

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY OFFICE OF THE INSPECTOR GENERAL OFFICE OF INVESTIGATIONS

1200 PENNSYLVANIA AVENUE NW ARLINGTON, VA 20460

REFERRED FOR ACTION REPORT OF INVESTIGATION CONCERNING

UNKNOWN SUBJECT: IP (EXTERNAL FIREWALL 2009-CS-0145

TABLE OF CONTENTS

	TABLE OF CONTENTS
Narrative Entities and Individuals Prosecutive Status Exhibits	Section A Section B Section C
Distribution:	Approvals:
DAIGI STEPHEN NESBITT, AIGI	Special Agent
	Special Agent in Charge

OFFICE OF INSPECTOR GENERAL OFFICE OF INVESTIGATIONS

CASE NO .: DATE OPENED: 2009-CS-0145 09/24/2009

UNKNOWN SUBJECT: CASE AGENT: CASE TITLE:

(EXTERNAL FIREWALL

COMPUTER INTRUSION OFFICE: OFFICE OF CASE CATEGORY:

INVESTIGATIONS -

NERC

PHILADELPHIAEASTER N RESOURCE CENTER

JOINT AGENCIES: None

MARYLAND JURISDICTION:

SECTION A - NARRATIVE

Predication

On August 13, 2009 the Environmental Protection Agency (EPA), Office of the Inspector General (OIG), Office of Investigations (OI) received notification from Computer Sciences Corporation (CSC) of an intrusion detected on the EPA's application development site.

Investigation revealed that an alert was detected by the CSC August 12, 2009 at 4:00PM. An intrusion was detected from several IP addresses with up to 10,000 outbound events noted from one single system. In depth review of the CSC system reports revealed unidentified attackers had made 10776 attempts to exploit a

detected inbound connection attempts from multiple Internet The CSC

Protocol (IP) addresses

Possible violations:

- 1. TITLE 18 USC SEC 1030, Fraud and related activity in connection with computers
- 2. TITLE 18 USC SEC 1029, Fraud and related activity in connection with access devices

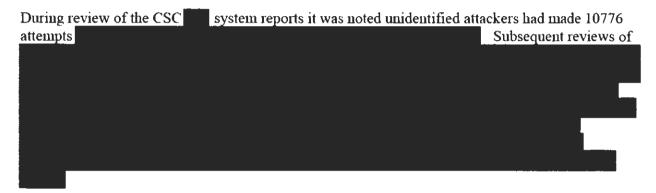
Impact/Dollar Loss

2

No dollar loss; Potential threat & vulnerability to EPA Information Exchange Network; Flawed & vulnerable testing procedures, No due diligence

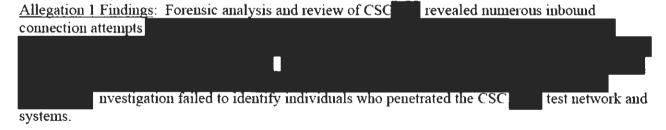
Synopsis

Investigation and forensic analysis revealed an intrusion was detected which targeted several Agency systems utilized by CSC to perform testing of applications. These systems were created, maintained and operated as a developmental network by CSC within their corporate network. Verification was obtained that no CBI or other sensitive data was available to the intruders on the systems compromised. The entire severity and impact was not determined based on the limited availability and destruction of digital evidence for analysis.



Details

Allegation 1: TITLE 18 USC SEC 1030, Fraud and related activity in connection with computers



Allegation 2: TITLE 18 USC SEC 1029, Fraud and related activity in connection with access devices

Allegation 2 Findings: Forensic analysis and review of
. Investigation failed to identify individuals who compromised system access devices for the
'SC test network and systems.

Disposition

During the course of investigation it was discovered that the intrusion occurred against the CSC company domain where they were testing a upgrade. During the early phase of the investigation the contract was transferred to CGI federal for continued execution. In that transition data and systems transferred to CGI federal were unrecoverable.

No other hostile activity

has been reported. This investigation is being closed.

SECTION B - ENTITIES AND INDIVIDUALS

Name of Person: UNKNOWN

Title & Company: UNKNOWN & UNKNOWN

Role: Subject

Business Address: UNKNOWN, Business Phone: UNKNOWN

EPA Employee: N

SECTION C – PROSECUTIVE STATUS

ADMIN/CRIMINAL/CIVIL ACTION(S): UNKNOWN
Investigation failed to identify individuals who penetrated the CSC network and systems.
No referral is made for action.

EXHIBITS

DESCRIPTION	EXHIBIT
EPA Form 2720-15 - Date Attached: 10/13/2009 Time Attached: 4:03:30	1
EPA Form 2720-15 - Date Attached: 10/13/2009 Time Attached: 4:11:15	2
EPA Form 2720-15 - Date Attached: 10/13/2009 Time Attached: 4:13:39	3
EPA Form 2720-15 - Date Attached: 10/13/2009 Time Attached: 4:36:56	4
EPA Form 2720-15 - Date Attached: 10/13/2009 Time Attached: 4:15:21	5
EPA Form 2720-15 - Date Attached: 9/18/2009 Time Attached: 2:38:34	6
EPA Form 2720-15 - Date Attached: 9/18/2009 Time Attached: 2:40:15	7
EPA Form 2720-15 - Date Attached: 9/18/2009 Time Attached: 3:03:10	8
report	9
EPA Form 2720-15 - Date Attached: 10/7/2009 Time Attached: 3:47:19	10
EPA Form 2720-15 - Date Attached: 10/7/2009 Time Attached: 3:58:40	11
EPA Form 2720-15 - Date Attached: 10/7/2009 Time Attached: 4:00:46	12
Tiger Documents 1	13