digital shadows_

Account Takeovers Targeting the United States

Kacey Clark

Commercial in confidence

16.09.2020

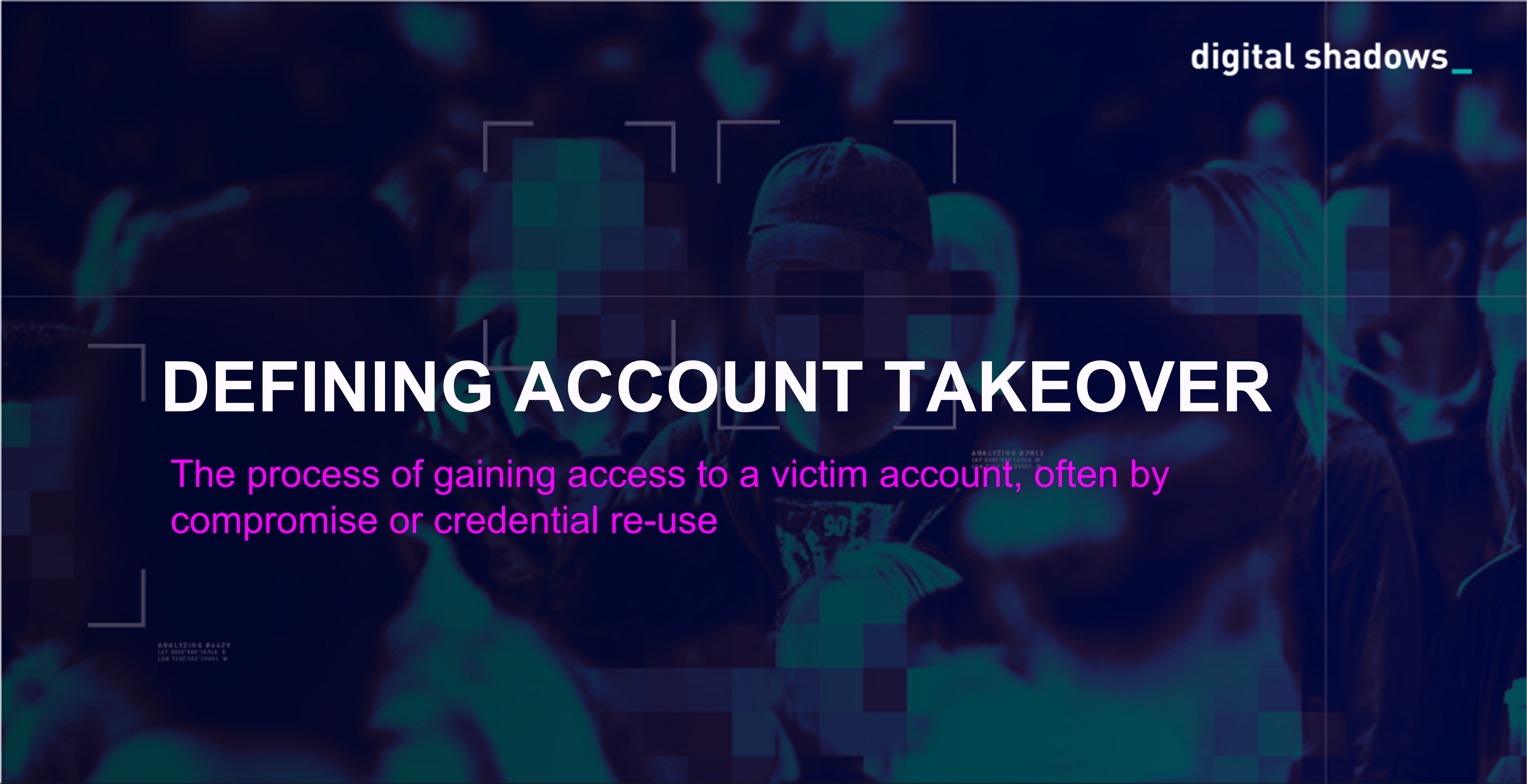
www.digitalshadows.com

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

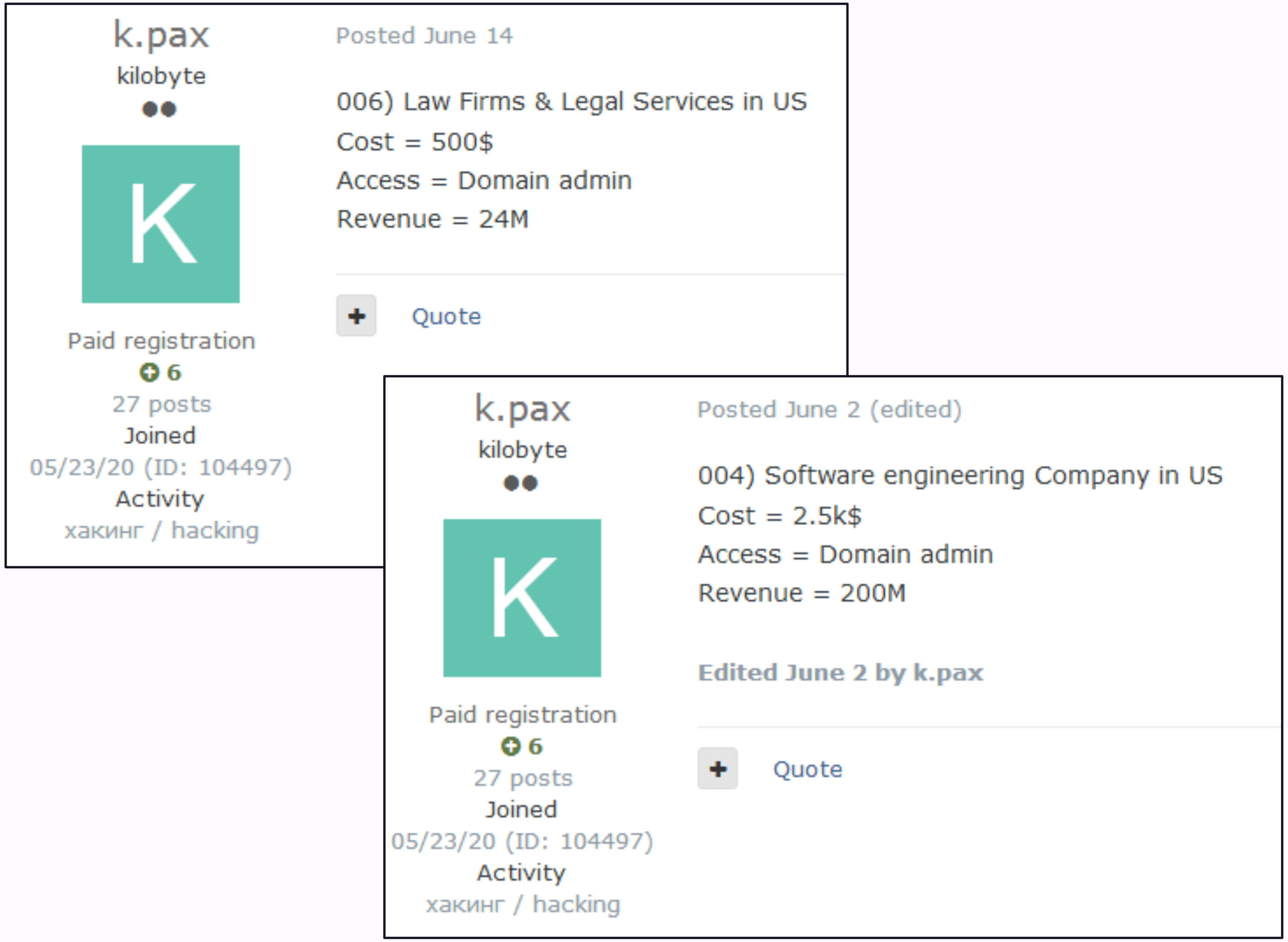
ATO - A Proven Technique

80%

Breaches related to hacking involved brute-force cracking or the use of lost or stolen credentials.

The Market for Exposed Credentials

Accounts For Sale



k.pax
kilobyte
●●

K

Paid registration
⊕ 6
27 posts
Joined
05/23/20 (ID: 104497)
Activity
хакинг / hacking

Posted June 14

006) Law Firms & Legal Services in US
Cost = 500$
Access = Domain admin
Revenue = 24M

