Trellix Global Threat Research

In the Crosshairs: Organizations and Nation-State Cyber Threats

Trellix

Table of Contents

3 Executive Summary

4 Key Findings

5 Section I. Threat Perceptions

6 Threats

9 Motives

12 Section II. Decision-Making in an Uncertain Environment

13 Attribution

14 Notification and Disclosure

18 Section III. Responding to the Threat

21 About Trellix

21 About CSIS

21 About Vanson Bourne

Executive Summary

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

Executive Summary

The constant outpouring of news highlights that nation-state cyberattacks are a growing threat. Governments are behind many of the most dramatic successes. These nation-state cyberattacks create service disruptions, expose data, and create substantial financial costs. SolarWinds, Colonial Pipeline and the Microsoft Exchange "Hafnium" incident are examples, and if nothing else show that victims have to spend heavily to repair damage to reputation and brand and in cases where there is intellectual property theft, can lose the advantage of their investment in innovation. State attackers are relentless and there is considerable room for improvement in cyber defense and how most organizations — regardless of sector or size — go about doing this.

Industrial espionage, ransomware, the theft of personal information, or disruption of services — the impact from a cyberattack take many forms, all damaging. While attackers can range from cybercriminals, individual hackers, or governments, nation-states and their criminal proxies are the most dangerous because they are the most capable, best-resourced, and persistent. Many of the high-profile events in recent years involved state actors, whether acting directly, using proxies, or by allowing cybercriminals to operate from their territory.

The growing number and severity of cyberattacks is a problem for the international community, and while there has been progress in agreeing on norms of responsible state behavior (and what to do if these norms are not observed), it will be years before the state-actor threat recedes, because it is so rewarding and because there are so few penalties. Previous reports in this series estimate that cybercrime costs the world perhaps $1 trillion dollars, and the cost is growing. Most of this is due to attacks by nation-states or their proxies, by a failure of certain governments to enforce the law against criminal groups operating from state territory, and by the opportunities created by weak defenses and often a reliance on multiple vendors for network services and software.

In order to better understand how organizations perceive and prepare for the threat nation-state actors present and how this perception aligns with the motivations and effects these incidents have, we conducted a survey of 800 IT security decision makers from the United States, the United Kingdom, Germany, France, Japan, India and Australia between November and December 2021. Respondents belonged to organizations with 500 or more employees from a range of industries, mainly focused on critical infrastructure.

The burden of defense falls as much on companies as it does on their governments. Understanding the perceptions under which organizations make decisions about cybersecurity can help guide decision makers as they develop policies to respond to nation-state actors.

Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an
Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

Key Findings

1. The line between state and non-state actors continues to blur. Eighty-six percent of respondents believe they have been targeted by a cyberattack by an organization acting on behalf of a nation-state.

2. State actors are more likely to focus on retrieving data rather than benefitting financially. The estimated cost for organizations that are victim to a successful state-backed cyberattack exceeds more than $1 million per incident.

3. Ten percent of organizations surveyed still do not have a cybersecurity strategy. Organizations that have developed strategies to deal with cyber incidents — and particularly those that provide guidance for state-backed incidents — have higher levels of confidence when differentiating between state-backed and other cyber incidents.

4. It is common for there to be 'leave behinds' after an incident. The attackers use these to provide later access to a victim network and they can help point to the attacking nation-state actor. However, most organizations lack a high level of confidence in their ability to determine the function of any leave behind.

5. Only 27 percent of respondents said they have complete confidence in the ability of their organization to differentiate between nation-state cyberattacks and other cyberattacks.

6. Survey respondents indicated that limited skills and outdated network technology and security tools increased vulnerability..

7. A majority of respondents (more than 90 percent) say they have shared information on attacks, but not always with full details of the attack or its effect.

8. Around nine in ten respondents think the government should do more to support organizations (91%) and protect critical infrastructure (90%) against state-backed cyberattacks.

Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an
Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

Section I. Threat Perceptions

More countries are developing and using cyber capabilities, but according to the 2021 Annual Threat Assessment of the Office of the Director of National Intelligence, the main source of threats facing the United States are Russia, China, Iran, North Korea, and the cybercriminals that operate at their behest.[1] These actors lie outside the ambit of western law and law enforcement.

Different countries pursue different objectives and states have a diverse set of motivations. North Korea, for example, wants money to prop up the Kim Jong-un regime, circumventing international financial sanctions. While it uses disruption and misinformation against South Korean targets, it is the state that acts most like a criminal group. The Sony Pictures hack proved to be unique because it began with what was seen as an insult to the "Great Leader." According to a recent report preview by Chainalysis, North Korean attackers "extracted nearly $400 million worth of digital assets" in 2021.[2] The same report places a high level of likelihood that the North Korean intelligence service is behind the cyberattacks.

In contrast, Russia, China, and Iran all have political, military, and industrial motives.[3] The Russian state focuses on espionage (particularly in the energy sector), disinformation, and coercion; its cybercriminals focus on financial gain and their actions are tolerated (when not encouraged) by the Kremlin.[4] Even some of its political actions create risks for global business: NotPetya allegedly came from a Russian intelligence agency attack on the Ukrainian government but rapidly spread to companies around the world.[5] China engages in massive IP theft: there are more than 2,000 open espionage cases currently, according to FBI Director Christopher Wray, directed by Beijing to support economic and technology goals.[6] Iran focuses on Israel and the Gulf States, and has targeted energy companies. This list provided details on dozens of cyberattacks carried out by state actors for more than a decade.

