Hacker System

Table of Contents

Hacker System Process Overview

The Hacker System is comprised of two front end components:

- Traffic Check (Local Firewall)
    - The Local Firewall component is run first. Incoming traffic for each site is tracked by the Site Location and IP Address and is tested against our table of existing IP addresses (Blocked IP) to determine List Type.
    - An IP address in the Blocked IP table likely has been either previously reported to Xiolink and/or BlockDOS for inclusion in their firewalls or has been previously banned by the Local Firewall.
    - Based on the List Type associated with the IP, the incoming request is treated as follows:
        - A **Black** List IP is blocked by the Local Firewall.
        - A **White** List IP is allowed through without going through Local Firewall testing.
        - A **Gray** List IP will be tested by the Local Firewall (has typically been banned and released previously by the Local Firewall).
        - An IP that is **Not Found** in the Blocked IP table is one that has not been banned and released previously and will be tested by the Local Firewall.
    - As indicated, only traffic for **Gray** List and **Not Found** IP addresses are tested by the Local Firewall. The Local Firewall will automatically halt traffic for an IP address that has reached a designated number of hits (Hit Counter = 1,000) within a specified time period (Delete parameter = 60 minutes/ 1 hour). Subsequent attempts are recorded but still halted.
    - A banned IP address may be manually released at any time through the back end. The release process results in an insert to the Archive table, an insert or update to the Blocked IP table (typically set to Gray unless malicious activity also detected in Translation Check), and the current Traffic Check record is deleted.
    - A banned IP that is not manually released will be auto released at any point that traffic for the IP address is encountered once the Release parameter (1,440 minutes/24 hours) has been reached.
    - A banned IP that is not manually or auto released and has not hit one of our sites prior to the Archive parameter (4,320 minutes/72 hours) being reached will be released at that point.
    - An incoming IP address that completes the Local Firewall test successfully will proceed to the Translation Check. This includes White List IP addresses as well.

- Translation Check
    - The Translation Check component is run second. Each query string and form element is tested for a % character to determine if the data is encoded. Encoded data is decoded for testing.
    - Each query string and form element is tested for the presence of one or more designated characters, symbols, or words. Requests that fail this test are considered potentially malicious and are redirected to a message page.
    - An incoming IP address that completes the Translation Check test successfully will proceed on to regular site processing.
    - IP addresses with potential malicious activity may be set as Black List and inserted or updated to the Blocked IP table to block subsequent attempts.
    - A general review of error emails is performed daily to identify both incidents of malicious activity as well as any potential changes to characters, symbols, and words in the testing script.

Problem Description

Overview/Time Line

- Beginning in May, 2013, we began experiencing an increase in the frequency and scope of malicious attacks on our sites. Attacks are generally recognized by reviewing error emails which often include valuable information on the location of the attack, the data elements and queries utilized, and the IP address of the attack source.
- As attacks were experienced, the IP addresses were reported to our service providers Xiolink (hosting) and BlockDOS (DDOS protection) to include in the Black List for their corresponding firewalls.
- Around December, 2013, the Traffic Blocked IP table was created and the IP addresses that had been reported to our service providers were added to this table to allow for better traffic management.
    - A firewall configuration report was obtained from Xiolink in January, 2014 and was used to reconcile with our Traffic Blocked IP table.
    - A firewall configuration report was obtained from BlockDOS in September, 2014 and was used to reconcile with our Traffic Blocked IP table.
- Since May, 2013 we have continued to experience these attacks and have been frustrated by certain "gaps" in our protection. As an example, an automated attack may easily result in well over 10,000 hits before it is detected and stopped by one of our service providers.
- The Local Firewall component was a measure we came up with to fill this gap with the basic premise of automatically halting traffic for an individual IP address that has X # of hits in a designated period of time.
- The Local Firewall was introduced on 10/2/14 and has been gradually expanded to where all sites are now being monitored as of 10/13/14 (Calling Cards sites were the last ones to be implemented).
- The Local Firewall has now been turned OFF for all sites as of 10/16/14 at 2:50 PM ET.
- During the time when the Local Firewall was turned ON:
    - A total of 12 IP addresses were halted (see below for **Traffic Halt Steps**).
    - Traffic ranged from around 800 – 1,600 IP addresses being tracked per hour depending on time of day.