+ Quote

k.pax
kilobyte
●●

K

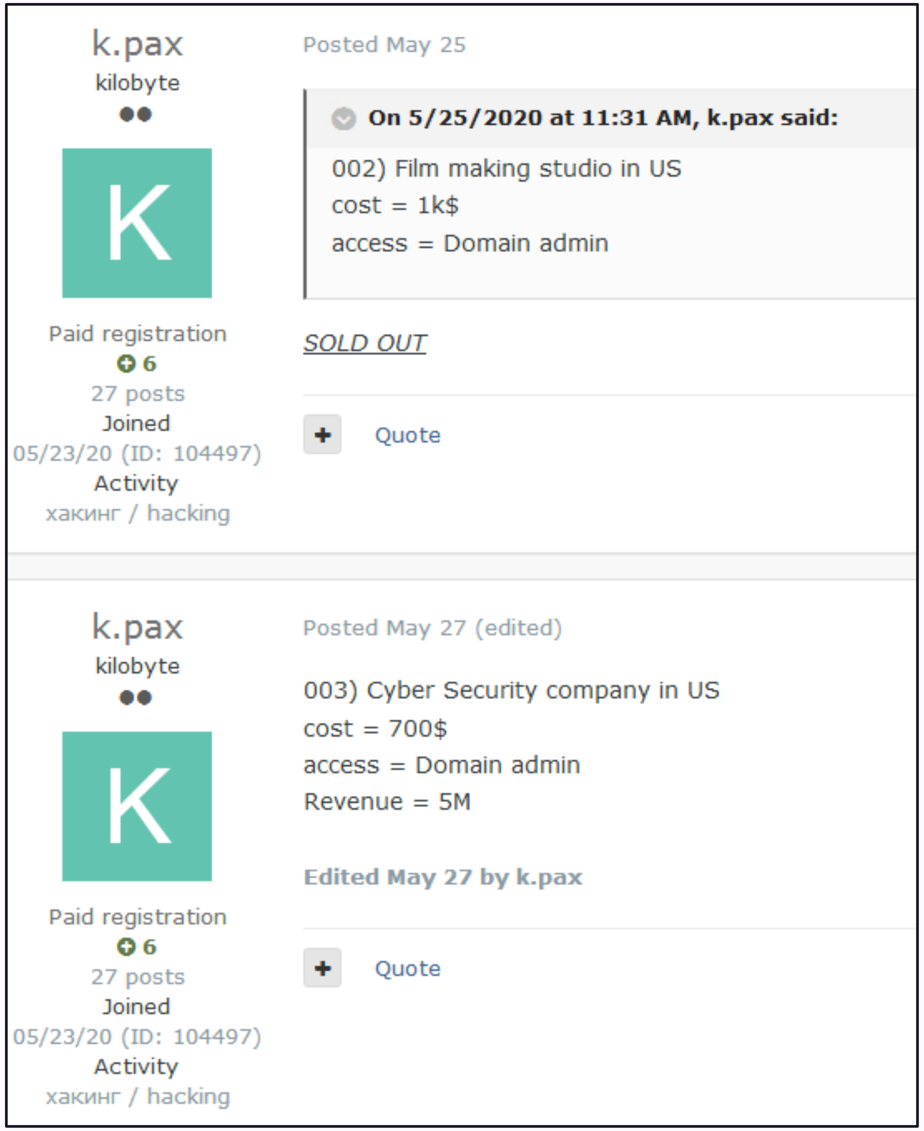
Paid registration
⊕ 6
27 posts
Joined
05/23/20 (ID: 104497)
Activity
хакинг / hacking

Posted June 2 (edited)

004) Software engineering Company in US
Cost = 2.5k$
Access = Domain admin
Revenue = 200M

Edited June 2 by k.pax

+ Quote



k.pax
kilobyte
●●

K

Paid registration
⊕ 6
27 posts
Joined
05/23/20 (ID: 104497)
Activity
хакинг / hacking

Posted May 25

> **On 5/25/2020 at 11:31 AM, k.pax said:**
>
> 002) Film making studio in US
> cost = 1k$
> access = Domain admin

