Identitätsdiebstahl in 5 Schritten erklärt

Stefan Mardak
Enterprise Security Architect. Principal

Akamai

We are safe! We got a firewall …
Please think again!

Akamai

The Account Takeover Kill Chain

Credential Acquisition | Weaponization | Delivery | Exploitation | Action

Akamai

The Account Takeover Kill Chain

1. Hack, Phish or Buy

Breach or skim site to steal credentials

Phish website users

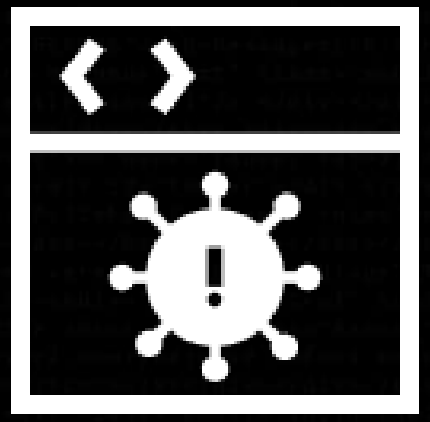
Purchase list of stolen credentials on dark web

Credential Acquisition | **Weaponization** | **Delivery** | **Exploitation** | **Action**

Akamai

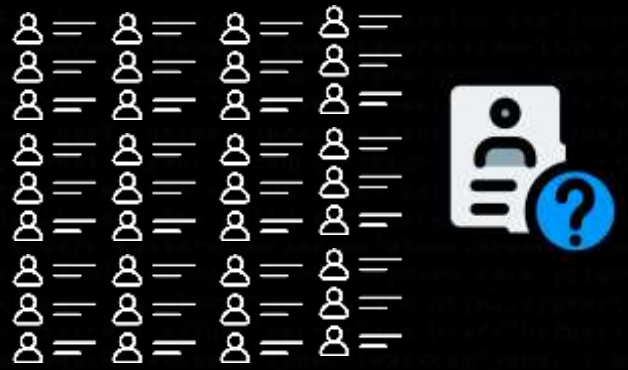
3 Ways to get user/pass Credentials

Hack



Skim or Phish

Buy



· This slide has been designed using resources from Flaticon.com

The Account Takeover Kill Chain

2. Buy or Build Botnet

Breach or skim site to steal credentials

Phish website users

Purchase list of stolen credentials on dark web

Leverage a botnet to automate validation

Credential Acquisition | **Weaponization** | **Delivery** | **Exploitation** | **Action**

Akamai

The Account Takeover Kill Chain

Breach or skim site to steal credentials

Phish website users

Purchase list of stolen credentials on dark web

Leverage a botnet to automate validation

3. Verify

Validate credentials against target website

Credential Acquisition | **Weaponization** | **Delivery** | **Exploitation** | **Action**

