Three Steps to Reduce the Risks of Account Hijacking for Cloud Applications

Dyre malware now targeting SaaS applications like Salesforce.

We all know that criminals tend to follow the money, and this is certainly true with recent malware attacks targeting the financial services industry. The Dyre (or Dyreza) malware strain, initially discovered in June 2014, is a new form of RAT (Remote Access Trojan), designed to steal account credentials from users of banking sites, including Bank of America, Natwest, Citibank, RBS, and Ulsterbank[i]. Rather than attacking the sites themselves, this Trojan using phishing techniques to infect remote end-user PCs, bypass SSL, and steal end-user banking credentials.

On its own, this latest attack is not novel or surprising. However, in a new twist, hackers are now going beyond just attacking banks, looking for SaaS applications widely used in the financial services industry. In September 2014, Salesforce announced that the Dyre malware was detected targeting end-user accounts, likely from financial services organizations[ii].

Salesforce has been widely deployed in financial services and other regulated industries, and its flexibility enables it to be rapidly customized for a wide range of internal and customer facing CRM uses. As the pioneer and leader in the SaaS industry, Salesforce has a well-earned reputation for maintaining very robust infrastructure and high levels of security.

Dyre does not exploit any flaws or vulnerabilities within the Salesforce platform, which is one of the most successful and trusted cloud applications used by businesses. But Dyre does exploit a more basic vulnerability of most web applications – you don't need to hack a well defended site if you can simply steal a user's credentials and walk right in the front door. While there has been lots of attention paid to high profile point-of-sale attacks (such as Target and Home Depot), account hijacking is potentially more widespread and pernicious. Many of the largest breaches in 2014 have been caused by account hijacking, including incidents with eBay, iCloud, Evernote and others.

Fortunately, there are effective steps that organizations can take to mitigate the risks, even if account credentials have been stolen.

The following three steps have become recognized as best practices to reduce the risks from account hijacking:

1 Restrict the IP addresses allowed to access the application. Salesforce provides tools to specify allowable IP ranges, forcing users to only access the application through corporate networks or VPNs. However, this approach can limit convenience for remote corporate users, and can be difficult to enforce for public-facing applications.

2 Require multi-factor authentication. Numerous tools exist that can require users to enter static passwords as well as dynamic one-time passwords which can be delivered via SMS, hardware tokens, biometrics or other schemes.

3 Encrypt sensitive data before it goes to the cloud. CipherCloud technology for encryption or tokenization of specific data fields at the enterprise gateway provides a very effective defense against account hijacking.

Authenticated users who access to Salesforce via the CipherCloud gateway can view, search, and access protected fields. But unauthorized outsiders bypassing the gateway will see only encrypted gibberish. Critical to this system is that enterprises maintain exclusive control over their encryption keys, never sharing them with the cloud provider.

Gateway encryption is fundamentally different from server-side encryption offered by some cloud providers. Server-side encryption is only effective against physical infrastructure theft, such as breaking into a data center and stealing a hard-disk – very unlikely with major well defended data centers. A hacker can much more easily steal credentials and access the applications unimpeded, from anywhere in the world. But by adding a separate, customer-controlled layer of security at the enterprise gateway can prevent hackers from accessing sensitive data, even if user accounts have been compromised.

This is why dozens of top global banks have required CipherCloud technology as a pre-requisite before moving sensitive data to the cloud. Many of these are the same banks targeted by Dyre, Zeus and dozens of other malware attacks.

They understand the risks of account hijacking and have taken proactive steps to assure that sensitive data is not vulnerable. By deploying CipherCloud these banks and enterprises in many other industries have successfully enabled the use of cloud applications, while mitigating the risk of account hijacking.

[i] *Project Dyre: New RAT Slurps Bank Credentials, Bypasses SSL, June 13, 2014 By Ronnie Tokazowski*
[ii] *Salesforce Security Alert: Dyre Malware, September 5, 2014*
Salesforce warns of Dyre malware possibly targeting users, SC Magazine, September 8, 2014
Dyre banking password stealer pursues Salesforce credentials, ZDNet, September 11, 2014

CipherCloud®
Trust in the Cloud™

CipherCloud, the leader in cloud information protection, enables organizations to accelerate their adoption of cloud applications while ensuring visibility and control of their data. CipherCloud delivers data privacy, regulatory compliance, and data residency in the Cloud through an open platform that provides comprehensive cloud application and data discovery, protection – strong encryption, tokenization, data loss prevention, key management and malware detection – and activity and anomaly monitoring services.

CipherCloud has experienced exceptional growth and success with over 2.6 million business users, across 25 countries, and in more than 11 industries.

The CipherCloud product portfolio protects popular cloud applications out-of-the-box such as Salesforce, Box, and Microsoft Office 365. CipherCloud, named as SC Magazine's 2013 Best Product of the Year, is backed by premier venture capital firms Andreessen Horowitz, Index Ventures, and T-Venture, the venture capital arm of Deutsche Telekom.

Headquarters:
CipherCloud
333 West San Carlos Street
San Jose, CA 95110
www.ciphercloud.com

linkedin.com/company/ciphercloud
@ciphercloud
sales@ciphercloud.com
1-855-5CIPHER (1-855-524-7437)