The Invisible Enemy Within

Insider Threats

When most organizations think of an insider threat, their focus is on a technically skilled, disgruntled and unethical employee or contractor with privileged access. However, there is also potential risk in an ignorant employee or contractor who provides privileged credentials to an external threat actor who then behaves like an insider within the enterprise network. Chief risk officers may feel as though they have taken all necessary measures to improve cybersecurity controls and pass external audits; however, threat actors continue to find new opportunities to compromise enterprise networks from within.

The US Department of Homeland Security defines an insider threat as "a threat in which an employee or a contractor uses their authorized access, wittingly or unwittingly, to do harm to the security of the United States."[1] Borrowing from this definition, an employee or contractor of an organization can also be considered an insider threat by using authorized access to do harm.

It is valuable for organizations to understand the surreptitious nature and complex national security implications that arise from insider threats and how they have evolved to be able to successfully address the challenges the cybersecurity community faces now and in the future.

The Shadow Insider Threat

Certain types of insider threats are largely ignored and evade detection in the face of most cybersecurity controls. There is a new type of insider threat, known as a persistent shadow insider threat, which is usually unknown to the organization and has unfettered backdoor access. Tainted software is one example of an invisible insider threat—it contains a backdoor that the remote threat actor uses to violate confidentiality.

There is no doubt the insider threat problem will remain a perpetual obstacle in enterprises' efforts to secure their systems. Some researchers believe it is the most difficult problem to deal with because insiders often have information and capabilities desired by external attackers and can, therefore, cause serious harm.[2]

The challenge posed by insider threats is made more complicated by the use of software that may be tainted with malicious code, allowing covert channels to exfiltrate trade secrets and other critical information. Most organizations test software for functionality, and if the software meets productivity requirements, then it is introduced into the production environment. However, without access to the source code, enterprises do not know if that software has a malicious backdoor that violates privacy rules.

Allen Ari Dziwa, CISA, CISSP, GIAC, PMP
Is a cybersecurity consultant and has worked for three of the largest US telecom companies in the last decade. He sits on the EC-Council's Advisory Board for Ethical Hacking and is a member of ISACA®, (ISC)² and the Information Systems Security Association (ISSA). He can be reached at allendziwa@hotmail.com or *www.allendziwa.com*. His views in this article do not represent any organization or entity. They are solely his own ideas to stir debate in the cybersecurity community.

Enjoying this article?

- Read *A Holistic Approach to Mitigating Harm from Insider Threats. www.isaca.org/insider-threats*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Trusted software distributors that are authorized to work on enterprise systems have the ability and access to violate confidentiality if they maintain backdoors unknown to the organization.

Insiders may also include third-party business partners, their employees and temporary staff.[3] As trusted third-party suppliers, it is hard to imagine they might deliver tainted software; however, well-established organizations that consistently pass external IT audits and meet regulatory requirements are increasingly becoming victims of cyberattacks.

If software used in database management or customer relationship management platforms is built by geopolitical rivals, then there is probability that the software could have backdoors. The presence of backdoors defeats the purpose of cybersecurity controls. Even if organizations spend millions of dollars building robust infrastructures, if they have no access to source code that has covert channels, then they cannot identify potential compromises, and risk management measures can be rendered ineffective.

Despite several decades of research on ways to detect and prevent insider threats, the advancement of modern networks has quickly outpaced these efforts.[4]

For example, beginning in March 2020, SolarWinds unwittingly sent out software updates to its customers that included hacked code.[5] Although SolarWinds was doing routine software updates that most organizations diligently perform to secure systems, they had no idea that the software updates were tainted.

In another report, Barnes & Noble announced that 63 of its stores had nefarious personal identification number (PIN) pads installed that allowed hackers to pull the credit and debit card numbers and PINs of customers' bank accounts.[6] This attack shows the serious risk insider threats continue to pose to organizations.

The issue of insider threats is an essential area of risk management because it threatens economic and national security.

Economic Costs of Insider Threats

According to the 2020 *Cost of Insider Threats Global Report*, the average global cost of insider threats increased by 31 percent in the last two years to US$11.45 million, and the occurrence of incidents increased by 47 percent in that period.[7] Therefore, the economic implications of these attacks are grave and mitigation methods should be seriously considered.

Many organizations do assess the suitability of third-party organizations to ensure that they meet certain established requirements. However, if a third-party organization provides a tainted software platform, then the certification is meaningless. An enterprise can get certified as meeting all standards, such as US National Institute of Standards and Technology (NIST) or International Organization for Standardization (ISO) 27000 while unknowingly using tainted software with undetectable backdoor malware carefully planted by malicious actors.

"THE ISSUE OF INSIDER THREATS IS AN ESSENTIAL AREA OF RISK MANAGEMENT BECAUSE IT THREATENS ECONOMIC AND NATIONAL SECURITY."

Organizations often perform cybersecurity awareness programs backed by boards of directors and implemented by senior management. These programs usually foster a great cybersecurity culture and reduce the ignorance of employees who may unwittingly and recklessly perform acts that make them potential threats.

