FBI Cyber Division

Private Sector Advisory

July 10, 2013

(U//FOUO) APT Actors Increased Interest in the Aviation Industry

(U) General Observations

(U//FOUO) Since June 2013, the FBI has observed advanced persistent threat (APT) actors' increased interest in the aviation industry. APT actors have sent spear-phishing e-mails targeting individuals associated with the air travel industry. Some of the spear-phishing e-mails originated from a spoofed sender in an attempt to make the e-mail appear more legitimate. E-mail recipients should be aware of suspicious and potentially malicious e-mail attachments or links.

(U) Impact of APT Activity

(U//FOUO) Every organization is at risk of being the target of an APT attack. APT actors, who are semi-sophisticated and difficult to detect while on network systems, have already cost US entities hundreds of millions of dollars over the past decade as a result of harvesting enormous amounts of critical information including proprietary data, source code, negotiation tactics, and strategic operational plans. These actors have also breached networks containing sensitive national security information. Going forward, this activity can best be mitigated with paradigmatic shifts in cyber security.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) APTs versus Hackers/Cyber Criminals

(U//FOUO) Advanced persistent threat actors differ from common hackers or cyber criminals by conducting targeted, rather than opportunistic, attacks that seek precise information rather than monetary gain, more closely resembling espionage. While the activity cannot often be definitively linked to any particular nation state, the sophistication, resources, and types of information sought suggests governmental support.

(U//FOUO) A general overview of the process by which APT actors compromise networks and systems is detailed in the table below, the vector of infection being most crucial:

1 - Infiltration	Reconnaissance	Actors search open sources to identify and assess targets for collection and entities/relationships to exploit in the attack.
	Infection	Typically, well-crafted spear phishing e-mails with linked or embedded files containing malicious code serve as the intrusion vector.
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	Persistent threat intruders 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	With access and persistence established, intruders escalate their privileges and prepare for exfiltration.
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 intruders exfiltrate the compressed file to another compromised system in their command and control infrastructure.
	Conceal Activity	Finally, intruders either attempt to clean up their tools, maintaining persistence, or set the attack in a dormant state to evade detection while maintaining access.

(U) Defending Against APT Activity

(U) When weighing available options pertaining to the implementation of appropriate mitigation strategies, organizations must begin by asking themselves the following:

- (U) If proprietary data, personally identifiable information (PII), research and development-related data, e-mail, or other critical information were stolen, what would the current and future consequences be?

- (U) Has my organization evaluated data criticality based on risk? What must be protected in the organization?

(U) To mitigate the threat of APT activity, DHS's United States Computer Emergency Readiness Team (US-CERT) recommends the following actions:

- (U) Audit what needs to be networked and remove ("air gap") vital information from networked devices to ensure data protection.

- (U) Monitor for and report on suspicious activity, such as spear phishing e-mails, leading up to significant events and meetings.

- (U) Educate users about social engineering and e-mail phishing related to high-level events and meetings.

- (U) Measure expected network activity levels so that changes in patterns can be more easily identified.

- (U) Always treat unsolicited or unexpected e-mail containing attachments or links with caution, even (and perhaps especially) when the e-mail appears related to known events or projects.

(U) Reporting Notice

(U) The FBI and US-CERT encourage recipients of this document to report information concerning suspicious or criminal activity to the local FBI field office. The FBI's 24/7 Strategic Information and Operations Center can be reached by telephone at 202-323-3300 or by e-mail at SIOC@ic.fbi.gov. FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm. US-CERT can be reached by telephone at 888-282-0870 or by e-mail at SOC@us-cert.gov. The US-CERT homepage can be found online at www.us-cert.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) Administrative Note: Law Enforcement Response

(U) Information contained in this product is for official use only. No portion of it should be released to the media, the general public, or over non-secure Internet servers. Release of this material could adversely affect or jeopardize investigative activities.