FBI Cyber Division

Private Industry Notification

21 October 2014

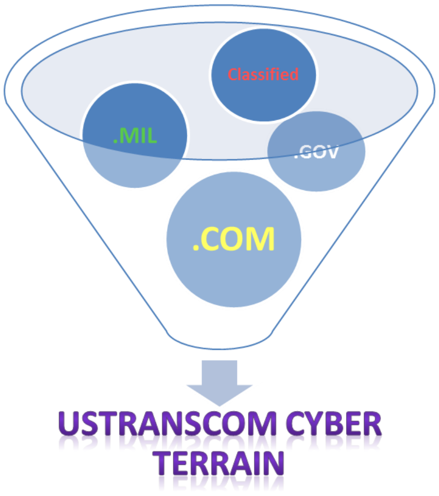
PIN #: 141021-001

(U) USTRANSCOM Contractors Vulnerable to Cyber Targeting

(U) This Private Industry Notification (PIN) highlights foreign cyber actors targeting Department of Defense (DoD) maritime contractors and the need for timely reporting of intrusions. During a 12-month period beginning on 1 June 2012, there were approximately 50 computer intrusions or other cyber events where the networks belonging to the US Transportation Command (USTRANSCOM) maritime and aerial services contractors were targeted. The US Intelligence Community believes that at least 20 of the 50 incidents were attributed to state-sponsored actors employing *advanced persistent threat* [a] tactics. Yet, in some instances, USTRANSCOM remained unaware that foreign cyber actors were actively targeting its maritime contractors. There are several explanations as to why USTRANSCOM was unaware that its contractors were being targeted: a failure on the part of the contractors to report intrusions, a failure on the part of the contractors to report attempted intrusions to USTRANSCOM, and the contractor's inability to detect successful cyber attacks or report intrusion attempts that were being dismissed as having failed, considered isolated and/or insignificant.

(U) Cyber Threats to Defense Operations

(U) According to a September 2014 report from the Senate Armed Service Committee (SASC)[b], foreign governments regularly probe DoD and contractor computer networks to identify vulnerabilities that could allow them access to proprietary information, collect intelligence, or establish footholds for future exploitation. Although the intrusions were in many instances attributed to Chinese cyber actors, it is unknown to what degree other adversaries are engaged in similar activity.



(U) The private sector plays a crucial role in force mobilization, deployment, and sustainment operations, according to the report. The overwhelming majority of DoD deployment transactions occur over

[a] (U) **Advanced Persistent Threat** (APT) describes cyber attacks mounted by organizational teams that have deep resources, advanced penetration skills, specific target profiles and are remarkably persistent in their efforts. They tend to use sophisticated custom malware that can circumvent most defenses, stealthy tactics and demonstrate good situational awareness by evaluating defenders responses and escalating their attack techniques accordingly. (Source: www.hackingtheuniverse.com/infosec/isnews/advanced-persistent-threat; accessed 21 October 2014)

[b] (U) SASC, Committee Report; 17 September 2014; (U) Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors; UNCLASSIFIED.

unclassified networks, many of which are operated by private companies. Private companies also play an integral role in the development of software and systems to support military logistics. These arrangements, while necessary, create vulnerabilities that can be exploited as a method of degrading or disrupting the US military's response to contingencies.

- (U) In addition to the Maritime Administration's (MARAD) ready reserve fleet and Military Sealift Command (MSC) ships, USTRANSCOM relies on commercial ships provided under the Voluntary Intermodal Sealift Agreement (VISA) to support its activities when called upon.

- (U) In other instances, foreign cyber actors targeted Commercial Reserve Air Fleet (CRAF) transportation companies. Although in peacetime, these companies perform little or no CRAF-related business, in wartime they become a critical element of USTRANSCOM's plan for moving troops and equipment around the world.

(U) Chinese military analysts, for example, have identified logistics and mobilization as potential US military vulnerabilities given DoD's requirement for precision in coordinating transportation, communications, and logistics networks, according to the SASC. According to the same report, Chinese military doctrine ***"advocates[s] targeting adversary command and control and logistics networks to impact their ability to operate during the early stages of a conflict."*** The need to use unclassified military and commercial communications exacerbates the logistics vulnerability.

- (U) Foreign cyber actors likely target the business networks of maritime and aerial contractors, focusing their efforts on establishing a foothold and then exploiting the Enterprise Resource Planning[c] (ERP) and Customer Relation Management[d] (CRM) systems supporting shipping and logistics activities for both commercial and military customers. Additionally, the Terminal Operating Systems[e] (TOS) used by containerized cargo ports are potential targets for cyber exploitation or attack by foreign cyber actors.

- (U) In a July 2014 report, a US-based security company highlighted the vulnerability of shipping and logistics systems to attacks by APT threat actors. In this instance, malware was delivered into shipping and logistics enterprise environments from a Chinese manufacturer that sold proprietary hardware for handheld scanners. The attackers obtained access to sensitive data resident on business systems used by the victimized companies.

[c] (U) **Enterprise Resource Planning** (ERP) business process management software that allows an organization to use integrated applications to manage the business and automate many back office functions. ERP software integrates all facets of operations, including product planning, development, manufacturing, sales and marketing.