For example, with regard to electronic payments that occur every day, it becomes even more critical to understand the economic implications that can arise due to compromised software systems. In one example involving The Society for Worldwide Interbank Financial Telecommunications (SWIFT) messaging network:

> *The Bank of Bangladesh faced a major cyberattack resulting in [US]$81,000,000 unrecovered. The attackers gained control over SWIFT systems by deploying trusted Windows software to the bank's internal systems. Potentially, [US]$951,000,000 was at stake.*[8]

In this case, the attackers were able to steal SWIFT credentials used by banks by posing as legitimate insiders that could initiate transactions. After more attacks involving SWIFT transactions:

> *SWIFT launched its Customer Security Programme (CSP) in 2016 to provide a forum for industry-wide collaboration against the growing threat from cyber-attacks and to help reinforce and safeguard the security of the wider ecosystem.*[9]

The SWIFT messaging network is critical to prevent and thwart insider threats of any kind, and if software systems used by depository institutions are compromised, it can lead to systemic risk with serious economic implications.

The Automated Clearing House (ACH) handles an average of 70 million transactions every day, amounting to approximately US$2,000 per transaction. Fedwire Funds Service processes only approximately 670,000 transactions per day worth an average of US$4 million, which amounts to US$2.8 trillion.[10] Such large volumes of transactions should be executed by systems with proper security controls and no room for manipulation. This is why it is essential to have an industrywide agreement to establish ways to identify tainted software from third-party vendors. Creating in-house software to interface with SWIFT or ACH systems can prevent organizations from buying tainted software; however, smaller organizations without the ability to create in-house software must still buy or rent software from third-party providers. These smaller organizations have to trust that the third-party providers they work with have done their due diligence to provide a secure software product.

Although organizations can put a limit on privileged access, raise awareness to reduce cases of social-engineering attacks gaining employee credentials and add other controls, there is no clear solution for the issue of trusted third-party software providers acting like shadow insider threat actors with backdoor access.

"STATE-SPONSORED ACTORS CAN INFILTRATE SOFTWARE-CREATING ORGANIZATIONS AND PLANT BACKDOORS THAT FUNNEL ENCRYPTED DATA TO THEIR SERVERS WITHOUT DETECTION."

The Remediation Challenge

Even if software developers pass background checks, there is really no way to tell if they are working for geopolitical adversaries. They could work as spy agents and plant backdoors that evade detection with known technology. This is how some organizations that follow the best security practices are still hacked.

State-sponsored actors can infiltrate software-creating organizations and plant backdoors that funnel encrypted data to their servers without detection. There is also the possibility that threat detection software itself may have malicious software that gives a full view of security operations to adversaries thousands of miles away.

Unfortunately, threat actors seem to be miles ahead of research teams in terms of technical sophistication and tricks to bypass detection. By using the dark web, there is no doubt the information sharing capabilities of malicious threat actors are superior to the slower speed at which cybersecurity threat intelligence teams disseminate information needed to prevent and adequately respond to cyberattacks.

Threat actors have always known that using phishing emails has gotten old and fewer people open the links and enter their credentials. Many enterprises have put considerable effort into educating their employees, and threat actors know that many organizations now follow strict processes to issue privileged credentials and terminate them when there is no business need for access. Organizations also now better understand data leak prevention systems and that they can also be compromised by unscrupulous threat actors masquerading as employees.

Conclusion

The existence of insider threats due to tainted software from original software manufacturers whose employees might include rogue developers sponsored by geopolitical rivals, means that shadow insider threats should remain a cause for concern. Because of sophisticated and evolving coding techniques, there might not be auditing tools that have the technical capability to detect such backdoors and covert channels. There is even the possibility that firewalls, intrusion detection systems and intrusion prevention systems currently being used might already be compromised, allowing certain traffic to pass through undetected, as predetermined by the rogue developers.

The persistent shadow insider threat is real and here to stay. The cybersecurity industry can agree to prioritize finding ways to detect and reject tainted software by developing standards and, if possible, with support of legislative instruments to enforce the review of third-party software by an authoritative body to validate whether the software used in critical systems is free of backdoors.

Endnotes

1 US Department of Homeland Security, "Insider Threat," *https://www.dhs.gov/science-and-technology/cybersecurity-insider-threat*

2 Hunker, J.; C. Probst; *Insiders and Insider Threats—An Overview of Definitions and Mitigation Techniques*, 2011, *http://isyou.info/jowua/papers/jowua-v2n1-1.pdf*

3 Schultz, E. E.; "A Framework for Understanding and Predicting Insider Attacks," *Computers and Security*, vol. 21, iss. 6, p. 526–531

4 Liu, L.; O. De Vel; Q. L. Han; J. Zhang; Y. Xiang; "Detecting and Preventing Cyber Insider Threats: A Survey," *IEEE Communications Surveys and Tutorials*, vol. 20, iss. 2, 2018

5 Jibilian, I.; K. Canales; "The US Is Readying Sanctions Against Russia Over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal," *Business Insider*, 15 April 2021, *https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12*

6 Piercy, R.; "The Persistent Insider Threat: Is Enough Being Done?" *ISACA® Journal*, vol. 1, 2017, *https://www.isaca.org/archives*

7 Saxena, N.; E. Hayes; E. Bertina; P. Ojo; K. K. R. Choo; P. Burnap; "Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses," *Electronics*, vol. 9, iss. 9, July 2020

8 Deloitte, SWIFT Systems and the SWIFT Customer Security Program, Belgium, 12 September 2019, *https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-ra-swift-customer-security-programme.pdf*

9 SWIFT, "How to Spot, Stop and Defend Against Cyberattacks," *https://www.swift.com/your-needs/financial-crime-cyber-security/financial-fraud/how-defend-against-cyber-attacks*

10 Federal Reserve Bank of San Francisco, "What Is the Fed: Payment Services," USA, *https://www.frbsf.org/education/teacher-resources/what-is-the-fed/payment-service*