

RSAConference2019 **Asia Pacific & Japan**

Singapore | 16–18 July | Marina Bay Sands



BETTER.

SESSION ID: SEM-T03A

ATO and the Underground Credential Ecosystem

Brandon Hoffman

VP, Intelligence Solutions
Intel 471
@bshoffman



#RSAC

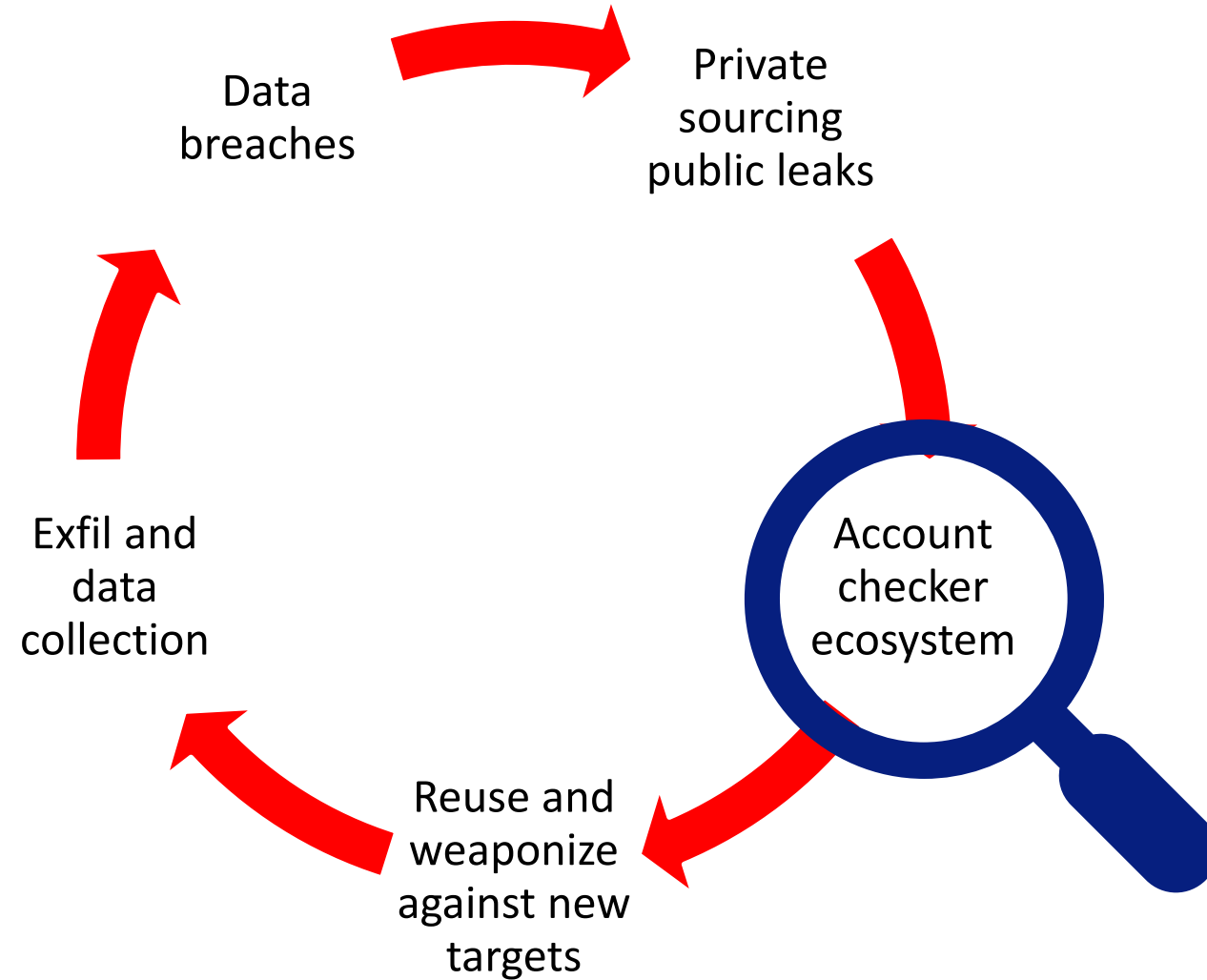
Introduction to account takeover (ATO)

- What is ATO? The act of taking over legitimate accounts using compromised or stolen credentials.
- Our approach to CTI focuses on adversary actions
- Identifying these core factors which further enable cyber crime, fraud and PII sales is the key to protecting vulnerable assets