How It Works

- The Local Firewall component is encapsulated in an include file (traffic_check.asp). The traffic_check.asp file is included at the top of the already existing translation_check include file that is in db.asp for each site.
- A unique site identifier (gTrafficId) is placed in the db.asp file for each site and is available to the Local Firewall to determine the site/location as well as database (BAPC or CallingCards) as there are differences between the database sites that must be taken into account.
- The default value for the IP address is read from the ServerVariables (using Remote_Addr) to provide an initial IP address value. We perform specific tests using

other relevant ServerVariables values to make sure we obtain the proper IP address value taking into account such scenarios as forwarding and proxies. The CallingCards sites are handled in a separate manner since the originating IP address is masked by BlockDOS.

- IP addresses tracked by the Local Firewall that "pass" the tests below are stored in the Traffic Check table.
- Tests (performed on each hit attempt for all traffic):
  - Select the global firewall parameters from the Traffic Parameters table:
    - Global On/Off
    - Delete Minutes (default = 60 minutes)
    - Hit Counter (default = 1,000 hits
  - If the Global On/Off setting is OFF, we bypass the rest of the tests.
  - If the Global On/Off setting is ON, we check the setting for the specific Site/Location from the Traffic Locations table (this allows us to have the Local Firewall turned ON/OFF for specific sites).
  - If the Global On/Off setting is ON but the Site/Location is turned OFF for the selected site/location, we bypass the rest of the tests.
  - If the Global On/Off setting is ON and the Site/Location is turned ON, we check the Traffic Blocked IP table to determine if the specific IP address already exists and, if so, determine the List Type (White, Gray, or Black) – see List Type below for explanation.
  - If the Global On/Off setting is ON, the Site/Location is turned ON, and the specific IP address is not set as White List in the Traffic Blocked IP table, we proceed with testing. Otherwise, we bypass the rest of the tests.
  - We delete all existing entries in the table that are older than the Delete parameter (default = 60 minutes). This step ignores entries that have been banned (reached 1,000 hits in 60 minutes) as they are handled by **Traffic Halt Steps**.
  - We check for the existence of the specific IP address in the Traffic Check table.
  - If the specific IP address exists in the Traffic Check table (means that IP address has hit within past 60 minutes), we obtain the current Counter value and Status (0 = Current, 1 = Banned).
  - If the IP address exists in the Traffic Check table with a Status of 1 = Banned, we stop the attempt. Otherwise, we increment the Counter by 1.
  - If the IP address does not exist in the Traffic Check table, we set the Counter to 1.
  - An IP address with a Counter of 1 is inserted into the Traffic Check table.
  - An IP address with a Counter of > 1 already exists in the Traffic Check table so the table is updated for the IP address with the Counter incremented by 1.
  - For those IP addresses that were found to already exist in the Traffic Blocked IP table with a List Type of Black, we send an "Existing Black List" email notification and stop the attempt.
  - For those IP addresses that did not already exist in the Traffic Blocked IP table with a List Type of Black but reached the designated Counter value (default =

1,000), the Status is set to 1 = Banned and we send a "Traffic Status Change" email notification and stop the attempt.

Components

- gTrafficId variable stored in db.asp
- Traffic_check.asp include file
- Traffic Blocked IP table
- Traffic Parameters table
- Traffic Locations table
- Traffic Check table

Administration

- The Administration component may be accessed from the CallingCards.com Administration Menu. Select the Other/Utility option at the bottom left:
    - IP Tracking Report – This report displays the contents of the Traffic Blocked IP table and may be sorted by IP Address and Date Entered.
    - Manage Local Firewall
        - Manage Parameters
        - View Current Activity
        - View Current Status (by Site)

List Types

- Black – All traffic for the specific IP address is stopped.
- Gray – This category represents IP addresses that were identified as malicious based on the signature of the error emails but were not reported to our service providers at that time.
- White – All traffic for the specific IP address is allowed to continue unabated.

