SOC IMS: SOC-20110515-216798

Last Updated: 2/28/2014 1:41 AM

SOC Incident Management System

IMS User Contact:	(b) (6), (b) (7)(C)	**Restrict Access To:**	All IMS
Record Permissions Group:	All IMS Users	**Record Source:**	

Contact Details

Enter the NASA AUID or email address of the Contact, and click "Lookup Contact Details" to automatically retrieve the information.

AUID:		**Email:**	

Enter Contact information below if the primary contact is not an IMS user

Contact Last Name:		**Contact First Name:**	
Contact Role:		**Contact Office Phone:**	
Contact E-mail:		**Contact Cell Phone:**	
Contact AUID:		**Contact NASA Center:**	
Contact Building:		**Contact Room Number:**	
Contact Type:			

General Details

SOC Tracking Number:	SOC-20110515-216798	**Categorization:**	Incident
Date Record Created (UTC):	5/15/2011 2:12 PM	**Incident Time Zone:**	UTC - Coordinated Universal Time Zone (GMT)
Title:	US-Cert providing open source report of possible breach of security at various agencies.		
Brief Description:	US-Cert providing open source report of possible breach of security at various agencies, including NASA. Report link at: hxxp://www.thehackernews.com/2011/05/exclusive-report-is-department-of.html Please investigate. Message from US-Cert: NASA SOC, The incident was opened by us but the specific reason may not have been included in our initial notification. An open source report was brought to our attention and in it, a possible breach of security affecting your agency was included. A portion of the article is shown below. We are not able to confirm the vulnerabilities stated below and leave it to the various agencies to investigate. Sorry for any confusion. Respectfully, (b) (6), (b) (7)(C) Asst. Sr Watch Officer US-CERT Operations Center Department of Homeland Security (b) (6), (b) (7)(C) (b) (6), (b @(b) (6), (b) (7)(C) ~~FOR OFFICIAL USE ONLY~~ More information included in the journal section.		
Current Status:	Resolved	**Assigned To:**	CTA (Cyber Threat Analysis)

Current Priority:	Medium	**Also Notify:**	
Notify on Save:	Yes	**Notify US-CERT on Save:**	
CUI:	No CUI or PII		
Ok To Close:	No		

US CERT Reporting

Risk Rating:			
Information Impact:		**Functional Impact:**	
Recoverability:		**Attack Vectors:**	
Critical Service or System:		**Classified Incident:**	
Major Incident:		**High Value Assets (HVA):**	
Reportable to Congress:			
Observed Activity:		**Number of Records Impacted:**	
Location of Observed Activity:		**Number of Systems Impacted:**	
Actor Characterization :		**Number of Users Impacted:**	
Action Taken to Recover:		**Number of Files Impacted:**	

The fields below hold the US-CERT Reporting fields that were in force from October 1, 2015 through March 31, 2017. The are included here for reporting purposes only.

Functional Impact old:		**Informational Impacts old:**	
		Recoverability Impact old:	

Related Tasks

Task ID	Assigned To	Due Date (UTC)	Priority	Status	Description	Resolution
216799	M&D (Monitoring and Detection)	5/16/2011 5:00 AM	Medium	Complete	(b) (6), (b) (7)(E)	Data was uploaded 5/17.

following: (b) (7)(E), (b) (6)
(b) (7)(E), (b) (6)
(b) (7)(E), (b) (6)
(b) (6), (b) (7)(E) [redacted]

According to the post there are "Lots More" IPs that have not been posted. Probably wise to search/mine the following for anomalous traffic:

(b) (6), (b) (7)(E) [redacted]

Related Incidents

Select Relationship:		**Relationship Description:**	

Parent Incident

SOC Tracking Number	Current Status	Title
No Records Found		

Child Incidents

SOC Tracking Number	Current Status	Title
No Records Found		

Sibling Incidents

SOC Tracking Number	Current Status	Title
No Records Found		

Incident Details

Time Incident Started:		**Time Incident Started (UTC):**	
Time Incident Detected:		**Time Incident Detected (UTC):**	
Center Affected by Incident:	(b) (6), (b) [redacted] (b) (6) [redacted] (b) (6) [redacted]	**Overall Impact (reference):**	Low
US-CERT Category:	CAT 5 - Scans/Probes/Attempted Access	**Incident Subcategory:**	
US-CERT Tracking Number:		**ESD Ticket #:**	
Resolution Status:	Concluded	**Malware Family:**	

		Highest level of access gained:	
Primary Method used to Identify Incident:	Notified by 3rd Party		
Primary Attack Category:			
Primary Vulnerability Type:		**Lost or Stolen NASA Equipment:**	

Lost or Stolen NASA Equipment Application

Tracking ID	Cause of Loss	Type of System Lost	Description of Circumstances
No Records Found			

Host Information

NASA Hosts

IP Address	IPv6 Address	Host Name	Center/Facility
No Records Found			

External Hosts

IP Address	External IPv6 Address	Host Name	Position in this attack
No Records Found			

Campaigns

Campaign Name:		**Reviewed By TVA:**	
Campaign Comment:		**Confirmed By TVA:**	
		Is APT:	

Indicators of Compromise

IOC Domain

FQDN	Do Sinkhole	Comment
No Records Found		

IOC IP

IP Address	IP Block	Comment
No Records Found		

IOC File

Filename	MD5 Hash	Comment
No Records Found		

IOC Registry Key

Key Name	Key Value	Comment
No Records Found		

IOC Email

Sender Email	Subject	Comment
No Records Found		

IOC Detection

Name	Type	Comment
No Records Found		

Root Cause Statement

The Root Cause Statement can be constructed from the following fields like so:
"SOURCES source realized CATEGORIES using METHODS exploiting CAUSES (with additional FACTORS) gaining OBJECTVES."
See the help for the individual fields for more information about what the various values mean and their context.