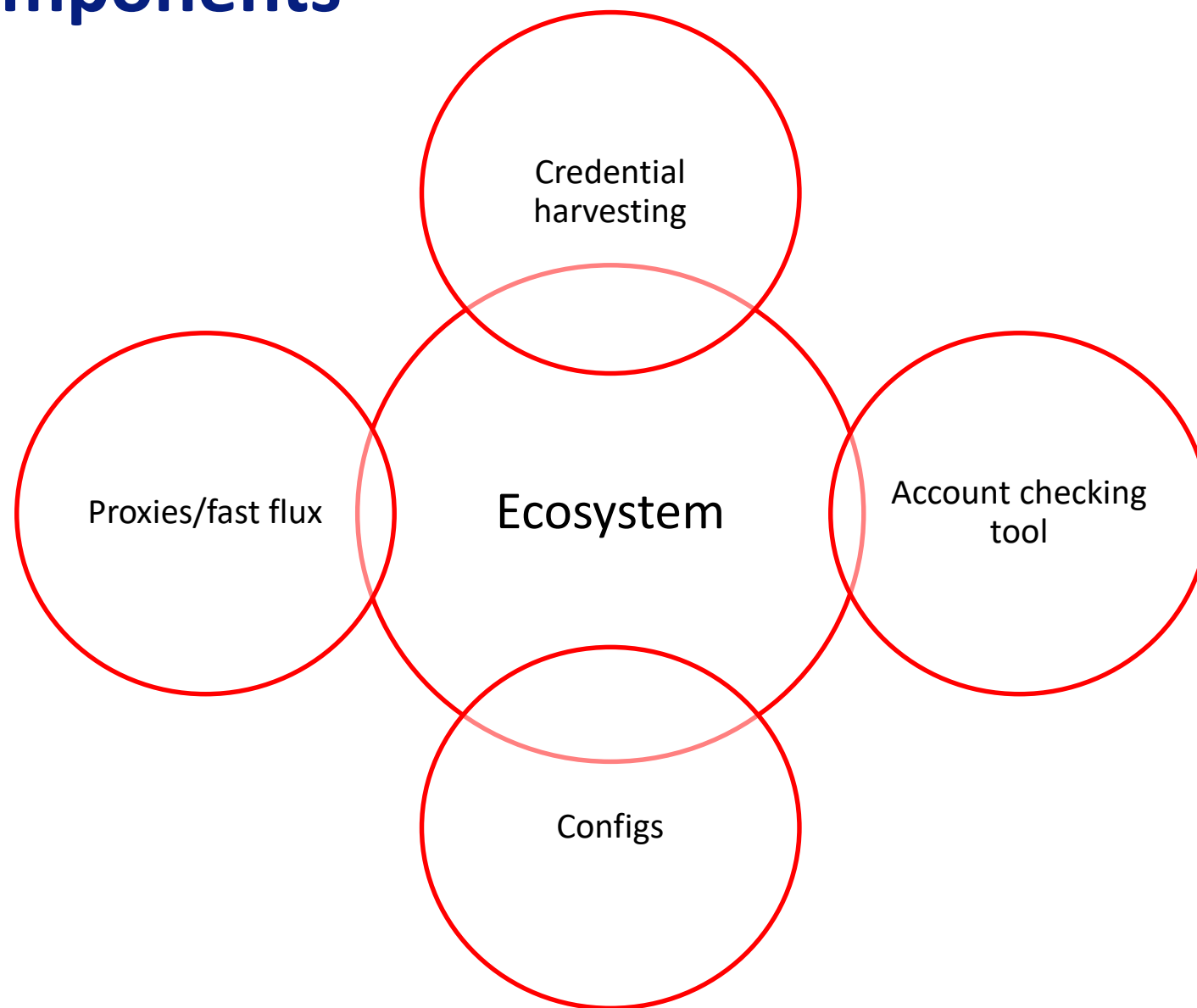
Threats vs Solution

- Bank fraud
 - Remains extraordinarily profitable despite all advancements in security in the last three decades
 - Customer account fraud
 - Healthcare accounts, Rewards programs, miles, points etc
 - Gift card
 - Redeeming compromised retail credit card points for in-store cash, points
- VS
- Use threat intelligence to:
 - Track actors in the ecosystem
 - Understand tools and TTPs
 - Obtain configs and dissect them
 - Identify popular credential attacks and tools
 - Understand malicious IaaS and take action

ATO Lifecycle



ATO Key Components



RSA®Conference2019 **Asia Pacific & Japan**

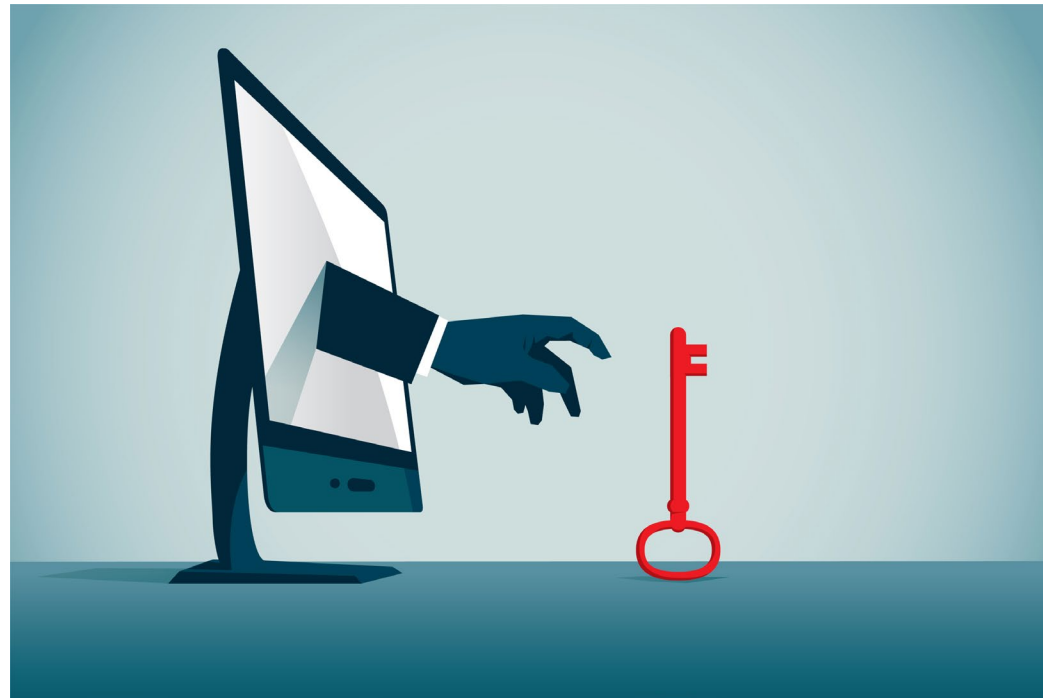
Credential Harvesting

Feeding ATO

Credential Harvesting

Credential harvesting via malware and other tools is another critical input to ATO and part of the ecosystem. Recent tools of interest for credential harvesting include:

- Vidar
- Azorult



Credential Harvesting – Vidar logs

Possible British actor Junx (aka xSweg, ItsJamie, osnapitzjamie, Jamie Jackson) offers compromised logins from botnet logs

PUBLISHED: 19 APR 2019 11:47:16 UTC

RAW TEXT

RESEARCHER
COMMENTS

On Feb. 28, 2019, the actor **Junx** posted following on the forum Hack Forums:

[SELLING] Almost ANY Account Online! [Harvard] [Backends]

Code

Almost ANYTHING on the internet! (Just ask when you are ready to buy!)

Harvard

Stanford

Github

PMA Logins

Cpanels

Teamviewer Accounts

Wordpress

Pizzahut Backend

Bestbuy RMA

RS/Habbo/UMG/GB | Games

SMM Panels

Twitter/Facebook/Instagram/Youtube | Social Media

If you are lucrative you can find good ways to make money from this!

It is simple, I am offering almost any websites account. It is not cracking, rather from Botnet.

Malware campaign has ran hundreds of thousands, we will find what you need.

Also it is not sifted through beforehand, if you understand the immense amount of accounts, no one would attempt this task.

Credential Harvesting – Azorult logs

Actor mmilolika trades compromised personal information, malware logs; Health care organizations in Belgium, France, Hong Kong, US impacted; Allegedly runs AZORult stealer

