Analysis and Prevention of Account Hijacking based INCIDENTS in Cloud Environment

Sreenivas Sremath Tirumala
Auckland University of Technology,
Auckland, New Zealand

Hira Sathu
UNITEC Institute of Technology,
Auckland, New Zealand

Vijay Naidu
Auckland University of Technology,
Auckland, New Zealand

***Abstract*—Cloud computing is a technological breakthrough in computing. It has affected each and every part of the information technology, from infrastructure to the software deployment, from programming to the application maintenance. Cloud offers a wide array of solutions for the current day computing needs aided with benefits like elasticity, affordability and scalability. But at the same time, the incidence of malicious cyber activity is progressively increasing at an unprecedented rate posing critical threats to both government and enterprise IT infrastructure. Account or service hijacking is a kind of identity theft and has evolved to be one of the most rapidly increasing types of cyber-attack aimed at deceiving end users. This paper presents an in depth analysis of a cloud security incident that happened on The New York Times online using account hijacking. Further, we present incident prevention methods and detailed incident prevention plan to stop future occurrence of such incidents.**

I. Introduction

Cloud computing has brought a paradigm shift in IT and has redefined the way businesses and government systems operate. Cloud computing has unearthed its huge potential with the concept of server to service based transformation along with benefits like coherence, high availability and economies of scale. However, along with the technological advances, cloud computing has also become an avenue for advanced security challenges with new threats and vulnerabilities over time. These threats are questioning the efficiency of security practices implemented to safeguard the IT infrastructure. Securing IT infrastructure is more about protecting the intellectual assets than defending the security perimeters. Almost 60% of organizations have started using cloud services globally and the rate of migration to cloud environment in developed countries is exponential. For instance, New Zealand is experiencing around 175% growth in migration of small and medium scale companies to cloud. However, moving organizational data stored in a centrally located server to cloud storage increases the risk of data being compromised. Hence, it is of ample significance to identify the possible risks and accordingly formulate feasible counter measures prior to moving the IT infrastructure to the cloud.

Realizing the promises offered and the risks associated with cloud computing, most advanced and effective security solution are of highest importance [1]. An efficient security solution is one that strictly follows the best practices to combat the most uniquely featured sophisticated threats, thus manifesting the organization specific security policies. The most predominant security risk associated with cloud computing is its tendency not to note of or consider sensitive IT information[2]. Though cloud technologies offer inexpensive and speedy services, security of IT processes are compromised if appropriate safety measures are not enforced. To competently handle cloud security challenges and to benefit from the gains offered by the cloud, efficient security policies need to be designed and implemented thus protecting the organizations intellectual assets [3], [4].

Earlier, most organizations, Small and Medium Scales Enterprises (SMEs) in particular, have not considered the importance of cyber risks, as they lack in effectively identifying and quantifying the losses that would occur as a result of cyber-attacks. Due to recent cybercrime and cyber terrorism activities, nowadays, every organizations adopt a cyber security policy and look towards more affordable cyber security solutions. With this, the development of cyber security software has entered a new phase with a number of open source and freeware solutions coming into market which was once dominated by proprietary software from big organizations like IBM, Cisco, Norton etc [5].

In a cloud computing environment, the central component to manage risks is to understand the nature of security threats [6]. Fundamental element in risk management is, to be aware of the current happenings and keeping track of expert' views on vulnerabilities and threats in order to make well informed risk management decisions regarding cloud adoption strategies. Therefore, designing and implementing properly structured security strategies is of vital importance to deal with the cyber threats and help the organization to bounce back to its normal operations as soon as possible and to efficiently manage the costs incurred due to the loss [7]. The NYT website was attacked using account hijacking which is considered as one of the most famous security breaches where in the site was down for almost 6 hours. In this paper we are going to present the incident analysis report on the outage of The New York Times (NYT) online version (http://www.nytimes.com/). Further, we present incident prevention methods and detailed incident prevention plan to stop the future occurrence of such incidents.

This paper is organized as follows. Section I presents introduction to cloud security concepts. Section II briefly presents the analysis on NYT outage incident. Incident response and prevention is presented in Section III followed by conclusion as Section IV.