Root Cause Sources:		**Root Cause Categories:**	
Root Cause Methods:		**Root Cause Causes:**	
Root Cause Factors:		**Root Cause Objectives:**	

Reporting Organizations

Reporting Date (UTC)	Reporting Local Date	Reporting Local Time Zone	Reporting Notes	Reporting Number	Reporting Organization	Reporting Organization Contact
No Records Found						

Impact of Incident

NASA Programs, Projects, and/or Operations:		**People:**	
Data (at Rest or Transmission):		**System:**	
Cost:		**Sophistication / Nature of Attack:**	

Number of systems affected by this incident:		**Number of NASA Centers/ Facilities affected by this incident:**	
Number of accounts affected by this incident:		**Critical Infrastructure Impacted:**	
Other Impacts:			
Overall Impact:	Low -- Incident Considered Low if none of the below Categories are rated Moderate or High		

Containment Actions

Incident Containment System Action:	
Incident Containment Network Action:	

Recovery Actions

Incident Recovery System Action:	
Incident Recovery User Action:	

Recommendations

Root Cause:	
Lessons Learned:	

Costs

Center (Hours):		**Center (Dollars):**	
NASA SOC (Hours):		**NASA SOC (Dollars):**	
NASA NOC (Hours):		**NASA NOC (Dollars):**	
Other Costs (Hours):		**Other Costs (Dollars):**	

Total Costs in Hours and Dollars are automatically calculated as the sum of the individual costs above. Center IR teams or managers should enter the Center costs, the NASA SOC Manager should enter the SOC Costs and the NOC Manager should enter the NOC costs, if any, in order to arrive at the Total Cost.

Total Cost (Hours):	0	**Total Cost (Dollars):**	0
Description of Costs:			
System Down Time (Days):		**System Down Time (Hours):**	

Timeline

Date Record Opened (UTC):	5/15/2011 2:12 PM	**Date Record Confirmed (UTC):**	7/11/2011 3:35 PM
Date Record Contained (UTC):	7/11/2011 3:35 PM	**Date Record Resolved (UTC):**	7/11/2011 3:35 PM
Date Record Closed (UTC):			

Time in Open:	57.06		
Time in Confirmed:	0.00	**Time to Confirm:**	57.06
Time in Contained:	0.00	**Time to Contain:**	57.06
Time in Resolved:		**Time to Resolve:**	57.06
Time in Closed:		**Time to Close:**	

Number of Days to Resolve:	57.06

Journal Entries

Entry	Entry Date	IMS User
Center was not affected. Closing.	7/11/2011 3:33 PM	(b) (7)(C), (b) (6)
Reviewed (b) (6), (b) (7)(E) logs for the past two weeks and noted no connections. This system is not open to the public and is restricted from any (b) (6), (b connections from the general (b) (6), (b) (7)(E). Claims not confirmed.	5/18/2011 7:45 PM	(b) (7)(C), (b) (6)
All single IPs (b) (6), (b) (7)(E) mine are uploaded.	5/17/2011 9:32 PM	(b) (7)(C), (b) (6)
Attached (b) (6), (b) (7)(E) mine/csv for ip (b) (6), (b) (7)(E) from May 1 to May 15. No hit on ip (b) (6), (b) (7)(E) Will upload (b) (6), (b) (7)(E) when available.	5/16/2011 9:29 PM	(b) (7)(C), (b) (6)
Looked at this over the weekend and the majority of it	5/16/2011 1:26 PM	(b) (7)(C), (b) (6)

seems to be bogus so far. Verified with (b) (7)(E yesterday that those (b) (6), (b) (7)(E) IPs are not in use and that the entire (b) (6), (b) (7)(E) subnet is not used. There is also the claim of a database with all NASA webmail passwords, which would be a complete (b) (6), (b) (compromise for the Agency. This seems unlikely. Other associates of ours listed in the article also state that the information referenced is either bogus or all found on public websites (e.g. it's not restricted, private, or compromised information). A spot check of the (b) (7)(E), (b) host ((b) (6), (b) (7)(E) [redacted] does show that they are valid and have (b) (6), (b) open though. SOC investigating. (b) (6), (b) (7)(E)	5/15/2011 4:02 PM	(b) (7)(C), (b) (6)
-------- Original Message --------	5/15/2011 2:10 PM	(b) (7)(C), (b) (6)

Subject: RE: Follow-Up on Incident call number:
INC000000150399 regarding 06-Investigation
05152011-NASA
Date: Sun, 15 May 2011 07:29:45 -0500
From: (b) (7)(C @us-cert.gov
To: (b) (6), (b) (7)(C)
Corporation] , (b) (7)(C @us-cert.gov
CC: (b) (7)(E) @nas.nasa.gov
References:
<(b) (7)(C), (b) (6) @tritan>
<(b) (7)(E) @nasa.gov>

NASA SOC,

The incident was opened by us but the specific reason may not have been included in our initial notification.

An open source report was brought to our attention and in it, a possible breach of security affecting your agency was included. A portion of the article is shown below. We are not able to confirm the vulnerabilities stated below and leave it to the various agencies to investigate. Sorry for any confusion.

hxxp://www.thehackernews.com/2011/05/exclusive-report-is-department-of.html

============ Beginning of web report ===============
Well ! Over the past couple of weeks, There are series of discussions, that around why U.S defense and Intelligence agencies are moving so quickly to adopt cloud computing. Is their any Security Holes in their Security ? or had someone already hack Them and their Documents ?. In last week we have notice lots of Hackers activity,If you miss something Then have a look to Super Saturday : The Hacker News Featured Articles !