PUBLISHED: 24 JAN 2019 13:44:37 UTC

TRANSLATED
TEXT

RAW TEXT

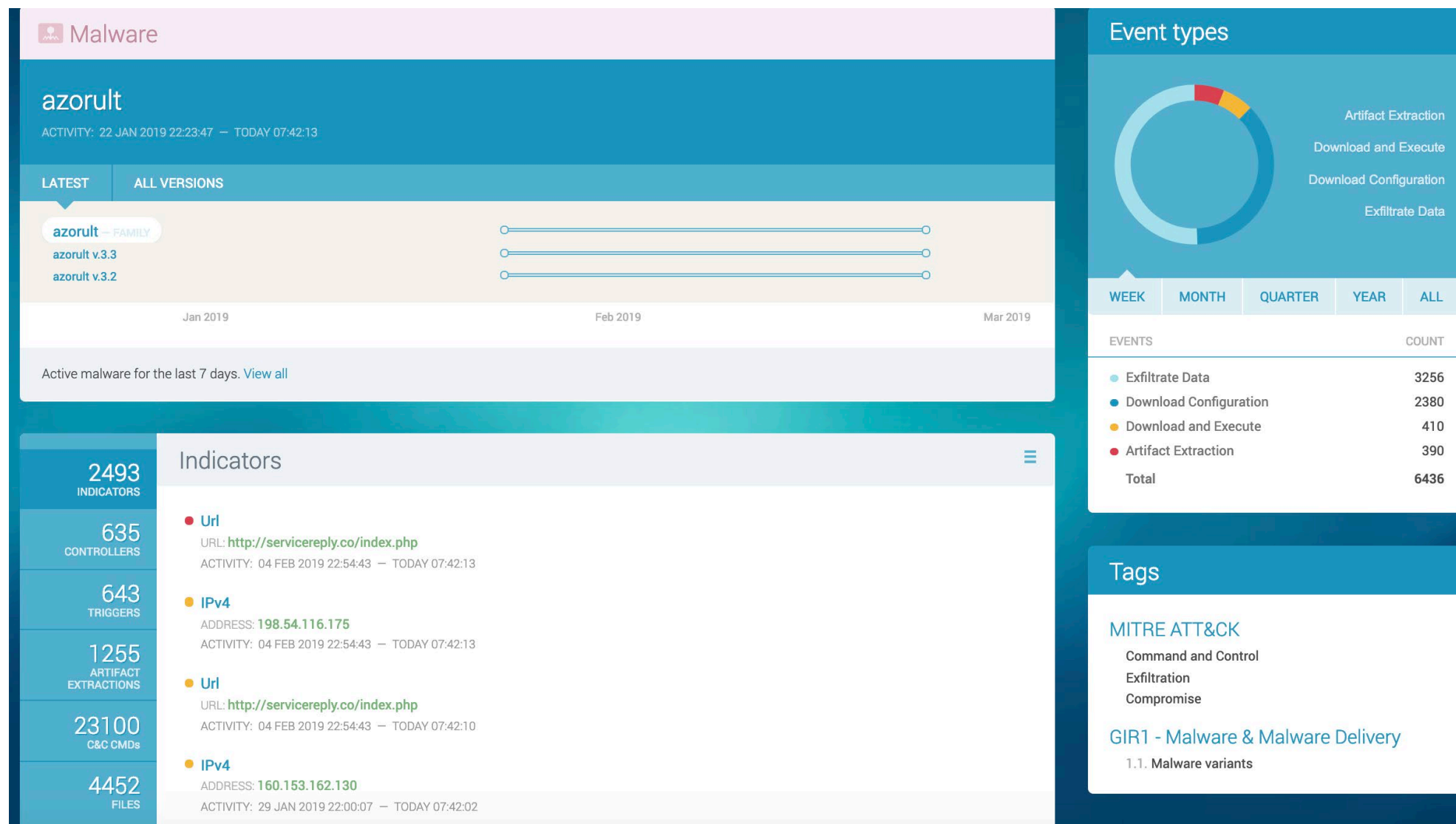
RESEARCHER
COMMENTS

Information from our source and assessment of credibility

The actor **mmilolika** surfaced in the underground in November 2018 and created accounts across 19 cybercrime forums. The actor's primary area of expertise is trading personal information and malware logs. The actor said the logs are sourced from the AZORult stealer. The actor claimed to be female in the xaker.name forum, but no information is available to support this claim. Our sensitive and reliable source who has direct access to **mmilolika**, reported the actor possessed email address and password combination lists stolen from various adult, dating, financial, health care and sports nutrition-related entities, including:

- clpsct.org — a website of the Local Health Promotion Center in Charleroi-Thuin, Belgium.
- ecas-hearthrhythm.org — a website of the European Cardiac Arrhythmia Society (ECAS) in Marseille, France.
- eco-sapiens.com — an online shop of organic, natural, and ecological products in Marseille, France.
- essentiellelements.com.hk — a website of the pharmaceutical and cosmetic product producer Essential Elements based in Hong Kong.
- healthlink.hk — a health care-related portal service based in Hong Kong.
- huisarts.be — a website of a nonprofit organization in Huisarts, Belgium.
- hvpros.com — a website of the surgery center specialists Healthcare Venture Professionals LLC in the U.S.

Azorult IOCs



Tracking Dumps to Malware

58563_US_172.58.153.78_18-02-19
 58566_BR_187.115.49.167_18-02-19
 58569_GH_41.189.181.186_18-02-19
 58571_FR_62.34.30.124_18-02-19
 58573_US_173.239.199.113_18-02-19

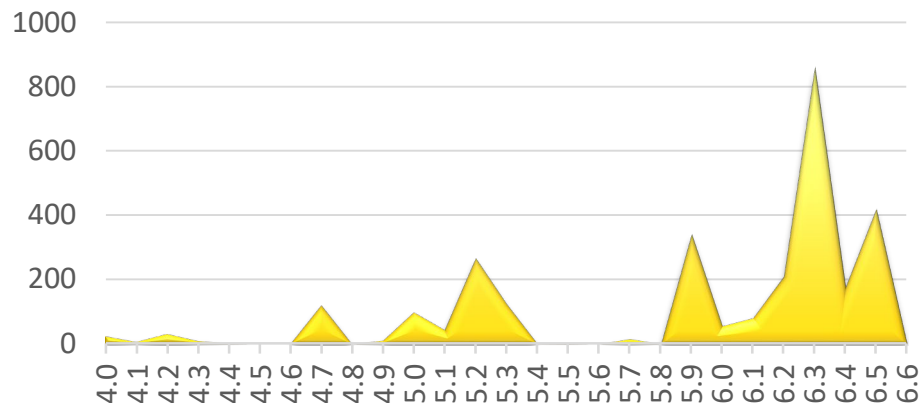
Log #

Date of Infection

Victim IP

IP Based Geo-Location

VIDAR Datasets - 2019



```

1 Version: 6.6
2
3 Date: Mon Feb 25 19:48:07 2019
4 MachineID: 5c3eee87-f262-4c8b-a787-1311464cf7d0
5 GUID: {f2dabe0a-aab5-11e8-b900-806e6f6e6963}
6
7 Path: C:\Users\herma\AppData\Roaming\terra.exe
8 Work Dir: C:\ProgramData\CP8Z9ZN3KMUJ03RJRFJ2
9
10 Windows: Windows 10 Pro [x64]
11 Computer Name: HERMAN
12 User Name: herman
13 Display Resolution: 1920x1080
14 Display Language: nl-BE
15 Keyboard Languages: Nederlands (België) / Nederlands (Nederland)
16 Local Time: 25/2/2019 19:48:7
  
```

Autofill
 CC
 Cookies
 Downloads
 History
 Telegram
 cookie_list.txt
 information.txt
 outlook.txt
 passwords.txt
 screenshot.jpg
 screenshot.jpg
 passwords.txt
 outlook.txt

File names:

- cookie_list.txt
 - information.txt
 - outlook.txt
 - passwords.txt
 - screenshot.jpeg

Disruption via Credential Harvesting tool/actor tracking

- Tracking the actors behind credential harvesting tools allows you to disrupt this part of the ecosystem by:
 - Understanding the tools and updates to the tools to invoke preventative measures such as:
 - Delivery methods of the tool (loaders, BPH etc)
 - IOCs related to the tool
 - How token interception works allows reworking of the 2FA implementation
 - Obtain logs and dumps from these tools:
 - Early identification of victim accounts for resets etc
 - Identification of affected applications

RSAConference2019 **Asia Pacific & Japan**

Account Checking Tools

The Core Tech

Account Checkers In The Underground

INFO REPORT

C2

Possible Russian actor Badabing (aka Almanah, Bor88, borisik, Borisik, Bory, Bumsms, MAXsms, milord) offers account-checking tool for uber.com

02 MAY 2019 13:03:06 UTC

INFO REPORT

C3

Possible Moroccan actor DsWeb19778 (aka Thewhat, nabil33, Nabil Saber) shares Python-based Apple account checker

