Recorded Future®

Five Critical Third-Party Risks You Need to Monitor

How to find ransomware, data breaches, exposed credentials, and other signs that business partners are placing your organization at risk

Third Parties and You: More Collaboration, More Risk

By increasing collaboration with third parties, forward-thinking enterprises like yours have made remarkable progress in streamlining supply chains, accelerating product deliveries, spurring innovation, increasing efficiency, and lowering costs.

But there is a price to pay for integrating third parties into business processes. You must give them access to information systems that support core functions such as product design, manufacturing, logistics, order fulfillment, and finance. Cybercriminals and hackers know this, and target your partners as potentially pathways into your organization.

In fact, a threat actor who compromises one of your suppliers, contractors, service providers, or resellers has the potential to:

1. Attack your information systems, using credentials acquired from the partner
2. Steal your sensitive information that resides on the partner's systems
3. Disrupt your business by shutting down the partner's operations

What can you do about this?

It certainly helps to have a good third-party risk management program. You can vet potential partners to verify that they have adequate defenses. You might help existing partners deploy effective controls and build security awareness among employees. However, even with the best third-party risk management program, you have to expect that some of your partners will be vulnerable and can't, or won't, inform you (see sidebar).

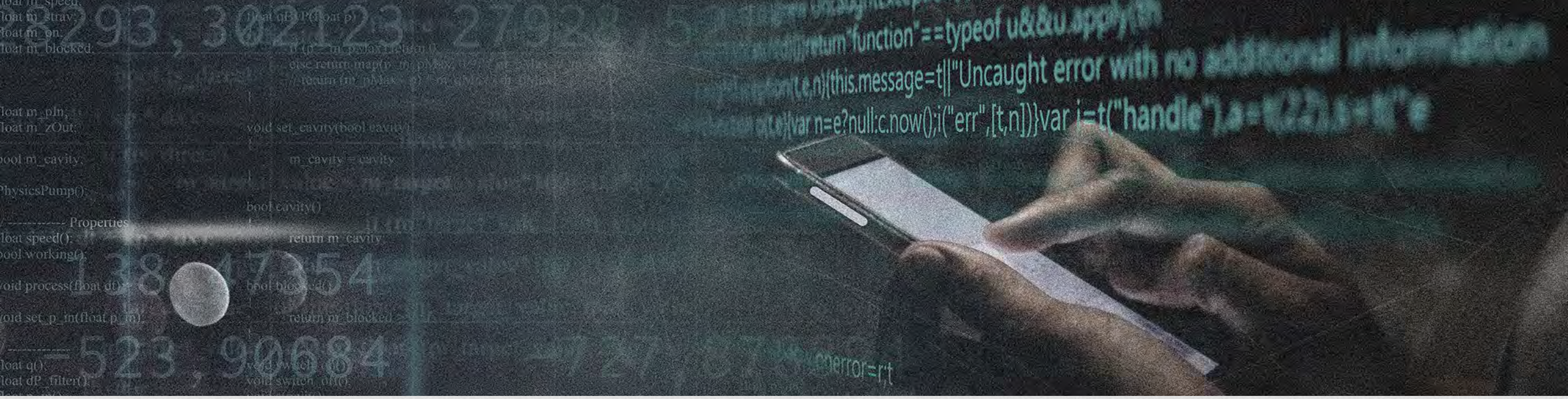
To meet this threat, you can monitor the open web and dark web to find direct evidence that your partners are at risk. You can then:

- Work with the partners to help them block or contain attacks on their systems
- Take measures to mitigate risks to your organization

In this paper we will highlight five critical third-party risks facing your organization, with advice on how to detect and mitigate them.

Partners Don't Know What They Don't Know

Many third-party risk management programs rely on self-reporting. However, although questionnaires about security controls and policies provide much useful information, they don't present a complete picture of an organization's security posture. Respondents have an incentive to stretch the truth a bit. Even more important, many partners lack the knowledge and resources to discover holes in their defenses. As long as they remain in ignorance, they jeopardize your security.



