of Chinese cyber espionage against Zoom users, although Zoom enables paid users to opt out.

Conclusion and Recommendations

One of the key challenges of any cyber threat intelligence program is to formulate priority intelligence requirements (PIRs) and manage the flow of incoming reports to ensure coverage of the most relevant topics. In the case of the technology industry, Chinese cyber espionage groups stand out as the single most significant threat. They target technology companies both as primary targets in their own right and also as infection vectors for supply chain attacks on those technology companies' customers. Accordingly, technology companies should make Chinese APTs – specifically APT10, APT17, and APT41 – high-priority topics for coverage in their cyber threat intelligence programs.

The popularity of MSPs as a conduit for delivering ransomware to their enterprise customers is important to consider from a regulatory perspective. MSPs and the vendor technology they use can no longer afford to ignore the business use of data they consume; or rather, they need to consider having a conclusive data collection and use policy that can be aligned with adequate safeguards against the regional regulatory policy or data-focused compliance regulations that are in place to protect data. Since MSPs and their underlying technology have become a target, many data protection laws and mandates require a high-level risk assessment or basic attestation of the technology that these MSPs use to collect security information, especially if it includes any data that is classified or covered by a local or national data protection policy.

Threats to technology companies pose risks to organizations in other industries that use their products and services. Those threats enable attackers to compromise targets outside the technology industry through the technology products and services that they use. All organizations should thus establish and maintain third-party risk programs to assess and mitigate risks stemming from their use of external technology products and services. For example, MSPs are a popular infection vector for attacks on MSP customers. Businesses should consider the risks of outsourcing when deciding whether or not to use MSPs. If they do decide that outsourcing to MSPs is worth the additional layer of third-party risk, they should establish defenses to prevent attackers that have compromised their MSPs from infecting them through the software or tools the MSP uses to maintain or administer their infrastructure. "Zero-trust" security models can serve as useful references in developing such defenses.

Technology companies should identify key assets that attackers are most likely to target in attempts to infect or otherwise harm them and provide additional layers of defense around those targets. Source code is a high-value target for attackers of technology companies, as they can: sell it; threaten to expose it if they do not receive ransom payments; study it for as-yet unidentified vulnerabilities; or alter it to include their own malicious code. Code signing certificates are another high-value target for threat actors, particularly those of state-sponsored cyber espionage groups, that seek to evade detection in attacks on other targets. Software update infrastructure is another key target, as its compromise can enable attackers to disguise their own malicious code by bundling it into legitimate software updates. MSPs and other technology companies with trusted or highly privileged access to their enterprise customers' networks should also provide additional layers of defense to prevent attackers from compromising whatever software or tools they use to access customer networks. Additional layers of defense for these key assets can include encryption, network segmentation, or supplementary authentication.

Technology companies that have embraced remote work should take steps to mitigate the added risks that it poses. It is worth encouraging employees to practice better security hygiene on their home routers, such as changing default passwords and updating firmware. Companies that have or are considering BYOD policies should assess the additional risks that BYOD poses. If an organization decides to adopt or maintain BYOD policies despite these risks, then it should take steps to ensure more thorough security support for those devices, such as ensuring that they receive security updates and network monitoring coverage. Remote access services, such as RDP and VPNs, warrant special attention due to their popularity as attack vectors. Organizations should disable RDP if they do not need it and require 2FA with strong, unique, and frequently changed passwords if they do need it. VPN installations should receive regular software updates to patch vulnerabilities. VPN users with less technical literacy may benefit from user education designed to prevent exploitable misconfigurations. Organizations that use Zoom for remote communication should take advantage of its security features, such as waiting rooms. Zoom users with paid accounts should opt out of Chinese servers for encryption keys, given the high level of interest in foreign technology companies among Chinese actors.