Akamai
FASTER FORWARD

Account Checkers and Fraud

Carders in Action

VERSION: 2013-0005-G

Table of Contents

Executive Summary

Akamai has observed attempted account takeover behavior for a customer resulting from reuse of credentials obtained from other sites. Attackers are using automated tools (“account checkers”) to quickly determine valid userid/password combinations across a large number of ecommerce sites. Attackers using these tools can identify valid accounts rapidly, gain access and acquire names, addresses and credit card data from user profiles, as well as fraudulently acquire merchandise.

Observed Behavior

The following are indications that an account checker has been used against an ecommerce site:

- User complains that their account mailing address has been altered.
- Multiple other users altered in a similar time frame.
- Many failed logins detected in a short period of time from a small number of IP addresses.
- Locked accounts.
- Higher than normal rate of fraud activity.

Attacker Tactics, Techniques and Procedures

Build Tools Server

Attackers will usually compromise a hosted webserver and upload the script. Several known groups also have semi-permanent or permanent domain names where they host their tools (tools.nbteam.us, tool.kid1232.com,ugchecker.cc). Since these scripts make use of proxy sites for the actual attack, however, it is not helpful to block these sites. However, we have seen instances of attackers using Amazon Web Services (AWS) to host their attack tools.

Once appropriate web space has been acquired, the attackers will upload their scripts.

Cultivate List of Open Proxies

Integral to the success of the attack is the use of web proxies. By routing traffic through open proxies, the attackers hope to bypass IP blocks. The tools we have observed allow the attackers to use a list of proxy side and cycle through them with after a fixed number of attempts. The

attackers need to ensure their list of proxies is both of sufficient length to disguise the attack and contains valid proxies, or they risk compromising their attack.

Acquire Compromised Logins

Once the tools are in place, the attackers need to acquire a list of account names and passwords that may be valid on a given domain. These kinds of lists are readily available on sites like pastebin and frequently passed around carder chat forums or offered for sale.

Check/Alter Compromised Accounts

Once the attackers have a list of potential accounts, they user their tools to rapidly check the validity of the accounts. Accounts that work are marked, and the attackers log in using the credentials. Once logged in, the attackers can collect the user's personal data and credit card information to use for further fraud

Make Fraudulent Purchases

Attackers can also modify the shipping address of the victim and make purchases with their stored information. The merchandise is sent to an address near the attacker and picked up. Recently gift cards, both physical and electronic have been key items for purchase as they are easily available, difficult to trace and easy to transport.

Indicators, Detection and Defense

Altered Account Data

Users complain that the mailing address on their account has been changed.

Sites that send emails when account details change report an increase in calls from customers reporting unauthorized changes. Attackers will often set multiple compromised accounts to have the shipping address, and use that as a "canary". If the name or address is later changed, they know that their compromise has been discovered.

A sudden spike in gift card purchases is often an indicator that a company is being attacked. Attackers will use stolen cards to make gift card purchase as an easy way of preserving stolen funds. If there is a sudden increase in fraudulent gift card purchases it may also be a sign of an attack underway.

Failed Login Attempts

Large number of failed account logins in a short period of time

A large number of login attempts that are out of expected customer demographics. For example, users with .uk, .fr, or .de email addresses when 99% of the site's customer base resides in North America.

IP Network Characteristics

When an attacker is using one of these "checker" tools, targets should expect to see a sudden increase in the number of failed account logins. Specifically, multiple hits to the login and checkout pages from a single IP address. Further investigation will show that these hits originate from web hosting providers or Amazon Web Services instances, not residential routers.

If desired, these IP can be blocklisted, although the sheer number of locations an attacker can launch an attack from makes this tactic only minimally effective.

Defenses

The use of a CAPTCHA or other validation step requiring user intervention will defeat the tools described in this advisory.

The use of Akamai's User Validation Module (UVM) will also confirm that the login is coming from a browser and will defeat these tools.

If the customer base is primarily from a known country or region, geoblocking may be an option to minimize the locations an attack can originate from.

Careful review of authentication logs can identify likely proxy servers being used by the attackers. Sequences of different logins from the same IP may be an indication.

Akamai Defenses

Organizations that are on the Akamai platform and are using Kona Site Defender can readily block these kinds of attacks by using a combination of rate controls and IP blocklists.

Akamai recommends that ecommerce customers configure a bucket for the path to their login page.

Customers should then configure a rate control set to 5 requests/sec average and 2 requests/sec burst for that path only. This will ensure that excessive numbers of requests are only blocked to the login page.

When the rate control fires, customers can use the Luna portal to determine the IP addresses that are triggering the rule by attempting an excessive number of logins in a short amount of time. These IP addresses can then be added to a blocklist.

