Tribune Technology Post Mortem Report
LATimes Web Defacement Incident

Executive Summary

On Dec 14, 2010, at 3:49 p.m. CST it appears that a page in the LATimes.com website (http://www.latimes.com/news/politics/la-pn-hoyer-tax-vote-20101215,0,4770429.story) was a victim of a digital defacement that affected and targeted specific articles, by-lines and other journalistic content. The content that was changed was substituted with the chippy1337 moniker. The malicious person(s) of this crime created or garnished an ID for the Assembler content management system (CMS). They (he/she) then actively viewed and edited content in an unauthorized manner with the Oxygen framework which utilizes the Assembler (CMS) application to facilitate changes. This application is used to update content of new stories, bylines, etc. by Tribunes'/LATimes authorized users. The logs we collected from the web server and Assembler application log illustrate and identify the IP address and User ID the offenders used to gain access and perpetrate the web site defacement. The change in the article was noticed and reported to Mr. Daniel Gaines-Managing Editor, Operations, latimes.com who facilitated its restoral. The incident was then reported by email at Tuesday, December 14, 2010 5:02 PM to the Market Services and Jason Jedlinski. The article was restored to its original format by LAT Editorial at 4:29 p.m. CST the same day (December 14, 2010). To help rectify, diagnose and troubleshoot these issue twenty three individuals responded to this emergency situation. These individuals included personnel from editorial department all the way to systems people. The team worked in identifying are remediated this issue as much as possible.

This document contains security recommendations to help prevent this type of web site defacement in the future. The staff of individuals should be recognized for not only their dedication to duty to resolve this issue in crisis mode but for follow-up guidance that is represented here later in this document. In conclusion we are cooperating with federal law enforcement authorities to pursue criminal charges against this perpetrator.

Overview of Change

The picture below represents what the article should look like in its unaltered form.

Pressure builds in House to pass tax-cut package

House Democratic leader Steny Hoyer sees 'very good things' in the tax-cut deal, which many representatives oppose. But with the bill set to clear the Senate, reluctant House Democrats are feeling the heat to pass it.

By Lisa Mascaro, Tribune Washington Bureau
December 14, 2010 | 2:28 p.m.

Reporting from Washington — After the Senate overwhelmingly voted to advance the tax-cuts package, House Majority Leader Steny Hoyer acknowledged Tuesday the urgency in passing the legislation to avoid a tax hike on Jan. 1.

RELATED


Tax plan imperfect but still a 'good deal,' Obama says


Tax-cut deal now taking fire from both sides as Republicans speak out

---

The picture below represents the various defacement alterations that were introduced to this same article.

Pressure builds in House to elect CHIPPY 1337

House Democratic leader Steny Hoyer sees 'very good things' in the deal cut which will see uber skid Chippy 1337 take his rightful place, as head of the Senate, reluctant House Democrats told to SUCK IT UP

14 Share | 0 tweets Tweet | 0 Digg

RELATED

Tax cuts will pass despite Democratic uprising, Obama advisor says

Tax plan imperfect but still a 'good deal,' Obama says

By CHIPPYS NO 1 FAN, Tribune Washington Bureau
December 14, 2010 | 10:04 a.m.

E-mail Print Share Text Size

Like 14 people like this. Be the first of your friends.

Reporting from Washington — After the Senate overwhelming voted to advance the tax-cuts package, House Majority Leader Steny Hoyer acknowledged Tuesday the urgency in passing the legislation to avoid a tax hike on Jan. 1.

The main difference in the article story is that various plugs, keywords and by-lines were altered to reflect the CHIPPY, CHIPPY 1337 or other non-Tribune edited references. While other references are present hackers such as Chippy1337 who want to generate a high degree of visibility of their exploits, typically will alter content of websites they deface to reflect the misguided pride of their illegal conquest. Web sites like http://www.zone-h.org/ archives defaced websites for educational purposes. Zone-H also catalogs the cybercrime archive's mirror of the hacked website as well as a mirror of the vandalisms perpetrated, which like Chippy1337, typically has the hacker's moniker that was responsible for the defacement. While conducting further investigation, we discovered that the Chippy1337 hacker has in "hacker" forums for the most part claimed or known to have claimed credit for the Dec 14, 2010 web defacement that occurred against the LATimes website.