No issue ! Now let me explain : Yes you are going to Read about Security Holes in U.S defense and Intelligence agencies. A Hacker named "sl1nk" Claim that, He Has :

1. (b) (6), (b) access to a Network of (b) (6), (b machine's layer (b) (6), (b) (7) in the Pentagon
2. Access to APACS (automated personell air clearance system)
3. Thousand's of documents ranging from seizure of a vehicle up to private encryption key request forms.
4. Database of all usernames/passwords of Webmail of Nasa

Attachment(s)

Name	Size	Type	Upload Date	Downloads
(b) (6), (b) (7)(E).csv	1286	.csv	5/16/2011 9:28 PM	0
(b) (6), (b) (7)(E).csv	91593	.csv	5/17/2011 9:32 PM	0
(b) (6), (b) (7)(E) .csv	124022	.csv	5/17/2011 2:04 AM	0
(b) (6), (b) (7)(E).csv	16608	.csv	5/17/2011 5:32 AM	0
(b) (6), (b) (7)(E).csv	18630	.csv	5/17/2011 3:49 AM	0
(b) (6), (b) (7)(E) .csv	16168	.csv	5/17/2011 9:09 PM	0
(b) (6), (b) (7)(E).csv	17666	.csv	5/18/2011 2:05 AM	0

History Log

View History Log

SOC IMS: SOC-20131112-315641

Last Updated: 6/20/2014 5:15 AM

SOC Incident Management System

IMS User Contact:	(b) (6), (b) (7)(C)	**Restrict Access To:**	All IMS
Record Permissions Group:	All IMS Users	**Record Source:**	

Contact Details

Enter the NASA AUID or email address of the Contact, and click "Lookup Contact Details" to automatically retrieve the information.

AUID:		**Email:**	

Enter Contact information below if the primary contact is not an IMS user

Contact Last Name:		**Contact First Name:**	
Contact Role:		**Contact Office Phone:**	
Contact E-mail:		**Contact Cell Phone:**	
Contact AUID:		**Contact NASA Center:**	
Contact Building:		**Contact Room Number:**	
Contact Type:			

General Details

SOC Tracking Number:	SOC-20131112-315641	**Categorization:**	Incident
Date Record Created (UTC):	11/12/2013 2:22 AM	**Incident Time Zone:**	UTC - Coordinated Universal Time Zone (GMT)
Title:	Confirmed (b) (6), (b Web Server Compromise via (b) (7)(E), (Injection		
Brief Description:	A trusted third party advised us of potential compromise of a NASA system. Received a tipper from (b) (6), (b) (7)(E) notifying us of a potential compromise of a NASA system. A Source has reported that hacktivist group NullCrew gained access to a vulnerable NASA server, which MAY contain PII. The vulnerable server is (b) (6), (b) (7)(E) . It appears that NullCrew either got the password for, or added the user '(b) (6), (b'.		
Current Status:	Closed	**Assigned To:**	Fairchild, Yvette L

			(b) (6), IRM (b) (6) IRT (b) (6), ITSM
Current Priority:	Medium	**Also Notify:**	CTA (Cyber Threat Analysis)
Notify on Save:	No	**Notify US-CERT on Save:**	
CUI:	No CUI or PII		
Ok To Close:	Yes		

US CERT Reporting

Risk Rating:			
Information Impact:		**Functional Impact:**	
Recoverability:		**Attack Vectors:**	
Critical Service or System:		**Classified Incident:**	
Major Incident:		**High Value Assets (HVA):**	
Reportable to Congress:			
Observed Activity:		**Number of Records Impacted:**	
Location of Observed Activity:		**Number of Systems Impacted:**	
Actor Characterization :		**Number of Users Impacted:**	
Action Taken to Recover:		**Number of Files Impacted:**	

The fields below hold the US-CERT Reporting fields that were in force from October 1, 2015 through March 31, 2017. The are included here for reporting purposes only.

Functional Impact old:		**Informational Impacts old:**	
		Recoverability Impact old:	

Related Tasks

Task ID	Assigned To	Due Date (UTC)	Priority	Status	Description	Resolution
315640	SOC Tier-1	11/16/2013	Medium	Complete	Please assign back to	1. How did the attack impact

		2:19 AM			SOC teir 1 when complete. 1. How did the attack impact operations? 2. Resolution 3. Do you require assistance? 4. If you implemented measures to mitigate further attack, what were your mitigation measures? Second request: US-CERT requests the following details for this incident: 1. Explanation 2. Resolution 3. How did the attack impact operations? 4. Do you require assistance? 5. If you implemented measures to mitigate further attack, what were your mitigation measures?	operations? 2. Resolution - The website was taken offline to perform isolation and data collection activities. Once the collection was complete, the dynamic content that was used in the sqlmap attack was removed, and the website was reconnected to the network. - The actors actions appear to be limited to a single website on a single webserver, and an underlying (b) (7)(E), (b) (6) database. There are no indications that lateral movement or any additional system exploitation occurred. 3. Do you require assistance? No. 4. If you implemented measures to mitigate further attack, what were your mitigation measures? Possible plans to implement input sanitization. Overall the website content is primarily static in nature, with the exception of a hurricane preparedness website ((b) (6), (b) (7)(E) driven) that is used by management to access personnel contact information. This was the part of the website that was used to perform the exploitation activities that we're investigating, I haven't done an analysis of the code, but at a glance there doesn't appear to be input sanitization on all the input fields,
315903	(b) (6), IRM (b) (6), (IRT (b) (6), (ITSM	11/17/2013 5:45 PM	Medium	Complete	(b) (6), (b) (team, OCIO would like more information on the following questions:	- The website was taken offline to perform isolation and data collection activities. Once the collection was complete, the