SOLD OUT

+ Quote

k.pax
kilobyte
●●

K

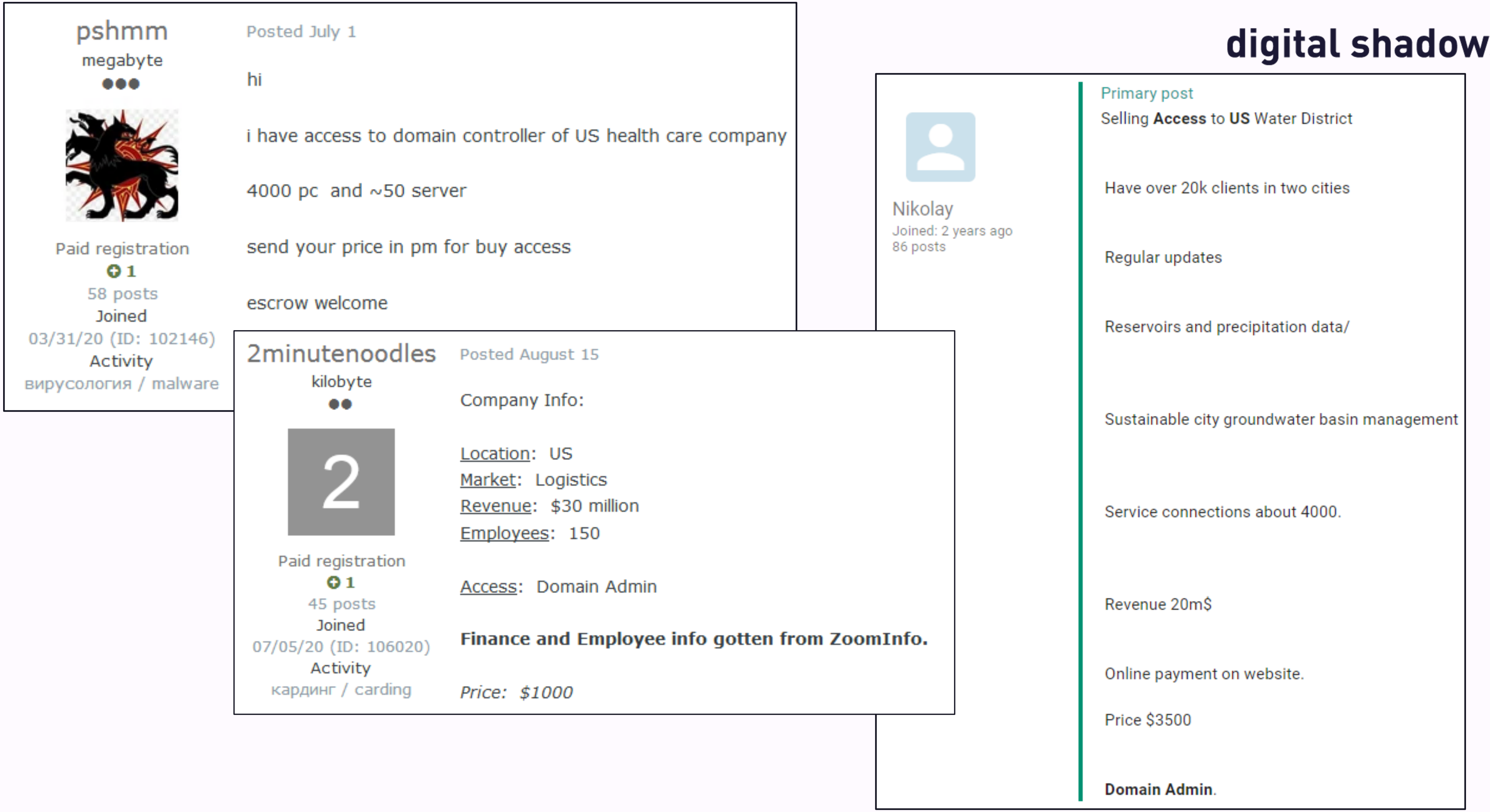
Paid registration
⊕ 6
27 posts
Joined
05/23/20 (ID: 104497)
Activity
хакинг / hacking

Posted May 27 (edited)

003) Cyber Security company in US
cost = 700$
access = Domain admin
Revenue = 5M

Edited May 27 by k.pax

+ Quote



pshmm
megabyte
●●●

Paid registration
⊕ 1
58 posts
Joined
03/31/20 (ID: 102146)
Activity
вирусология / malware

Posted July 1

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
kilobyte
●●

Paid registration
⊕ 1
45 posts
Joined
07/05/20 (ID: 106020)
Activity
кардинг / carding

Posted August 15

Company Info:

Location: US
Market: Logistics
Revenue: $30 million
Employees: 150

Access: Domain Admin

Finance and Employee info gotten from ZoomInfo.

Price: $1000

Nikolay
Joined: 2 years ago
86 posts

Primary post
Selling **Access** to **US** Water District

Have over 20k clients in two cities

Regular updates

Reservoirs and precipitation data/

Sustainable city groundwater basin management

Service connections about 4000.