II. Incident Analysis

A. Background

The New York Times is one the most famous newspaper established in 1851 with an on line addition that started in 1996. The New York Times website was attacked by Syrian Electronic Army (SEA), a hackers group from Syria on 27th August, 2013 [8], [9], [10]. SEA attacked NYT website by hacking and hijacking the sensitive DNS information of Melbourne IT, an Australian based domain registrar organization, which manages the domain registry services of the NYT website along with the websites of other global organizations like Twitter, Yahoo, etc.

The ultimate target of the Syrian group was the NYT website for which they attacked the IT infrastructure of Melbourne IT [11]. As a result the NY Times website was intermittently down for almost 6 hours and visitors to the website had been redirected to a Syrian website displaying information about Syrian conflict. The service disruption was the result of a sophisticated attack for which the SEA had hacked the account information of a reseller associated with Melbourne IT. Using the hijacked reseller credentials, SEA had sent a specially crafted phishing email and notified the recipients to update their passwords [12]. The changed passwords had been logged by the attackers and eventually they easily gained access to the DNS information and modified the DNS names of NYT thus leading the domain being redirected to a Syrian website displaying some political information [13].

Domain Name: NYTIMES.COM
Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
Whois Server: whois.melbourneit.com
Referral URL: http://www.melbourneit.com
Name Server: DNS.EWR1.NYTIMES.COM
Name Server: DNS.SEA1.NYTIMES.COM
Status: serverDeleteProhibited
Status: serverTransferProhibited
Status: serverUpdateProhibited
Updated Date: 27-aug-2013
Creation Date: 18-jan-1994
Expiration Date: 19-jan-2014

Fig. 1: Screen shot of Web traffic of The New York Times Domain [13]

The screen shot presented in Fig. 1, clearly shows how the web traffic of NYT had been successfully rerouted to their desired website by changing the DNS server information. The attackers had also set a Time-to-Live option which usually will globally cache the changes on the DNS servers for the entire day. The reversal of these changes might usually take one full day except if the network personnel purge the caches on time. Directly hacking the web server of a globally renowned organization and undermining it by redirecting the visitors to a political website is not an easy task. Hacking the IT infrastructure of a DNS hosting service provider and hacking the information is considerably easier than hacking the infrastructure of New York Times web infrastructure [12]. Considering the time of the incident and affected user base, this attack on NYT website is categorized as very severe as per the threshold diagram mentioned in Fig. 2. Further, targeting

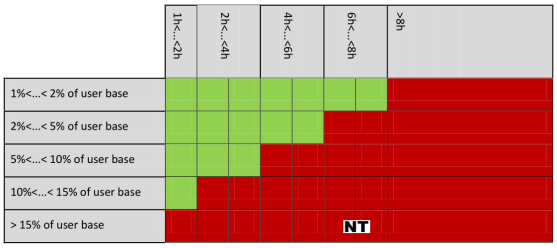

Fig. 2: Incident Severity Matrix

a domain registration organization that also holds accounts of internet giants like twitter and yahoo shows the severity of the attack. The security incident that had brought the NYT website offline is a domain hijacking that belongs to account or service hijacking cloud security vulnerability [12]. Domain hijacking implies that the attackers would gain control of the domain name from the lawful domain owner. It is noteworthy that in the list of top security threats [14], this type of threat was ranked at 6 in 2010 and is at number 3 in 2013 which is a major security concern.

Account or service hijacking is a kind of identity theft and has evolved to be one of the most rapidly increasing types of cyber-attack aimed at deceiving end users. It is a process in which the attackers dishonestly gain access to an individuals uniquely identifiable information associated with an IT device or service (email account, bank account, computer account, etc.) and the information stolen is thus used for unlawful purposes. Typically the compromised account information is used to impersonate the original account owner. Account hijacking is usually accomplished through tactics like phishing emails, spoofed emails, and faux pop-up windows. Users unaware of the actual motive unknowingly respond to these emails providing the attackers with credential information, which the attackers use to modify user accounts, create new accounts and leave little or no trace by deleting transaction history [15].