01 MAY 2019 12:51:45 UTC

INFO REPORT

B3

Russian actor Shadder (aka RDP4you, GODLIKEx, greedsgood, Анатолий) seeks brute-forcing tools, checking services targeting US-based banks

30 APR 2019 03:42:40 UTC

INFO REPORT

C2

Possible Ukrainian actor goodnik7 (aka Goodnik77, Bond009) promotes superman-shop.info web shop of stolen accounts

26 APR 2019 13:05:40 UTC

INFO REPORT

B4

Possible Russian actor reiq (aka eskort, McRapist, MOLESTO, rnm) sells source code for brute-force project targeting BB&T, Capital One, Charles Schwab, Comerica, Discover, Fifth Third Bank, Hanmi Bank, KeyBank, OneAZ Credit Union, Regions Bank, Southwest Missouri Bank, SunTrust Bank, TD Bank, USAA, Walmart

25 APR 2019 12:00:12 UTC

INFO REPORT

B3

Actor TopFuel sells about 100,000 Reddit accounts

24 APR 2019 01:27:07 UTC

INFO REPORT

C1

Maldivian actor ZIZ (aka 717, bobby6991, BOBBY, kickace7, nazween, Nazween KickAce, Nazween Mohamed) offers Hilton honor rewards points, suggests gift card monetization at Amazon; Possible real identity revealed

22 APR 2019 13:41:57 UTC

INFO REPORT

B2

Actor SHERIFF sells information about unspecified US-based online payment platform to leverage for banking fraud

09 APR 2019 12:41:46 UTC

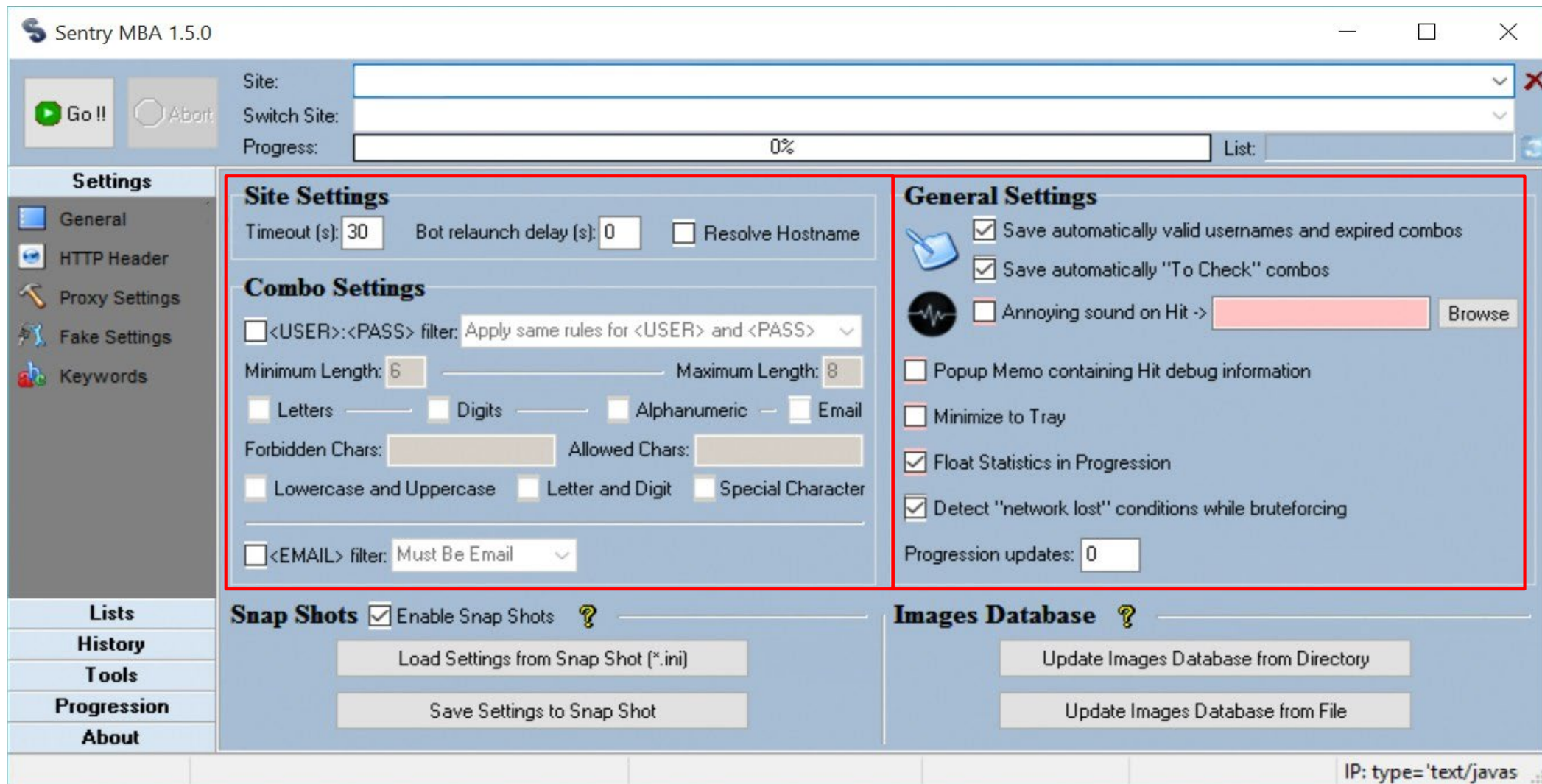


Sentry MBA History

- Developed around 2007
- Called “Sentry”
- 2011 - Source code released
- Development taken over by Astaris



