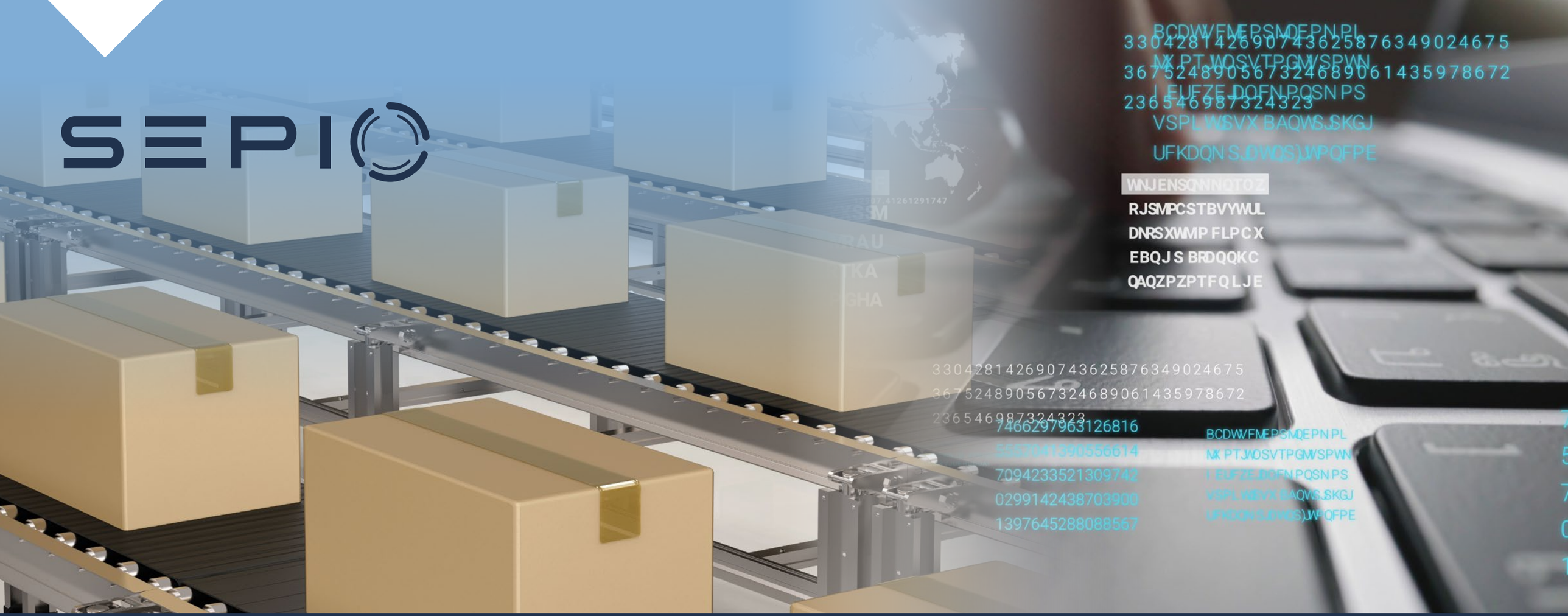


EBOOK

Supply Chain Security

For Federal

CONTENTS

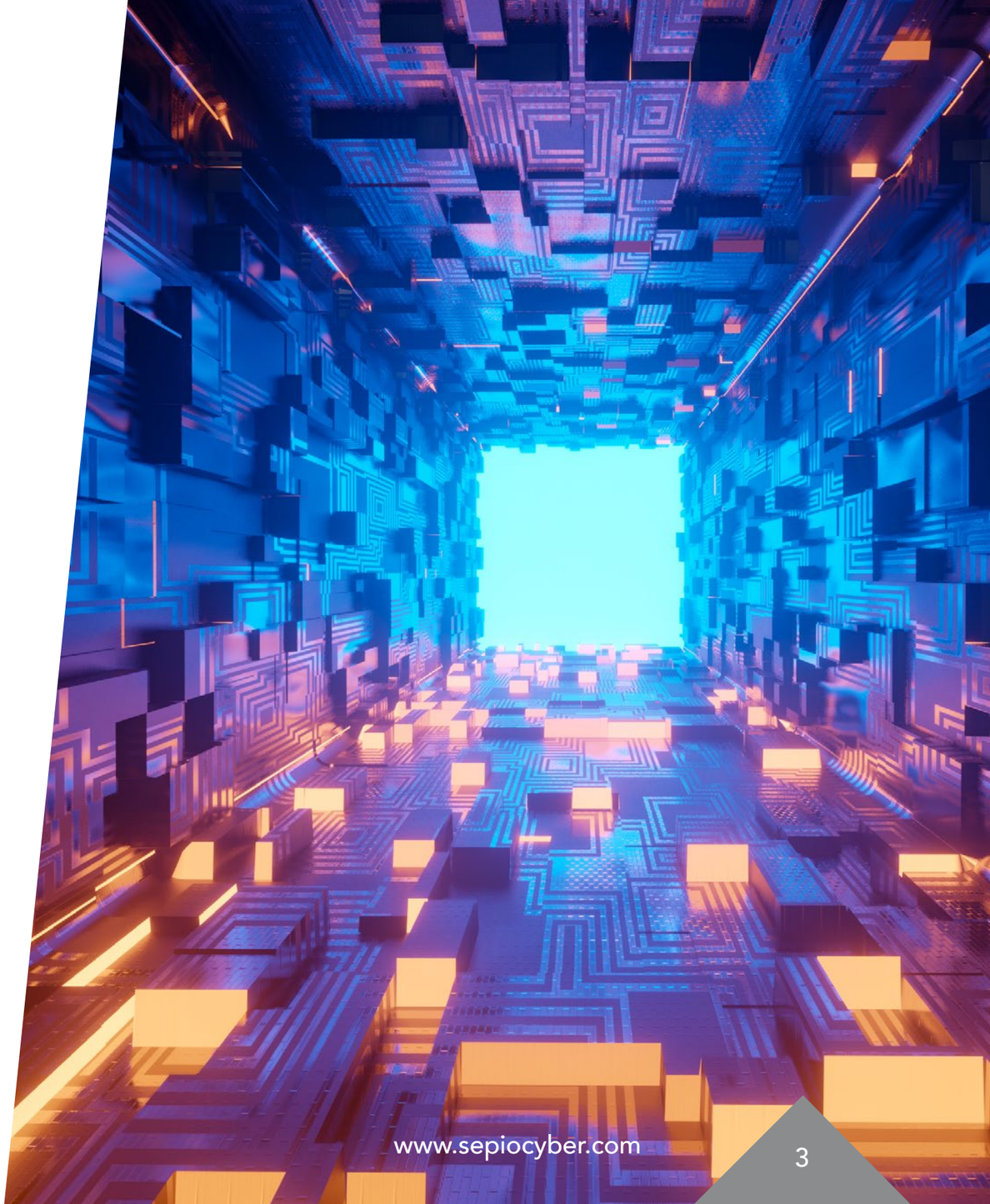
INTRODUCTION

The success of a business is undoubtedly linked to its supply chain. Yet, because of this, an organization is only as strong as its weakest link.

According to the GAO-18-667T, Reliance on a global supply chain introduces multiple risks to federal information systems. Supply chain threats are present during the various phases of an information system's development life cycle and could create an unacceptable risk to federal agencies.

These threats can have a range of impacts, including allowing adversaries to take control of systems or decreasing the availability of materials needed to develop systems. These threats can be introduced by exploiting vulnerabilities that could exist at multiple points in the supply chain. Examples of such vulnerabilities include the acquisition of products or parts from unauthorized distributors; inadequate testing of software updates and patches; and incomplete information on IT suppliers. Malicious actors could exploit these vulnerabilities, leading to the loss of the confidentiality, integrity, or availability of federal systems and the information they contain.

Today, organizations have a greater choice of suppliers and have become more reliant on third parties. This, however, also means that the supply chain has become a more complex web of interdependent companies who might not even be aware that they are connected. As a result, it is impossible to cover the entire supply chain. Additionally, technology is becoming an essential tool in the supply chain for all operations. These factors – on their own, but even more so



when combined – have precipitated an inadvertent expansion of vulnerabilities within supply chains, especially in regard to cyberattacks.

There are various actors who might target an organization's supply chain and, with that, come numerous motives behind an attack; be that an individual looking to gain financial benefits, or a nation-state or state-sponsored actor seeking to sabotage an adversary by conducting espionage.