In the case of NYT incident, the actual intent of the attackers was to defame the NYT website. To achieve this, attackers had tricked the staff of a US-based reseller associated with Melbourne IT who happened to manage the contracts of The New York Times and Twitter websites and in due course bypassed the credential information and went on to change the DNS record information , also known as DNS poisoning.

B. Incident Analysis

The incident mentioned above occurred as a result of phishing activity that occurred at one of the retailers of Melbourne IT. The series of activities resulting in the incident are explained in the steps below and is presented in Fig. 3.

1) A reseller of Melbourne IT receives a phishing email
2) Fooled by it the reseller provides personal credentials
3) Attacker enters the Melbourne IT infrastructure with personal credential.
4) Attacker redirects the NYT website traffic.

Though there are multitude of attack vectors, emails had always been the most popular initial or probing attack vectors. Phishing is a form of social engineering and is the most

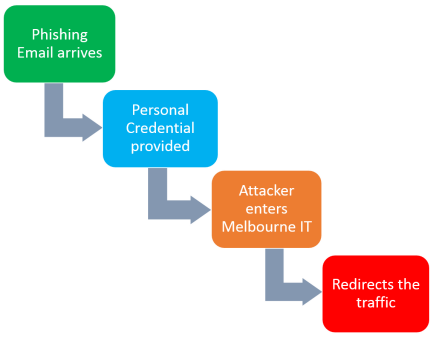

Fig. 3: Step wise representation of The New York Times Outage Incident

common type of internet fraud where attackers illegitimately gain access to the user/client credentials and snoop on the user activities. Subsequently the hackers get hold of sensitive information of the organization and alter it with false information and might ultimately reroute the visitors/users of the website to spurious sites. Several times the attackers might log the user activities and might plan for future attacks based on this logged information. Attackers typically send out custom emails to clients in the disguise of a genuine request asking for credential verification. An example of account or service hijacking threat is the cross-site scripting (XSS) that is an application layer hacking technique which is most commonly aimed at web applications. In April 2010, Amazon has experienced XXS attack which resulted in their user credentials been hijacked. XSS enables hackers to infuse malicious code in the web pages and would then gather the user data which is used to bypass the access controls. The impact of the attack depends on the sensitivity of the data handled by the affected website and also on the security policies implemented by the organization.

CCM IS-07: Information Security - User Access Policy
CCM IS-08: Information Security - User Access Restriction/Authorization
CCM IS-09: Information Security - User Access Revocation
CCM IS-10: Information Security - User Access Reviews
CCM IS-22: Information Security - Incident Management
CCM SA-02: Security Architecture - User ID Credentials
CCM SA-07: Security Architecture - Remote User Multi-Factor Authentication
CCM SA-14: Security Architecture - Audit Logging / Intrusion Detection

Fig. 4: CSA: Threat Details cloud services

In a cloud computing environment, the attackers might often acquire access to sensitive information that is crucial for deploying the services violating the authenticity of those services. Hence the cloud service provides must be well acquainted of the nature of threats and should be well prepared with defensive techniques to safeguard the organizational IT infrastructure. An efficient incident response plan has to be in place to analyzes and measure the loss incurred by the attack. Through the attack for redirection, there was a threat of major data loss which was not targeted by the attacker. With this type of attack, the attacker will have access to critical areas to compromise the cloud services. For this category, CSA Guidance considers Governance and Enterprise Risk Management, Incident Response, Notification and Remediation and Identity and Access Management [14]. These types of incidents may affect all three cloud services IaaS, PaaS and SaaS.

According to CSA report, this type of threat implies access control [14]. A detailed description of each one of them with the reference is presented in Fig. 4. The CSA references for account and service hijacking is presented as Table I. The relevance of this threat is stated as 87% in 2013.