1 Office of the Director of National Intelligence, "Annual Threat Assessment of the US Intelligence Community," April 9, 2021, 20, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

2 "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-Time High," Chainalysis, January 13, 2022, https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/.

3 "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure | CISA," January 11, 2022, 3, https://www.cisa.gov/uscert/ncas/alerts/aa22-011a.

4 Frank Bajak, "How the Kremlin Provides a Safe Harbor for Ransomware," April 16, 2021, https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7eb3841be45dff2d93ed3102999

5 The White House, "Statement from the Press Secretary," February 15, 2018, https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.

6 Pete Willams, "FBI Director Wray Says Scale of Chinese Spying in the U.S. 'Blew Me Away,'" February 1, 2022, https://www.nbcnews.com/politics/politics-news/fbi-director-wray-says-scale-chinese-spying-us-blew-away-rcna14369.

Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

Seventy-four percent of respondents suspect that a state actor targeted their organization in the 18 months prior to the survey, with 32 percent of the total being highly certain that this has occurred. And while 18 percent of respondents expect this will be a problem in the future, 8 percent expressed they do not anticipate effectively dealing with this issue at all. It is particularly concerning that this belief is held by respondents whose organization is considered critical infrastructure. On average, organizations estimate they have been targeted by a nation-state twice in the 18-month timeframe.

Threats

During her remarks at the Department of Justice Criminal Division's Cybersecurity Roundtable on 'The Evolving Cyber Threat Landscape', U.S. Deputy Attorney General Lisa Monaco said that the line between cybercriminals and nation-state actors is blurred: "[states and criminal groups] are forming alliances of convenience, alliances of opportunity and sometimes alliances by design with nation-state actors."[7] Eighty-six percent of respondents believe it highly to somewhat likely that they have been targeted by a criminal organization acting on behalf of a nation-state. Judging from our survey results, banking, energy, defense, and healthcare are among the leading targets for nation-state attack.

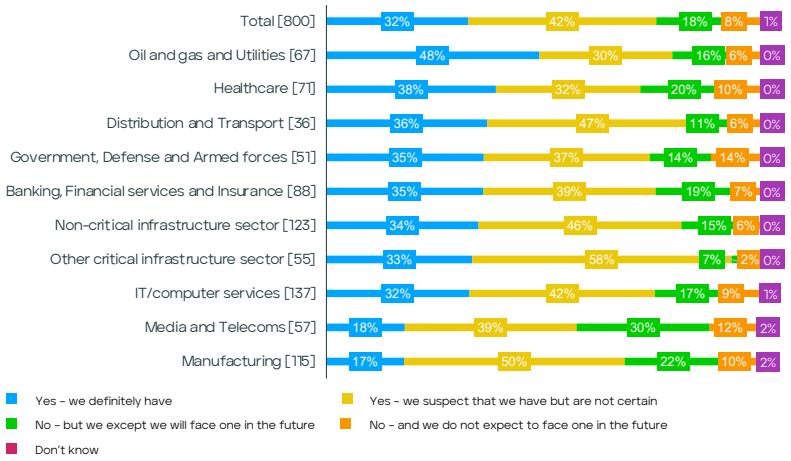


Figure 1. Do you believe that your organization has been the target of a nation-state cyberattack within the last 18 months?

Identifying and attributing an incident to a specific actor can be a technical challenge. The nature of these incidents allows for perpetrators to hide their origin, and provides a certain level of deniability. However, a surprising 63 percent of the survey respondents expressed high to complete levels of confidence in being able to differentiate between state-backed cyber incidents and others.

7 "Deputy Attorney General Lisa O. Monaco and Assistant Attorney General Kenneth A. Polite Jr. Deliver Opening Remarks at the Criminal Division's Cybersecurity Roundtable on 'The Evolving Cyber Threat Landscape,'" October 20, 2021, https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-and-assistant-attorney-general-kenneth-polite-jr

Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

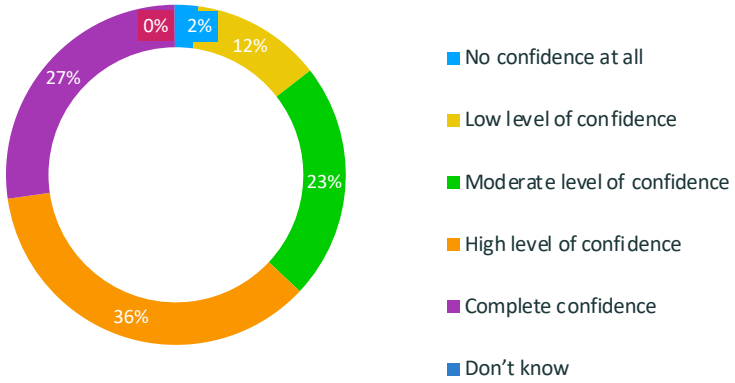


Figure 2. How confident are you that without assistance your organization is/would be able to differentiate between cyberattacks linked to nation-state actors and cyberattacks linked to other actors?

Who do organizations think are behind attacks to their systems? Seventy-four percent of respondents interviewed for this survey assess they have been the victims of a state-backed incident, or suspect they have. Forty-two percent blame a cybercrime group acting on behalf of an unknown nation-state. That percentage increases slightly for those organizations that expect to face such a threat in the future to 44 percent. This remained true across most of the countries analyzed, except for Germany and Australia, where organizations were more likely to suspect Russia was behind the incident (44 and 47 percent respectively). It is possible that respondents focused more on Russia given the publicity around incidents attributed to Russia that occurred around the time the survey was being conducted. In Australia, China is also seen as a likely threat: 46 percent of respondents suspected China to be behind an incident targeting their organization.