1 Ransomware

Ransomware attacks have been growing dramatically in scope and impact. A few recent attacks have disrupted entire sectors of the U.S. economy. An attack on the Colonial Pipeline system in May 2021 created chaos for gas stations and motorists and significant problems for refineries, airlines, and other industries that produce and consume fuel. The same month, an attack on meat processor JBS sent large segments of the livestock and restaurant industries into disarray.[1]

An example of even more egregious third-party risk on a global scale came to light in July 2021. The REvil cybercrime group infected the software of Kaseya, a company providing a solution to manage workstations and servers in remote locations. Most of the roughly 60 Kaseya customers compromised were managed service providers. Because each service provider was accessing the networks of many customers, REvil was able to launch ransomware attacks against more than 1,500 businesses around the world, and claimed to have encrypted files on more than one million systems.[2]

Recently the cybercrime organizations behind many ransomware campaigns have added a new weapon to their toolbox: "double extortion ransomware." In double extortion ransomware attacks, before malware encrypts data on the victim's systems, it exfiltrates copies to servers controlled by the cybercriminals. The attackers then publish samples of the victim's sensitive information on a ransomware extortion website, together with ransom demands and payment instructions. The threat of exposing intellectual property or sensitive financial and customer data gives the cybercriminals even more leverage in ransom negotiations.

---

[1] ComputerWeekly.com, May 11, 2021: Colonial Pipeline ransomware attack has grave consequences;
The Wall Street Journal, June 11, 2021: Ransomware Attack Roiled Meat Giant JBS, Then Spilled Over to Farmers and Restaurants.

[2] The Record by Recorded Future, July 6, 2021: Kaseya: More than 1,500 downstream businesses impacted by ransomware attack.

Attack on Supplier Threatens Apple with Loss of Product Data

> "On the day Apple was set to announce a slew of new products at its Spring Loaded event, a leak appeared from an unexpected quarter. The notorious ransomware gang REvil said they had stolen data and schematics from Apple supplier Quanta Computer about unreleased products, and that they would sell the data to the highest bidder if they didn't get a $50 million payment. As proof, they released a cache of documents about upcoming, unreleased MacBook Pros. They've since added iMac schematics to the pile... 'Our team is negotiating the sale of large quantities of confidential drawings and gigabytes of personal data with several major brands,' REvil wrote in its post of the stolen data. 'We recommend that Apple buy back the available data by May 1...' By hitting a vendor downstream in the supply chain, attackers give themselves more options about the companies they can extort. Quanta, for example, also supplies Dell, HP, and other large tech companies."

Wired, April 23, 2021: Apple's Ransomware Mess Is the Future of Online Extortion.

If one of your partners is hit by a double extortion ransomware attack, that is definitely bad news for them. However, there is a silver lining for you. If you monitor ransomware extortion websites, you will get early notice that the partner has been compromised. When this happens, you can:

- Assess the nature of your relationship with the organization and determine what sort of response is necessary
- Notify your partner so they can determine which systems have been impacted and isolate them
- Change credentials or cut off VPN access to ensure the attacker can't access your systems
- Identify the type of malware used against the third party and ensure that your defenses can counter it
- Switch to an alternative source to ensure business continuity in case your partner's operations are affected

Speed of response is critical. If you can take action while the negotiations between the attacker and the victim are still going on, you may be able to harden your defenses before the attackers turn their attention to you.

2 Evidence of Data Breaches

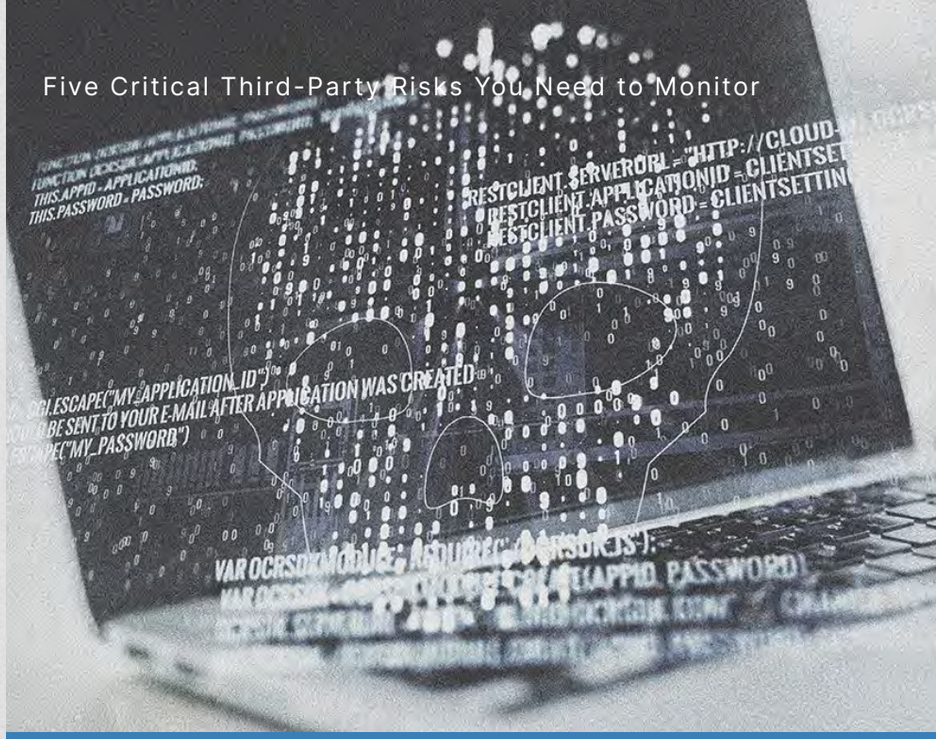
What if your third-party partners are slow to tell you about security incidents? What if it takes weeks or months before they realize they have been breached?

