RSA Conference2016

Singapore | 20-22 July | Marina Bay Sands

Connect to Protect

SESSION ID: GPS1-F03

Web Attacks of Past, Present, and Future

Michael Smith

APJ Security CTO

Akamai Technologies

@rybolov

#RSAC

2 types of Web Attacks

High-Impact, Low Frequency

- DDoS
- Data Breaches
- Defacement
- Third-Party Content Compromise
- DNS Hijacking
- Datacenter Outages
- Scrapers

Low-Impact, High-Frequency

- Vulnerability Scanners
- Web Attack Farms
- Login Abuse/Account Checkers
- “Noise of the Internet”
- Scrapers

Account Takeover

SC MAGAZINE FOR IT SECURITY PROFESSIONALS

New variant of Apple malware once again puts users at risk

Download our latest spotlight issue on insider threats!

NEWS | PRODUCTS | BLOGS | RESOURCES | VIDEOS | SC MA

SC Magazine > News > Police arrest "Mattfeuter" site operators, break up $200M carder racket

Danielle Walker, Reporter

Follow @daniellewlkr

June 06, 2013

Police arrest "Mattfeuter" site operators, break up $200M carder racket

International authorities have broken up a ring of scammers who sold consumers personal and financial information through a "dump" site, resulting in $200 million in fraudulent charges.

The group was disbanded when its alleged leaders, Van Tien Tu and Duy Hai Truong, were arrested last week in Vietnam. At least 10 others, including some who are unnamed, were apprehended by police in Vietnam and the United Kingdom.

Truong, 23, was charged in the United States with conspiracy to commit bank fraud in New Jersey for his role in the racket, in which fraudsters charged credit cards issued here and in Europe from 2007 until their arrest. Victims also include consumers in Vietnam.

SOCIETY

Last update 16:49 | 05/06/2013

0 0

The "boss" in £200mil credit card fraud ring arrested

VietNamNet Bridge - On June 4, the Supreme People's Procuracy approved emergency warrants for the arrest of eight suspects in the network that traded stolen data of credit cards worth 200 million pounds. The investigation agency defined a man named Van Tien Tu as the ringleader.

Akamai

Ho Chi Minh City jails 7 for abetting $200 mln transnational credit card fraud

Thanh Nien News

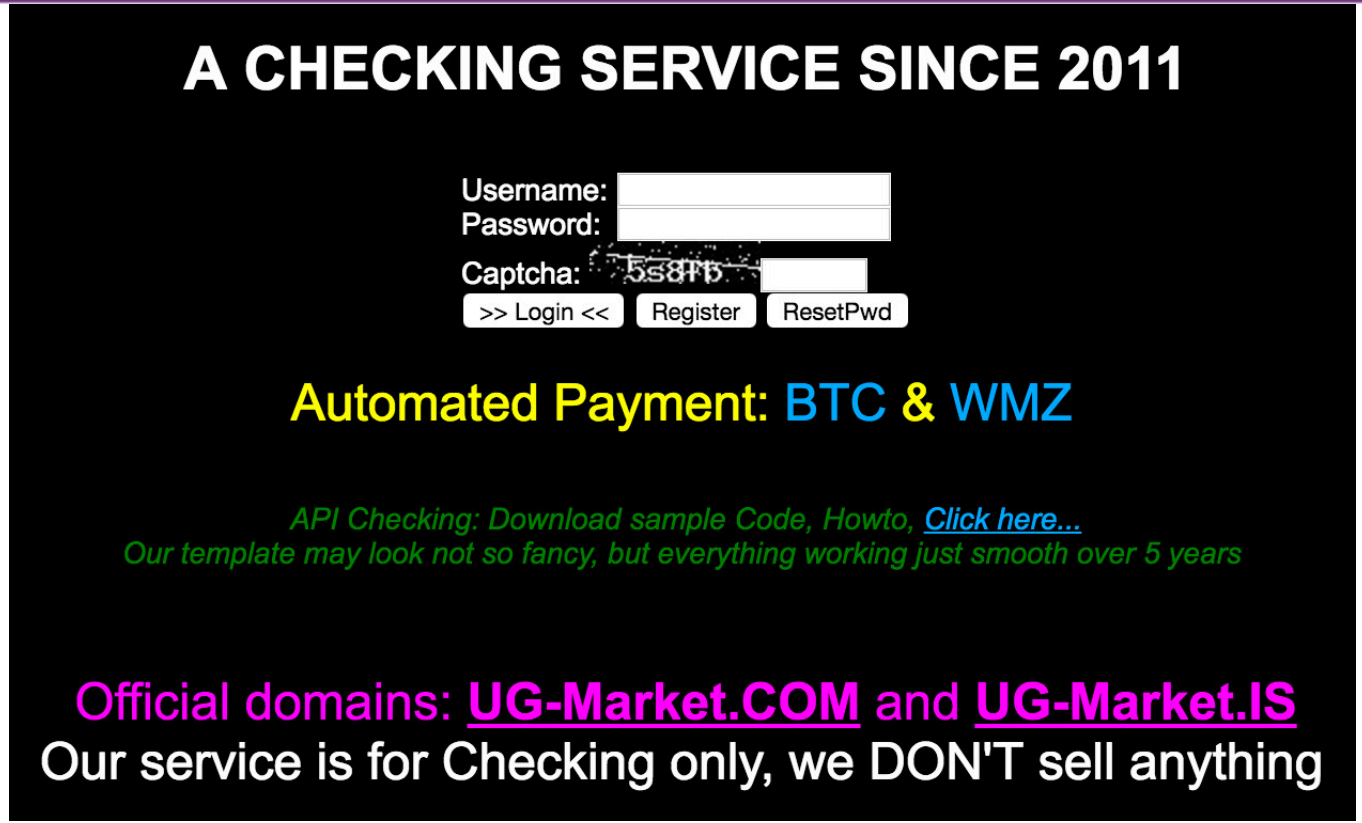
HO CHI MINH CITY - Friday, January 08, 2016 18:47