When attacking the supply chain, it is typically the hardware (but not limited to) especially when some hardware components include built-in firmware) that is tampered with. Devices can be compromised at any point throughout the supply chain and the Rogue Device can be delivered by a supplier to the end user. Moreover, due to the interconnectedness of the involved organizations, suppliers often have access to a target's sensitive information.

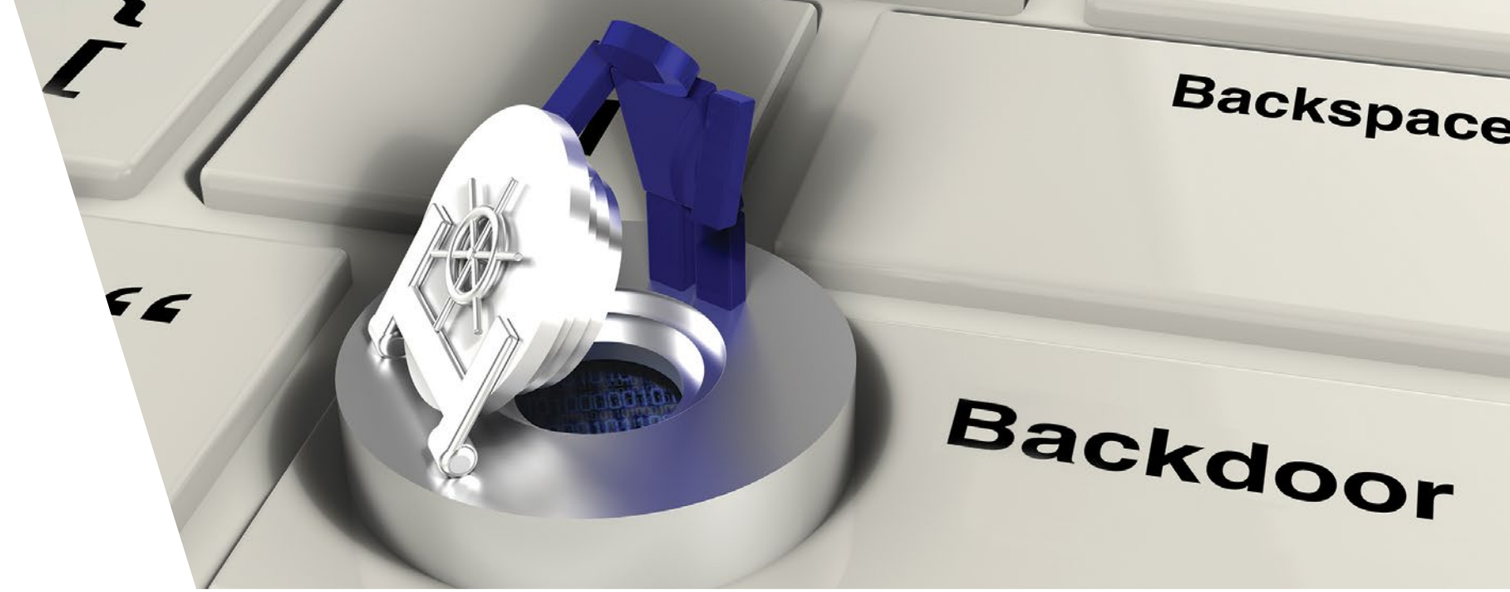
As mentioned, supply chains are becoming increasingly complex which makes detecting an attack, and its origin, extremely difficult and in many aspects supply chain attacks represent the "Holly Grail" of hardware based attacks. Additionally, implants can be microscopic and can easily go unnoticed to the human eye, avoiding any suspicion as to the device's true intentions. Sitting on the Physical Layer – Layer 1 – implants are not detected by security software solutions either. Furthemore, Spoofed Peripherals might be authorized as a genuine HID thereby not raising any security alarms. Ultimately, there are plentiful benefits that make attacking the supply chain favorable for bad actors.