Sentry MBA Functionality



OpenBullet Account Checker/Brute Forcer

The actor **info_hacker** has been prominently promoting open bullet. OpenBullet evolved from the popular brute forcer Black Bullet

- Chatter on the underground indicates this tool may be the next Sentry MBA
- Looking at the similarities of evolution it is possible; Both are open sourced, very easy to load/use, and have many users offering configs for free
- Configs are .loli format and are sought out heavily

“Bigger Products”

Private keeper:

- Released in 2014 by the actor deival909 likely from Lviv Ukraine
- Features include proxy (list) support, attack timing configurations and defeating of CAPTCHA using OCR

uAdmin:

- The actor kaktys1010 sells uAdmin for \$500 and began in February of 2017
- Base features include a phishing generator, victim tracker, and token interception.
- Additional framework plugins include a text manager, money mule manager, VNC capability, event logging, and log parsing

uAdmin

Robot AZ Drop manager Interac Logs II PL-Iban Token II Hi! admin

Sepa Swift **Uk internal**

+ New drop Edit drop Disable Enable Remove

10

Status	System Info	Names	Bic/Sort code	Account number	Reference	Minimum	Maximum	Comments	Tools
<input checked="" type="checkbox"/> Active		jay maj	779119	83337168	ref111	\$1.00	\$2,000.00		

Showing 1 to 1 of 1 entries

Previous 1 Next

Home / Token panel / Operation Panel for **rs.token**

Visitor Waiting

Static information & Settings

Browser & Access Comment Jabber Settings **Operations Settings**

User Agent
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.162 Safari/537.36
IP: 127.0.0.1

User: 5453453
Pass: 5345345

Operations

Redirect ☐ Off Block ☐ Off

Dynamic

2018-03-20 21:47:39 - Logins saved
2018-03-20 21:47:33 - User on Login page
2018-03-20 21:47:33 - New visitor registered

Clear logs

Static information & Settings

Browser & Access Comment Jabber Settings **Operations Settings**

User Agent
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.119 Safari/537.36
IP: 127.0.0.1

Logins

Must be used if login are incorrect and you need to relogin

Confirm Identity Barkdays

Ask to confirm identity

This must be done in case user preferred to login with main word. You will receive back the last 4 of the card + 8 digits token form reader.

Tokens Barkdays

Reference: xxxxxxxxxx
Amount: 0.00

Ask token

Some extra information

Redirect ☐ Off Block ☐ Off

Dynamic

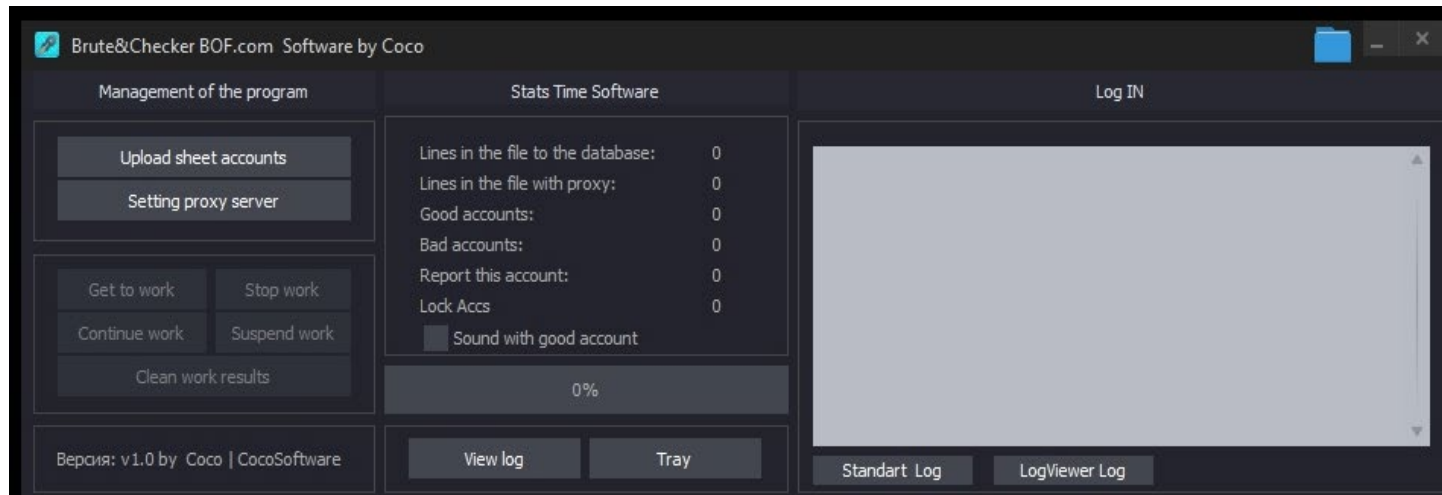
2017-09-14 09:20:59 - User currently on the Token page
2017-09-14 09:20:59 - Logins saved
2017-09-14 09:20:22 - User currently on the login page Step #2
2017-09-14 09:20:21 - Logins saved
2017-09-14 09:16:44 - New visitor registered

Clear logs



deival909's partners (for PrivateKeeper)

- Developers of tools for specific targets:
 - Ukrainian actor Coco (possibly lives in Ivano-Frankivsk) – targets US banks and e-commerce companies