Figure 3. Based on the information assets targeted within your organization, which nation-state(s) and/or affiliated actors do you suspect are most likely to have targeted your organization?

In addition to having cybercrime gangs conduct attacks on a government's behalf, there is a widely held view that nation-states are building out their cyberattack armories in collusion with cybercrime gangs, sharing tools, techniques, and skilled professionals.

When asked about their expectations for future incidents, however, respondents shifted towards perceiving China as the most likely actor

Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an
Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

(46 percent). Russia and cybercrime groups acting on behalf of unknown states followed closely with 44 percent each. Although the differences between the responses from organizations that were targeted within the last 18 months and those that are expecting to be targeted is slight, the responses show how organizations are assessing this threat, which informs their preparedness.

China and Russia are the nations most commonly identified as attackers by most organizations. This is consistent with other research that shows them to be most active in using cyberattacks, more than any other state attacker. Although the base number of respondents per sector that identified the most likely actor behind a future cyber incident was low, the answers point to the differences in threat perceptions and expectations among sectors on likely actor behind a past cyber incident versus a future cyber incident.

Sectors that perceive Russia to be the most likely actor behind a past cyber incident:

- Media and telecoms (59 percent)
- Banking, financial services and insurance (45 percent)
- Oil and gas and utilities (35 percent)

Sectors that perceive Russia to be the most likely actor behind a future cyber incident:

- Distribution and transport (75 percent)
- Media and telecoms (53 percent)
- Healthcare (43 percent)

Sectors that perceive China to be the most likely actor behind a past cyber incident:

- Healthcare (52 percent)
- Manufacturing (51 percent)
- Distribution and transport (37 percent)

Sectors that perceive China to be the most likely actor behind a future cyber incident:

- IT and computer services (70 percent)
- Government (57 percent)
- Manufacturing (44 percent)

This sectoral breakdown fits the pattern of cyber actions by these states. Energy, for example, is a likely Russian target because of the importance of the energy industry to Russia, while attacks on telecom companies could support other espionage activities. One recent change is the new focus on healthcare, likely a result of the pandemic.

Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

Motives

The 2021 Office of The Director of National Intelligence (ODNI) threat assessment says nation-states use cyber operations to "steal information, influence populations, and damage industry, including physical and digital critical infrastructure."[8] It also points out that state sponsored hackers can conduct espionage or sabotage operations.[9] This assessment mirrors the concerns from the organizations surveyed, most of which see the personally identifiable information (PII) they hold — related to either their customers or their employees — as one of the main factors for which they are targeted (46 percent and 40 percent respectively).

When it comes to assessing the motives behind a specific incident, respondents also include disruption of services, damage to their reputation or coercion as likely motives for a past or future event.

Sector	Most selected and %
IT/computer services [137]	PII we own for customers **(50%)**
Banking, Financial Services and Insurance [88]	PII we own for customers, etc. **(45%)** / PII we own for employees **(45%)**
Manufacturing [115]	PII we own for customers, etc. **(47%)**
Oil and gas and Utilities [67]	The sector we are in **(43%)**
Distribution and Transport [36]	The intellectual property we own **(50%)**
Media and Telecoms [57]	PII we own for customers, etc. **(53%)**
Government, Defense and Armed forces [51]	The links we have to our govt. in our country **(47%)**
Healthcare [71]	PII we own for customers, etc. **(45%)**
Non-critical infrastructure sector [123]	PII we own for customers, etc. **(53%)**

Figure 4. Which of the following variables do you think makes your organization most likely to be targeted by a nation-state cyberattack?

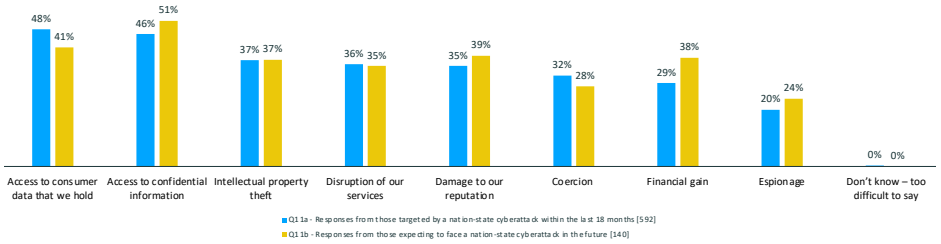


Figure 5. Which of the following do you believe were the motivation(s) for the nation-state cyberattack(s) that targeted your organization within the last 18 months?

8 Office of the Director of National Intelligence, "Annual Threat Assessment of the US Intelligence Community," 20.

9 Office of the Director of National Intelligence, 21

Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

The Main Targets: Customer Data, IP, Network Security Architecture[10][11]

Access to consumer data was the perceived motive for state-backed cyber incidents for 48 percent of respondents who believe they have been the victims of a state-backed incident, followed closely by access to confidential information (46 percent) and intellectual property theft (37 percent). The question is, then, what are nation-states seeking to achieve by acquiring this information? Figure 6 shows the type of data targeted. Information gathering about cybersecurity defenses and processes, with 42 percent stating cyberattacks target this data, could indicate a particular interest in collecting information that could assist in future attacks. When it comes to personal data, while cybercriminals may target the same data for financial gain, nation-states seem to be acquiring personal identifiable information for espionage or counterintelligence purposes. Respondents were almost evenly split on whether they thought their organization was the sole target or the attack was part of a campaign against many companies. But our survey results show defenders in healthcare, IT services and banks were considerably more likely to believe they were specifically targeted in individual attacks and there is evidence from ransomware groups, that this is the case for healthcare and finance.