You don't have to remain in the dark. Websites on the open web and dark web can provide evidence that your partners have been compromised. This evidence includes design documents and other intellectual property, personally identifiable information about customers and employees, proprietary software code, and credentials and technical information about the partners' information systems. The information can turn up in dark web marketplaces and on hacker forums, paste sites, and code repositories.

Also, many breaches are disclosed on news sites on the open web and in social media. Of course, you may need extensive language expertise to take advantage of these resources (see sidebar).

If you find any of these indicators that a partner has been compromised, you can:

- Inform your partner so they contain the attack and determine the root causes
- Work with the partner to discover if any of your data was lost in the breach
- Reevaluate the terms of your relationship with the partner, and if necessary, require them to upgrade their security controls and processes



Languages on the Web

W3Techs has estimated that 62% of websites use English, while 38% use another language. The leaders after English are Russian, Turkish, Spanish, Persian, French, German and Japanese. Social media posts contain an even wider spread of languages: according to Internet World Stats, English speakers make up about 26% of internet users, followed by Chinese (19%), Spanish (8%), Arabic (5%), Indonesian/Malaysian (4%), Portuguese (4%), French (3%), and Japanese (3%).

Sources: https://w3techs.com/technologies/overview/content_language and https://www.internetworldstats.com/stats7.htm.

3 Malicious Network Activity

Cyberthreat models such as the Lockheed Martin Cyber Kill Chain® illustrate that advanced cyberattacks involve a lot of network communication between systems controlled by the attacker and the target organizations. Threat actors use servers and bots to send phishing emails that contain malware or links to counterfeit websites that capture credentials. Malware and scripts planted in the target's network create command and control (C&C) channels to exchange information about the victim's environment and instructions on how to find and collect sensitive data. As a final step, captured data is exfiltrated to the attacker's servers.

Many of the servers and bots used by adversaries are "known bad." That is, during investigations of previous attacks their IP addresses have been associated with malicious or suspicious activities. These IP addresses have been collected and published by cybersecurity vendors, industry consortiums, and government agencies, and many enterprises block web traffic between them and their own environment.

But what about monitoring the network traffic of your suppliers, contractors, service providers, and others who have access to your systems? Malicious network activity provides insight into planned and ongoing attacks on third parties. If you find such indicators you can:

- Log the malicious IP addresses and share them with your partner, so they can block traffic to the malicious websites
- Work with the partner to determine if they have already been compromised and to improve their controls to stop spam, malware, and C&C traffic
- Change the partner's credentials for your systems
- Check that you have blocked traffic from your own networks to the malicious websites and that your defenses can counter the attacks being used against the partner

4 Exposed Credentials

You give partners credentials so they can integrate their operations with yours. But credentials are literally “the keys to the kingdom.” Threat actors who obtain credentials to one of your partner’s information systems have the power to steal your information residing there, shut down the partner’s operations, and impersonate the partner to access your systems. Because credentials are so valuable, many attackers make a special effort to find and exfiltrate them during data breaches.

Which brings us to another example of dark clouds with a silver lining.