Detailed Description

The original story is presented here in this link http://www.latimes.com/news/politics/la-pn-hoyer-tax-vote-20101215,0,4770429.story. The timeline of events is given below in the section marked "Timeline of Events" Here is where we found who updated the content and what ID they garnered to make the unauthorized changes, through the Assembler User Interface Application. We matched the time of the previous and last change of content with the Assembler User Interface. The Content Item Update Log showed four ID's used to make changed to the affected storyline and another used to make corrections post incident. From the time of the last authorized change to the story to the use of a garnered user ID (ngarcia.) From the content item update log entries below we can surmise several clues.

The content item update log displays the last known update to the web content through the Assembler application which is from where this specific type of content is updated. From viewing the log we surmised the content items history number is 58266801. This number is significant because it is the referenced number used in the web servers logs and can be tied to a specific IP address.
http://assembler.tila.trb/content/contentitem/view-contentitemhistory.ui?contentitem=58266801

Of the ID's that made changes to the web content on the web servers through the Assembler user interface, we found that specific ID's were legitimate and one was not.

- ✓ The "feeds" line is the export from our editorial system.
- ✓ The "tgarrison" (Tim Garrison) and "mfarr" (Frank Farrar) ID's are two producers working on the story in the morning.
- ➢ The "ngarcia" ID is where we see the curseword headline and byline was changed. We could not tract this ID to a known user who would have access to update this type of web content.
- ✓ The "BHANRAHAN" (Brian E Hanrahan) ID is a copy editor who looked at and eventually fixed the defacement article.

Tom Commings the system admin gathered the information displayed below while looking into the issue.

In Assembler, logs, he grepped for the time stamp and found this:

grep '14\/Dec\/2010\:13\:49' httpd.log.assembler.tribuneinteractive.com-secure

Once we figured out what content item time and login was used due to the time the change was discovered we looked for the specific content item ID "58266801". This content item from the UI (user interface) used this number to track changes made though the web session from the user to the web server. Tom then and I verified this content item ID was associated with the change though the web UI and discovered the IP Address that was responsible for the unauthorized changes that were made to the article.

> Here is a sample of the output of the session that clearly identifies the web posts to the assembler ui with an exact content item id of 58266801 originating from this specific IP address 188.165.6.178. It even gives specific detail about the browser used to complete these web requests (Mozilla/5.0 (en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2).

188.165.6.178 - - [14/Dec/2010:13:49:15 -0800] "POST /content/contentitem/edit/components/validatereport.jsp HTTP/1.1" 200 8192 "https://assembler.tribuneinteractive.com/content/contentitem/edit-contentitem.ui?id=58266801" "Mozilla/5.0 (en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2"
188.165.6.178 - - [14/Dec/2010:13:49:19 -0800] "POST /content/contentitem/save-story.ui HTTP/1.1" 200 1876 "https://assembler.tribuneinteractive.com/content/contentitem/edit-contentitem.ui?id=58266801" "Mozilla/5.0 (en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2"

We attempted to trace the offenders IP address (188.165.6.178) and it geolocates to the below information according to RIPE:

organisation: ORG-OH5-RIPE
org-name: OVH Hosting Limited
org-type: OTHER
address: 5 Fitzwilliam Place
address: Dublin 2
address: Ireland
abuse-mailbox: *****@ovh.net
e-mail: ***@ovh.net
mnt-ref: OVH-MNT
mnt-by: OVH-MNT
changed: ***@ovh.net 20090916
source: RIPE

Here is a sample of the assembler log matches for this IP from the web server logs on these two assets, s15 (assembler15.tribuneinteractive.com) and s16 (assembler16.tribuneinteractive.com).