Since the rate controls are set in excess of what a human would do, and since the attack tools route through open proxies, businesses do not need to worry about blocklisting a customer

trying to authenticate to their site. Furthermore, since rate controls only prevent access for 10 minutes, in the unlikely event of a false positive, say a large number of logins from a corporate NAT, legitimate users are not permanently blocked from accessing the site.

Customers should review the list of rate limited IP address during and after the attack. If the IP addresses can be confirmed to be open web proxies, those IPs can be placed onto a permanent IP blocklist to proactively prevent these kinds of account checkers from operating in the future.

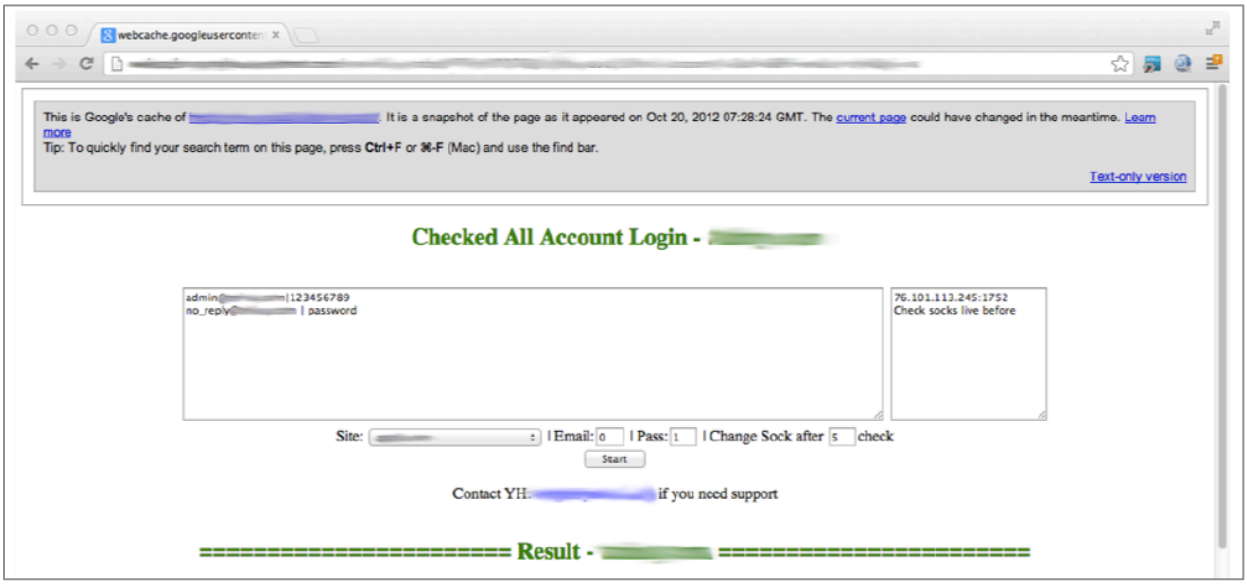
Research Data

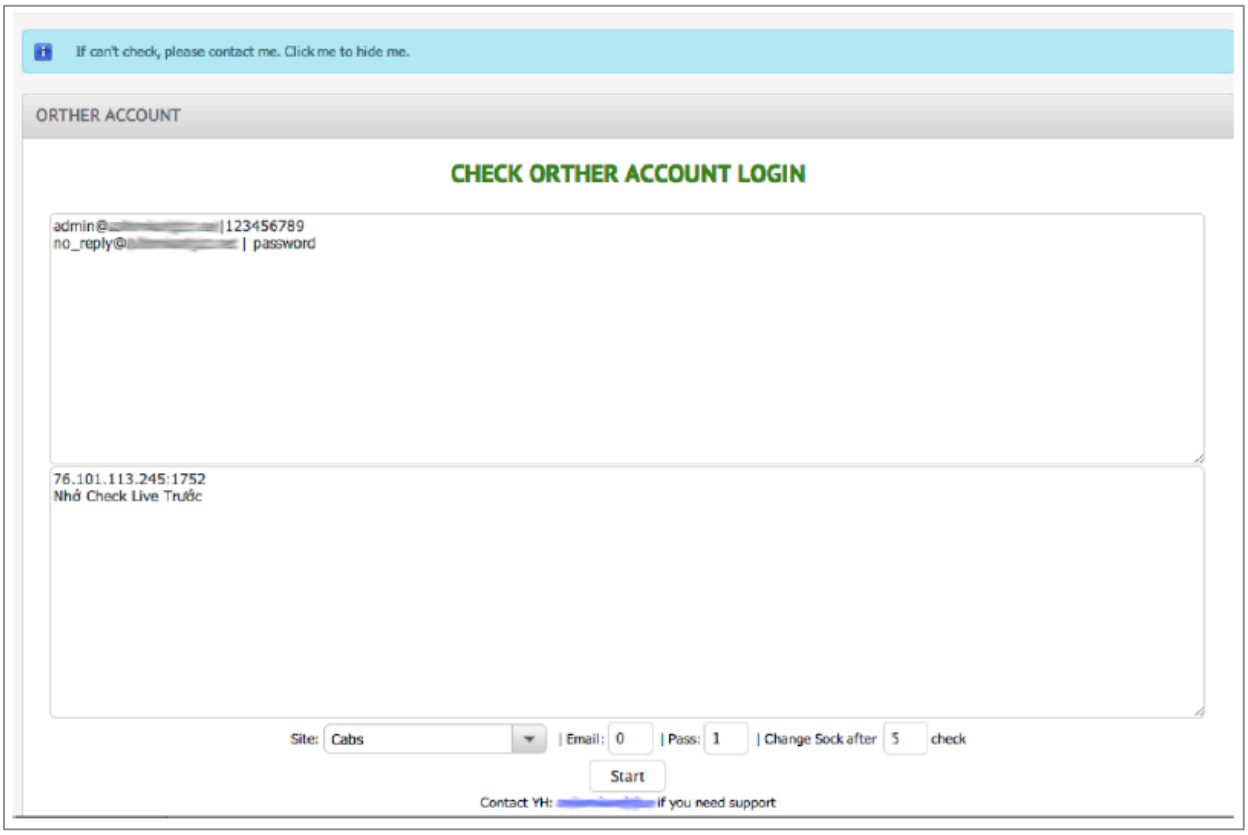
Mechanisms of Attack

The attackers use lists of previously compromised accounts. These are harvested via phishing and readily available on sites like pastebin or underground forums.