VULNERABILITIES OF THE SUPPLY CHAIN

Complex Supply Chain

The more suppliers an organization has the more difficult it is to exert control, including over cybersecurity. Additionally, a large supply chain makes it difficult to detect an attack since only a handful of devices will be manipulated. If, however, an attack is detected the subsequent investigation is extremely arduous as there are a large number of players involved in the supply chain – some of which are subcontracted – making it onerous to identify its origin. Special tools are required, and a careful examination of complex equipment needs to take place. For attackers, this is ideal as it reduces the chances of being caught and reprimanded. Large supply chains also provide perpetrators with greater entry points so that if one supplier has strong security measures, there are others to infiltrate instead.

With more suppliers comes more employees. Insiders are often considered the greatest risk to a company's cybersecurity either due to careless action which causes an attack, or from malicious insiders who act with intent. Carelessness is often the result of a lack of education and awareness regarding cybersecurity and how employees themselves can cause, or prevent, an attack from taking place simply through their actions. Malicious insiders might act out for opportunistic reasons or as a form of revenge against the organization should they feel that they have been mistreated. As such, the more individuals involved in the supply chain, the greater the risk of a successful cyberattack.



Foreign Suppliers

The rise of globalization means that organizations are frequently outsourcing jobs to suppliers overseas. This on its own can provide intelligence to adversaries as it indicates which states trust each other and are willing to engage with one another for business purposes. This intelligence can be valuable in a world where the threat of cyberwarfare is rising. Increasing in prevalence, cyberwarfare allows almost any state to cause damage to an adversary. The supply chain can be an ideal entry point if the adversary's suppliers operate within the perpetrator's borders since governments have the capabilities to interject and breach the supply chain; clandestinely or not.

Alternatively, foreign suppliers pose a threat if the country in which they operate have lax security regulations. It is easier to infiltrate a supplier in a country that has fewer regulations regarding cybersecurity and data management and, from here, a perpetrator can gain access to a foreign target operating in a heavily regulated state.

Insufficient Security

Despite many countries heavily regulating cybersecurity and data management – which is addressed later on – there are still gaps in the efficacy of suppliers' security features; sometimes due to financial restraints that do not allow for a supplier to deploy high levels of sophisticated security features or simply because there are some aspects of cybersecurity that are not covered by any existing tools. Either way, it is impossible to know the security measures of all suppliers and an organization is only as strong as its weakest link. Should a supplier have insufficient security, they could be the target of an attack; either being the primary victim, which will then have a ripple effect on the entire supply chain, or they could unwittingly allow for a manipulated device to be passed through.

ATTACKS

Manipulation

Attacks on the supply chain commonly involve hardware being intercepted and manipulated. This can include the manipulation of the printed circuit board (PCB) whereby bad actors inject malicious functionality after a reverse engineering process has identified areas in which new capabilities can be added. Additionally, chips can be manipulated in order to carry out an attack and everyday peripherals can be spoofed to act with malicious intent, in this scenario, the original functionality of the chip will remain intact, while the "additional" functionality may be triggered by an external event (physical - by sending a specific RF signal or logical - via a certain access to a memory area that usually is nonexistent)

Manipulation can happen at any point throughout the device's route along the supply chain. The device will be unpackaged, modified, repackaged and put pack in transit.

Side Channel Attack

These attacks aim to extract secrets from a chip or system through measurement and analysis of physical parameters. Side channel attacks have proven to be successful in breaking algorithmically robust cryptography operations, thus meaning that anything else protected by conventional cryptographic methods is no longer protected.

Attacks:

- **Sound-based attack.**

In this type of attack, the sound of the user's keystrokes is recorded to steal passphrases. By listening to the sound of the keys being pressed, the attacker attempts to determine the text that is being produced. It requires a sophisticated Machine Learning model to distinguish one key press from another but, nonetheless, can be of great value to a bad actor.

- **Timing attack.**

Here, perpetrators will attempt to compromise a cryptosystem by analyzing the time taken to execute cryptographic algorithms. Since every logical operation in a computer takes time to execute, the time can differ depending on the input. By precisely measuring the time for each operation, the attacker can work backwards to decipher the input.

- **Electromagnetic field (EMF) radiation.**

This attack allows the electromagnetic radiation that is emitted from a device to be measured. From here, a signal analysis can be performed since different operations produce different amounts of radiation. An electromagnetic trade of encryption may reveal the exact operations being performed and attackers can retrieve full or partial private keys.

