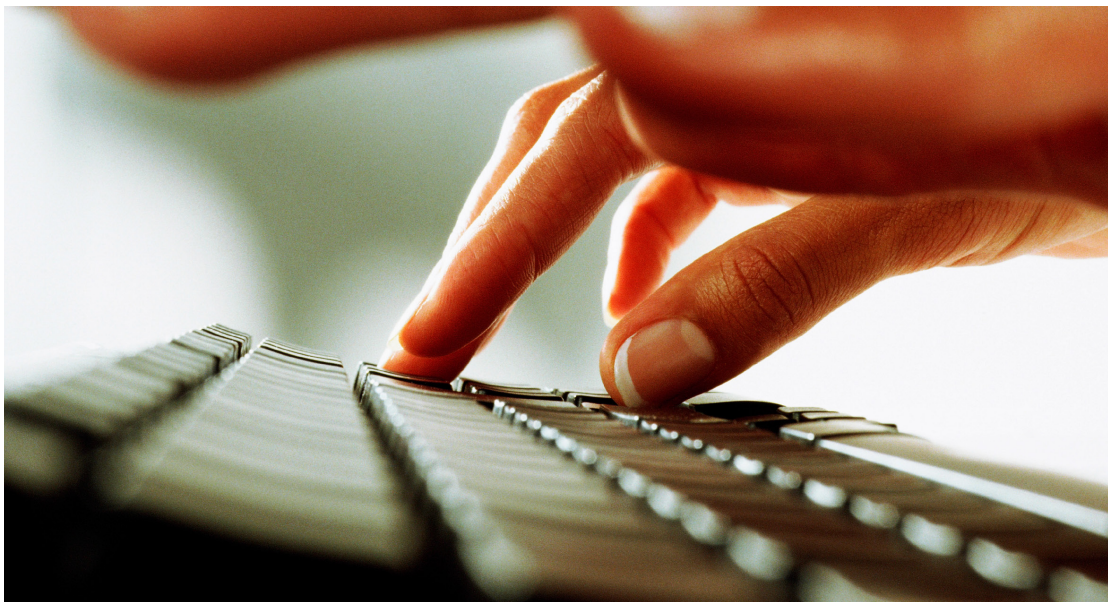
MasterCard Worldwide

Brute Force Attacks—Overview and Best Practices for Merchants



Attack Methodology Overview

A brute force attack against a merchant's retail terminals or its web site's online payment system typically begins with the criminal using malware installation, phishing schemes, or a combination of both to obtain the access privileges needed to carry out the attack.

Obtaining Access Through Malware

The criminal introduces malware into a merchant's network by targeting systems that may be vulnerable to compromise due to weak data security controls, such as the system having:

- No firewall, or a misconfigured firewall, in place
- A weak or non-existent anti-virus solution or intrusion detection system (IDS)
- Open ports or vulnerable web-facing applications
- Default or easily guessable system user IDs and passwords

Once installed on the merchant's system, the malware can capture merchant account logon credentials.

Obtaining Access Through Phishing

Alternatively, the criminal may use traditional phishing techniques to obtain the merchant's account credentials. For example, the criminal may call or send an e-mail to a merchant purporting to be the merchant's processor, service provider, or acquiring bank and request sensitive merchant account credentials, such as the merchant's user ID and password.

Performing Test Transactions Through Brute Force

Once the criminal hacker has gained network access, the merchant's terminal or system can be exploited as a venue for performing test transactions: the hacker's own high-speed computer programs submit numerous authorization requests for small dollar amounts using stolen card account information from victims of other phishing scams in combination with sequential three-digit card validation code 1 (CVC 1) values (e.g., 999, 998, 997, etc.) until the hacker receives a valid authorization (i.e., the CVC 1 value matches the stolen account number).

These submitted authorization requests can accumulate into the thousands in just a short period of time

Perpetuating Subsequent Fraud

Using the valid authorization information, the criminal can then combine the valid CVC 1 value (found in a payment card's magnetic stripe) obtained via the brute force attack with other phished payment account information to create a counterfeit card for use in fraudulent point-of-sale (POS) or ATM transactions.