					System Off Line for Investiga Types of Data on Server? Signs of data exfiltration duri PII, SBU or ITAR data exfiltra Data from specific NASA pro Breach Response Team Initi Criminal Investigation Initiate Can you confirm the actors' a Was there lateral movement	dynamic content that was used in the sqlmap attack was removed, and the website was reconnected to the network. - There is no ITAR, SBU, PII, or any sensitive data on the server. The affected website/database contained occupational/institutional safety metadata for the website and nothing mission related is contained on the server. This could change based on the (b) (7)(E), (b) (6) investigation, but initial analysis supported this assessment. - At this time the only data that appears to be exfiltrated was some database structure/scheme information for the (b) (6), (b) institutional safety website. No data content appears to have been exfiltrated. - At this time no OIG or Breach investigations have been formed. - The actors actions appear to be limited to a single website on a single webserver, and an underlying (b) (7)(E), (b) (6) database. There are no indications that lateral movement or any additional system exploitation occurred.
316168	M&D (Monitoring and Detection)	11/15/2013 12:00 AM	High	Complete	Please gather network flow data for all traffic between (b) (6), (b) (7)(E) and (b) (6), (b) (7)(E) from 20130924 through	(b) (6), (b) (7)(E)

Related Incidents

Select Relationship:		**Relationship Description:**	

Parent Incident

SOC Tracking Number	Current Status	Title
No Records Found		

Child Incidents

SOC Tracking Number	Current Status	Title
No Records Found		

Sibling Incidents

SOC Tracking Number	Current Status	Title
No Records Found		

Incident Details

Time Incident Started:	9/25/2013 11:45 PM	**Time Incident Started (UTC):**	9/25/2013 11:45 PM
Time Incident Detected:		**Time Incident Detected (UTC):**	
Center Affected by Incident:	(b) (6),	**Overall Impact (reference):**	High
US-CERT Category:	CAT 1 - Unauthorized Access	**Incident Subcategory:**	CAT 1(1) (b) (7)(E Injection
US-CERT Tracking Number:	INC000000325737	**ESD Ticket #:**	
Resolution Status:	Concluded	**Malware Family:**	
		Highest level of access gained:	
Primary Method used to Identify Incident:	US-CERT Einstein Program		
Primary Attack Category:			
Primary		**Lost or Stolen**	None

Lost or Stolen NASA Equipment Application

Tracking ID	Cause of Loss	Type of System Lost	Description of Circumstances
No Records Found			

Host Information

NASA Hosts

IP Address	IPv6 Address	Host Name	Center/Facility
(b) (6), (b) (7)(E)			(b) (6),

External Hosts

IP Address	External IPv6 Address	Host Name	Position in this attack
(b) (6), (b) (7)(E)			Attacker

Campaigns

Campaign Name:	Hacktivist - NullCrew (0rbit / Doc / 3cho / Siph0n / Nop / crazyboris)	**Reviewed By TVA:**	
Campaign Comment:		**Confirmed By TVA:**	
		Is APT:	Confirmed

Indicators of Compromise

IOC Domain

FQDN	Do Sinkhole	Comment
No Records Found		

IOC IP

IP Address	IP Block	Comment
(b) (6), (b) (7)(E)		

IOC File

Filename	MD5 Hash	Comment
No Records Found		

IOC Registry Key

Key Name	Key Value	Comment
No Records Found		

IOC Email

Sender Email	Subject	Comment

No Records Found

IOC Detection

Name	Type	Comment
No Records Found		

Root Cause Statement

The Root Cause Statement can be constructed from the following fields like so:
"SOURCES source realized CATEGORIES using METHODS exploiting CAUSES (with additional FACTORS) gaining OBJECTVES."
See the help for the individual fields for more information about what the various values mean and their context.

Root Cause Sources:		**Root Cause Categories:**	
Root Cause Methods:		**Root Cause Causes:**	
Root Cause Factors:		**Root Cause Objectives:**	

Reporting Organizations

Reporting Date (UTC)	Reporting Local Date	Reporting Local Time Zone	Reporting Notes	Reporting Number	Reporting Organization	Reporting Organization Contact
No Records Found						

Impact of Incident

NASA Programs, Projects, and/or Operations:	Low	**People:**	Low
Data (at Rest or Transmission):	Low	**System:**	Low
Cost:	Low	**Sophistication / Nature of Attack:**	Low
Number of systems affected by this incident:	2-5	**Number of NASA Centers/ Facilities affected by this incident:**	
Number of accounts affected by this incident:		**Critical Infrastructure Impacted:**	No
Other Impacts:			
Overall Impact:	High -- Incident Considered High if any of the Categories are rated High		

Containment Actions

Incident Containment System Action:	
Incident Containment Network Action:	

Recovery Actions

Incident Recovery System Action:	
Incident Recovery User Action:	

Recommendations

Root Cause:	
Lessons Learned:	

Costs

Center (Hours):	112.00	**Center (Dollars):**	11200.00
NASA SOC (Hours):	13.00	**NASA SOC (Dollars):**	1300.00
NASA NOC (Hours):		**NASA NOC (Dollars):**	
Other Costs (Hours):		**Other Costs (Dollars):**	

Total Costs in Hours and Dollars are automatically calculated as the sum of the individual costs above. Center IR teams or managers should enter the Center costs, the NASA SOC Manager should enter the SOC Costs and the NOC Manager should enter the NOC costs, if any, in order to arrive at the Total Cost.

