Recorded Future®

REAL EXAMPLES OF THIRD-PARTY RISK:

LAWSUITS, MILLIONS OF DOLLARS, AND REPUTATIONAL DAMAGE

THE GROWTH OF RANSOMWARE

Third-party vendors are integral to a company's tech stack and business operations, offering everything from human resources management to antivirus solutions. The interdependency between an enterprise and its third-party providers expands the potential attack surface and introduces risk in several ways: cloud storage solutions, internet-of-things (IoT) devices, email clients, IT management, customer service tools, and more.

Cybersecurity incidents are ever-present, and many of these incidents resulted from vulnerabilities in third-party tools. Three third-party risk categories have emerged as the most prominent:

1. Ransomware attacks resulting in data breaches
2. Infrastructure management software
3. Data exposure/breach as the result of misconfigured cloud storage solutions.

As incidents such as the broad-swath SolarWinds attack have illustrated, the ramifications of cyberattacks against infrastructure management software platforms can be disastrous to third-party users. While preventing third-party breaches is out of an organization's control, steps can be taken to manage and mitigate associated risk.

The best way to understand the potential risks your organization faces from third-party risks is to examine real-world cases. Below we are going to explore three notable supply chain attacks and their ramifications to understand how to create better third-party risk management practices.

BLACKBAUD BREACH IMPACTS OVER 200 ORGANIZATIONS

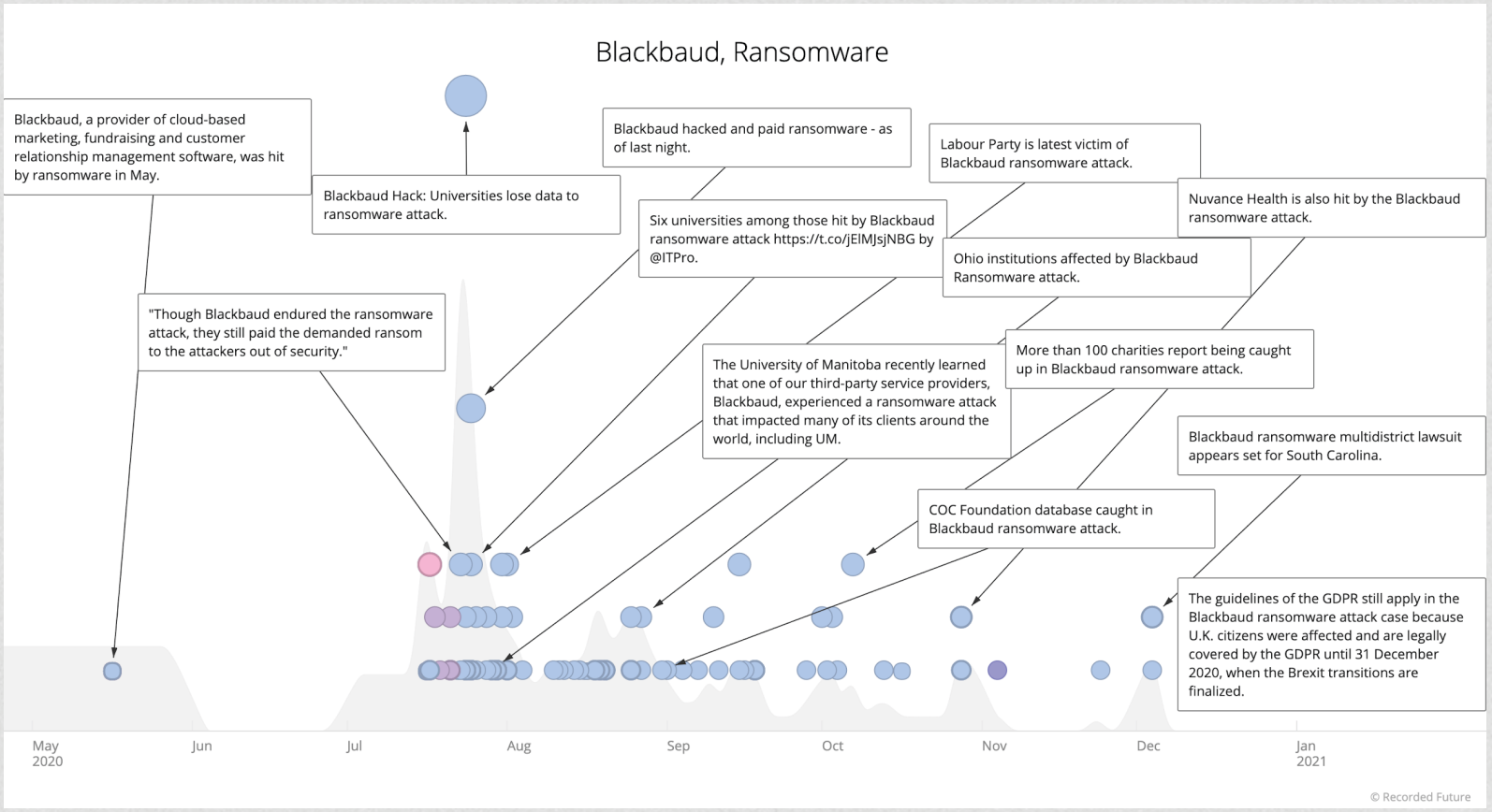

Figure 3: Timeline of Blackbaud ransomware attack and ripple effects 2020 (Source: Recorded Future)

Blackbaud is a South Carolina-based cloud solutions provider that serves the “social good community”, including nonprofits, educational institutions, and healthcare organizations. In a statement the company acknowledged a ransomware attack by an undisclosed variant, claiming that the threat actors were ultimately expelled from the network before a system-wide encryption was completed. However, threat actors were still able to steal a “copy of a subset of data from [their] self-hosted environment”. Blackbaud also paid the demanded ransom with the “confirmation that the [stolen data] had been removed”.