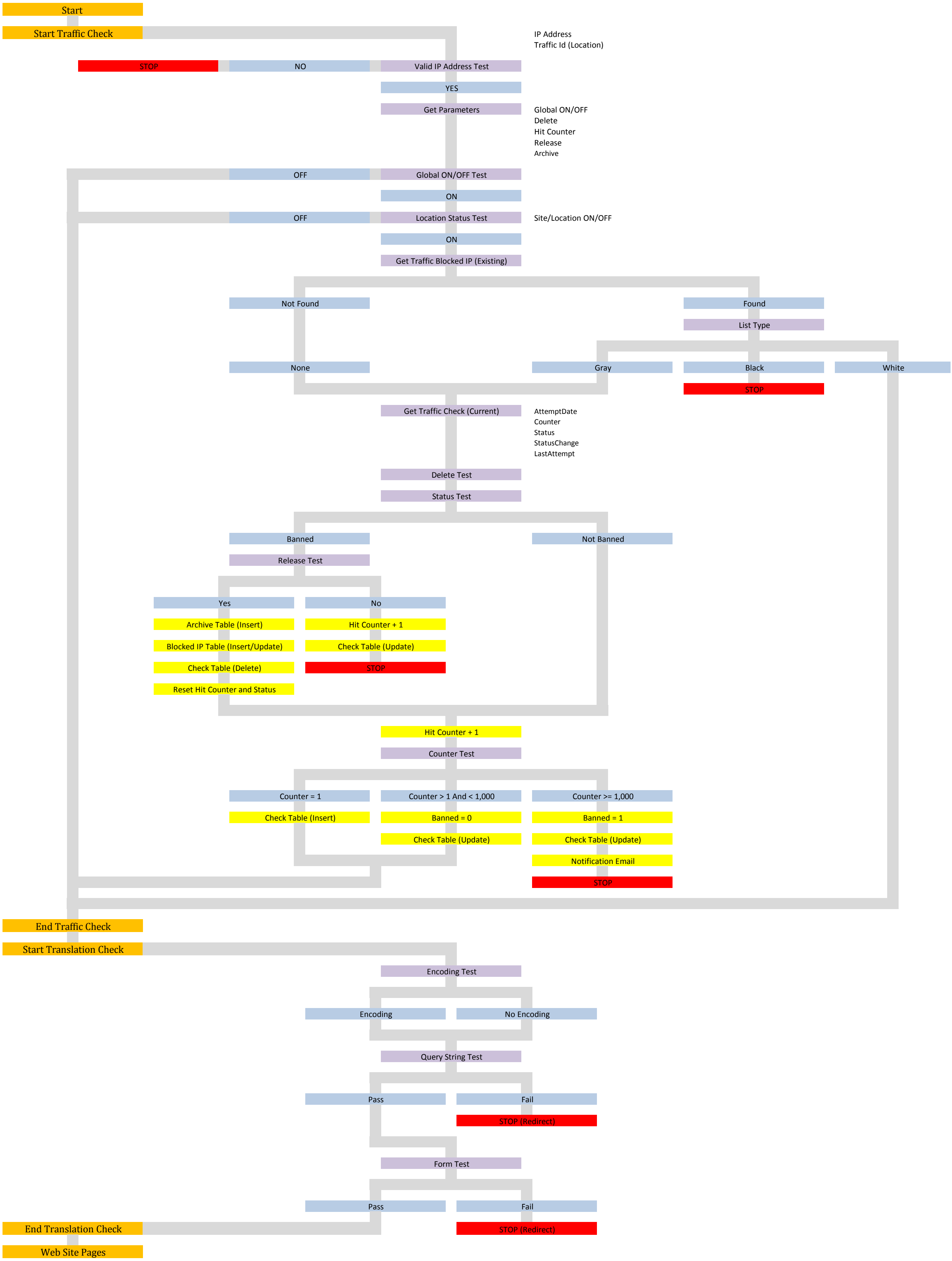
Traffic Halt Steps

- All current Local Firewall activity is stored in the Traffic Check table and may be viewed in Manage Local Firewall/View Current Activity. By default, banned IP addresses are listed at the top:
    - Select Get Current History to verify not an existing customer with order activity:
        - A check is performed to determine if existing orders in BAPC database for selected IP address.
        - A check is performed to determine if existing orders in Calling Cards database for selected IP address.
        - A check is performed to determine if selected IP address is in the External Recharge table (Topup API customers).
    - Utilize IP Lookup function in WhatIsMyIPAddress.com web site for more information.
    - Report IP Address to BlockDOS and Xiolink.

- Upon verification from BlockDOS and Xiolink, select Move to Blocked IP. This function removes the banned IP address from the Traffic Check table and allows the Black List status in Traffic Blocked IP to be utilized to halt future traffic from the selected IP address.

Pending Thoughts/Action Items

- Incorporate mechanism for handling Gray List IP addresses.
- Identify “good” bots and SEO tools that need to be on White List.
- Move check for existing Black List outside if existing tests to allow that test to be performed when Local Firewall global and/or Site/Location parameter is OFF.
- Add appropriate individuals to notifications (currently just Scott and Cherie).