- **Thermal-imaging attack.**

The infrared images that come from observing the surface of a Central Processing Unit (CPU) can provide information about the code being executed on that CPU.

- **Power-analysis attack.**

The attacker can study the power consumption of a cryptographic hardware device, allowing them to “see inside” otherwise tamperproof hardware. This non-invasive attack provides the ability to extract cryptographic keys and other secret information from the device.

- **Acoustic cryptanalysis attack.**

Power consumption of devices cause heating, which is offset by cooling effects. These temperature changes create thermally induced mechanical stress which can create low-level acoustic emissions from operating CPUs, thus giving perpetrators information about the operation of cryptosystems and algorithms.

Fault Attack

These attacks target a physical electronic device whereby the attacker essentially causes stress to the device through an external mean e.g. incorrect voltage, excessive temperature or signal power interference. The stress generates errors in such a way that it results in a security failure of the system. This failure allows the bad actor to obtain faulty outputs or behaviors for the key recovery.

Power Line Attack

Through malware, perpetrators can control the workload of the device's CPU, thus having the ability to also control its power consumption. The emissions conducted on the power cables are measured and the signal is processed and decoded back into binary information by the attacker. Modulating changes in the current flow allows for passwords, encryption keys and other sensitive information to be stolen by bad actors.

Wireless Implants

Through the HID, computer operating systems have allowed for devices to be accepted when they are plugged in to make keyboard, mice and other input devices as easy to connect as possible. By exploiting this weakness, attackers have utilized devices that act like HIDs to carry out attacks since they will be recognized as genuine by the computer. These Rogue Devices look authentic to the human eye – such as a charging cable or a keyboard – and are used by victims without questioning their intent. The device incorporates a remote access point that allows the attacker to control the endpoint without ever needing to gaining physical access to it, thus making the job easier.

Spy Chips

These are malicious chips which can access the configurations of the target's firewall. From here, the firewall settings can be changed to provide the attacker with remote access to the target device, disable its security features and provide access to the device's log of all the connections it is exposed to. Spy chips are tiny in size – just bigger than a grain of rice – and can go easily unnoticed on a motherboard. The activation of a spy chip can occur in one of two ways – either as a "ticking time bomb" whereby it automatically activates after a certain period of time; or through "cheat codes" which activate the chip based on input conditions. As such, a spy chip may be embedded long before it causes any actual damage.

CONSEQUENCES

Loss of Productivity

Operations might be halted either by the attack itself or in order to investigate and properly remediate the attack. This is a long process since the entire supply chain will need to be investigated and every step needs to be effectively monitored.

Furthermore, attacks have shown to have an effect on employees' productivity since they are less willing to work under such circumstances i.e. when there is great disruption following the discovery of an attack.

Reputational Losses

Attacks often cause data breaches, and this will likely leave a negative feeling among customers and other components of the organization's supply chain. A poor reputation is often extremely difficult to recover from and can be the aspect an organization is most recognized for, thus harming its future.

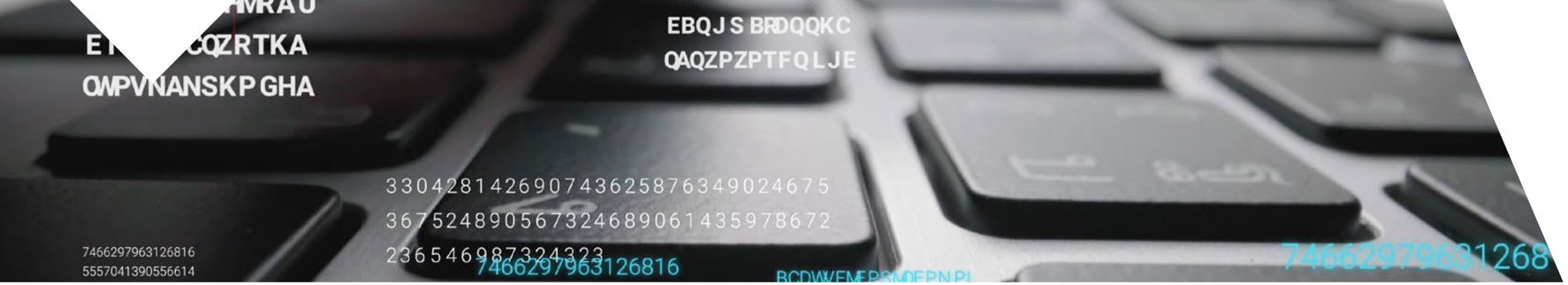
In terms of government agencies that are victim to an attack, this can have serious reputational damage on the state's ability to protect itself. This can be perilous as it demonstrates to adversaries that it is an easy target.