Total Cost (Hours):	125	**Total Cost (Dollars):**	12500
Description of Costs:			
System Down Time (Days):		**System Down Time (Hours):**	

Timeline

Date Record	11/12/2013 2:22 AM	**Date Record**	11/21/2013 4:10 PM

Opened (UTC):		**Confirmed (UTC):**	
Date Record Contained (UTC):	11/21/2013 4:10 PM	**Date Record Resolved (UTC):**	3/25/2014 5:32 PM
Date Record Closed (UTC):	3/26/2014 5:30 AM		
Time in Open:	9.58		
Time in Confirmed:	0.00	**Time to Confirm:**	9.58
Time in Contained:	124.06	**Time to Contain:**	9.58
Time in Resolved:	0.50	**Time to Resolve:**	133.63
Time in Closed:	2849.80	**Time to Close:**	134.13
Number of Days to Resolve:	133.63		

Journal Entries

Entry	Entry Date	IMS User
Jun 16, 2014	6/20/2014 5:11 AM	(b) (6), (b) (7)(C)

Alleged Associate of "NullCrew" Arrested on Federal Hacking Charge Involving Cyber Attacks on Companies and Universities

CHICAGO — A Tennessee man was arrested and charged with federal computer hacking for allegedly conspiring to launch cyber attacks on two universities and three companies since last summer, federal law enforcement officials announced today. The defendant, TIMOTHY JUSTIN FRENCH, is allegedly associated with a group of individuals, known as "NullCrew," who have claimed responsibility for dozens of high-profile computer attacks against corporations, educational institutions, and government agencies.

French, 20, was arrested without incident by FBI agents at his home in Morristown, Tenn., east of Knoxville, last Wednesday. He waived a detention hearing today in Federal Court in Knoxville, and will be transferred in custody to face prosecution in U.S. District Court in Chicago, where no court date has yet been scheduled. French was charged with conspiracy to commit computer fraud and abuse in a criminal complaint that was filed under seal on June 3 and was unsealed upon his arrest.

French, also known as "Orbit," "@Orbit," "@Orbit_g1rl," "crysis," "rootcrysis," and "c0rps3," and members of NullCrew allegedly launched computer attacks that resulted in the release of computer data and information, including thousands of username and password combinations.

"Cyber crime sometimes involves new-age technology but age-old criminal activity — unlawful intrusion, theft of confidential information, and financial harm to victims," said Zachary T. Fardon, United States Attorney for the Northern District of Illinois. "Hackers who think they can anonymously steal private business and personal information from computer systems should be aware that we are determined to find them, to prosecute pernicious online activity, and to protect cyber victims."

According to the complaint affidavit, NullCrew has used Twitter accounts to announce dozens of attacks against various victims, including the websites of two organizations in July 2012 and eight computer servers belonging to a large company in September 2012. In both instances, the announcements included links to posts on Pastebin, a website that allows uploading of text files for others to view, containing usernames and passwords associated with those victims. In November 2012, NullCrew announced an attack on a foreign government's ministry of defense, releasing more than 3,000 usernames, email addresses, and passwords purportedly belonging to members of the

~~SENSITIVE BUT UNCLASSIFIED~~

Resolving incident after receiving final report from (b) (6), (b) (7)(C)	3/25/2014 5:31 PM	(b) (6), (b) (7)(C)
Attached the (b) (6), (b) (7)(C) report. Investigative and analysis conclusions are consistent with expected and previous results.	3/17/2014 7:12 PM	(b) (6), (b) (7)(C)
still waiting on (b) (6), (b) (7)(C) report.	1/16/2014 7:07 PM	(b) (6), (b) (7)(C)
(b) (6), (b) (7)(C) completed disk imaging on 11/19 and analysis is ongoing. Initial review of the log data by (b) (6), (b) IRM, (b) (6), (b) (7)(C) and SOC personnel indicated that sqlmap was used to successfully enumerate through the (b) (6), (b) (7)(E) database structure hosted on (b) (6), (b) (7)(E), but that no actual database content was leaked. Additionally, the associated database table that would have contained the (b) (6), (b) (7 mentioned in the original report was found to be clean. Once the disk imaging was completed, I had the content owner ((b) (6), (b) (7)(C)) remove the dynamic (b) (7)(E), content that was used to perform the sqlmap enumeration. The (b) (7)(E), (b) (6) site was returned to service on 11/20, and (b) (6), (b) IT Security will be working with (b) (6), (b) (7)(C) to find a better place to host the content, assess it for any vulnerabilities, and add it to the list of sites that will need periodic vulnerability scanning. Any signficant vulnerabilities that are found as part of the initial assessment will need to be mitigated before returning the (b) (7)(E), content back to service.	11/21/2013 4:01 PM	(b) (6), (b) (7)(C)
I interviewed one of the data owners (b) (6), (b) (7)(C) to get	11/18/2013 5:01 PM	(b) (6), (b) (7)(C)