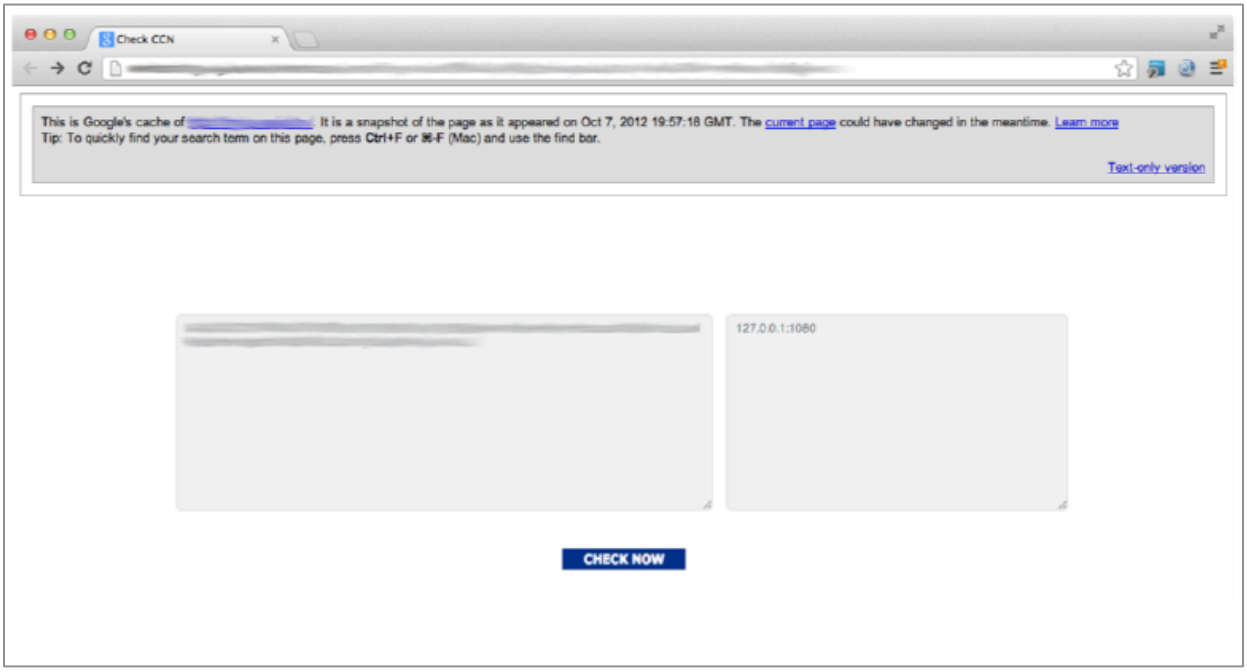
The attacker calls the appropriate page on the site with a web browser that returns a web form. The attacker pastes pipedelimited email addresses and passwords into a text box on the form and submits the data. The script pieces together a login request, then connects to a listed proxy, if any. The request is transmitted to the ecommerce site and the script monitors the response codes to determine if the account is valid or not.

Multiple Site Account Checkers





Credit Card Number Checker



As the global leader in Content Delivery Network (CDN) services, Akamai makes the Internet fast, reliable and secure for its customers. The company's advanced web performance, mobile performance, cloud security and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move *faster forward*, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on www.akamai.com/locations.