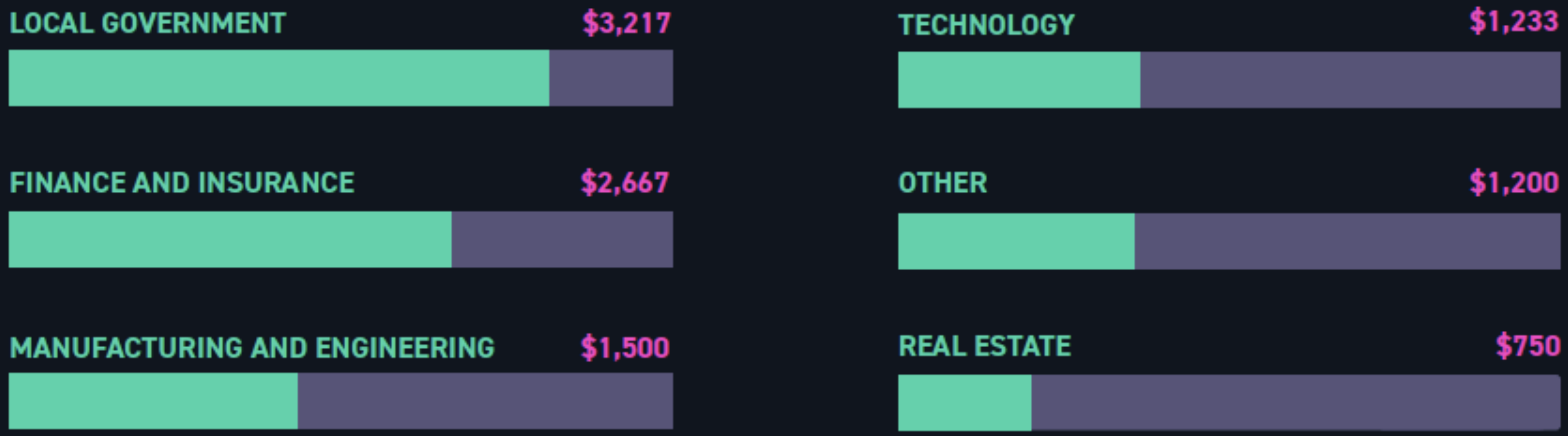
Revenue 20m$

Online payment on website.

Price $3500

Domain Admin.

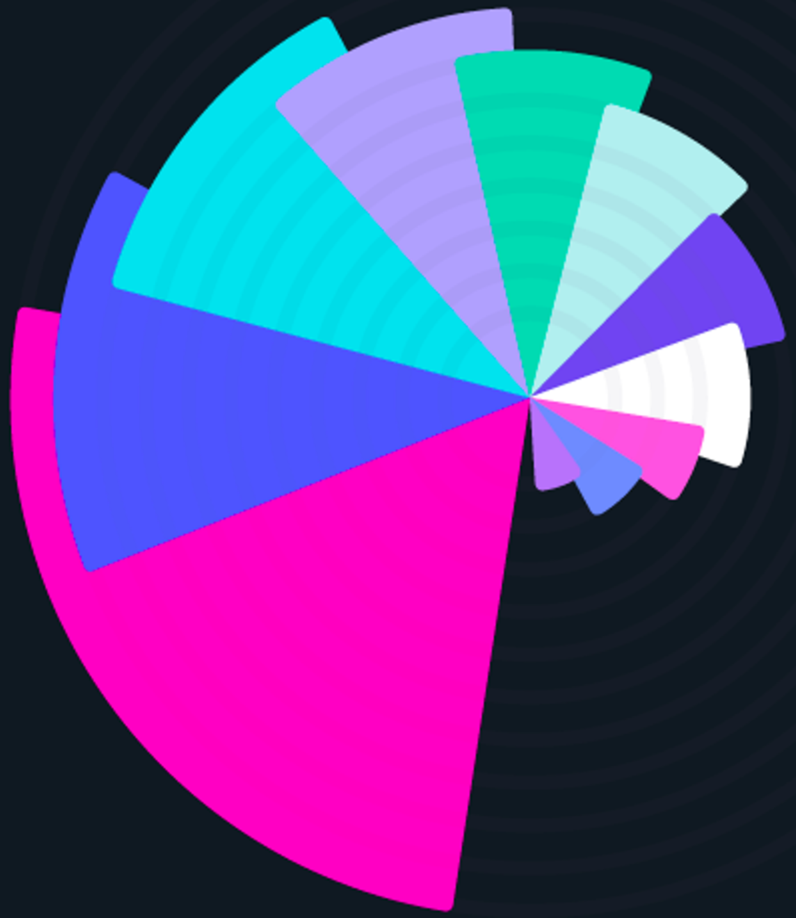
AVERAGE PRICE OF LISTINGS BASED ON AN ANALYSIS OF DOZENS OF LISTINGS BY THREE SAMPLE VENDORS IN 2020.