Loss of Business

With globalization, consumers are not short of choice; therefore, making it easier to switch to a competitor should they feel displeased with the quality of service an organization provides. Thus, a loss of business is a very likely consequence following an attack.

A diminishing reputation will likely encourage customers to switch to a competitor. If customers feel as though their data is not protected, they might want to stop supporting the organization and, moreover, potential customers might be deterred. Government departments might lose out on collaborating with other states as they are not perceived as secure enough to handle highly classified information.

A loss of business can also arise from the productivity interferences an attack can cause. Customers are usually not concerned with why their service or product has been negatively impacted, but only with the fact that it has, hence leaving them unsatisfied and wanting to move to a competitor, especially if the problem is not rectified quickly.



Financial

The aforementioned consequences all contribute to the financial costs associated with an attack. The financial costs can add up to a significant amount as there are both direct and indirect costs that accrue. Additionally, legal costs can be very likely following a data breach. Customers could file lawsuits against the organization and there are often regulatory fines that companies are required to pay. These fines, depending on the institution and the extent of the attack, can be in the millions of dollars.

State Tension

With the proliferation of cyberwarfare, states are becoming increasingly suspicious of one another and often accuse each other of carrying out an attack. For example, the United States is extremely cautious of China and Russia and vice versa. When an attack takes place on a government agency or critical infrastructure, it is common that an adversary state is blamed. This can impact all other aspects of the states' relationship, including economic and political relations.

National Security Risks

The target of an attack is often critical infrastructure, such as healthcare facilities, security agencies and financial service providers. Should any of these industries be attacked, there can be a serious risk to the direct security of the country and its citizens. Furthermore, an attack on critical infrastructure might act as indication that the country is not adequately protected, thus serving as a potential incentive for an adversary to carry out an attack, adding to the risk towards national security.

MITIGATION

Automated Optical Inspection

An Automated Optical Inspection (AOI) test, originally used in the assembly lines, enables fast and accurate inspections of populated PCBs to ensure that the item is built correctly and without any manufacturing modifications. This is done by verifying that the device is assembled according to a comparison of a golden image. An AOI solution can detect soldering changes of certain components and inconsistency in the assembled components. The main shortcoming of this solution is the fact that you need to have direct visual of the PCB, which requires significant effort when the devices are already deployed.

JTAG Boundary Scan

This is a method for testing interconnects on PCBs or sub-blocks inside an integrated circuit. Thus, JTAG is an essential tool for testing boards in development, production and in the field meaning it can be used to test at any time through the supply chain. Overall, JTAG provides information about the state of a board with minimal access. Direct internal access to the PCB is required, making post-deployment tests challenging.

Radio Frequency Power Detector

One should keep in mind, that as the attackers are aware of various RF geo-location sensor characteristics, they will use more "exotic" RF bands, and "bury" the signals using spread spectrum direct sequence or other concealment options.

Power Line anomaly detection

As ex-filtration of data and C2 connection can be implemented by using Power-Line communication (where data is transmitted over standard power cabling) Analyzing the physical layer characteristic of these power cables can provide detection of digital data "piggy-backing" over this physical channel.

X-ray

X-ray scan can be helpful for those cases where you do not want to open the unit (for various possible reasons, including voiding warranty). X-ray can detect the existence of additional/modified modules inside the supplied unit (while comparing it to a golden image or a vast database of similar devices). Nevertheless, technology for detecting when a certain unit has been X-rayed exists , which might allow the attacker to terminate its activity once suspicion has risen.

Physical Layer Fingerprinting

Through in-depth analysis of the device's physical layer characteristics - voltages, currents, eye-pattern of signals, PoE parameters etc. One can create a unique physical fingerprint for each device, later making this information usable for anomaly detection - through AI or ML based algorithms. Such detection algorithm is implemented in Sepio SepioPrime solution.

