VISA SECURITY ALERT

13 November 2015

UPDATE - CYBERCRIMINALS TARGETING POINT OF SALE INTEGRATORS

Distribution: Value-Added POS Resellers, Merchant Service Providers, Point of Sale Providers, Acquirers, Merchants
Who should read this: Information Security managers and staff, IT Support Providers

November 2015 Update

In October 2015, Visa Inc. learned of several new "FindPOS" malware infections impacting various businesses across North America, to include the following:

- **Automobile dealerships**
- **Dental offices**
- **Golf courses**
- **Gas stations**
- **Mortgage lenders**
- **Restaurants**

Additionally, at least one restaurant group in the southern United States and an integrator not registered with the Qualified Integrator and Reseller (QIR) program, is among the victims of this infection. The information reviewed by Visa Inc. shows infections started in August 2015 but appeared to increase dramatically in the middle of October 2015. Windows XP and Windows 7 (both 32 bit and 64 bit) are the primary operating systems infected and user accounts of various privileges, including "Administrator", appear to be compromised. Visa Inc. is diligently working with their ecosystem partners to properly identify and notify victims.

June 2015 Summary

To promote the security and integrity of the payment system, Visa periodically prepares informative materials related to securing cardholder data and protecting the payment industry. To ensure continued preparedness for new and emerging cyber security vulnerabilities, please review this urgent Security Alert.

Visa has observed a considerable increase in malicious remote access activity associated with unauthorized access to merchant Point-of-Sale (POS) environments via POS integrators. POS integrators are businesses that resell, install, configure, and maintain POS software and hardware for many different types of merchants. POS integrators often provide IT support and ongoing maintenance

over remote network connections, many of which are established through third-party providers of remote desktop access. Properly secured, these connections pose little risk to merchants. Recently, however, cyber criminals have exploited inadequate security controls to gain unauthorized access to a substantial number of merchant POS systems and payment card data.

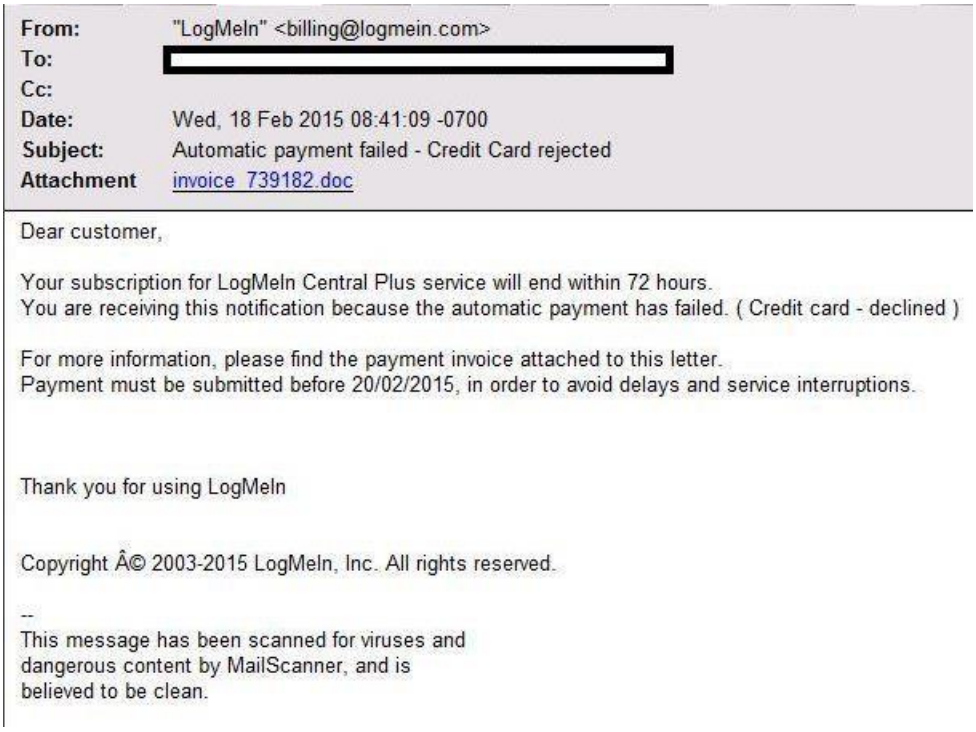
Since at least January 2013, and as recent as May 2015, LogMeIn has utilized social media and other public forums to educate its customers about known phishing scams linked to malware attacks. See facebook.com/logmein, logmein.com, blog.logmein.com, and community.logmein.com for more details.

Additionally, several recent account data compromise events have been traced back to a spoofed LogMeIn phishing email which then leads to the compromise of user credentials at the POS integrator. Examples of recent phishing emails were published by LogMeIn and are included below. Once the credentials are stolen, the attacker traverses the POS integrator network for means of access to the integrator's merchant customer base, thus infecting merchant POS systems with "RAM scraping" malware designed to collect payment card track data.