S15:
$ grep '188.165.6' httpd.log.assembler.tribuneinteractive.com-secure

188.165.6.178 - - [14/Dec/2010:11:37:03 -0800] "GET / HTTP/1.0" 302 0 "-" "Mozilla/5.0 (en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2"
188.165.6.178 - - [14/Dec/2010:11:37:31 -0800] "GET /images/ti.jpeg HTTP/1.1" 200 32965 "https://assembler.tribuneinteractive.com/" "Mozilla/5.0 (en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2"
188.165.6.178 - - [14/Dec/2010:11:37:32 -0800] "GET /images/buttons/login.gif HTTP/1.1" 200 334 "https://assembler.tribuneinteractive.com/" "Mozilla/5.0 (en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2"
188.165.6.178 - - [14/Dec/2010:11:37:38 -0800] "GET /favicon.ico HTTP/1.1" 200 3574 "-" "Mozilla/5.0 (en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2"
188.165.6.178 - - [14/Dec/2010:11:37:42 -0800] "POST /access/loginmodule.ldap HTTP/1.1" 200 1859 "https://assembler.tribuneinteractive.com/" "Mozilla/5.0 (en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2"
188.165.6.178 - - [14/Dec/2010:11:38:04 -0800] "POST /access/loginmodule.ldap HTTP/1.1" 200 1859 "https://assembler.tribuneinteractive.com/" "Mozilla/5.0 (en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2"
188.165.6.178 - - [14/Dec/2010:11:38:08 -0800] "GET /stylesheets/ui.css HTTP/1.1" 304 0 "https://assembler.tribuneinteractive.com/access/loginmodule.ldap" "Mozilla/5.0 (en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2"
188.165.6.178 - - [14/Dec/2010:11:38:10 -0800] "GET /images/buttons/login.gif HTTP/1.1" 304 0 "https://assembler.tribuneinteractive.com/access/loginmodule.ldap" "Mozilla/5.0 (en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2"
188.165.6.178 - - [14/Dec/2010:11:38:13 -0800] "GET /favicon.ico HTTP/1.1" 200 3574 "-" "Mozilla/5.0 (en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2"
188.165.6.178 - - [14/Dec/2010:11:38:23 -0800] "POST /access/loginmodule.ldap HTTP/1.1" 200 1859 "https://assembler.tribuneinteractive.com/access/loginmodule.ldap" "Mozilla/5.0 (en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2"
188.165.6.178 - - [14/Dec/2010:11:38:39 -0800] "POST /access/loginmodule.ldap HTTP/1.1" 200 1859 "https://assembler.tribuneinteractive.com/access/loginmodule.ldap" "Mozilla/5.0 (en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2"
188.165.6.178 - - [14/Dec/2010:11:38:42 -0800] "GET /favicon.ico HTTP/1.1" 200 3574 "-" "Mozilla/5.0 (en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2"

The complete logs and other information gathered during the course of this investigation are contained here:

Logs captured:

Web Server

1. \\163.192.80.103\Infosec\Investigations\LATimes-P2P-CaseNo-20101214-0001\ForensicData\la.20101214\Logs\WebServer\X-httpd.log.assembler15.tribuneinteractive.com-secure.20110106.11.49.gz
2. \\163.192.80.103\Infosec\Investigations\LATimes-P2P-CaseNo-20101214-0001\ForensicData\la.20101214\Logs\WebServer\X-httpd.log.assembler16.tribuneinteractive.com-secure.20110106.11.48.gz.

LDAP-Server

3. \\163.192.80.103\Infosec\Investigations\LATimes-P2P-CaseNo-20101214-0001\ForensicData\la.20101214\Logs\LDAP\access
4. \\163.192.80.103\Infosec\Investigations\LATimes-P2P-CaseNo-20101214-0001\ForensicData\la.20101214\Logs\LDAP\access.20101214-093034

5. \\163.192.80.103\Infosec\Investigations\LATimes-P2P-CaseNo-20101214-0001\ForensicData\la.20101214\Logs\LDAP\access.20101214-032315
6. \\163.192.80.103\Infosec\Investigations\LATimes-P2P-CaseNo-20101214-0001\ForensicData\la.20101214\Logs\LDAP\access.20101214-114840
7. \\163.192.80.103\Infosec\Investigations\LATimes-P2P-CaseNo-20101214-0001\ForensicData\la.20101214\Logs\LDAP\access.20101214-064233

Investigation Documentation:

\\163.192.80.103\Infosec Investigations\LATimes-P2P-CaseNo-20101214-0001\

Timeline of Events

The list of events in a timeline fashion is listed below. A brief description of the events that transpired is also included.