Know Your Supply Chain

It is not enough to have high levels of security protecting your own organization; all components of the supply chain need to be secured, too. It is imperative to know the answers to the following questions:

- Which organizations make up the supply chain?
- Where do vendors source their parts?
- Who integrates the components that your vendor buys?
- Who do your vendors outsource jobs to when they are overloaded?
- What security features does your vendor have in place?

Employee Training

Cyberattack techniques are outpacing security software solutions and some attacks are not even covered by any existing software. As such, it is imperative that staff are educated and trained regarding the risks of cyberattacks and how they can take action to prevent them from occurring. Importantly, since attackers are becoming increasingly crafty, the education needs to be continuous and up to date. Organizations can no longer rely on their staff being reactive; they now need to be proactive.

Continuous Checks

Although tedious, all components of the supply chain need to be continuously monitored to reduce the risk of a cyberattack by checking to ensure no hardware has been manipulated. In some cases, this is not possible purely based on the size of the supply chain. In this case, following regulations and guidelines as to how to approach this will be highly beneficial.

THE SEPIO SOLUTION

Sepio's Asset Risk Management platform sees, assesses, and mitigates all known and shadow assets at any scale, as fast as they are added by anyone, anywhere. By leveraging the physical layer data source, we get to the true source of asset risk, providing you and the security tools you've invested in with a new dimension of asset visibility that simply wasn't possible before. In a single product, Sepio unleashes the power of the entire asset security ecosystem with agnostic, actionable visibility and infinite scalability that is critical to asset risk management.

Holistic, objective truth

Sepio gets to the true source of asset risk by harnessing properties at the physical layer to generate an objective DNA profile for every known and shadow asset, regardless of its functionality and operability. Our unique approach and patented algorithms mean Sepio is untainted by misleading profile perceptions and behavioral assumptions that can deceive even the most robust cyber tools and result in erroneous risk management practices. With Sepio, your enterprise benefits from a centralized source of holistic and reliable asset visibility.

Actionable visibility

Seeing is the critical prerequisite – but what you see is only as useful as what you can do with this knowledge. Sepio helps you instantly understand what needs attention by automatically generating an Asset Risk Factor (ARF) score for every asset. Based on asset DNA profiles and contextual business, location, and rules, the ARF score prioritizes risk to provide a new element to complete asset visibility.

The ARF score alerts you of high-medium-low risks to expedite time to resolution, identify regulation gaps, and prevent crises. Sepio accounts for any changes to an asset's ARF score by continuously monitoring the entire asset infrastructure to detect any behavioral changes or anomalies. Big data and machine learning, augmented by OSINT data sources, provide up-to-date threat intelligence on known-to-be-vulnerable assets to further optimize IT efficiency. The real-time actionable visibility helps your security team better understand your asset attack surface and manage risks proactively.

Control and mitigation

The Sepio platform controls asset risk by automatically enforcing specific hardware usage through granular access controls, which are predefined by the system administrator. The solution compares an asset's DNA profile and ARF score with your preset rules and directly connects it to an enforced policy. Any changes to an asset are accounted for, and the appropriate policy applied. Assets that breach the preset rules or get recognized as known attack are immediately blocked, enabling instant and automated risk mitigation.

Infinite scalability

You can't protect assets without scale. Sepio's unique trafficless approach enables painless asset risk management across the entire ecosystem by eliminating the need for a resource draining analysis. With

Discover all known & shadow assets

Mitigate risks from uncontrolled assets

Reduce hardware clutter and optimize efficiency

Enforce asset policies and meet regulatory compliance

Integrate seamlessly with existing security tools

no IT nightmares, no privacy infringements, and no compliance issues, the platform is easy to deploy and run, taking less than 24 hours to implement – it's a product, not a project.

Greater ROI

The Sepio platform integrates seamlessly with leading cybersecurity solutions, such as NACs, EDRs, XDRs, Zero Trust solutions, and more, to bring them greater visibility and context – without us, these solutions can't complete their mission. By radically augmenting the power of existing tools, Sepio gets you more value from your IT and security investments.

We are also available on:

Linkedin >>
https://www.linkedin.com/company/sepiocyber/

Facebook >>
https://www.facebook.com/cybersepio

X (Twitter) >>
https://x.com/sepiosys

<< LEARN MORE >>