Disruption via Account Checking tool/actor tracking

- Get latest copy of the tool to understand defaults and provide critical input into the security stack for adjustment:
 - Default user agent strings
 - Understand captcha solving limitations
 - Understand brute force avoidance techniques
 - Anti-gateway modules (cyclic parsing)
- Understand “business” partners and related tool for TTP insights

RSA®Conference2019 **Asia Pacific & Japan**

Configurations













Targeting



Configurations

- All of these tools take a configuration
- These configurations are part of the ecosystem as they are generally sold by different actors than the tool
- Even frameworks like PrivateKeeper can take separate configs
- These configs are usually organization specific so finding yours early is key

Sentry MBA

 [WTB] Starbucks accounts [1 2] by Armada	15 Replies	1,034 Views	 08-25-2018, 05:00 PM by Dontfeedgizmo
 [WTB] WALMART CONFIG by Jamie	8 Replies	991 Views	 07-02-2018, 10:24 AM by Yuki
 [WTB] KOHLS CONFIG PAPA CONFIG DOMINOES CONFIG PAPAJOHNS CONFIG SENTRY MBA by JoeFlacko	3 Replies	688 Views	 08-21-2018, 01:10 PM by Abdullah346
 Sling Tv / Directv Now Config (Sentry MBA) by Cubstick	2 Replies	721 Views	 08-12-2018, 08:14 PM by lover2006
 configuration gmail.com sentry MBA by info_hacker	7 Replies	909 Views	 10-27-2018, 05:04 PM by kidpk
 Amazon Config by Adesa	6 Replies	531 Views	 01-12-2018, 04:16 PM by mcnez1

OpenBullet

28 MAR 2019

TODAY

on forums

06:46:40

XD

06:46:47

Quick

QU

it have been on bhf ages

06:46:47

just don't know russian kekera

06:46:58

Rick

RI

<https://cdn.discordapp.com/attachments/570038130221121557/570151133725589506/>

.lol openbullet config How to get the Credit Card Number from a Account: Go to Statements & Activity click "Billing Statements & Documents" Then click "Quicken" Download the most recent file/one the file should be name ofx qfx left click it and open with notepad++ then search / find for without the <> Then right next to ACCTID you have the cc number <http://prntscr.com/nhwwpb> How to get Billing Address Go to Statements & Activity click "Billing Statements & Documents" Download a Billing Statement For a recent month. On page one near to the end. The billing is right there in the open. <http://prntscr.com/nhww6f> How to get Phone Number And EXP Date: For Phone Number and EXP Date use any. This legit sounds crazy but it works ! Phone Number - Any USA Number. I do either a random or dominos [Image: tongue.png] CVV - I mostly do 06/21, but you can use any.

11:34:12

Rick

RI

Freee method!!!!

11:34:16

FastReward

FA

Okey and what can we do with that @Rick

13:58:59

sentry.mba

[Video] How to load Config on the OpenBullet

info_hacker

Video: [//www.youtube.com/embed/CchgkOeW-pY](https://www.youtube.com/embed/CchgkOeW-pY)

<http://www.aliinfo.cf/2019/04/video-how-...ullet.html> [<http://www.aliinfo.cf/2019/04/video-how-to-load-config-on-openbullet.html>]

13 APR 2019 02:52:00

aowen03443

thank you sir "info_hacker"..

13 APR 2019 06:04:00



OpenBullet Config Example (.loli format)

```
[[SETTINGS]
{
  "Name": "██████",
  "SuggestedBots": 1,
  "LastModified": "2019-04-22T13:36:30.1326612-05:00",
  "AdditionalInfo": "",
  "Author": "The Killer Rkil",
  "Version": "1.0.0",
  "IgnoreResponseErrors": false,
  "NeedsProxies": true,
  "OnlySocks": false,
  "OnlySsl": false,
  "MaxProxyUses": 0,
  "AllowedWordlist1": "UserPass",
  "AllowedWordlist2": "",
  "DataRules": [],
  "CustomInputs": [],
  "ForceHeadless": false,
  "AlwaysOpen": false,
  "AlwaysQuit": false,
  "DisableNotifications": false,
  "CustomUserAgent": "",
  "RandomUA": false,
  "CustomCMDArgs": ""
}

[SCRIPT]
FUNCTION RandomNum 10000 90000 -> VAR "num"
FUNCTION RandomNum 10 90 -> VAR "num2"
FUNCTION RandomNum 100 900 -> VAR "num3"
```


OpenBullet Config Example (cont'd)

```
CONTENTTYPE "application/x-www-form-urlencoded; charset=utf-8"
HEADER "User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like
Gecko"
HEADER "Pragma: no-cache"
HEADER "Accept: */*"
HEADER ": scheme: https"
HEADER "accept: */*"
HEADER "accept-encoding: gzip, deflate, br"
HEADER "accept-language: en-US,en;q=0.9"
HEADER "content-length: 1566"
HEADER "dnt: 1"
HEADER "origin: https://global.██████████.com"
HEADER "referer: https://global.██████████.com/login/en-GB?inav=gb_utility_login"
HEADER "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/73.0.3683.103 Safari/537.36"
KEYCHECK
KEYCHAIN Failure OR
  KEY "{\"statusCode\":1,\"errorCode\":\"LGON001\", \"\"}
KEYCHAIN Success OR
  KEY "{\"statusCode\":0, \"\"}
```

