U.S. Customs and Border Protection

Customs-Trade Partnership Against Terrorism

Alert

Cyber Intrusions

The Customs-Trade Partnership Against Terrorism (C-TPAT) program is one layer in U.S. Customs and Border Protection's (CBP) multi-layered cargo enforcement strategy. Through this program, CBP works with the trade community to strengthen international supply chains and improve United States border security.

To enhance communication with its members, C-TPAT routinely highlights security matters for the purpose of raising awareness and renewing Partners' vigilance, and recognizing best practices implemented to address supply chain security concerns.

The purpose of this C-TPAT Alert is to make U.S. Customs Brokers and Importers aware of a potential security threat that could possibly compromise their Information Technology (IT) systems and the importer information contained within.

Cyber thieves recently hijacked credit-card and bank information belonging to the customers of a well-known retailer during the 2013 Christmas holiday season. The attack and data breach continued undetected for a number of days and resulted in the theft of approximately 40 million credit and debit card records. In addition, the personal information of approximately 70 million customers was compromised.

In a similar instance, consumer credit card payment details were compromised when hackers infiltrated the computer system of a national hotel management company. The company stated that information subject to potential theft by cyber criminals included names and numbers on consumers' debit or credit cards, security codes and card expiration dates. These attacks are the latest in a series of incidents where personal information has been stolen by criminals hacking into systems designed to protect retailers, banking institutions, and consumers. One method of compromising computer systems and devices is through socially engineering the victim to unknowingly introduce malicious malware on their network in order to acquire personal information such as account numbers and PIN codes.

Malware is software designed to attack and disrupt computer operations, gather sensitive information, or gain access to private computer systems and networks. It can appear in the form of code, scripts, active content, web pages and other software. Malware is a term used to describe a range of threats including viruses, worms, spyware, and other malicious programs. Importers and U.S. Customs Brokers, who are responsible for the clearance of goods through CBP using importers' information in the entry process, should also be aware of corporate information theft. Unsuspecting U.S. Customs Brokers may have their computer systems compromised with the introduction of malware.

Legitimate importer information, such as Importer Employee Identification Numbers (EIN) and company addresses have been stolen by cyber criminals who then approach U.S. Customs Brokers with the hijacked information. This information is then used to submit a customs entry under the legitimate importer's name to import contraband and counterfeit goods into the United States. It could also be used to import weapons and ammunition. The importer information, once obtained, can also be used to create a forged power of attorney, which is required for entry. Once the illegitimate shipment obtains customs release, fees related to broker services, as well as applicable duties and taxes, are not paid. The importer is usually not aware of the theft of its corporate information or the illegitimate importation until after the criminals abscond with the imported goods following the release of the goods from CBP.

There are many ways in which malware can be introduced into an IT system. Unwary users may be tricked into clicking on a link, opening an unsolicited email (SPAM) containing the malware, visiting a page that contains malware, or when current anti-virus software installed to protect the system is out of date.

Indicators that an IT system has been infected with malware include a slower than normal operating system; users encountering messages indicating the computer is infected and requesting software be purchased or downloaded; the computer system crashing or freezing due to corruption of data; users getting error messages that indicate a file cannot be opened or a command cannot be completed; files disappearing; random network activity when the router is constantly blinking when no programs are being run; unexpected anti-virus disabling; and changes in web browser settings.

C-TPAT U.S. Customs Brokers are required to adhere to specific security criteria designed to mitigate the possibility of terrorists exploiting the supply chain and to reduce the risk of loss, theft, and contraband smuggling. All C-TPAT Partners, including U.S. Customs Brokers, must have security measures in place to safeguard computer access and information and to identify the abuse of IT including improper access, tampering, or the altering of business data. IT systems must also be protected with anti-virus and anti-spyware software which must be updated periodically. Company employees must also receive training to recognize how to detect, avoid, and report malicious attempts to introduce malware into the company's IT system.

C-TPAT Program

CBP.GOV/CTPAT
1300 Pennsylvania Avenue, NW
Washington, DC 20229

(202) 344-1180
Industry.partnership@dhs.gov