Email Print

Account Takeover in a Nutshell

- Set up a tools site
- Cultivate proxy list (“socks”)
- Obtain username/password list
  - Phishing
  - Data dumps
  - Buy them
- Check accounts on multiple sites with account checker (1:12 success rate!)
- Cash out
- ?????
- Profit!

UG Sites


A CHECKING SERVICE SINCE 2011
Username:
Password:
Captcha:
5s8fb
>> Login <<
Register
ResetPwd
Automated Payment: BTC & WMZ
API Checking: Download sample Code, Howto, Click here...
Our template may look not so fancy, but everything working just smooth over 5 years
Official domains: UG-Market.COM and UG-Market.IS
Our service is for Checking only, we DON'T sell anything

Cashout Schemes

- Pre-paid credit cards
- Gift cards (physical and digital)
- Other cash equivalents
- Purchase vouchers
- Loyalty points
- High-value items such as electronics

Fighting Account Takeover

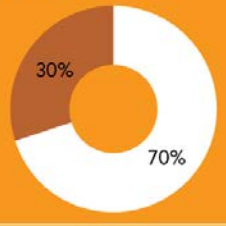
- Better workflow for profile changes
  - Shipping address
  - Email
- “Factor and a Half” authentication
- Rate Controls for /path/to/login/login.php
- Googledork for account checkers aimed at you
- Harvest socks IP addresses
  - Observed traffic (and share)
  - From attackers’ own sites
- Takedown/forensics on tools sites
- Get public password dumps and compare them to your users

Bots and Scrapers

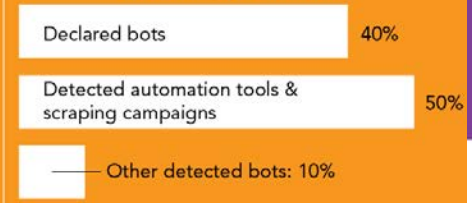
- Booking agents
- Competitors
- Stock price calculators
- Natural language translators
- Consumer Price Index calculators
- Real estate price calculators
- Aggregators
- Business partners

Overall Bot Traffic

During a full day sample, bot traffic accounted for 30% of all web traffic

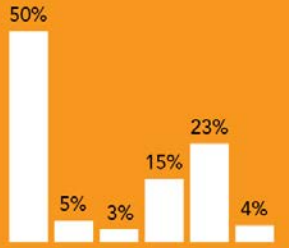


Bot Category Distribution



Declared Bots Breakdown / 40% of Bot Traffic

- Web search engines & indexers: 50%
- Media aggregators (social media, news, RSS): 5%
- Commercial aggregators (price comparisons, enterprise data aggregators, scraping enterprise services): 3%
- Analytics & research bots (advertising, SEO analyzers, audience analytics, business intelligence): 15%
- Web monitoring services (performance & health, link checkers): 23%
- Other declared bots: 4%



Detected Automation Tools & Scraping Campaigns / 50% of Bot Traffic

- Web-browser impersonators: 55%
- Search-engine impersonators: 8%
- Development frameworks: 30%
- Other detected web scrapers: 7%

Other Detected Bots / 10%

Fighting Bots

- Identification is key: know your traffic
  - Friendly
  - Hostile
  - Ambiguous
- Business rules for each bot type
  - Off-hours v/s peak time
  - Don’t just block: slow down, misdirect, give “cheaper” content

Resources for You to Use

- 2 Quarterly Reports at https://www.stateoftheinternet.com/
  - Internet: broadband speeds, content consumption
  - Security: web application, DNS, and DDoS attacks
- Quarterly Threat Brief Webinar
  - SotI data
  - Incident response lessons
- Read the security piece of our blog at https://blogs.akamai.com/security/
  - Advisories
  - Vulnerability and patch information
  - Product updates