- Consider an additional List Type category for bots and tools where we monitor the traffic but do not ban the IP address if parameters are met.
- Administration piece needs work – right now is just the basics.
- Traffic Check table entries are not deleted on global OFF but are instead deleted on next hit once turned ON.


Start
Start Traffic Check
IP Address
Traffic Id (Location)
STOP
NO
Valid IP Address Test
YES
Get Parameters
Global ON/OFF
Delete
Hit Counter
Release
Archive
OFF
Global ON/OFF Test
ON
OFF
Location Status Test
Site/Location ON/OFF
ON
Get Traffic Blocked IP (Existing)
Not Found
Found
List Type
None
Gray
Black
White
STOP
Get Traffic Check (Current)
AttemptDate
Counter
Status
StatusChange
LastAttempt
Delete Test
Status Test
Banned
Not Banned
Release Test
Yes
No
Archive Table (Insert)
Hit Counter + 1
Blocked IP Table (Insert/Update)
Check Table (Update)
Check Table (Delete)
STOP
Reset Hit Counter and Status
Hit Counter + 1
Counter Test
Counter = 1
Counter > 1 And < 1,000
Counter >= 1,000
Check Table (Insert)
Banned = 0
Banned = 1
Check Table (Update)
Check Table (Update)
Notification Email
STOP
End Traffic Check
Start Translation Check
Encoding Test
Encoding
No Encoding
Query String Test
Pass
Fail
STOP (Redirect)
Form Test
Pass
Fail
End Translation Check
STOP (Redirect)
Web Site Pages

Site Version Matrix 2/28/16

translation_check.asp + comments/notes in translation_check_readme.asp(in IR/Admin only)
** Date corresponds to backup of existing hacker code source (db or general) using date of file - i.e. - general_050814.asp*

