Account Takeovers Targeting the United States

Kacey Clark

Commercial in confidence
kaceyclark@digitalshadows:~$ whoami

- Threat Research Team Lead
- ShadowTalk Host (US)
- Recovering US Gov IT Recruiter
- Avid Outdoorswoman
- GSD Mom
Agenda

- Defining Account Takeover
- The Market For Exposed Credentials
- ATO Attacker’s Toolkit
- Taking a Proactive Stance
- Resources & Shameless Plug
- Questions
DEFINING ACCOUNT TAKEOVER

The process of gaining access to a victim account, often by compromise or credential re-use
ATO - A Proven Technique

80%

Breaches related to hacking involved brute-force cracking or the use of lost or stolen credentials.
The Market for Exposed Credentials
hi

i have access to domain controller of US health care company
4000 pc and ~50 server
send your price in pm for buy access
escrow welcome

2minutenoodles

Company Info:
Location: US
Market: Logistics
Revenue: $30 million
Employees: 150
Access: Domain Admin

Finance and Employee info gotten from ZoomInfo.
Price: $1000
AVERAGE PRICE OF LISTINGS BASED ON AN ANALYSIS OF DOZENS OF LISTINGS BY THREE SAMPLE VENDORS IN 2020.

- LOCAL GOVERNMENT: $3,217
- TECHNOLOGY: $1,233
- FINANCE AND INSURANCE: $2,667
- OTHER: $1,200
- MANUFACTURING AND ENGINEERING: $1,500
- REAL ESTATE: $750
BREAKDOWN OF FREQUENCY OF DIFFERENT ACCOUNT LISTINGS

PERCENTAGE OF LISTINGS
- 25% BANK/FINANCIAL
- 13% STREAMING
- 12% PROXY/VPN
- 9% CABLE
- 8% EDUCATION
- 7% ADULT
- 7% MUSIC
- 7% FILE SHARING
- 5% SOCIAL MEDIA
- 5% ANTIVIRUS
- 2% VIDEO GAMES
DID SOMEONE SAY
FREE STUFF?
15,000,000,000
Credentials Exposed
TYPES OF PASSWORD HASHES COLLECTED BY DIGITAL SHADOWS, EXCLUDING THOSE STORED IN PLAINTEXT.

- **MD5**: 45.99%
- **SHA1**: 34.91%
- **PBKDF2**: 9.06%
- **BCRYPT**: 3.86%
- **SHA256**: 2.01%
- **PHPBB3**: 1.04%
2 Million Accounting Usernames
AVERAGE CREDENTIALS PER ONE ORGANIZATION PER SECTOR

- **Food & Beverage**: 87,352
- **Technology**: 47,603
- **Education**: 47,972
- **Financial Services**: 25,077
- **Automobiles & Parts**: 17,240
- **Conglomerates**: 21,747
- **Healthcare**: 15,016
- **P&B**: 14,955
- **Oil & Gas**: 13,352
- **Chemicals**: 12,647

*PHARMACEUTICALS & BIOTECHNOLOGY*
ATO ATTACKER’S TOOLKIT
Rent Your Own
PREVALENCE OF DISCUSSIONS RELATED TO THREE FINGERPRINTING SERVICES BY TOTAL REFERENCES

JANUARY 2020-JUNE 2020

- 11.4% UNDERWORLD MARKET
- 23.6% TENEBRIS
- 65% GENESIS
ATO ATTACKER’S TOOLKIT

- Brute-force tools
- Account checkers
- Credential stuffing tools
- SentryMBA
- Rising star: OpenBullet
Mentions of various credential stuffing tools across criminal locations in 2020.

- **OpenBullet**: 1,198
- **SentryMBA**: 799
- **Private Keeper**: 572
- **Vertex**: 433
- **Account Hitman**: 193
- **Snipr**: 156
- **BlackBullet**: 110
Moving to a Proactive Stance
Prioritize Patching

Хакеры эксплуатируют уязвимость в корпоративном VPN

проблема известна под идентификатором CVE-2019-11510, инструменты для ее использования можно свободно ... уязвимостью CVE-2019-11510 успели воспользоваться разные хак...-группы, но за инцидентами, обнаруженными

Source: https://dubik2ugjorycsj.onion/threads/xakery-ehkspluatinvujt-ujazvimost-v-korporativnom-vpn.153522/

Хакеры эксплуатируют уязвимость в корпоративном VPN

проблема известна под идентификатором CVE-2019-11510, инструменты для ее использования можно свободно ... уязвимостью CVE-2019-11510 успели воспользоваться разные хак-группы, но за инцидентами, обнаруженными

Source: https://tenec.biz/index.php/posts/49491

После раскрытия уязвимостей на Black Hat начались атаки на ...


Source: http://verified2ebdpwms.onion/showthread.php?p=1060315#post1060315
ID Early Discussions and Advertisements

Observables
- None
- Email (1)
- Domains (2)

Post content
- Primary post
  - Hi Gary, I am very pleased for the opportunity to build malware for many years and update my skills.
  - Thanos Private Ransomware (February 7, 2019)
  - [Image: https://i.imgur.com/NP46K4N.png]
  - [Image: https://i.imgur.com/9yf9kA4.png]

Observables
- None

Thread content
- Primary post
  - [Image: https://i.imgur.com/3l9Q6K3.png]

Data source:
- Thanos Ransomware Affiliate Program
  - [Image: https://x.x.x.x/threads/34517/post-2071630]
Description
Founded in 1998, Google, Inc. is a multinational corporation that provides Internet-related services and products, including an Internet search engine. Read More

Headquarters: 1600 Amphitheatre Parkway, Mountain View, California, 94043, United States

Phone: (650) 253-0000
Website: www.google.com

Employees: 118,899
Revenue: $161 Billion
Stock Symbol: GOOGL

Update Company | View contact profiles from Google

SIC Code: 67,671 NAICS Code: 335921,5415 Ticker: NASDAQ: GOOGL
Monitor for Leaked Access Keys

truffleHog

Gitrob: Putting the Open Source in OSINT

Gitrob is a tool to help find potentially sensitive files pushed to public repositories on Github. Gitrob will clone repositories belonging to a user or organization down to a configurable depth and iterate through the commit history and flag files that match signatures for potentially sensitive files. The findings will be presented through a web interface for easy browsing and analysis.

GitHub Secret Scanning
Monitor for Potentially Malicious Domains

- Buy domains similar to yours
- Monitor domain registration activity
Resources & Shameless Plug
FROM EXPOSURE TO TAKEOVER
The 15 billion stolen credentials allowing account takeovers

Authors: Digital Shadows Photon Research Team

https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover


ATO Part 3: https://www.digitalshadows.com/blog-and-research/account-taking-over-expanding-on-impact/

Ransomware Trends in Q2: https://www.digitalshadows.com/blog-and-research/ransomware-trends-in-q2-how-threat-intelligence-helps/

Not Another Ransomware Blog: https://www.digitalshadows.com/blog-and-research/not-another-ransomware-blog-initial-access-brokers-and-their-role/

Access Keys Exposed: https://www.digitalshadows.com/blog-and-research/access-keys-exposed-more-than-40-are-for-database-stores/
Questions