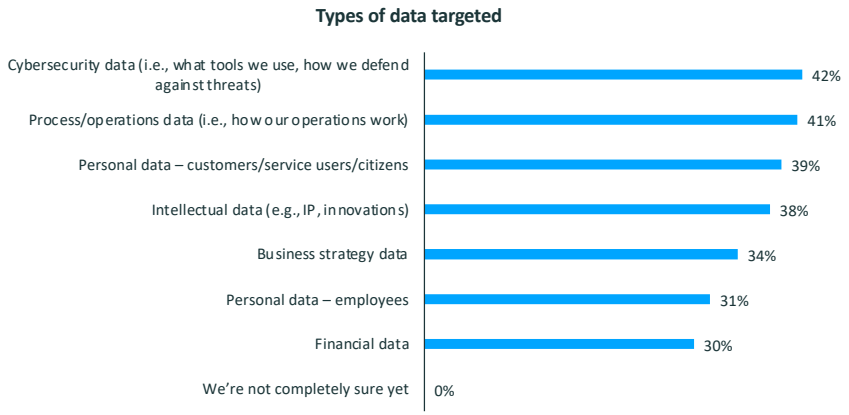


Figure 6. Which of the following types of data were targeted during the nation-state cyberattack

10 Ohad Zaidenberg, "CTIL Darknet Report – 2021," February 11, 2021, https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf.

11 "Advisory: APT29 Targets COVID-19 Vaccine Development," July 16, 2020, https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development.

Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an
Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

A Tempting Target: COVID-19 Vaccine Information

Throughout the Covid-19 pandemic there was a marked uptick in cyber incidents surrounding healthcare. Ransomware, data breaches, fraud schemes, theft, and espionage against vaccine researchers added a new layer of pressure to an already stressed system. Cybercriminal groups were behind many of these incidents, mainly seeking to benefit financially from the crisis. But the abundance of information on medical staff in underground forums presented opportunities for state actors as well: compromised credentials provide a potential future avenue for entry into these systems.10

In July of 2020, the United Kingdom's National Cyber Security Centre (NCSC) and Canada's Communications Security Establishment (CSE) reported on the high likelihood that a group belonging to the Russian intelligence services was targeting organizations involved in the research and development of the Covid-19 vaccine. The group, the report warns, attempted to gain authentication credentials that would allow access into "a large number of systems globally," with the "intention of stealing information and intellectual property relating to the development and testing of COVID19 vaccines."11

Healthcare organizations surveyed considered that the most likely motivations behind a state-backed cyberattack were intellectual property theft (48 percent) and coercion (46 percent).

Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an Uncertain Environment

Section III:
Responding to the Threat

About Trellix

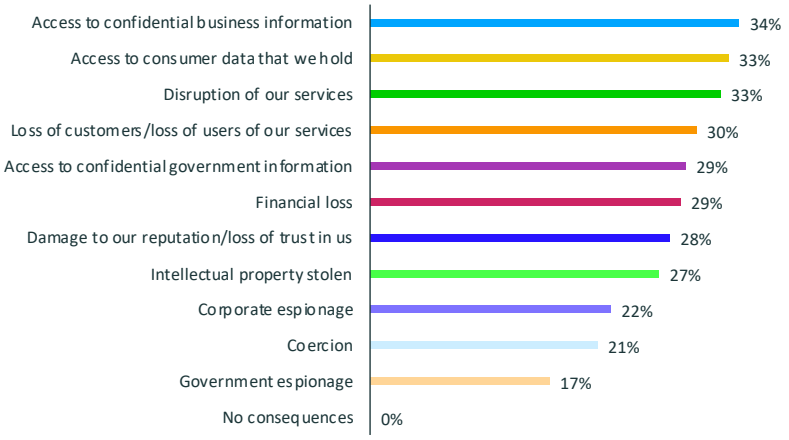
About CSIS

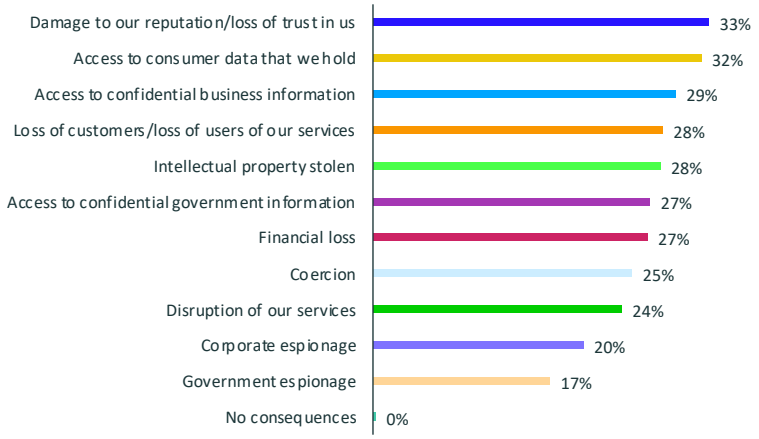
About Vanson Bourne

Section II. Decision-Making in an Uncertain Environment

Companies and government agencies need to make decisions in an uncertain environment, to protect against a range of threats. Not doing so can lead to serious consequences: the estimated cost for organizations that are victim to a successful nation-state-backed cyberattack exceeds $1 million (the average cost to organizations was $1.6 million per incident). Besides the financial cost that a cyber incident can generate, there are many other consequences an organization should take into consideration. Our survey data collects the responses from 402 respondents from organizations that had been successfully infiltrated within the last 18 months, and shows how concerns evolve over time. In the short term, the focus was on the commercial impact of unauthorized access to stored consumer or business data. Ninety-eight percent stated they faced a data-related consequence after a successful attack, with the majority suffering data exposure (51 percent), followed by data loss (50 percent). Short term consequences also included disruption of services and a loss of customers or users. In the longer-term, organizations are more concerned with the damage

Short- and long-term consequences





Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

to trust. Faced with threats of unclear provenance, and with expensive consequences, organizations need to make tough decisions on how to allocate resources and what level of priority cybersecurity should take.

Attribution

A state-backed cybersecurity incident can be more sophisticated than one orchestrated by a criminal group. One key distinction between criminal and nation-state attackers is time on network. Criminals operate quickly, get in and get out quickly while nation-states tend to get in carefully and then loiter for years. As the previous section discussed, 92 percent of those surveyed have faced or suspect they have faced a nation-state attack within the last 18 months, or expect to face one in the future. While the vast majority of respondents' organizations have a cybersecurity strategy in place, only 41 percent distinguish and provide specific guidance for state-backed cyberattacks. Startlingly, 10 percent of respondents say they still do not have a formal cybersecurity strategy. This is particularly concerning when we consider that this is true for 9 percent of the organizations considered critical infrastructure.

Figure 7. To what extent does your organization's cybersecurity strategy differentiate between nation-state cyberattacks and cyberattacks linked to other threat actors?

Most organizations place a high or crucial level of importance to being able to determine whether a nation-state is behind an incident impacting their organization, even if their cybersecurity strategies do not reflect this, or their capacity to do so is limited. Seventy-eight percent of the 800 respondents considered this to be a matter of high or crucial importance. There was very little variation across regions, or sectors, or organization size, which reveals the importance of attribution. The hope, for most organizations, is that a better understanding of the source of an attack can help safeguard them against a future attack. Holding the attacker accountable was also a high priority for most of the respondents.

Despite the importance assigned to attribution, only around one in four respondents claimed complete confidence in the ability of their organization to distinguish between state-backed cyberattacks and

Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

others. Organizations expressing the highest levels of confidence in their ability to differentiate among attackers did so having implemented cybersecurity strategies that distinguish between nation-state and non-state actors and thereby provide specific guidance on how to respond to each. This highlights one of the greatest challenges facing organizations in relation to nation-state attacks — it is often very difficult for many of them to confidently and correctly determine whether a cyberattack is actually linked to a nation-state.

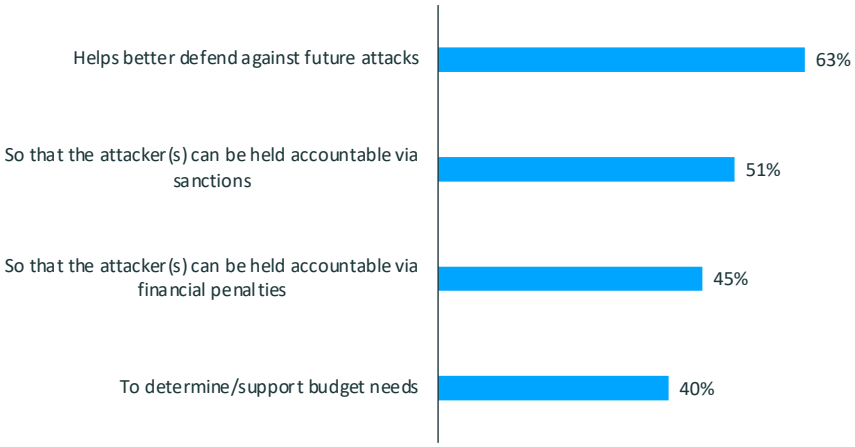


Figure 8. Why do you believe that attribution is/would be important?

It is not just up to the organizations by themselves to be able to determine who is behind an incident. Most frequently, respondents indicate that a cybersecurity partner (see Figure 9) was able to assist them in determining whether a cyberattack was state-linked or not, either via direct communication or via a cybersecurity tool already in place. Many companies rely on cybersecurity vendors to identify and remediate threats.

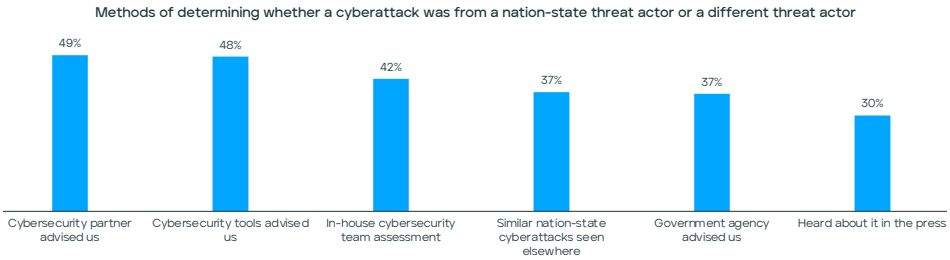


Figure 9. How did your organization determine that the cyberattack faced was from a nation-state actor as opposed to a different actor?