TABLE I: CSA references for account hijacking

Domain No	Description
2	Enterprise Risk Management
5	Information Management and Data Security
7	Disaster Recovery
9	Incident Response
11	Encryption and Key Management
12	Access Management

C. Root Cause Analysis

After the initial analysis of the incident Third Party error and Human error are considered as major reasons for the occurrence of the incident. Third Party Error is considered since the attack has been done through service providers not directly on the infrastructure of NYT. This can be due to the errors committed by employees of the service provider or resellers. This is a domain attacking and can be done only by the intended / unintended security incident within the service provider organization like opening phishing mails or weak passwords etc., which come under account or service hijacking. The human error aspect also involves malicious software attack which most of the time occurs through email in internet or domain service providers. Though this is not a direct attack, Melbourne IT is considered as responsible since their level of access and security policy for changing domain key is evidently quite low. Following are the immediate steps (in sequence) that are supposed to be taken in response to the incident and the sequences is presented below.

1) Password reset of all the accounts involved
2) Accounts involved have been notified about the incident and accounts suspended for possibility of their current passwords having been compromised
3) Immediate password change request for affected accounts
4) Restoring DNS records back to their original values

III. Incident Response Plan

Incident Response plan plays a major role in mitigating the loss or damage occurred and aids by way of a quick response to stop the immediate re-occurrence of the same incident. Looking at the incident response section mentioned above, the first and foremost measure was to reset all the passwords to stop the attacker from continuing his work which complies with the Incident Response Plan which will be introduced later in this section. If DNS values are set back to the originals before resetting the passwords, the attacker has an opportunity to re-launch a similar attack. For account or service hijack cloud incident, we propose the Incident Response Plan as show in Fig. 5.

Be ready to Face (BRF) strategy, expecting the occurrence of worst possible incident. This includes the lessons learnt

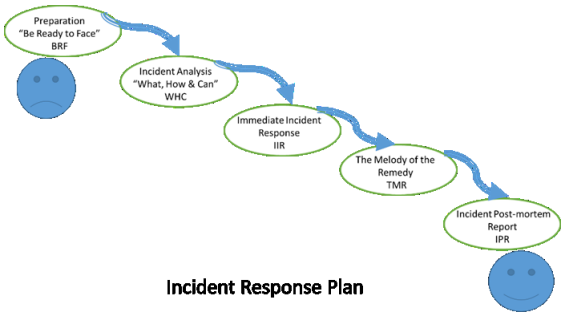

Fig. 5: Incident Response Plan

from earlier experiences as well as anticipating future attacks. Documentation & strategic decision making are the key factors. Incident Analysis includes but not limited to

What: What has happened? Includes the detailed description of the Incident

How: Cause of the Incident (root cause analysis)

Can: Can we handle the incident? Has similar incident been handled in the past?

Immediate Incident Response (IIR) varies with the incident. If similar incident has been identified in the knowledge repository, the same procedures can be followed. Else, primary step is containment, i.e. safeguard the other services from the attack. Counter attack procedures may be identified and implemented. Melody implies linear succession. The Melody of the Remedy (TMR) consist of sequence of actions to be followed as a remedies for the incident. This includes extermination of the incident and proposing remedies to stop further and future manifestation of the incident which is identifying and blocking all the possible trespassers. This is followed by Incident post-mortem Report (IPR) which consists of documenting the steps and procedure followed for this particular incident including pre and post incident activities.

IV. Incident Prevention Measures

After considering the existing standards for these incidents I propose two types of prevention methods for Melbourne IT. Firstly, Account credential and User access policy reforms for Melbourne IT and secondly preventing phishing attacks.

Since the incident is in the category of account or service hijacking of Cloud Security Incident Framework, there is a requirement to scrutinize the information security policy of the cloud service provider organization. We recommend to impose the following information security policies as a preventive measure.

A. Account Credential Reforms

Austere control over user credentials should be implemented for accessing any IT resources. When a request for resetting a password is made, the identity of the user has to be thoroughly verified. And if the password is reset by the network administrator, user has to right away change the password after first time usage. Password protection policies had to be very strictly formulated and implemented. These policies need to be reviewed and should be up-to-date with the business requirements. Emails should be sent to all the users to reset their passwords in compliance with the changes in the password policy. For instance, according to the new password policy, the user should not use passwords used in recent times. Length of the password should be a minimum of 7 characters and the combination of characters in the password should be uniquely set. Password strength should be very high. Passwords expiry process has to be automated and the user needs to set a new password for every 90 days.