The attack began on February 7, 2020, and lasted until the network intrusion was detected on May 20, 2020. Estimates put the number of impacted individuals at at least 6 million, with compromised records including unencrypted Social Security numbers, banking data, and patient records. The company is now embroiled in at least 23 class action lawsuits (17 in U.S. federal courts, four in U.S. state courts, and two in Canadian courts), and is being accused of negligence, breach of contract, and “unreasonable lack of oversight and lax security measures”.

Outside of reputational damage, the financial cost to Blackbaud has totaled at least $3.6 million in mitigation expenses related to the attack.

RAMIFICATIONS

Outside of reputational damage, the financial cost to Blackbaud has totaled at least $3.6 million in mitigation expenses related to the attack, with $2.9 million recovered from insurance payouts. These figures are independent of the financial outlay required by impacted organizations, which likely total significantly more. Early reports on July 9, 2020 estimated that at least 12 organizations were impacted; this figure grew to at least 125 organizations by July 30, and now totals more than 247.

There has been a pivot in ransomware operational behavior to double-extortion tactics, wherein operators threaten to expose stolen data if the ransom is not paid. This pivot has been accompanied by the rise of dedicated extortion websites run by ransomware operators, such as the “Maze News” site run by Maze ransomware operators.

Due to this operational pivot, if an organization shares sensitive data with a third party, then a ransomware attack on that third party needs to be treated as a data breach. While Blackbaud paid the ransom and the threat actors allegedly removed the stolen data from the extortion site, dozens of Blackbaud customers still had to issue breach disclosures to their own customers.