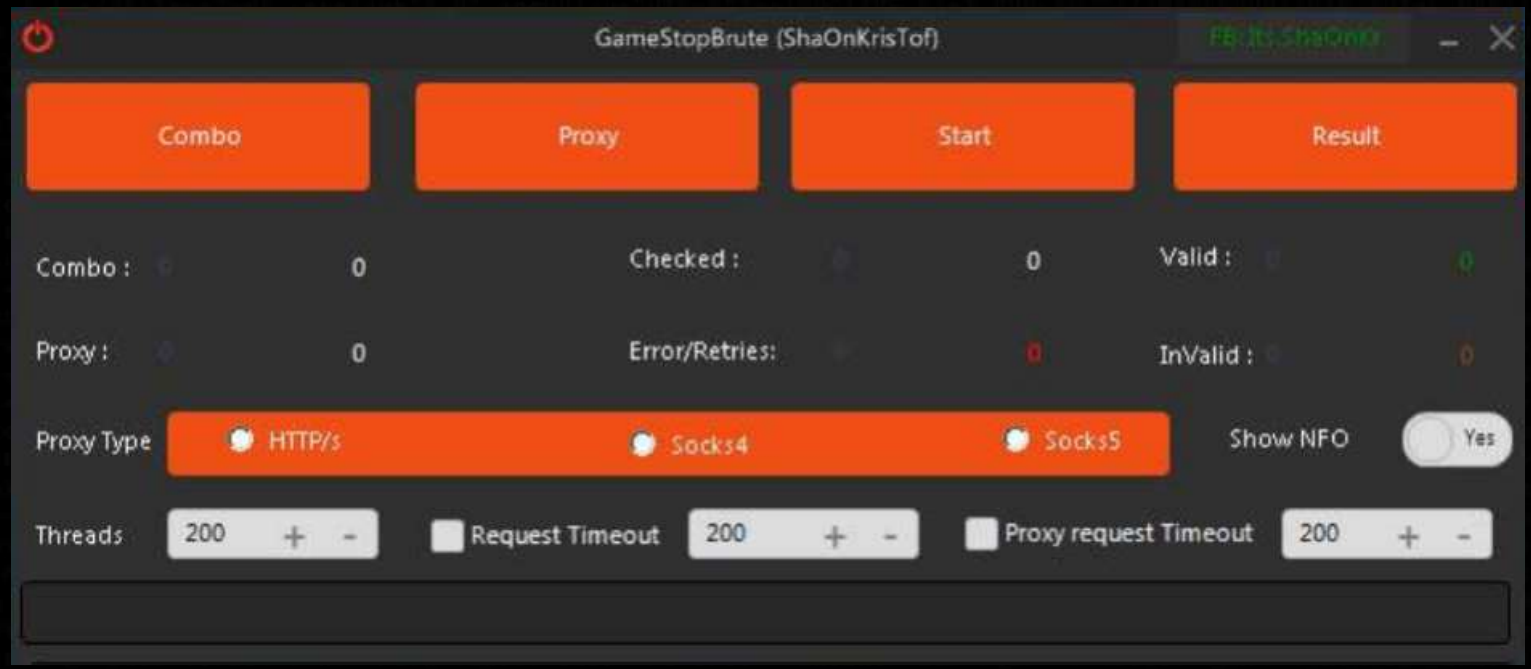
Akamai

It’s Easy For Attackers To Execute Credential Stuffing Attempts

GameStop

POWER TO THE PLAYERS

GameStopBrute.exe



Akamai

The Account Takeover Kill Chain

Breach or skim site to steal credentials

Phish website users

Purchase list of stolen credentials on dark web

Credential Acquisition

Leverage a botnet to automate validation

Weaponization

Validate credentials against target website

Delivery

4. Identity Theft

Use compromised account credentials to login

Exploitation

Action

Akamai

The Account Takeover Kill Chain

5. Account Takeover

Breach or skim site to steal credentials

Phish website users

Purchase list of stolen credentials on dark web

Credential Acquisition

Leverage a botnet to automate validation

Weaponization

Validate credentials against target website

Delivery

Use compromised account credentials to login

Exploitation

Perform fraudulent actions using compromised account

Action

Akamai

Is That My Customer? Or An Imposter?

```
Akamai-User-Risk:
uuid=ff9c3d04-4e5c-4412-bbe0-9cde27842278;
requestid=a79efad;
status=2;
score=50;
risk=asnum:2856/L|geo:GB/M|os:Mac OS X 10/L|browser:Chrome 89/L|device_id:9d3a93a9b6690df
ba78d74b201451e347fe96cb3/L;
allow=0;
action=none;
```

COPY

Akamai

The Account Takeover Kill Chain - Stopped by Akamai

1. Hack, Phish or Skim

2. Buy or Build Botnet
You can't stop that

3. Verify

4. Identity Theft
5. Account Takeover

Akamai

APP & API Protector
Protect your web application estate.

Page Integrity Manager
Audience Hijacking
Detect and prevent in-browser threats and PII-Data Skimming

Enterprise Thread Protector
Enterprise Application Access
Guardicore Micro Segmentation
Protect your Enterprise from Phishing-, Command&Control-, Ransomware-Attacks

Bot Manager
Detect & manage bot traffic
Prevent against Credential Stuffing

Account Protector
Recognize authentic user interaction.
Dynamically add & remove user friction based on trust & risk factors
Prevent against Account Takeover

Akamai MFAr

Akamai


Akamai