TIMELINE

----------December 14th 2010----------

On December 14th 2010 at approximately 3:49 PM-CST an unauthorized addition was implemented to a specific article in the LATimes.com website. The story was edited by "ngarcia" at 3:49 p.m. CST, and was restored by LAT Editorial at 4:29 PM. CST. It was reported by Daniel Gaines, Managing Editor, Operations, latimes.com. It was later discovered that the ngatrcia Id used belonged to a user that had been previously terminated.
The following investigative and restorative actions were taken by our Information technology staff.

- Tad Lin conducted or examined P2P/Assembler Secuirty Action - LDAP Change (SuperUser).
- Dwayne Butler conducted or examined P2P/Assembler Security Action - LDAP Change (SuperUser).
- Tom Comings conducted or examined P2P/Assembler.
- Jason Potkanski conducted or examined P2P/Assembler Security Action - LDAP Change (SuperUser).
-

A group discussion was commenced in order to decide on course of action- The attendee's consisted of Chris Phillips, Kyle McClusky, Lucy Jacobson and Diane Yamazaki.

----------December 15th 2010----------

Planning, implementation the remediation and code changes including preventative measures were performed by the following personnel.

- Tad Lin conducted or examined P2P/Assembler Security - Maintenance, Release Planning.
- Dwayne Butler conducted or implemented P2P Assembler Security.
- Tom Comings conducted or examined Assembler/P2P Web Log Analysis.
- Brandon Zylstra conducted or examined Assembler SuperUser LDAP Report.

- Greg Noth conducted or implemented Assembler Change.
- Jason Potkanski conducted or examined Assembler SuperUser LDAP Review.

A discussion with software engineering was commenced in order to discuss potential assembler and P2P changes with Tad Lin and Chris Phillips's group.

----------December 16th 2010----------

Planning, implementation the remediation and code changes including preventative measures were performed by the following personnel.

- Tad Lin examined and conducted P2P/Assembler Security.
- Dwayne Butler conducted Assembler LDAP URL Review.
- Tom Comings conducted Assembler and P2P Web Log Analysis.
- Richard Benjamin conducted Assembler LDAP Review.
- Jason Potkanski conducted Assembler LDAP Review.
- Brandon Zylstra conducted Assembler LDAP Review.

----------December 17th 2010----------

Chris Phillips documented P2P code changes for this recent change.

----------December 18th 2010----------

Nothing to report.

----------January 4th 2011----------

Tim Rodriguez was assigned to gather evidence, case information and submit that information to FBI - Special Agent John Cauthen. This includes the information gathered in the LATimes-P2P-CaseNumber-0001 packet.

----------January 7th 2011----------

Tim Rodriguez initiated a follow up call with FBI area headquarters in Sacramento, California- Special Agent John Cauthen. Tim Rodriguez then explained the progress we were making on case number 0001 (LATimes hack and defacement). I sent two emails which included the progress and logs and data that we were able to gather. Most importantly we were able to identify the P2P User ID and corresponding IP Address that made the change that caused the defacement hack.

The following Items are outstanding and need to be garnered and submitted to FBI - Special Agent John Cauthen:

- ✓ List of all employees, assets, consultants and personnel that worked this case- **Provided**.

- ✓ List of all employees, assets, consultants and personnel's hourly payment schedule that worked this case. This is to help provide exact costs the Tribune incurred during this investigation – **Outstanding**.

----------January 25th 2011----------

Sent followup email to FBI - Special Agent John Cauthen with details of LDAP logs. Created and named incident report, will submit to Armando Caro by EOB today.

One item is outstanding:

- ✓ List of all employees, assets, consultants and personnel's hourly payment schedule that worked this case. This is to help provide exact costs the Tribune incurred during this investigation – **Outstanding**.

Resources Involved in Investigation

The list of employees, contractors, Law enforcement personnel is included below as well as the time spent troubleshooting, examining, remediation, development and investigation of this issue. Their functional title, name, assignment tasks in hours and total hours spent is also included.