an idea of the types of data contained on the website and underlying database that was accessed. Based on (b) (6), (b) (7)(C) [redacted] input, the (b) (6), (b) (7)(E) [redacted] website is the central repository for the Consolidated Institutional Safety Services (CISS) contract. The data is more occupational/institutional safety in nature, and not spaceflight safety-related at all. There is no PII, SBU, ITAR, or contract proprietary data is stored in the website or database that was accessed. The information stored on the website and database is primarily “metadata” in nature, and is used to drive content for the CISS website (things like URLs, policy documents, high level personnel information such as phone numbers, email addresses, etc.). Any sensitive mishap information is stored on a separate server that is not connected to the website. Overall the website content is primarily static in nature, with the exception of a hurricane preparedness website ((b) (6), (b) (7)(E) [redacted] driven) that is used by management to access personnel contact information. This was the part of the website that was used to perform the exploitation activities that we’re investigating, I haven't done an analysis of the code, but at a glance there doesn't appear to be input sanitization on all the input fields, and overall it has not been evaluated or scanned for vulnerabilities. I attached a copy of "HFP_Contact_NT.txt" to the ticket.		
I additionally did some manipulation of the web server logs	11/14/2013 4:14 AM	(b) (6), (b) (7)(C) [redacted]

to pull out the useless stuff and left a timeline along with the database data returned that was evident at the time and in the logs.

I attached that to this email, and uploaded it into IMS, as "315641 - Confirmed Compromise 20131113-B.xlsx". I highlighted several entries on the first tab ("Compromise Timeline") to identify the fields I am about to describe, below.

As a quick rundown, there were 210 databases identified by name, and then the field names and field data types within each database were in turn identified.

Long story short, there are a number of fields containing the name "password", several dozen fields containing the name "Name" or "User", and several dozen that appear, upon field name inspection ONLY, to have potential to contain PII - including some database entries about illnesses, mishaps, surveys, including allocations for names, phone numbers, gender, and other items of sensitive personal information. As far as content that may be "technically" sensitive (such as ITAR or SBU), I cannot judge that from field names alone.

As it stands right now, the extent of the CONFIRMED compromise is limited to database names, database field names, and database field data types, but I am as yet unable to confirm data BREACH. There is no confirmed PII / ITAR / SBU / etc. exposure at this time, but the investigation and analysis continues.

This information should be useful to the SOC and (b) (7)(E) teams continuing the detailed investigation, as well as to prepare (leadership, technical, and LE staff) for the scoping of the potential impact of this compromise. Typically, only a single database will be compromised through (b) (7)(E) Injection via a web site front end (normally only the single database that supports that particular web application). In this case, there was clearly (some level of) access to over 200 databases, so this is a much wider scope than most would initially conceive, and continued investigation should be regarded in that light.

--

(b) (6), (b) (7)(C)

Analyzed the Database Logs contained within the file "11_13_2013_security_investigation.zip". There is no significant or anomalous activity during, or in relative proximity to, the compromise that would indicate additional or elevated database access or manipulation beyond that realized during the (b) (7)(E) Injection attack.	11/14/2013 3:04 AM	(b) (6), (b) (7)(C)
References: We are currently tracking this as IMS Incident	11/14/2013 1:50 AM	(b) (6), (b) (7)(C)

315641. This is related to IMS Event 308991 (Category 5).

I have been able to confirm compromise of the (b) (6), (b) (7)(E) server as of 20130925 through (b) (7)(E) Injection using the sqlmap tool.

The attack was detected by (b) (6), (b), and documented in 308991 on 27 September, but incorrectly attributed as unsuccessful. It is clear during that attack the attacker leveraged the (b) (7)(E), (b account with the (b) (7)(E), (b password, and was able to enumerate the database content. Upon initial inspection, the attack results do appear to be unsuccessful, as all are met with a server error (HTTP Code 500), indicating the server was not able to process the request successfully. This was by design, and established in the beginning of the sqlmap attack (how and when the server provides errors). The database contents are enumerated WITHIN the error messages. Some samples below:

```
2013-09-25 23:48:07 (b) (6), (b) (7)(E) POST
(b) (7)(E), (b) (6)
|44|80040e14|Incorrect_syntax_near_')'. (b) (6), (b) (7)(E)
sqlmap/1.0-dev+(http://sqlmap.org) - - (b) (6), (b) (7)(E)
(b) (6), (t
```

This request was to establish how the database and web front end handle errors.

The following are attempts to further scope the server - what it allows and how it responds. These are purposely induced errors to facilitate this technique.

```
2013-09-25 23:48:48 (b) (6), (b) (7)(E) POST
(b) (7)(E), (b) (6)
|44|80040e07|Conversion_failed_when_converting_the_var
char_value_'qccvq1qfxoq'_to_data_type_int. (b) (6), (b
(b) (6), (b) (7)(E) sqlmap/1.0-dev+(http://sqlmap.org) - - (b) (6), (b) (7
```

```
2013-09-25 23:49:51 (b) (6), (b) (7)(E) POST
(b) (7)(E), (b) (6)
|44|80040e57|Arithmetic_overflow_error_converting_expres
sion_to_data_type_int. (b) (6), (b) (7)(E)
sqlmap/1.0-dev+(http://sqlmap.org) - - (b) (6), (b) (7)(E)
```

~~SENSITIVE BUT UNCLASSIFIED~~

Conducted some open source research on the group	11/13/2013 6:17 PM	(b) (6), (b) (7)(C)

referred to as "NullCrew":

NullCrew is a hacktivist group founded in 2012 that takes responsibility for multiple high profile computer attacks against corporations, educational institutions, and government agencies. The group has four core members: 0rbit, Doc, 3cho, Siph0n, Nop and crazyboris. Past members include Saturnine, sl1nk, and Timoxeline, @0rbit_g1r1.