Organized Campaigns Attacking Remote Access

A number of remote access solutions are commonly used to provide remote management and support for retailers (e.g., LogMeIn, PCAnywhere, VNC, and Microsoft Remote Desktop). Used correctly, remote management applications are an efficient and cost effective method of providing technical support among large numbers of merchants. However, if exploited, they potentially expose payment card data and other sensitive information to cybercriminals. Insecurely deployed remote access applications create a conduit for cybercriminals to log in, establish additional "back doors" by installing malware, oftentimes with the capability to record keystrokes, capture audio and video from the affected computer and steal payment card track data. The risk of data compromise is increased when remote access applications are configured in a manner that does not comply with the Payment Card Industry Data Security Standard (PCI DSS).

Over the last several months, phishing campaigns have focused on spoofed LogMeIn emails designed to steal login credentials, which in turn provide attackers access to merchant networks using those POS integrators. The emails often contain either a malicious link or an attached document with a malicious payload. Actual emails recently sent to POS integrators in an attempt to implant malware or steal LogMeIn usernames and passwords are shown below:



From: "LogMeIn" <billing@logmein.com>
To: [redacted]
Cc:
Date: Wed, 18 Feb 2015 08:41:09 -0700
Subject: Automatic payment failed - Credit Card rejected
Attachment invoice_739182.doc

Dear customer,

Your subscription for LogMeIn Central Plus service will end within 72 hours.
You are receiving this notification because the automatic payment has failed. (Credit card - declined)

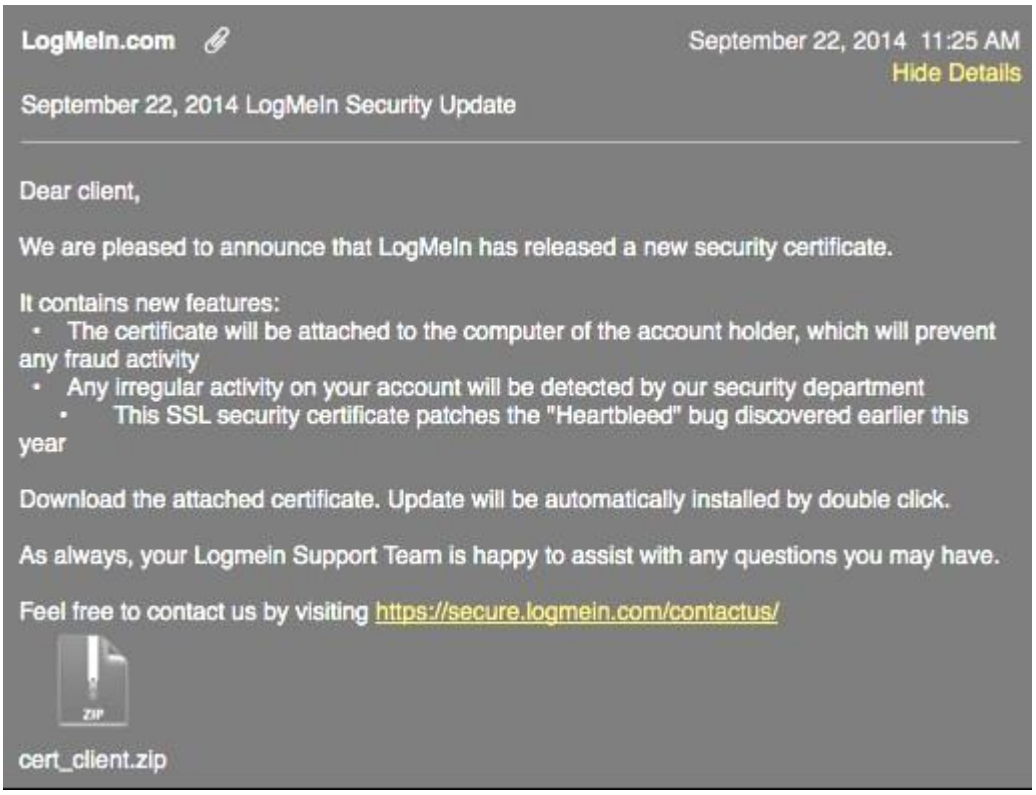
For more information, please find the payment invoice attached to this letter.
Payment must be submitted before 20/02/2015, in order to avoid delays and service interruptions.

Thank you for using LogMeIn

Copyright Â© 2003-2015 LogMeIn, Inc. All rights reserved.

--
This message has been scanned for viruses and
dangerous content by MailScanner, and is
believed to be clean.

Source: Email sample as discussed on http://community.logmein.com/t5/Miscellaneous/Phishing-emails/td-p/130039



LogMeIn.com September 22, 2014 11:25 AM
Hide Details

September 22, 2014 LogMeIn Security Update

Dear client,

We are pleased to announce that LogMeIn has released a new security certificate.