User IDs had to be unique and restriction on group IDs and shared IDs should be stringently enforced. When the system is inactive for more than 15 minutes, the password has to be re-entered by the user to access the system. The User ID should be locked after four unsuccessful attempts to login after which only the administrator can enable the User ID. Furthermore, unused user accounts had to be disabled and removed periodically. Management has to keep track of the account activities of users and an activity log has to be maintained.

B. User Access Policy reforms

User access policies and procedures need to be appropriately and amply documented, authorized and strictly implemented to grant and revoke user access to any of the IT resources based on the user privileges. The access permissions should comply with business requirements and be on par with security and service level agreement (SLA) requirements. Users should be authenticated prior to granting access to application data, databases and information related to network configurations etc., Permissions granted to users should be restricted when requested for mission critical information. The management has to verify the credibility of the user before approving the users request to hypersensitive information. Whenever there is a change of status to a single person at any level of the organization, user access to the organizational systems should be timely de-provisioned and revoked. Changes include inclusion of new business partners, contracts/agreements with new clients, service alterations to old clients, relocation or termination of employees etc. Management has to review the user access information periodically and should carefully document it. If any access violations are noticed on a particular user account, the issue has to be resolved with due attention and should follow the guidelines in access control policies and procedures. Multi-factor authentication (MFA) adds an extra layer of defence in which the user authentication process requires a combination of more than two credentials. Usually Multi-factor authentication will require a knowledge factor (something which only the user knows), a possession factor (something which is specifically possessed by the user) and an inherence factor (biometric factor). When a user needs to remotely access the organisational information, MFA adds an additional level of security thus preventing unauthorized access. All the activities including authorised and unauthorised attempts to access the organisational information, information related to system exceptions, information on security events should be retained in compliance with information security policies and regulations. Audit logged information has to be reviewed on a daily basis. Proper tools should be implemented

to detect intrusions in time and suitable response measures are necessary to expedite the process of investigation such that it helps in preventing the re-occurrence of such security incidents. Access to audit log information should be restricted to a small group of trustworthy personnel.

C. Preventing Phishing attacks

Cyber criminals are adopting more sophisticated phishing techniques to forge the identity credentials and critical information of an organisation. Phishing attacks cannot be completely prevented rather it is possible to lower their frequency of occurrence thereby reducing the damage/loss that might be incurred. Organisations should adopt proactive approaches to combat the phishing threats. Ample training should be provided to users on how to identify and avoid phishing emails. Professional hackers use cutting-edge techniques to attack their desired targets. Organizations have to figure out and be familiar with those tools and techniques employed by the hackers. In depth analysis has to be performed by organizations to identify their security shortcomings and thus develop a proper plan to face and obstruct the incoming attack. Organization level security practices include Mail server authentication, digitally signed emails, domain monitoring, gateway services and managed services.

Additionally, organizations should train their customers & resellers by conducting awareness programs. Official communications should be effectively authenticated. Web applications should be secured and there should be a token based authentication in place such that whenever the user needs to login using his/her credentials, a one-time usage PIN number should be sent to their mobile devices and the generation of this number should be automated. Users should only be able to access their accounts when they enter this PIN number along with their credentials.

Most common type of deceptive technique used by the attackers would be to make the victim follow to follow a link attached in the phishing email. The naming conventions of the host services should not be too complex as they might sometimes confuse the users. In order to avoid being a target to any sort of phishing activity, organizations should educate their users such that they does not hastily respond to emails sent requesting to reset the user account information, and also a warning message saying that failing to do so might result in their accounts being suspended. Attackers also send messages to threaten the users saying that failing to respond to that particular email would result in security compromises. In such situations, users have to make sure if the email was actually sent by the legitimate website administrators by calling them over the phone.

Moreover users should be very vigilant and should not click on links included in the email messages which might inject malicious virus into the computer and might hijack sensitive user information and use it for illegitimate purposes. Hackers might often spoof the websites of renowned organizations and make them look like the actual sites thus making users believe that the spoofed site is the original website. Several times attackers might direct the users to the original website and setup faux pop-up windows and when the user clicks on these pop-ups, they provide outsides their sensitive information.