[d] (U) **Customer Relationship Management** (**CRM**) tools are used to manage a company's interactions with current and future customers. It involves using technology to organize, automate and synchronize sales, marketing, customer service, and technical support. These systems can track customer analysis by customer clicks and sales. Places where CRM is used include call centers, social media, direct mail, data storage files, banks, and customer data queries.

[e] (U) **Terminal Operating Systems** (TOS) are a key part of the supply chain and are used to control the movement and storage of various types of cargo in and around a Container terminal or Port. The TOS database can then provide useful reports about the status of goods, locations and machines in the terminal.

(U) The FBI and USCG jointly published PINs 130903-001 and 140326-008, which highlighted the vulnerability of the TOS used by the maritime industry to cyber-based criminal actors. These publications, as well as the July 2013 Brookings Institute policy paper *"The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities,"* provide additional information maritime cyber vulnerabilities.

(U) Adersary Tactics, Techniques and Procedures used in Cyber Attacks

This chart is UNCLASSIFIED in its entirety.

(U) Adversary Tactics, Techniques and Procedures

- ***Social Engineering***
    - Adversaries conduct open-source research to gather data to facilitate activity:
        - Targets are sent **spear-phish** emails to elicit sensitive information
        - Targets are sent **spear-phish** emails with malicious attachments or links to infect computers
            - Emails will look legitimate and may appear to be from within target group
            - Other possible themes include natural disasters, health issues, holidays
            - Pay attention to the URL of websites
    - May approach targets through a variety of **social media** and **networking sites**
        - May appear to be a member of the group or seeking employment
        - Do not provide sensitive / personal information
- ***Waterholing***
    - Utilizes websites the target group frequents
    - The websites are compromised and seeded with malware
    - Member(s) of the target group visits the malicious website and is infected
    - Adversaries use criminal **exploit kits** to facilitate exploitation from waterholing
- ***Network/Website Scanning / SQL Injection***
    - Many adversaries use commercial off-the-shelf tools to scan networks/websites for vulnerabilities
    - May lead to intrusion and lateral movement across the network

(U) Notice of Coordination

(U) This FBI product has been coordinated with USTRANSCOM and the Defense Security Service (DSS).

(U) Reporting Notice

(U) The FBI and USTRANSCOM continuously monitors threats to the computer and information technology systems used to support DoD logistics and mobilization activities, and encourages recipients to report information concerning suspicious cyber activity to FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or cywatch@ic.fbi.gov, or to their local FBI field office, www.fbi.gov/contact/fo/fo.htm. Incidents may also be reported telephonically to the USTRANSCOM Cyber Operations Center (CyOC) Duty Officer at (618) 220-4222.

(U) When available, each cyber incident report should include: the date; time; location; an initial list of technical indicators of activity including IP addresses, domains, tools observed; specific details on the activity including an initial list of affected systems/programs; name of the submitting company or organization; and a designated point of contact with phone number and email.

(U) If you are a member of the FBI InfraGard public-private sector alliance, you may take advantage of the iGuardian reporting capability on the InfraGard portal. If you are not an InfraGard member but wish to join the InfraGard alliance, please refer to the procedures found on their portal at www.infragard.org.

(U) If you are a member of the Department of Defense's Defense Industrial Base Cyber Security/ Information Assurance (DIB CS/IA) Program, you may report information on the DIBNet Portal at dibnet.dod.mil. If you are not a DIB member enrolled with the program, please see the procedures listed on their website.

(U) Administrative Note: Law Enforcement Response

(U) In addition to federal, state and local law enforcement agencies, the information contained in this product is authorized for release to InfraGard partners; our Information Sharing and Analysis Center (ISAC) partners including the Defense Industrial Base ISAC, Maritime ISAC, and Supply Chain ISAC for distribution to their members; and to the US Coast Guard and the Defense Cyber Crime Center (DC3) for uploading their respective web portals.

(U) This product is marked **TLP: GREEN**. The information in this product is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels. No portion of this product should be released to the media, posted to public-facing Internet Web sites, or transmitted over non-secure, external communications channels.

(U) For comments or questions related to the content or dissemination of this document, please contact the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or cywatch@ic.fbi.gov.

(U) APT Intrusion Phases

This chart is UNCLASSIFIED in its entirety.

(U) Advanced Persistent Threat Phases		
Step 1 Infiltration	Reconnaissance	Actors search open sources to identify and assess targets for collection and entities/relationships to exploit in the attack.
	Infection	The initial intrusion, typically spear phishing e-mails with a linked or embedded malicious file containing different techniques.
Step 2 Persistence	Establish backdoors	Attackers maintain network footholds by obtaining domain administrative credentials and moving laterally through a network, establishing multiple backdoors.
	Enumerate the Network	APT attackers laterally enumerate a network gathering valid credentials (user accounts and passwords) for multiple systems.
	Install Utilities	Attackers install any number of several malicious utilities necessary to maintain persistence and ultimately steal information
	Escalate Privileges	Attackers install any number of several malicious utilities necessary to maintain persistence and ultimately steal information
Step 3 Exfiltration	Harvest Data	Specific documents and e-mails containing targeted data are collected and packaged into a single, encrypted, and password-protected compressed file.
	Exfiltration	The attackers exfiltrate the compressed file to another compromised system in their command-and-control infrastructure
	Conceal Activity	Finally, attackers either attempt to clean up their tools, maintaining persistence, or set the attack in a dormant state to evade detection while maintaining access.