Notification and Disclosure

Transparency and communication regarding the existence of a cyberattack is considered crucial, particularly if organizations are concerned about the potential effects on consumer trust and company reputation. Ninety-two percent made a cyberattack against them public knowledge, and half of those say they disclosed the details in full. But

Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

even if respondents from organizations that have been or suspect they have been the subject of a state-backed cyberattack are transparent about these incidents, some probing shows some concerning trends.

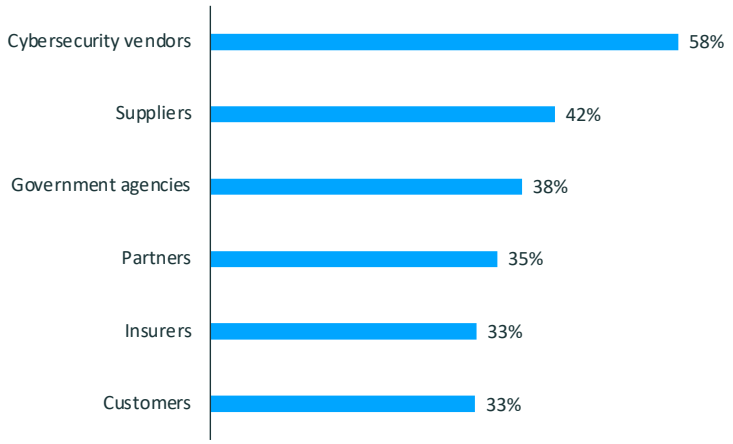


Figure 10. Which external stakeholders did you specifically reach out to in order to disclose the details of the nation-state cyberattack you were targeted by?

Most organizations are relatively prompt in informing their stakeholders and making the incident public knowledge, with 61 percent disclosing details within two days from when the incident was discovered. However, direct communication with customers does not appear to be that high a priority, with only 33 percent reaching out to them specifically. While ensuring direct communication with cybersecurity vendors, partners and government agencies is understandable, organizations need to remember that loss of trust and damage to their reputation is one of the likely long-term consequences of a cyberattack. This damage can be difficult to repair and taking steps at the beginning of a crisis is essential to preempt this.

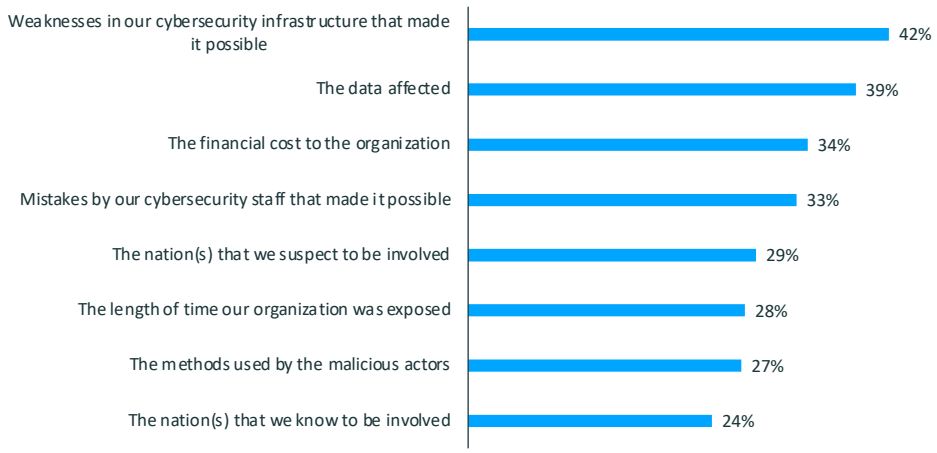


Figure 11. Which details did your organization choose not to disclose in full to external stakeholders?

Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

It is interesting to note what information organizations are reluctant to share with external stakeholders. Forty-two percent of the respondents said they did not fully disclose weaknesses in their cybersecurity infrastructure that made the attack possible, and 33 percent did not share whether their staff made mistakes leading up to the incident.

The Role of Government

Information sharing between the public and private sector enhances cybersecurity as a whole. As the CISA Federal Government Cybersecurity Incident and Vulnerability Response Playbooks explains, reporting and notification helps the United States "maintain awareness of the status of vulnerability response for actively exploited vulnerabilities."[12] Fortunately, there seems to be little reluctance in the private sector to report cyber incidents to law enforcement partners. Regardless of whether this is the result of voluntary or mandated action, 97 percent of respondents say they would do so.

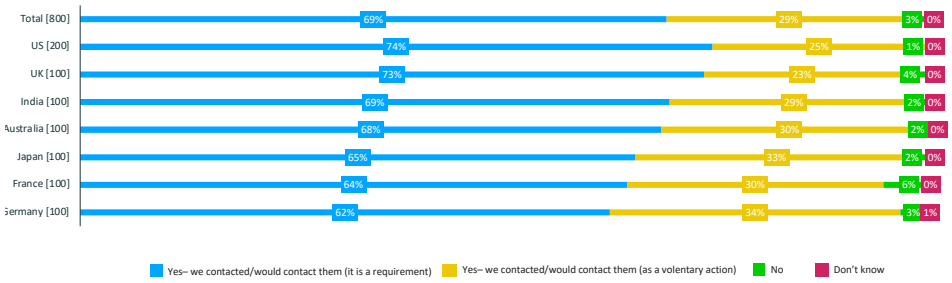


Figure 12. Has your organization partnered/would your organization partner with law enforcement as a result of being targeted by the/a nation-state cyberattack?