The websites security certificate has to be thoroughly verified before submitting any personal information. Entering personal information into pop-up windows should be avoided. Furthermore, the anti-virus software on the computer must be up-to-date.

V. Conclusion

The analysis of cloud security incident considered for this report indicates the flaws in the security policy implementation of Melbourne IT. To achieve their target (NYT), the attacker has performed extensive and detailed study of NYT's IT Infrastructure, its hosting, its service providers as well as the retailers of the service providers. The attacker found it easy to target the resellers rather than directly attacking NYT or Melbourne IT. This paper further proposes both response and preventive measures in compliance with best industry practices and international standards. However, cloud service providers should strictly forbid sharing the account credential information between clients/users and services and implement austere authentication techniques where ever necessary.

Along with the authentication practices, organizations should try to get as minimal information as possible, to uniquely identify and authenticate their users. Most publicly available information should not play a key role in the user authentication process. It can be concluded that an Incident Response Plan is of paramount importance irrespective of nature of the incident.

References

[1] N. Doe and V. Suganya, "Secure service to prevent data breaches in cloud," in *Computer Communication and Informatics (ICCCI), 2014 International Conference on*, pp. 1–6, Jan 2014.

[2] L. Maghrabi, "The threats of data security over the cloud as perceived by experts and university students," in *Computer Applications Research (WSCAR), 2014 World Symposium on*, pp. 1–6, Jan 2014.

[3] K. Hashizume, D. Rosado, E. Fernndez-Medina, and E. Fernandez, "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications*, vol. 4, no. 1, 2013.

[4] A. Behl and K. Behl, "An analysis of cloud computing security issues," in *Information and Communication Technologies (WICT), 2012 World Congress on*, pp. 109–114, Oct 2012.

[5] S. S. Tirumala, H. Sathu, and A. Sarrafzadeh, "Free and open source intrusion detection systems," in *Machine Learning and Cybernetics (ICMLC), 2015 International Conference on*, vol. in press, July 2015.

[6] P. Mell, "What's special about cloud security?," *IT Professional*, vol. 14, no. 4, pp. 6–8, 2012.

[7] M. Almorsy, J. Grundy, and A. Ibrahim, "Collaboration-based cloud computing security management framework," in *Cloud Computing (CLOUD), 2011 IEEE International Conference on*, pp. 364–371, July 2011.

[8] Cloutage, "1198-melbourne-it-dns-registration," August 2013. Available: urlhttp://cloutage.org/incidents/1198-melbourne-it-dns-registration.

[9] R. Chirgwin, "New york times, twitter domain hijackers 'came in through front door," August 2013. Available: urlhttp://www.theregister.co.uk/2013/08/27/twitter_ny_times_in_domain_hijack/.

[10] P. Dave and R. Lopez, "new-york-times-cites-malicious-external-attack-in-website-outage," August 2013. Available: urlhttp://www.securityinfowatch.com/news/11132681/new-york-times-cites-malicious-external-attack-in-website-outage.

[11] J. Vijayan, "Ny times fingers melbourne it hack for site outage," August 2013. Available: urlhttp://www.computerworld.com.au/article/524916/ny_times_fingers_melbourne_it_hack_site_outage.

[12] M. IT, "Statement regarding reported domain hijacking incident," 2013. Available: urlhttp://www.melbourneit.info/news-centre/Releases/statement-regarding-reported-domain-hijacking-incident.xml.

[13] J. Ong, "Domain registrar melbourne it at center of sea meddling with new york times, twitter," August 2013. Available: urlhttp://thenextweb.com/twitter/2013/08/28/domain-registrar-melbourne-it-at-center-of-sea-meddling-with-new-york-times-twitter-whois-info.

[14] C. S. Alliance, "The notorious nine: Cloud computing top threats 2013," 2013. Available: urlhttps://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.

[15] D. Ahmad, "The confused deputy and the domain hijacker," *IEEE Security & Privacy*, vol. 6, no. 1, pp. 74–77, 2008.