It contains new features:
- The certificate will be attached to the computer of the account holder, which will prevent any fraud activity
- Any irregular activity on your account will be detected by our security department
- This SSL security certificate patches the "Heartbleed" bug discovered earlier this year

Download the attached certificate. Update will be automatically installed by double click.

As always, your Logmein Support Team is happy to assist with any questions you may have.

Feel free to contact us by visiting https://secure.logmein.com/contactus/

cert_client.zip

Source: http://tools.cisco.com/security/center/mviewThreatOutbreakAlert.x?alertId=36120

Forensic analysis of the files attached to these emails showed the malware attempts to connect to an overseas server, downloads additional malware, disables anti-virus applications, installs keystroke logging to steal login credentials, injects custom code into web pages and establishes “backdoor” remote access connection to infected systems. The subsequent infection of systems then leads to theft of payment card data via “RAM scraper” malware capable of scanning memory for payment cards.

"FindPOS" Malware

The most common family of POS malware attached to these phishing attacks is called by several names, including "FindPOS". Two sites that explain the behavior of this malware are listed below:

http://researchcenter.paloaltonetworks.com/2015/03/findpos-new-pos-malware-family-discovered/

http://blogs.cisco.com/security/talos/poseidon

Both sites contain numerous helpful indicators of compromise (IOCs). POS integrators or their partners should carefully review these IOCs as part of their general information security practices.

Mitigation

Visa strongly urges acquirers, processors, POS vendors, resellers and integrators to share this alert with their merchants. Be aware that this threat is very active and malicious actors are diligently searching for additional vulnerable POS integrators to attack. Visa is currently investigating several breached integrators who were initially compromised using the LogMeIn remote access service. Merchants with always-on LogMeIn services operating on POS systems are particularly at risk. Merchants should immediately examine their payment processing environment to determine whether LogMeIn is deployed on their systems in a compliant manner.

The following security practices will help mitigate this threat and other risks to payment card data:

- Always use two-factor authentication for remote access. Two factor authentication can be something you *have* (a device) as well as something you *know* (a password).
- Ensure proper firewalls rules are in place, only allowing remote access only from known IP addresses.
- If remote connectivity is required, enable it only when needed. Contact your POS vendor or integrator to take immediate steps to disable remote access when not in use.
- Restrict access to only the service provider and only for established time periods.
- Contact your support provider or POS vendor and verify that a unique username and password exists for each of your remote management applications.
- Use the latest version of remote management applications and ensure that the latest security patches are applied prior to deployment.
- Enable logging in remote management applications and examine the logs regularly for signs of unknown activity.
- Do not use default or easily-guessed passwords.
- Only use remote access applications that offer strong security controls.
- Plan to migrate away from outdated or unsupported operating systems like Windows XP.

The following are examples of remote access vulnerabilities that are enabling attackers to gain access to merchant POS environments. Please note that most of these are violations of the PCI DSS.

- **Remote access services always on and available on the Internet.** An attacker only needs to perform a port scan against a merchant's IP address space to identify potential targets of opportunity. Remote access applications running all the time are particularly at risk of attack.

- **Single-factor authentication.** Remote access can be vulnerable to brute force and passwordguessing attacks**,** particularly when authentication only requires a username and password.

- **Outdated or un-patched applications and systems.** Older versions of application and operating system software are known to be susceptible to attack and are easily exploited to gain unauthorized access.

- **Use of default passwords or no password.** Using default settings and passwords to access system components will increase the likelihood of a compromise. New hardware devices and software generally arrive from vendors configured with default settings. These default settings must be changed prior to production deployment, as they can be easily guessed and information about these settings is readily available on the Internet.

- **Use of common usernames and passwords.** Often, a vendor or service provider will use a common username and password at multiple client locations to facilitate service calls.

- **Improperly configured firewalls.** In some cases, the POS system has a public IP address that is directly accessible from the Internet.

PCI Qualified Integrators & Resellers (QIR) Program

The PCI Qualified Integrator & Reseller (QIR) program provides training and best practices to ensure a secure installation of merchants' payment systems. The program identifies and engages integrators and resellers who are qualified to install their PA-DSS validated applications in a manner that facilitates PCI DSS compliance.

A trained PCI QIR enjoys the following benefits:

- Achieve industry-recognized qualification (good for 3 years)
- Be included on merchants' go-to global list of qualified integrators and resellers
- Receive specialized training from PCI SSC experts on guidelines for implementing and maintaining payment applications
- Earn CPE credits
- As of June 1, 2015, Visa will add QIRs to its Visa Global Registry of Service Providers

For more information and to submit an application, please visit www.pcisecuritystandards.org/training, call +1 781-876-6231 or email qir@pcisecuritystandards.org with questions.