	Version						
Site/Location	**Traffic**	**Last**	**Translation**	**Last**	**Traffic Id**	*****	**Comments/Notes**
activate/inc/db.asp	15	2/28/16	21	2/28/16	17	8/6/07	No mobile site + no DEV location + no previous hacker code
activate/LQ/inc/db.asp	15	2/28/16	21	2/28/16	18	6/16/08	No mobile site + no DEV location + no previous hacker code
callingcard/inc/general.asp	15	2/28/16	21	2/28/16	4		URL Decode originally added 5/8/14
callingcard/mobile/inc/general.asp	15	2/28/16	21	2/28/16	7	3/12/13	Added 8/13/14
callingcards/ap/inc/db.asp	15	2/28/16	21	2/28/16	10		URL Decode originally added 1/21/14
callingcards/chinese/shopping/inc/db.asp	15	2/28/16	21	2/28/16	11	9/10/12	No mobile site
callingcards/export/export*.asp	N/A	N/A	N/A	N/A	N/A		Added 8/20/14 + uses db.asp from shopping
callingcards/french/shopping/inc/db.asp	15	2/28/16	21	2/28/16	12	6/14/12	No mobile site
callingcards/german/shopping/inc/db.asp	15	2/28/16	21	2/28/16	13	6/19/12	No mobile site
callingcards/shopping/inc/db.asp	15	2/28/16	21	2/28/16	15	3/14/13	
callingcards/shopping/mobile/	N/A	N/A	N/A	N/A	N/A		Uses db.asp from shopping
callingcards/spanish/shopping/inc/db.asp	15	2/28/16	21	2/28/16	14	6/19/12	No mobile site
conferencecaller/inc/db.asp	15	2/28/16	21	2/28/16	19	9/6/12	No mobile site
conferencecalls/inc/db.asp	15	2/28/16	21	2/28/16	20	10/9/13	Executive + View Reports + reports 1 and 4 include "Subscription"
conferencecalls/brightspot	N/A	N/A	N/A	N/A	N/A		Uses db.asp from main inc folder
conferencecalls/mobile/inc/db.asp	N/A	N/A	N/A	N/A	N/A	10/9/13	Uses db.asp from main inc folder
corporate/inc/db.asp	15	2/28/16	21	2/28/16	22	5/24/11	
corporate/mobile/inc/db.asp	15	2/28/16	21	2/28/16	23	5/24/11	No previous hacker code
instantrecharge/inc/db.asp	15	2/28/16	21	2/28/16	21		URL Decode originally added 3/13/14
instantrecharge/admin/HackerScriptTest.asp	15	2/28/16	21	2/28/16	1		**MASTER LOCATION w/ previous versions (test location only)**
interpreter/inc/general.asp	15	2/28/16	21	2/28/16	5	2/14/13	Mobile uses general.asp from main inc folder
mobile/inc/general.asp	14	2/27/15	20	10/12/15	8	3/1/13	
mobile/phone/inc/general.asp	14	2/27/15	20	10/12/15	9	3/8/13	
onetranslator/inc/general.asp	15	2/28/16	21	2/28/16	6	2/2/13	No mobile site
requestcaller/inc/db.asp	15	2/28/16	21	2/28/16	24	5/24/11	
requestcaller/iphone/	N/A	N/A	N/A	N/A	N/A		Uses general.asp from main inc folder
requestcaller/mobile/	N/A	N/A	N/A	N/A	N/A		Uses general.asp from main inc folder
topup/inc/general.asp	15	2/28/16	21	2/28/16	2	9/11/13	
topup/admin	N/A	N/A	N/A	N/A	N/A		Uses general.asp from main inc folder
topup/mobile/inc/general.asp	15	2/28/16	21	2/28/16	3	4/23/14	

Translation Check

Input Character(s) or Word(s)	Live	Comments
'	X	Consider replace single quote with double quote on all input
--	X	Comments
"	X	
(	X	Exclude test for callingcards (process recharges)
)	X	Exclude test for callingcards (process recharges)
*/	X	Prevent masking input such as UN/**/ION
/*	X	Prevent masking input such as UN/**/ION
;	X	Exclude test for topup and conferencecalls
@		Exclude for Email field
@@		
[	X	
]	X	
<	X	Exclude test for subscription in conferencecalls
>	X	
1=1	X	This is common but hacker can use similar like a=a
alter		
begin		
cast		
char		
char(	X	
chr(	X	
create		
cursor		
declare	X	
delete		
drop table	X	
end		
exec		
execute		
fetch		
insert		
kill		
nchar		
nvarchar		
open		
script	X	With space after word to allow subscription (conferencecalls)
select	X	SELECT must have space after + added v1
sys		
syscolumns		
sysobjects		
table		
union	X	
update		
varchar		
xp_		For catalog extended stored procedures