NullCrew is a hacking team that bears some similarities to the defunct LulzSec: it has sympathy with Anonymous, but is separate from Anonymous. It does, however, operate with none of the taunting flamboyance that probably led to the downfall of LulzSec

On July 13, 2012, the group breached the World Health Organization(Who) and PBS releasing a pastebin post containing 591 plain-text usernames, and passwords; relating to the WHO attack, as far as the PBS attack goes, it was mostly database information, as well as 1,000 emails, and passwords.[1] On July 16, the group breached ASUS aka ASUSTeK Computer Inc. releasing a pastebin post, containing 23 administrator usernames, and hashed passwords.[1] The group targeted several universities in the United Kingdom including Cambridge in August 2012.[2]

In September, the group claimed on its Twitter account to have taken control of eight servers run by entertainment corporation Sony.[3] Also in September, the group responded to the arrest of a Pirate Bay co-founder in Cambodia by officials; the response was an attack against the Cambodia Government, leading in several governmental servers being pillaged.[4]

The group released the first in what is supposed to be a series of mini e-zines under the operation of "FuckTheSystem" on September 28, 2012. The first mini e-zine contained the column and table structure to the U. S. Department of State, as well as the administrator and webmaster password in plain-text; it also contained exposure of vulnerabilities on the Foxconn website.[citation needed] On October 6, 2012, the group posted on two twitter feeds; both claimed to have hacked the ISP Orange. The first post, from the official Twitter account, was a pastebin, containing table, columns, and databases of the Orange website. The second post came from 0rbit and contained more sensitive information, such as (b) (7)(E), (b) (6) [redacted] hosts, users, passwords, and fifty two corporation and government officials email addresses.

The crew had alsopublished what it terms its e-zine on Pastebin – but this was rapidly removed. It is still available on AnonPaste and details hacks into www.mt.gov (boolean-blind base (b) (7)(E) [redacted] injection), www.la.gov (unspecified method, and "nothing worthwhile in the databases"), un.org (XSS in webtv.un.org), www.texas.gov and fhpr.osd.mil (both unspecified). A related post still on Pastebin and posted on Thursday 25 October, explains the rationale: a new international protest against what it calls "corrupt governments and agencies. By agencies, I'm talking about organizations like Monsanto for example."

Analyzed "20131111_(b) (6), (b) (7)(E) .pcap" for relevance to this compromise investigation. Hostile content consisted of Leaseweb (US-based ISP) IP (b) (6), (b) (7)(E) performing an unsuccessful ZmEU Web Vulnerability Scan. This traffic is likely unrelated to this compromise investigation. Sample: GET /w00tw00t.at.blackhats.romanian.anti-sec:) HTTP/1.1 Accept: */* Accept-Language: en-us Accept-Encoding: gzip, deflate User-Agent: ZmEu Host: (b) (6), (b) (7)(E) Connection: Close HTTP/1.1 400 Bad Request Content-Type: text/html Date: Mon, 11 Nov 2013 01:28:52 GMT Connection: close Content-Length: 39 <h1>Bad Request (Invalid Hostname)</h1> GET /w00tw00t.at.blackhats.romanian.anti-sec:) HTTP/1.1 Accept: */* Accept-Language: en-us Accept-Encoding: gzip, deflate User-Agent: ZmEu Host: (b) (6), (b) (7)(E) Connection: Close HTTP/1.1 400 Bad Request Content-Type: text/html Date: Mon, 11 Nov 2013 01:28:52 GMT Connection: close Content-Length: 39 <h1>Bad Request (Invalid Hostname)</h1>	11/12/2013 8:12 AM	(b) (6), (b) (7)(C)
Analyzed	11/12/2013 8:03 AM	(b) (6), (b) (7)(C)

"20131111_(b) (6), (b) (7)(E) .pcap" for relevance. This contained a known hostile IP (b) (6), (b) (7)(E) performing a single HTTP request for an (b) (6), (b) (file from this same server (same IP address, different website (b) (7)(E), (b) (6) verses (b) (7)(E), (b) (6)). It is not believed this is related to this compromise investigation.

Sample:

```
GET (b) (7)(E), (b) (6)
Host: (b) (7)(E), (b) (6)
Accept: */*
Accept-Charset: GB2312,utf-8;q=0.7,*;q=0.7
Accept-Language: zh-cn, zh
User-Agent: Mozilla/4.0
Referer: (b) (7)(E), (b) (6)
Connection: close
HTTP/1.1 200 OK
Connection: close
Date: Mon, 11 Nov 2013 17:06:10 GMT
Server: (b) (7)(E), (b) (6)
X-Powered-By: (b) (7)(E), (b) (6)
Content-Length: 14735
Content-Type: text/html
Set-Cookie:
(b) (6), (b) (7)(E) IDCQQQQATQ=OHOJHJGALPNMBBBHCB
CCNHEN; path=/
Cache-control: private
GET (b) (7)(E), (b) (6)
Host: (b) (7)(E), (b) (6)
Accept: */*
Accept-Charset: GB2312,utf-8;q=0.7,*;q=0.7
Accept-Language: zh-cn, zh
User-Agent: Mozilla/4.0
Referer: (b) (7)(E), (b) (6)
Connection: close


HTTP/1.1 200 OK
Connection: close
Date: Mon, 11 Nov 2013 17:06:10 GMT
Server: (b) (7)(E), (b) (6)
X-Powered-By: (b) (7)(E), (b) (6)
Content-Length: 14735
Content-Type: text/html
Set-Cookie:
(b) (6), (b) (7)(E) IDCQQQQATQ=OHOJHJGALPNMBBBHCB
CCNHEN; path=/
Cache-control: private
```

Analyzed	11/12/2013 7:44 AM	(b) (6), (b) (7)(C)

"20131111_(b) (6), (b) (7)(E) .pcap" - traffic of interest was a ZmEu Web vulnerability scanner being improperly executed by (b) (6), (b) (7)(E) (Home ISP in Bangledesh) and receiving only error messages. This traffic would not be related to this reported compromise.