Functional Title	Name	Preventative Hours	Software\Code\ Redesign Hours	Analysis\ Investigative Hours	Total Hours
System Engineer	Heusinkveld, Brian	20	8		28
System Engineer	Downard, Sabrina	20	12		32
System Engineer	Casey, Conor	5	10		15
System Engineer	Hancock, Craig	12		15	27
System Engineer	Sahasrabudhe, Satish	3	6		9
Unix	Bezouska, Joe	20	12		32
System Engineer	Jones, Ken	2	3		5
System Engineer	Chung, Holly	3	4		7
Server MGR	Russ, Robin	3	10		13
Software Engineering	Tad Lin	16	4		20
Software Engineering	Dwayne Butler	5	2	2	9
System Engineer	Tom Comings		2	10	12
Applications Developer	Richard Benjamin			2	2
Applications Developer	Jason Potkanski	5		4	9
Applications Developer	Brandon Zylstra			5	5
Applications Developer	Greg Noth		1		1

Software Engineering	Chris Phillips	0.5	4.5		5
Market Liaison	Diane Yamazaki			1	1
Project Management Office	Lucy Jacobson			2	2
Software Engineer	Kyle McClusky			2	2
Software Development	Matthew Pulley			1	1
Managing Dir, Tech Architect	Armando Caro	36			36
Information Security	Tim Rodriguez			50	50
Total Hours					323

Systems Affected/Assets Lost

Two systems that were affected by the web defacement are listed below and have had web content restored and are up and running as of the data of this publication. No other loss to systems or services was reported or experience issues at that time.

- assembler15.tribuneinteractive.com
- assembler16.tribuneinteractive.com

Financial Loss

Financial loss did occur, however it occurred in the resulting clean up, diagnosing and preventative measures taken to remediate this issue. The total man hours devoted to the rectification of this web site defacement has exceeded three hundred and twenty three hours, which translated into costs may well exceed ten to fifteen thousand dollars. The costs of implementing two factor authentication, enhanced logging and auditing as well as the other protective measures in the "Solutions" section could translate into the hundreds of thousands of dollars. Overall the impact severity was medium; although it had unknown initial impact, is still a topic for search on other media such as Google. The severity of the site defacement incident may have had a detrimental impact on the reputation of the news site involved that ties back to tribune itself. The integrity of the content as well as the content itself that this news media we publish is of high value. This demonstrate-able defacement of the article in question could in the public eye tarnish the reputation of our publishing services. For over 163 years the Tribune and its holdings have built a solid reputation in the news media, the repercussions of this attack and its brand tarnishing could have detrimental effects on our sterling reputation. Our reputation is the one commodity that is earned, hard to obtain and cannot be purchased.

Contact list

The following list of technical and non technical resources that had been assigned the various tasks detailed above, have been listed and added to this contact list for reference.

Heusinkveld, Brian	bheusinkveld@tribune.com	312-222-7809
Downard, Sabrina	sdownard@tribune.com	312-222-3073
Casey, Conor	ccasey@tribune.com	312-222-2368
Hancock, Craig	chancock@tribune.com	312-222-3709
Sahasrabudhe, Satish	ssahasrabudhe@tribune.com	312-222-6690
Bezouska, Joe		
Jones, Ken	kenjones@tribune.com	312-527-8704
Chung, Holly	holly.chung@tribune.com	213-237-5858
Russ, Robin	roruss@tribune.com	312-222-5565
Tad Lin	tlin@tribune.com	312-222-2441
Dwayne Butler	dbutler@tribune.com	312-222-4304
Tom Comings	tcomings@tribune.com	312-222-6158
Richard Benjamin	rcbenjamin@tribune.com	312-222-5435
Jason Potkanski	jpotkanski@tribune.com	312-222-4210
Brandon Zylstra	bzylstra@tribune.com	312-222-4687
Greg Noth	gnoth@tribune.com	312-222-3565
Chris Phillips	ccphillips@tribune.com	317-379-3171
Diane Yamazaki	DYamazaki@tribune.com	312-222-2106
Lucy Jacobson	ljacobson@tribune.com	312-222-4392
Kyle McClusky	kmcclusky@tribune.com	312-222-5467
Matthew Pulley	mpulley@tribune.com	312-222-7879
Armando Caro	acaro@tribune.com	312-222-2708
Tim Rodriguez	tprodriguez@tribune.com	312-222-3938

Solution

The ease in which the hacker was able to login to the Assembler Web Content Management System from the internet and make changes to a specific storyline is illustrative to the ease of access to this system. Typically strong security mechanisms should exist to prevent unauthorized persons from making changes to important assets such as our news media sites. In this case by disrupting the article in question with the apparent ease that this exploit illustrated the hacker brings to light several deficiencies that exist in protecting our digital news media services. The next few sections will give our recommendations for the implementation of additional security protections, processes and procedures. These recommendations will provide a higher degree of protection to help combat the hordes of malicious individuals that seem to plague high value organizations such as ours, looking to damage and mar our news content that we bring online for the whole world to view and become informed. The protective mechanisms will also help strengthen the presentation of our valued product and help protect our "brands" already highly esteemed reputation. In order to help facilitate protection of your news media and mission critical applications all forward facing web, application servers and devices should be protected in the following manner.