Traffic/Translation Version History 2/28/16

Description	Traffic	Translation	Date	Comments
Previous version called XSiteScript.asp (pre-implementation) stored in IR Admin/Backup_092013		pre-v1	N/A	
Added [and } to translation check		pre-v1	5/8/14	
LIVE + SELECT must have space after		v1	6/10/14	
Bad external links for callingcards = origsel=Costa%Rica		v2	6/16/14	
Broke out test for conferencecalls to allow SUBSCRIPTION		v3	6/16/14	
Calling cards (maybe others) issue with % for(X % has been taken off your order)			6/25/14	
Allow iframe width/height (contains %)			6/27/14	
Allow password w/ "%" + unable to test in IR/A; need CheckName value = password			6/27/14	
Added tests for 1=1, ', ", CHR(, CHAR(, (,)		v8	7/22/14	
Broke out test for callingcards to skip test for (and)		v9	7/23/14	
Added ; and DROP TABLE		v11	7/29/14	
Take out Not Instr(strCheckName, "PASSWORD") on form test allows new strong passwords		v13	8/7/14	
Adjust form input tests for Email and Password (Instr)		v14	8/12/14	
Remove several non-special character tests from form input exclusion for email and password		v14	8/12/14	
Implemeted traffic_check INITIAL Delete = 60 and Counter = 500)	v1	v15	10/1/14	
LIVE (Current = 60, 500, ON) + changed Counter to 1,000 after live	v1	v15	10/2/14	
Added table for parameters - DeleteParameter (60 minutes) and HitCounter (1000 hits)	v2		10/2/14	
Added global parameter for FirewallStatus = ON/OFF	v3		10/3/14	
Stored procedures cross database + callingcard	v4		10/3/14	
Added location table + check for location ON/OFF setting	v5		10/8/14	
Added switch for difference in open/close connection (by Traffic Id)	v6		10/8/14	
Handling if no value for Traffic Id = use global setting	v7		10/9/14	
IP address checking to handle proxys/forwarding + special case for callingcards sites due to BlockDOS	v8		10/13/14	
Change form tests on SELECT and UNION to halt only if space before and after to reduce false positives		v16	10/28/14	
Change Response.End (blank page) to Redirect to display message page (CallingCards DB sites only)		v17	10/30/14	
Check/block existing Black list even if global or location is turned off	v9		10/30/14	
Add Traffic Id to notification emails	v9		10/30/14	
Added LastAttempt + StatusChange value (only if staus changes)	v9		10/30/14	
Added function to validate IP address for each applicable Request.ServerVariables value before using	v10		10/31/14	
Allow/monitor on ListType = Gray	v11		11/6/14	
Added ReleaseParameter with default of 1,440 minutes + Auto Release mechanism	v11		11/6/14	
Change Response.End (blank page) to Redirect to display message page (BAPC DB sites)		v18	11/20/14	
Still Response.End for foreign language sites		v18	11/20/14	
Added Auto Archive parameter	v12		12/10/14	
Added subnet functionality for existing records in Blocked IP (white and black) + Subnet Check ON/OFF	v12		12/10/14	
Completed rollout of traffic v12 and translation v19 + Subnet Check turned ON	v12	v19	1/22/15	
Add ArchiveDate to Archive table (determines date/time of when released)			2/5/15	
Auto archive release only one banned IP per hit attempt (avoid duplicate release)	v13		2/5/15	
Replaced existing subnet checking; upgraded to check within last quadrant (greater than /26 subnet)	v14		2/27/15	
Custom HitCounter parameter for 129.121.236.89 = 5,000 on 3/11/15 + changed to 10,000 on 3/16/15	v15		3/16/15	Not fully distributed
Verified sub-IP address not available for external XML feed site			3/20/15	
Special tests to stop scan tool activity		v20	10/12/15	
Special test to allow (and) in topup for product display variable		v21	11/23/15	Not fully distributed