Cybercriminals have created a niche economy to buy and sell credentials. Some hackers specialize in acquiring credentials through phishing attacks, keyloggers and other malware, social engineering, and password spraying (brute force testing of common passwords). Some data breaches aimed primarily at intellectual property or personal information sweep up credentials at the same time. In both cases attackers may use dark web marketplaces to sell the stolen credentials to other cybercriminals who specialize in advanced attacks. The sellers often provide information about the specific organizations that issued the credentials.

These dark web marketplaces make cybercriminality more efficient. However, you can monitor dark web forums and marketplaces, as well as paste sites, dump sites and other places where stolen credentials are exposed. If you find credentials providing access to one of your partners, you can:

- Offer your findings to the partner so they can disable the accounts with the stolen credentials
- Change the partner’s credentials for your systems
- Help the partner analyze how the credentials were stolen and how similar thefts can be prevented
- Work with the partner to determine if the stolen credentials are being used in an ongoing attack, and if necessary, help them contain the attack

Are Hashed Passwords Safe? Don’t Count on It

If you or a partner hash passwords before storing them in a database, can you be sure that the plaintext versions will never show up for sale on the dark web? Unfortunately, no. For a given password (say, “qwertyuiop”), the same hashing function (say, SHE-256) always gives the same result (in this case, “6eea9b7ef19179a06954edd0f6c05ceb”). Hackers have lists of the hashes of common passwords, so they can go through a file of hashes and find every one that was generated by the passwords “12345678,” “trustno1,” “iloveyou,” and a few thousand others.

5 Plotting on the Dark Web

On the dark web, cybercriminals and hackers communicate and transact business anonymously (and in fairness to the dark web, so do journalists and dissidents living under repressive governments). Users of the dark web typically hide behind nicknames ("handles") to conceal their identities and use TOR browsers and networks to obfuscate their IP addresses. Many forums and marketplaces on the dark web implement the digital equivalent of a nightclub rope line with a bouncer: would-be members are turned away unless they have been invited or can pass a test.

Threat actors often use forums on the dark web to plan attacks and to recruit other cybercriminals—and sometimes corrupt company insiders—to assist them. Politically motivated actors and "hacktivists" sometimes use the same forums to justify their actions or boast of their prowess. The participants in these forums frequently name their targets.

If you monitor dark web forums, you can uncover plotting against your partners (as well as your enterprise). Observing activity in these forums provides early warning of attacks and information about the tactics, techniques, and procedures that will be used.

With this information you can:

- Warn your partners so they can configure or upgrade their defenses to thwart the tactics and techniques of the attackers
- Ensure that your defenses are able to protect against the same attacks
- Notify law enforcement organizations so they can take down or impede the threat actors