Sample:

```
GET (b) (7)(E), (b) (6) HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: ZmEu
Host: (b) (7)(E), (b) (6)
Connection: Close
HTTP/1.1 400 Bad Request
Content-Type: text/html
Date: Mon, 11 Nov 2013 14:02:18 GMT
Connection: close
Content-Length: 39
<h1>Bad Request (Invalid Hostname)</h1>
GET (b) (7)(E), (b) (6) HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: ZmEu
Host: (b) (7)(E), (b) (6)
Connection: Close


HTTP/1.1 400 Bad Request
Content-Type: text/html
Date: Mon, 11 Nov 2013 14:02:18 GMT
Connection: close
Content-Length: 39


<h1>Bad Request (Invalid Hostname)</h1>
```

Analyzed initial QRadar results file ((b) (6), (b) (7)(E)). It consists of DNS requests only, from valid NASA clients. No impact on this investigation.	11/12/2013 7:22 AM	(b) (6), (b) (7)(C)
Contacted (b) (6), (b) (7)(C) at 19:00 and informed him of the cat 1.	11/12/2013 4:43 AM	(b) (6), (b) (7)(C)
Attached 30-day (b) (7)(E), (b) (query for domain:	11/12/2013 3:13 AM	(b) (6), (b) (7)(C)

(b) (7)(E), (b) (6)

Date of possible compromise unknown. Identified last three signature events for 11/11/2013, possibly unrelated, for (b) (7)(target ip: (b) (6), (b) (7)(E) and attached pcap.

Triggered signatures:

(b) (6), (b) (7)(E) User-Agent known malicious user-agent string ZmEu - vulnerability scanner

APT (Webmasters) Reconnaissance Scanner [T2 Pull & Attach PCAP / Cat 5 Medium / Assign US-CERT / Also Notify TVA]

11/12/2013 2:18 AM (b) (6), (b) (7)(C)

-------- Original Message --------

Subject: Follow-Up for US-CERT Incident number INC000000325737 -
Date: Mon, 11 Nov 2013 20:07:42 -0600 (CST)
From: (b) (6), (b) (@us-cert.gov>
Reply-To: (b) (6), (b) (@us-cert.gov>
To: (b) (6), (@nasa.gov
CC: (b) (6), (@us-cert.gov

US-CERT Ref.No:INC000000325737
Status: In Progress
Impacted Agency:National Aeronautics and Space Administration (NASA)
Impacted Agency Tracking No: Please Assign
****
NASA SOC,
A trusted third party advised us of potential compromise of a NASA system.

Received a tipper from (b) (6), (b) (7)(E) notifying us of a potential compromise of a NASA system. A Source has reported that hacktivist group NullCrew gained access to a vulnerable NASA server, which MAY contain PII.

The vulnerable server is (b) (6), (b) (7)(E). It appears that NullCrew either got the password for, or added the user (b) (7)(E), (b) (6)

The vulnerable URL is:
(b) (6), (b) (7)(E)

Through the vulnerability, NullCrew is able to access the site's (b) (7)(E), (b) (6) database, but does not appear to have shell access.

Please provide your incident number and, when available or applicable, any updates related to this incident.

1. How did the attack impact operations?
2. Resolution
3. Do you require assistance?
4. If you implemented measures to mitigate further attack, what were your mitigation measures?

Thank you in advance for your cooperation.
The Original (b) (6), (b) (7)(E) tipper is below.

Very Respectfully,

NCCIC/US-CERT Operations Center
(b) (6), (b) (7)(E)
@us-cert.gov

Attachment(s)

Name	Size	Type	Upload Date	Downloads
11_13_2013_security_investigation.zip	18932185	.zip	11/14/2013 2:46 AM	6
20131111_(b) (6), (b) (7)(E).pcap	58852895	.pcap	11/12/2013 3:10 AM	19
20131111_(b) (6), (b) (7)(E).pcap	40731281	.pcap	11/12/2013 3:21 AM	11
315641 - Confirmed Compromise 20131113.xlsx	178529	.xlsx	11/14/2013 1:53 AM	11
315641 - Confirmed Compromise 20131113-B.xlsx	322887	.xlsx	11/14/2013 4:15 AM	7
EventLogs_CSV_(b) (7Logs.zip	13357326	.zip	11/20/2013 9:49 PM	8
HFP_Contact_NT.txt	3325	.txt	11/18/2013 5:00 PM	6
IDS_(b) (6), (b) (7)(E)_9-18_9-30-NEW.zip	11954	.zip	11/20/2013 9:54 PM	5
(b) (6), (b) (7)(E).csv	6480	.csv	11/12/2013 3:11 AM	8
(b) (6), (b) (7)(E)_sep2013.zip	1470727	.zip	11/13/2013 10:16 PM	5
(b) (6), (b) (7)(E-ext_logs.zip	1602460	.zip	11/13/2013 9:31 PM	5
MFR13-178 - Server Forensic Report - (b) (6), (b) (7)(E)-EXT Final v2.docx	174449	.docx	3/17/2014 7:12 PM	8
OTHER_PCAPS.zip	50547106	.zip	11/20/2013 9:49 PM	7
(b) (7)(E), (b) (_IP_(b) (7)(E), (b) (6).csv	86451	.csv	11/14/2013 2:41 AM	5

History Log

View History Log