TO LEARN MORE

Please take advantage of the complimentary webinars and information available on the MasterCard PCI 360 Education Program web site: www.mastercard.com/pci360

For additional information about PCI DSS compliance, please visit the PCI Security Standards Council web site: www.pcisecuritystandards.org

CONTINUED FROM COVER

Best Practices for Merchants

The information provided below is intended to help merchants prevent and detect brute force attacks.

Defending Against Phishing Attempts

- Use caution when providing sensitive information, such as your user IDs and passwords
- Do not provide sensitive information to anyone, unless you are certain of the credentials of the potential recipient of the information
  - Guard your terminal information. **Do not** give out your merchant number, terminal ID, or your acquirer's bank identification number (BIN). Your acquirer already has this information and is highly unlikely to request it. Therefore, if you receive a call requesting this information, it is likely a phishing attempt by a criminal to gain terminal access. Instead, call your acquirer or processor, ask to be transferred to the appropriate person or department that handles your merchant account, and report the call that you received
- Avoid clicking on hyperlinks within e-mail communications. Type the URL into your web browser instead
- Do not download suspicious attachments
- Instruct your employees not to use business computers and workstations for non-business activities, such as web browsing or checking personal e-mail
- When reviewing or responding to e-mails, ensure that the sender's information is correct. Be vigilant for slight misspellings, which may indicate a phishing attempt
- If you receive a phone call, e-mail, or repair technician visit that is suspicious, do not respond or provide any information. Immediately contact your processor or acquirer to verify the legitimacy of the request
  - Beware of any unscheduled terminal repair technician arriving at your merchant location requesting access to your POS terminal. The technician may be a criminal attempting to gain access. If a repair technician arrives unannounced, contact your acquirer or processor to verify the technician's identity using your own contact information on file, not the contact information provided by the technician
- Educate your staff regarding anti-phishing strategies, such as only opening e-mail messages from a known or trusted source
- Limit employee access to the merchant number, terminal ID, or your acquirer's BIN to help prevent unintentional leaking of this information to a criminal

Strengthening Your Network Security

- Ensure that your business operations are in compliance with the *Payment Card Industry Data Security Standard* (PCI DSS)
- Regularly update your anti-virus applications
- Perform a credential and password review:
  - Identify any systems with weak or blank administrator passwords and remediate
  - Require regular password changes for users' system access and privileges
  - Strengthen your password policy
  - Remove generic or vendor default accounts
- Require two-factor authentication for all administrative remote access applications
- Review the firewall rules across your network
- Review web-facing applications for structured query language (SQL) injection vulnerabilities or other web application vulnerabilities
- Implement an IDS

Upgrading Your Terminal Security

- Turn off flag defaults upon installation of the terminal. Many terminals at POS merchant locations are shipped with flag defaults that allow a secure socket layer (SSL) connection. Retail stores do not need this access for a POS transaction
- Ensure that the terminal setting allows only the merchant category code (MCC) assigned by your acquirer or processor. Many terminals are also shipped with a default setting that allows any MCC to be used at the terminal. Criminals often do not know the MCC for the specific merchant location, and use rotating codes to gain access
- During your store's off-hours, if no inventory control or other upgrades are scheduled, turn off your terminals so that off-hours access is denied to the criminal
- Consider replacing terminals with EMV chip-capable terminals that connect through your acquirer or processor
  - As of 19 April 2013, all U.S.-based acquirers and processors must have the capability of processing contact and contactless EMV chip transactions. These terminals can greatly assist in preventing fraud losses to a merchant by reading the computer chip on the credit or debit card rather than the magnetic stripe
  - Fraud liability shifts within the payments industry likely will soon push fraud losses to whichever party in the POS transaction does not have the chip-supporting technology, whether it's the card issuer or the acquirer. Meanwhile, chip terminals at the merchant location may also allow advanced payment types such as tap-and-go, and may increase a merchant's financial performance by opening new payment avenues

In the Event of a Data Breach

If you believe that you have been the victim of a brute force attack by criminals, immediately notify:

- Your processor and/or acquiring institution
- Law enforcement
- MasterCard via e-mail at account_data_compromise@mastercard.com

MasterCard Worldwide