Beyond partnering with law enforcement, greater collaboration with governments is highly sought after. Around nine in ten respondents think the government should do more to support organizations (91%) and protect critical infrastructure (90%) against state-backed cyberattacks. The areas in which extra support would be most valued tend to align with the areas where respondents say they currently struggle. Organizations noted limited cybersecurity skills and outdated IT infrastructure as the two largest barriers to protect themselves against nation-state cyber threats. This aligns with where organizations want the government to help, with 49 percent noting additional cybersecurity tools and 46 percent noting additional staff as areas for increased government support. Respondents also listed providing real-time machine learning assistance as a top way the government can help companies defend against nation-state attacks. There is a general sentiment to have the government do more to support their organizations and protect critical infrastructure through increased intelligence sharing, supplying cybersecurity resources, and providing strategic guidance.

12 Cybersecurity and Infrastructure Security Agency, "Cybersecurity Incident & Vulnerability Response Playbooks," November 16, 2021, 24, https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerabilit

Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

There already is a trend in many countries toward expanding communication between the public and private sector. In the UK, the NCSC provides support, guidance and services for critical national infrastructure.[13] In August 2021, CISA established the Joint Cyber Defense Collaborative (JCDC), which brings together government and private sector representatives to coordinate cybersecurity planning, information sharing, and information product and guidance development. [14]In the face of the log4j vulnerability, one of CISA's first actions was to convene the JCDC, an action that was a highly praised approach to the crisis.[15] Furthermore, Sec. 1508 of the FY22 National Defense Authorization Act (NDAA) calls for the Commander of the United States Cyber Command (USCYBERCOM) to establish a voluntary process through which it can engage with private sector information technology and cybersecurity entities to defend against foreign malicious cyber actors.[16]

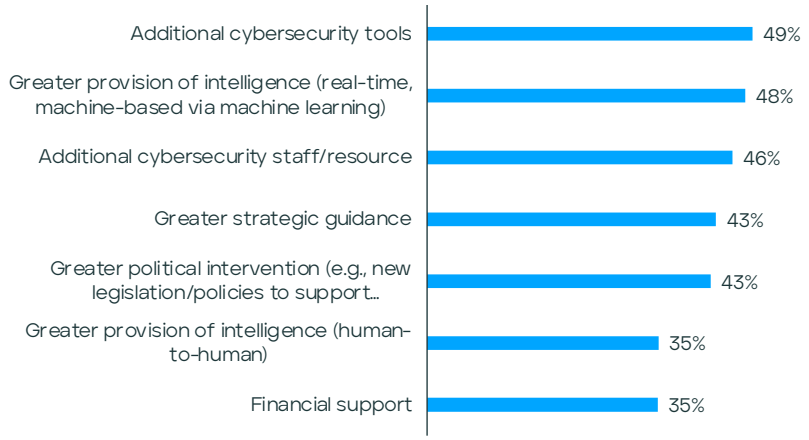


Figure 13. In which of the following areas do you believe that your country's government needs to provide additional support to organizations defending against nation-state cyberattacks?

Leave Behinds

"Leave behinds" are used by the attackers to provide later access to a victim network, but they can also provide evidence that help identify the government involved in a cyber incident. The survey data shows these "leave behinds" are not uncommon: 98 percent of the 402 organizations that suffered at least one successful state-backed cyberattack within the last 18 months found leave behinds. However, there are varying levels of confidence in being able to determine the function and origin of the code or tools found. Only 26 percent expressed high confidence in their

13 "CNI Hub," accessed January 25, 2022, https://www.ncsc.gov.uk/section/private-sector-cni/cni.

14 "JCDC Fact Sheet - Changing the Cybersecurity Paradigm: A Unified Cyber Defense" (CISA, January 2022), https://www.cisa.gov/sites/default/files/publications/JCDC_Fact_Sheet_508C.pdf

15 "Statement from CISA Director Easterly on 'Log4j' Vulnerability | CISA," December 11, 2021, https://www.cisa.gov/news/2021/12/11/statement-cisa-director-easterly-log4j-vulnerability.

16 Rick Scott, "S.1605 - 117th Congress (2021-2022): National Defense Authorization Act for Fiscal Year 2022," Pub. L. No. S.1605 (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1605.

Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an
Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

ability to do so. This uncertainty, however, does not prevent them from assessing one of the likely functions: most organizations agree that a purpose of these "leave behinds" was to allow the attackers to reenter their systems in the future.

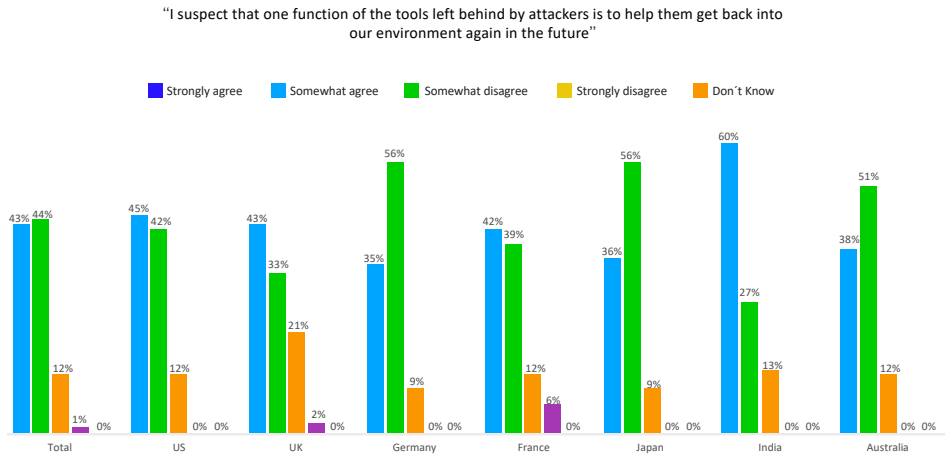


Figure 14. To what extent do you agree or disagree with the above statement?