EXAMPLE: Selling Access to Cloud Environments

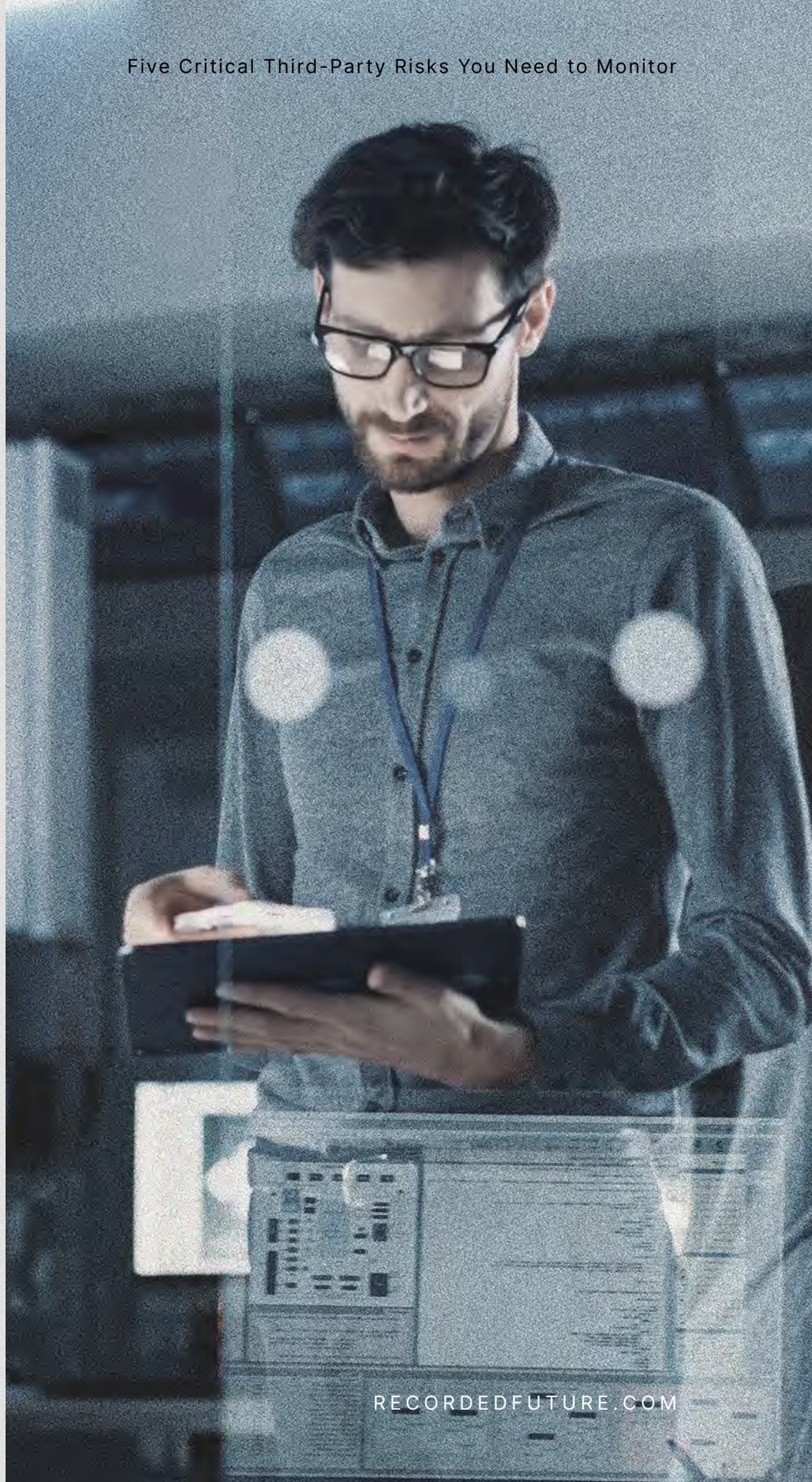
The screenshot below shows a message from a dark web site offering to sell root user keys for thousands of AWS accounts. An attacker who purchased the root key for one of your partner's accounts would gain complete control over that organization's public cloud environment. Your partners would really, really appreciate being notified if you find their name mentioned, because then they could disable the keys before they are used.

How to Protect Your Organization Using Third-Party Risk Intelligence

This paper has described five critical third-party risks and what you can do to detect and mitigate them. The same strategies will help you address many other third-party risks as well.

Of course, it is not easy to monitor hundreds of thousands of websites, forums, and marketplaces, or to track malicious network activity for a long list of third-party partners. In addition, many important sites on the dark web are invitation-only, and it can take years of effort to develop personas that will be accepted by cybercriminal communities.

That's where intelligence comes in. An intelligence service provider can invest in skills and resources to draw information from sources across the internet, including websites, forums, and marketplaces on the open web and dark web, ransomware extortion sites, paste and dump sites, news sources, blogs, social media accounts, and threat intelligence databases. A staff of experts with extensive knowledge of cybercriminal and hacker communities, and fluency in languages such as Russian, Chinese, and Arabic, can monitor corners of the web that few enterprises ever find.



Reducing Risk with Third-Party Intelligence

For more details on how Recorded Future can help you reduce risk with third-party intelligence, see our blog posts: Reducing Risk For the Modern Supply Chain With Third-Party Intelligence and Why Monitoring the Dark Web is Essential for Third-Party Risk Management.

Recorded Future, the world's largest provider of intelligence for enterprise security, offers a third-party intelligence service specifically designed to identify, manage, and mitigate third-party risk. Recorded Future:

- Supplies detailed information on hundreds of thousands of third-party organizations, so you can rapidly assess the cybersecurity risk of new vendors, streamline procurement, and negotiate security standards into your purchasing agreements
- Gives you visibility into the security posture of existing third-party partners, so you can find the "weak links" and work with them to strengthen their defenses
- Continuously monitors your vendors to provide early warning of impending and ongoing attacks and risks, including ransomware extortion, data breaches, malicious network activity, exposed credentials, and cybercriminal chatter
- Presents detailed context and actionable recommendations when a partner is at risk or is attacked, so you can respond quickly and protect your enterprise

Want to Know More?

See a Demonstration of Third-Party Intelligence

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.