Technology controls.
Web/Applications must have the ability to generate logs that support the following features:

They must have the ability to generate logs that support the following features:

1. A 2FA- two factor authentication mechanism should be put in place to help guarantee the authenticity of the user requesting access to Tribune resources. This is a critical path, especially for

users who sit beyond our company boundaries and that have access to mission critical resources like our news feeds.

2. Logs must be remotely consolidated to a centralized logging device and then compressed, hashed, categorized into specific venues, annotated and backed up to a SAN or other robust media. Each entry must have a reliable and universal timestamp that was synced from a trusted timeserver as well as a username or unique authentication server identification tag. Originating IP (External) Address or a traceable log balancer sequence ID that can be traced and used to correspond to a Globally Unique IP address.
3. Optimally an options performed log entry such as a post for web server content or an action performed such as updating content for a web authoring or content management system must be logged and transaction data be forensically available.
4. A correlation mechanism should be implemented to data mine information from application, web and system logs such as matching usernames, IP Addresses and access times to various and critical resources that require a high level of trapping and tracing access attempts successful or otherwise. A data mining mechanism should be implemented to harvest audit and forensic able data to create reports of access and unauthorized events.
5. Applications and services must be root jailed to help prevent a vulnerable or compromised application from gaining high level access to the operating system and other services.
6. Deploy a Web Application Firewall (WAF) to help protect critical assets against common attacks such as Cross-site Scripting (XSS), SQL Injection, brute force and other types of application layer attacks.

Process controls.

1. Accounts, ID's, roles and permissions values that have access to high value assets should be checked at least every month for termination, unauthorized addition or deletion and role changes. Creation of a formalized process that audits termination lists from HR and verify that the terminated user had all accounts disabled or removed within 24 hours. Communication needs to exist of terminated accounts and process that tracks if the account has been re-enabled.
2. Security awareness training will be conducted to provide and illustrate the proper procedures and security related processes that need to be followed and discuss common social engineering techniques and specific defense techniques used to combat them. Social Engineering exercises will be conducted to check account activation and deactivation processes and procedures are intact.
3. Applications that are available externally that cannot support the correct data protection; user or session authentication must be protected with a VPN.
4. Either a technical or non-technical approved and monitored process for maintaining the integrity of important and or critical news sites must be maintained. It must have notifications mechanisms for altering the content of these sites.

Repeatable security control processes.

1. The formal creation of a CSIRT (Computer Security Incident Response Team) to facilitate incident handling duties should be established. Creation and delegation of duties, roles, responsibilities and processes to support the CSIRT program.
2. Create a process to report security related incidents through the Service Manager ticketing system. This can help escalate events and create metrics to help measure effectiveness in responding to and measuring CSIRT related incidents.

3. A post incident wrap-up, root cause analysis (RCA) and incident summaries should be created to be reviewed and historically saved after any major Information Security Incident.
4. An audit of mission critical systems from their established base should be performed twice a year.
5. A penetration test of mission critical systems and there applications, services and operating systems should be performed twice a year.
6. Active vulnerability testing should be ongoing and run monthly to check for vulnerabilities, misconfigurations or unapproved services and configurations.

Follow-up Actions

This incident has been reported to the appropriate law enforcement authorities and an ongoing investigation with the full cooperation of the Information Security group, is underway. The "Solutions" portion of this document will be discussed and reviewed in order to create a more secure mechanism and process for assets that host our media services. These solutions will be intelligently implemented and given the upmost priority to protect our mission critical assets. These lessons learned in respects to the development of customized software for Tribune services will glean a more beneficial practice for the ongoing security development process.

Revision History

Authors	Date	Version	Comment
Tim Rodriguez-IT Security	01-14-2011	None	Started initial Draft.
Tim Rodriguez-IT Security	01-25-2011	.1	Created and revised initial draft, submitted for case approval.