Section III. Responding to the Threat

Thankfully, better cybersecurity is not dependent on full certainty in attribution on an attacker or their motives. Although organizations understand attribution of a cyber incident to a specific state as a necessary step to better protect against future threats, there is much they can do even if they cannot fully ascertain who was behind the incident. Many of the measures they take after becoming the victim of a state-backed cyber incident are no different from the ones put into place after a non-state actor targets them. Implementing these measures will be valuable for organizations regardless of whether they have been breached yet or not.

Many of the recommendations for tackling the threat from state actors will echo the recommendations for enhancing cybersecurity in general. Acquiring or updating cybersecurity tools, providing additional training for all staff, or recruiting new experts are all recommended actions that will help protect an organization from both nation-state and non-state threats. Regardless of their sector, organizations should ensure at least a baseline level of cyber hygiene and training to better face a wide range of incidents.

Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

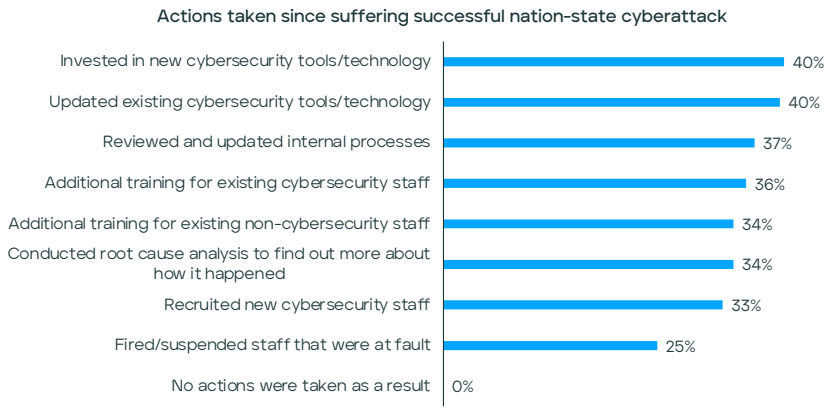


Figure 15. Which of the following actions, if any, has your organization taken since suffering from the successful nation-state cyberattack?

Cyber hygiene is critical

Incidents like SolarWinds showed that the absence of basic measures will greatly increase risk. These measures include routine patching and updating (even though there is a degree of "patch fatigue"), maintaining logs, using encryption for sensitive data and requiring multifactor authentication for all users. Easily implemented actions like these would go far in reducing an attacker's chance of success.

Update defense capabilities

The success of nation-state cyberattacks is often linked to lack of cybersecurity skills and the use of outdated IT infrastructure or cybersecurity tools. With threat actors' tools and techniques growing more sophisticated, there is a real need for organizations to modernize and improve their defenses at a similar (or faster) rate.

Identify what needs to be protected

Data is one of the most valuable assets that nation-states usually want. If the intent behind most state-backed attacks is to acquire information on customers or staff, organizations need to take extra steps to ensure the security of this data and build resilience in their use of it. In an ever-expansive threat environment, identifying high- and low-priority data targets should guide internal cybersecurity planning and processes.

Assess actual capacity

An interesting insight from the survey data is the dissonance, in some cases, between a respondent's assessment of their capacity and the actual implementation of that capability. For instance, while many expressed high confidence in their ability to conduct successful attribution without assistance, other results reveal most organizations rely on external assistance to identify a perpetrator. An overestimation or misunderstanding of actual technical capacity could lead to increased vulnerabilities and inefficient processes or solutions.

Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an
Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

Review third-party service providers

The Microsoft Digital Defense Report identifies the targeting of IT service providers as a trend for nation-state actors.[17] This allows state actors to gain access to multiple victims by only targeting one provider. While the highly publicized SolarWinds and Microsoft Exchange Hafnium cases last year gained significant attention, targeting a third-party service provider is not a new threat — all of which makes it more concerning and suggests that as a reliance on things like software-as-a-service (SaaS) and similar services implies a necessity for an additional level of effort in defense.

Increase communication to address threats

Communication between the public and private sectors is crucial to face state-backed threats. Governments can provide advice and information that identify both specific threats and vulnerabilities as well as broader trends, and notify companies of developments, but this can only be improved if there is sufficient information sharing from the private sector to ensure the government is up to speed on the threat environment.

17 Microsoft, "Microsoft Digital Defense Report," October 2021, 52, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi.

Introduction

Key Findings

Section I:
Threat Perceptions

Section II:
Decision-Making in an Uncertain Environment

Section III:
Responding to the Threat

About Trellix

About CSIS

About Vanson Bourne

About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.
More at https://trellix.com.

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges. CSIS's purpose is to define the future of national security. They are guided by a distinct set of values—non-partisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com.

Trellix

Copyright © 2022 Musarubra US LLC