SOLARWINDS SUPPLY CHAIN ATTACK: AN INTERNATIONAL INCIDENT

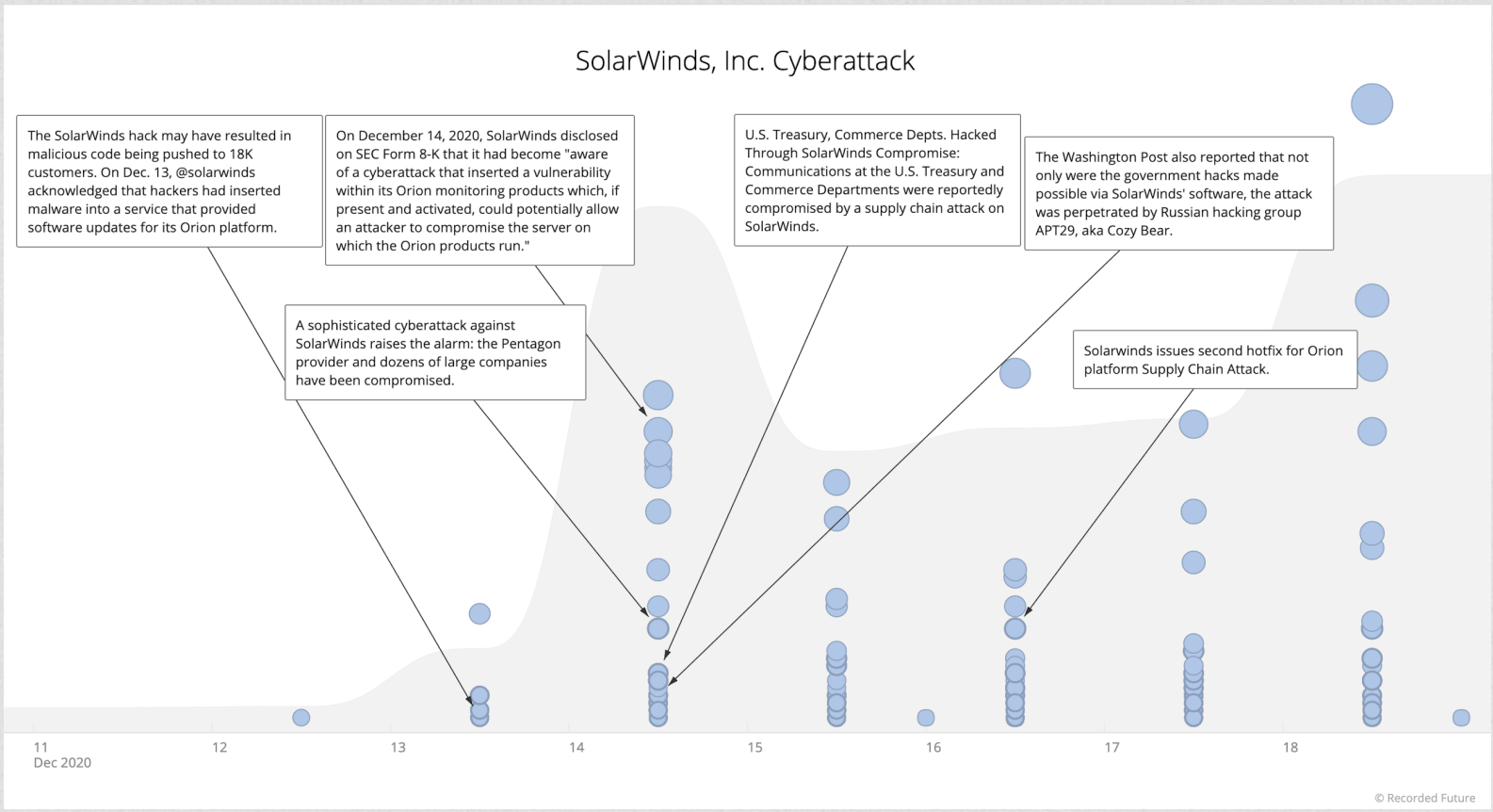

Figure 4: SolarWinds breach notification timeline 2020 (Source: Recorded Future)

On December 13, 2020, the Austin-based company SolarWinds disclosed a software supply chain attack targeting its Orion network infrastructure management platform. SolarWinds indicated that a backdoor, referred to as SUNBURST, was inserted into multiple software updates for the Orion Platform between March and June 2020. SUNBURST remains dormant within a network for up to two weeks and then begins to retrieve and execute commands via its command-and-control (C2) server. Once active, the backdoor can facilitate the deployment of additional malware families used to move laterally and exfiltrate data stored on the network.

SolarWinds has said that roughly 18,000 organizations used the versions of SolarWinds Orion software impacted by SUNBURST, and the number impacted by follow-on intrusion activity was likely "in the dozens".

On January 05, 2021 the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA) issued a joint statement indicating that the software supply chain attack was was "an intelligence gathering effort" by "an Advanced Persistent Threat (APT) actor, likely Russian in origin". The cybersecurity industry has ascribed various identifiers with the threat activity group responsible for the intrusion, including "UNC2452" and "Dark Halo". Open source reporting from the Washington Post reported that the Russian state-sponsored group APT29, also known as "The Dukes", was responsible.

The SolarWinds compromise led to follow-on network intrusions impacting numerous U.S. government agencies, including the U.S. Department of Treasury, Department of Commerce, Department of Homeland Security (DHS), DHS's Cybersecurity and Infrastructure Security Agency (CISA), and the Department of State. Even though 18,000 organizations were potentially impacted by downloading the weaponized Orion update, between 40 and 100 victims of the attack appear to be further compromised by the threat actors, confirming that the threat actors were selective and primarily pursued high-profile targets. SolarWinds has also confirmed that Microsoft Office 365 accounts were compromised.

On December 15, 2020, Microsoft seized the first stage C2 server domain used by SUNBURST, with the goal of forestalling additional intrusions. SolarWinds has also released Orion patches to remove the SUNBURST backdoor. Following public attribution by US government sources, and in response to the software supply chain attack, the Biden administration signed an Executive Order on April 15, 2021 expelling Russian diplomatic personnel, prohibiting US financial institutions from engaging with Russian sovereign debt, and issuing sanctions against several Russian companies supporting the Russian Intelligence Services.