Disruption via Configuration Monitoring

- Understand the specific app endpoint(s) being targeted
 - Make adjustments to the application
 - Wrap additional protection on legacy app endpoints
- Updates to the default settings (beyond the tools section)
 - New techniques
 - Specialty settings (rate limiting, obfuscation etc)
 - Captcha solving/captcha upgrades

RSAConference2019 **Asia Pacific & Japan**

Bulletproof Hosting and Proxy Nets

Where to launch attacks from

Malicious Infrastructure (BPH and Proxy Nets)

All of these tools operate through malicious infrastructure such as bulletproof hosting or proxy networks, including both the account checking tool and the credential harvesting. (rate limiting by IP, endpoint access tracking by IP is defeated via this method)

B2 USUALLY RELIABLE
PROBABLY TRUE

CC
CYBER CRIME

Russian actor, bulletproof hoster yalishanda (aka downlow, stas_vl) hosts new phishing campaign involving ABN AMRO, Banca Monte dei Paschi di Siena, Banca Popolare dell'Emilia Romagna, Commonwealth Bank, POSB Bank, Vodafone; Current proxy-net size sits at 90 IP addresses

PUBLISHED: 14 JAN 2019 13:51:57 UTC

IaaS BPH and Proxy Nets

By tracking the actors that provide these malicious infrastructure services we can obtain almost real time insight into the infrastructure being provided. We can see some of the domains targeting Asia Pacific are hosted in China but rented out by a Russian adversary.

49.51.136.239,CHN,TencentCloud
 49.51.137.76,CHN,TencentCloud
 49.51.146.62,CHN,TencentCloud
 49.51.170.17,CHN,TencentCloud
 49.51.170.102,CHN,TencentCloud
 49.51.171.96,CHN,TencentCloud
 49.51.172.220,CHN,TencentCloud
 49.51.173.30,CHN,TencentCloud
 49.51.173.192,CHN,TencentCloud
 49.51.173.225,CHN,TencentCloud
 79.143.28.108,RUS,Selectel Ltd.
 89.108.65.190,RUS,Reg.Ru Network Operations
 185.176.26.66,RUS,Cloud-services
 185.229.224.120,ISR,CloudWebManage
 185.247.117.183,NDL,EU-AMS-VPSSERVERCOM

In the last 72 hours, no hosts were added to the actor's fast-flux infrastructure.

— 49.51.171.96
 alosbwgs.com
 dbs-security.info
 deligvsiogsd.com
 digefinsed.com
 epinnora.com
 fiosbewos.com
 ing-verification.com
 ingbank-verify.com
 ingbankieren-online.com
 ingbankieren.org
 jestowendo.com
 mackdonatap.com
 mail.alosbwgs.com
 mail.dbs-security.info
 mail.deligvsiogsd.com
 mail.digefinsed.com
 mail.epinnora.com
 mail.fiosbewos.com
 mail.jestowendo.com
 mail.mackdonatap.com
 mail.personal-confirmation.com
 mail.personal-confirmation.info
 mail.personal-verification.info
 mail.posb-dbs-online.net
 *mail.posb-dbs-sg.org
 mail.posb-dbs-support.com
 mail.rbc-login.com
 mail.serverconnectionfailed.com
 mail.verification-online.net
 mail.westpac-verify.com
 mobile.rovalbank.com.rbc-login.com

Disruption via BPH Actor Tracking

- By having access to real time infrastructure updates and information it is possible to:
 - Block initial infection vector
 - Block second stage callback
 - Block exfiltration
- Information about the actor provides strategic insight on which actors are working with which other actors in the ecosystem to provide focus

RSA[®]Conference2019 **Asia Pacific & Japan**

Wrap Up and Review

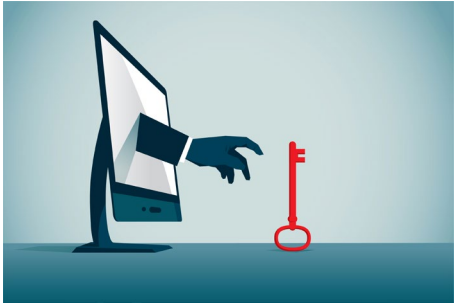


Whats Hot?

Investment in this ecosystem continues to grow as we can see just this year:

- Actor foxovsky has closed support for the stealer Arkei but retains a private version (Vidar) and has provided and open access to the bot builder.
- Actor oFFENDERS has offered up a new stealer with a full admin panel. (enabling ATO as a service/affiliate program)
- Actor Satoshi, behind much of the credential monetization apprehended in Belarus (bruteforce[.]online, fraud[.]im, rpg-club[.]com)
- STORM account checker remains immensely popular

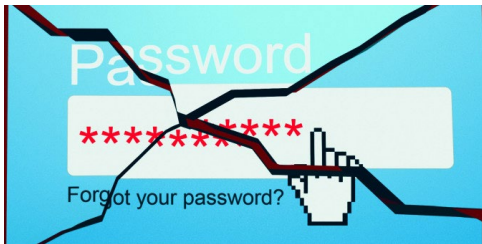
Review of the Ecosystem and Disruption Opportunity



Credential Harvesting: disruption by tracking the actors to understand techniques and get ahead of credential lists.



Configurations for account checkers: disruption by tracking the actors to obtain configs early and make application adjustments.



Account checking tools: disruption by tracking the actors to obtain copies of the tools for techniques, defaults and understand business partners for additional components and targets.



Malicious Infrastructure: disruption by tracking the actors to obtain infrastructure updates for blocking and prevention.



RSA[®]Conference2019 **Asia Pacific & Japan**

Questions and Thank You!