The National Security Question No Organization Wants to Face

Most organizations are aware they may be targeted by financially motivated cyber criminals at any time. They may even have an incident response plan in place. But what happens if a foreign nation or terrorist group exploits an organization's network or technology without its knowledge to further a political agenda — and a government intelligence agency asks the organization not to remediate so it can monitor the activity?

That scenario may sound far-fetched, but it is real and surprisingly common. Organizations of all sizes — from small businesses to Fortune 500s — have unwittingly become entangled in these matters of national security. Imagine getting a visit from an intelligence agency explaining that a foreign nation is funding its nuclear weapons program through your infrastructure, or that a terrorist group is using your servers to spread propaganda. The only consistent variable among incidents like these is the ability of the nefarious actor to breach the victim's network and remain undetected.

> One of the highest-profile nation-state attacks occurred in 2020 when threat actors breached numerous private companies and federal agencies through a commercial software application made by SolarWinds. The attackers embedded and hid malware in a legitimate SolarWinds' software update they had gained access to through a third party.

Although the likelihood of exploitation decreases with strong cybersecurity defenses, no organization is immune to such highly sophisticated efforts backed by resources of hostile foreign nations. Compounding the issue is the quandary exploited organizations can find themselves in when the government comes calling. Once authorities are aware of an unwitting nation-state entanglement, they often want to allow the cyber actors to remain on an organization's systems. The reasoning behind this is simple: Federal agencies want the opportunity to gather intelligence on the espionage activities of foreign countries.

An organization's decision to shut down its compromised network often results in government agencies losing all visibility into the adversarial nation's activities. Gaining this type of insight is a timely, costly and highly technical process, so the government's interest in retaining access is high. When organizations choose remediation rather than government cooperation, the cyber actors simply move their illicit spying infrastructure — often to places unknown to the government — and continue their activities.

The tension between organizational needs and government interests creates a complex choice for decision-makers, where any solution could have long-term consequences. Government officials will be persistent in their efforts to convince an organization to agree to continued cooperation, making it essential that an organization has its own resources to bring to the conversation. Of course, not every organization can have a national security specialist on staff or retainer, but it is important to know where to find one if needed.

Published

February 07, 2023

Key Contacts

Brian Boetig
Senior Managing Director

Categories

FORENSIC & LITIGATION CONSULTING

Topics

OPERATIONAL

REPUTATIONAL

There are serious considerations that must be weighed when an organization decides whether to cooperate with officials or shut down its network:

- What impact does allowing nefarious actors to remain on the network pose?
- What liability does the organization expose itself to by knowingly having a compromised system?
- What indemnification does the government or existing law offer for cooperation?
- What reporting of the breach is required to stakeholders?
- Is the information received from the government classified and unable to be shared?
- Is the government willing to help remediate the compromise regardless of cooperation?
- What reputational damage is possible if cooperation with the government is exposed?
- What impact does not remediating a known problem have on a cyber insurance policy?

While it is impossible for a business to be fully prepared for an unwitting cybersecurity entanglement with a nation-state, basic awareness of the topic and the knowledge that external resources are available for navigating these scenarios will provide a better chance of successfully recovering from this type of incident.