In response to the SolarWinds supply chain attack the US government expelled Russian diplomatic personnel and issued sanctions against several Russian companies.

RAMIFICATIONS

Despite the SolarWinds compromise providing initial access to a large number of organizations, the SUNBURST actors only capitalized on a subset of high-value targets for follow-on activity. The group also attempted to distance these later intrusions from the SolarWinds initial access vector as much as possible in an attempt to reduce the likelihood that the SUNBURST operation would be discovered. Disclosed targets from within the U.S. government, including the U.S. State Department and Homeland Security, lend credence to assessments that espionage was likely among the key goals of the threat actors associated with the intrusion.

The SolarWinds incident exposed just how big of a problem third-party risk is for an entire organization—from CEOs and board members, to PR, Marketing and Sales. This situation showed that even with the best people, processes, and technology in place, there's no guarantee you can always prevent something like this from occurring at your own organization.

MISCONFIGURED CLOUD STORAGE LEADS TO DATA EXPOSURE

Aside from third-party risks that are introduced to an enterprise network courtesy of threat actors, third-party risk can also grow closer to home as the result of improperly configured storage infrastructure hosted in the cloud. Public cloud storage solutions over the past decade have swelled to include Amazon Web Services (AWS) Simple Storage Service buckets (S3), Google Cloud, Microsoft Azure, and Oracle Cloud, to name a few. Other solutions run on top of these mainframe services, such as Snowflake, which runs on AWS. Similarly, Elasticsearch, a scalable big-data search and analytics engine, is often hosted by these providers.

As with all storage, protecting stored goods requires a proper security set-up: just because a door has a lock does not mean it is protected. Within the context of cloud storage, security requires proper configuration of the servers that host data. Misconfiguration (or lack of security configuration) can result in inadvertent data exposure, which can lead to detrimental breaches. The compromise of misconfigured servers can also allow for the insertion of malicious code, such as the payment information sniffer Magecart, further escalating the potential risk to both enterprises and their customers.

A handful of prominent examples follow that illustrate the scale at which data breaches have occurred recently, and the commonality of misconfiguration risk across all cloud storage platforms.

- Town Sports International, a sports fitness chain, inadvertently exposed the personally identifiable information (PII) of over 600,000 customers and staff members through an Amazon Web Services (AWS) misconfiguration. The PII included details like full names and addresses, phone numbers, and incomplete credit card information. The server was left unprotected for nearly a year before a security researcher discovered it on September 21, 2020 and reported it to Town Sports International, who resolved the issue the next day.
- Pfizer, the pharmaceutical organization, kept private medical data for customers, including personally identifiable information and phone transcripts, on a misconfigured Google Cloud storage bucket that could be accessed without usernames or passwords, leaking that data for months or potentially years. The data dated back to October 2018 and was not discovered until July 9, 2020, by researchers at vpnMentor.
- A misconfigured Elasticsearch cluster owned by gaming hardware company Razer resulted in the personally identifiable information of around 100,000 customers being publicly accessible and indexed by search engines. Razer did not fix the misconfiguration for at least three weeks after a security researcher reported it to Razer in August 2020.
- Another misconfigured Elasticsearch server, this one owned by Mailfire, a marketing software organization, resulted in the user data of 70 different dating services and e-commerce apps and websites being leaked. Around 320 million users worldwide had their personally identifiable information, including names, location data, IP addresses, and private conversations exposed and accessible for an unknown length of time before Mailfire was alerted and secured the server on September 3, 2020.

A misconfigured Elasticsearch cluster owned by gaming hardware company Razer resulted in the personally identifiable information of around 100,000 customers being publicly accessible and indexed by search engines.

RAMIFICATIONS

The exposure of company data quickly erodes public and client trust, leading to potentially indelible reputational damage. Stolen data can be used in future malicious activity, such as phishing campaigns, identity theft, or fraud. The data can also be exploited to gain further network access into an enterprise, which can jeopardize proprietary or otherwise sensitive information.

Today's modern businesses rely on cloud providers to store their information. The risk to cloud-storage is further compounded by the fact that the third-parties you share data with are also using cloud providers to store information. As a result of this configuration, the number of threats your organization faces is increased exponentially.

THREE WAYS TO REDUCE THIRD-PARTY RISK

Every enterprise relies on hundreds, if not thousands, of technologies to function at scale, and this extensive tooling results in a broad third-party risk surface. As highlighted in the case studies; the SolarWinds cyberattack gained broad access with the aim of ultimately compromising a handful of targets; conversely, the Blackbaud ransomware attack was narrow in scope and inadvertently impacted hundreds of Blackbaud's clients. Both entities provide infrastructure management software tools designed to be deeply integrated within enterprises. These two examples illustrate the expansive nature of third-party risk from a defender perspective, and how each can lead to infrastructural or vendor trust issues.

However, the cloud misconfiguration risks are closer to home, with enterprises much more in control of security protocols. In an attempt to circumvent third-party cloud storage risks, some enterprises will instead choose to host data themselves, rather than rely on an external provider, such as AWS. While self-hosting data transposes third-party risk to internal information security risk, self-hosting in no way eliminates data security risks. The Blackbaud ransomware attack, which exploited self-hosted data, exemplifies this reality.

The rapidly evolving third-party risk threat landscape requires that security teams be nimble and prepared to deal with potential incidents from all sides. At scale, this is not always feasible, which necessitates prioritization. Although trickle-down effects from third-party security incidents can be quite harmful, these risks are inherently more diffuse than cloud storage solutions selected, built, and managed in-house. Enterprises should audit all third-party storage solutions to confirm that proper configurations and protocols are in place, as well as more broadly audit and monitor for adverse third-party risks.

It is not possible to eliminate all risk, especially when dealing with third-party services, but a strategic defense-in-depth plan can help mitigate risk and reduce uncertainty. When assessing the use of third-party tools or resources, it is important to determine whether this resource is even necessary, in the sense of serving a critical business need, as the use of third-party tools and services increases the threat surface of an organization. If it is deemed necessary, at this point it is important to determine an exchange of responsibilities; that is, if this service can be brought on-premise versus paying an external provider (exchanging the convenience of a third-party provider versus the overhead of IT staff), as well as if that service has various deployment models.

1. DETECTION AND INTRUSION PREVENTION SYSTEMS

For third-party risk mitigation, having intrusion detection systems (IDS) and intrusion prevention systems (IPS) configured and deployed on organization endpoints is helpful to detect any anomalous traffic leaving or entering the firewall. An appropriately configured and monitored endpoint detection system can also help accomplish the task of monitoring anomalous traffic across the firewall boundary. Similarly, packet inspection, as well as internal monitoring with Snort and YARA rules, should be implemented to look for historical and emergent indicators of compromise (IoCs). In some cases, it is helpful to limit the types of outbound traffic allowed out of the firewall to prevent unauthorized exfiltration of data; this can be accomplished through allowlisting approved ports, IP ranges, and domains, or blocklisting undesirable ones, at a minimum. Regular monitoring of logs, and having an automated alerting system in place to monitor logs will also help mitigate the unauthorized exfiltration of data outside of an organization due to breaches in third-party appliances and applications. Alerting on anomalous log activity is critical to quickly remediating a potential threat to the organization.

2. PROTECTING THE CLOUD

When dealing with third-party cloud hosting providers, some best-practice mitigation steps can be established. Access to internally-facing cloud infrastructure should be accomplished only through an allowlist of accepted IP ranges, whenever possible, especially for administration or development purposes. Access should similarly be limited to only those who need it. For Unix-based cloud systems, root-user access should only be granted to users who need it, and authentication should be done through SSH keys rather than passwords. Once inside the cloud infrastructure, enable role-based authentication, and only grant access to users on a need-to-use basis. Organizational passwords to cloud infrastructure should be rotated regularly, and employ the use of a password management system to generate complex passwords.

In all cases, backups are critical to any disaster and recovery plan. Backups should at a minimum be kept off-site and air-gapped. It is important to have redundant backups, ideally a minimum of three full copies, and it is essential to test backups regularly — an untested backup could fail to produce data at a critical time.

3. THIRD-PARTY INTELLIGENCE

An ESG report on third-party risk found that 30% of IT professionals believe cyber risk difficulties are tied directly to increased efforts around third-party risk management. As outlined above this is because of the many different threats posed by third-party relationships. To optimize the process of third-party risk management the report recommends supplementing third-party risk assessments with real-time risk visibility metrics.

“Rather than rely on static manual audits alone, organizations need to collect, process, and analyze TPRM data on a continuous basis. This should include providing threat intelligence for all relevant third parties with a view into infrastructure risk and hacker/activity/chatter on the dark web as well as the ability to employ tunable alerting. This means adopting new tools that enable ubiquitous visibility into third-party risk and can adapt to changes associated with threats and vulnerabilities.”

Employing a third-party intelligence platform provides a real-time view of the cyber risks your third parties face which can potentially place unneeded business or IT security risk to your organization. Comprehensive security intelligence empowers teams to understand, analyze, and take action against potential risks by monitoring for key indicators including data leakage, incident reports, domain abuse, email security, vulnerable infrastructure, web application security, dark web attention, and more.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.