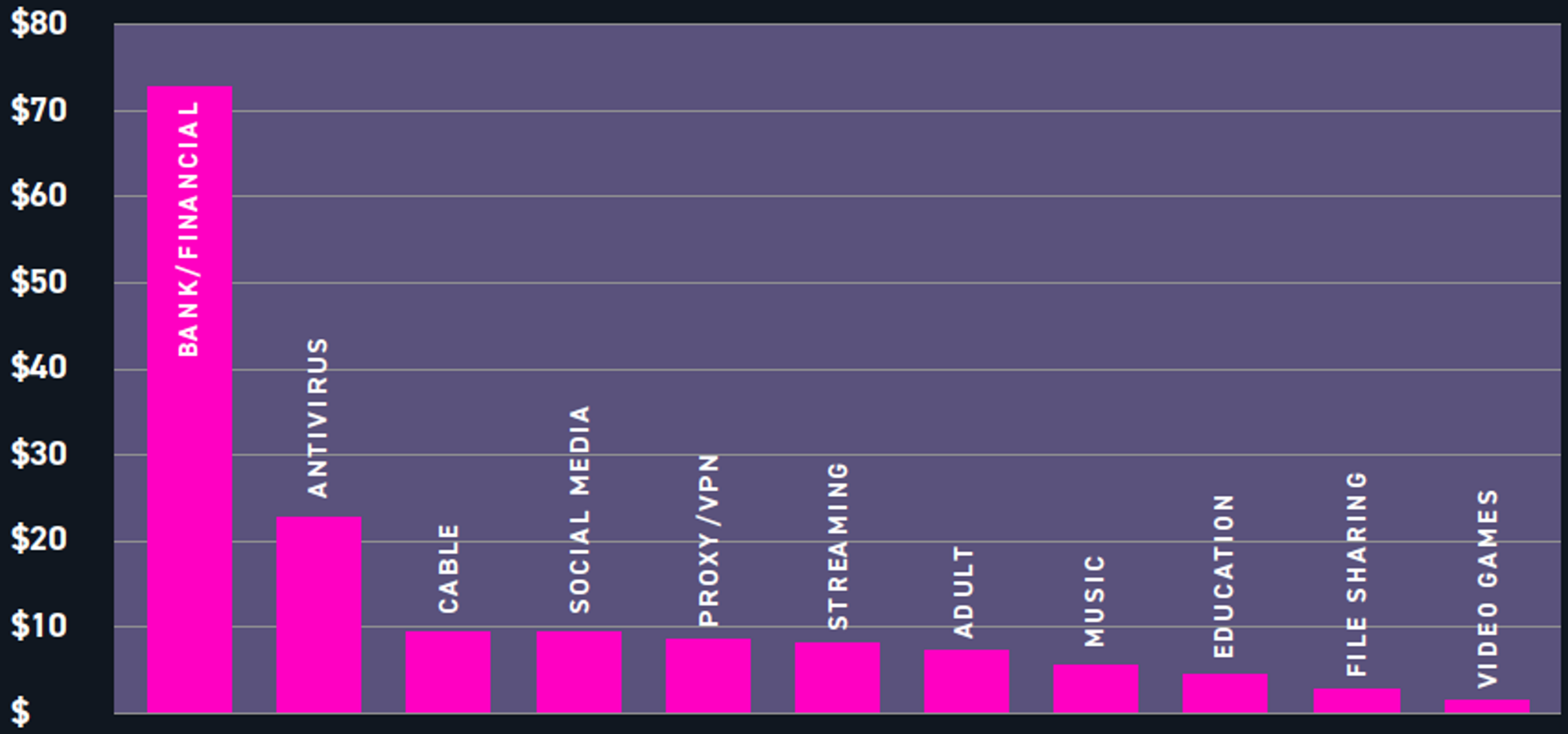
BREAKDOWN OF FREQUENCY OF DIFFERENT ACCOUNT LISTINGS

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



AVERAGE COST OF ONE ACCOUNT FOR DIFFERENT ONLINE SERVICES

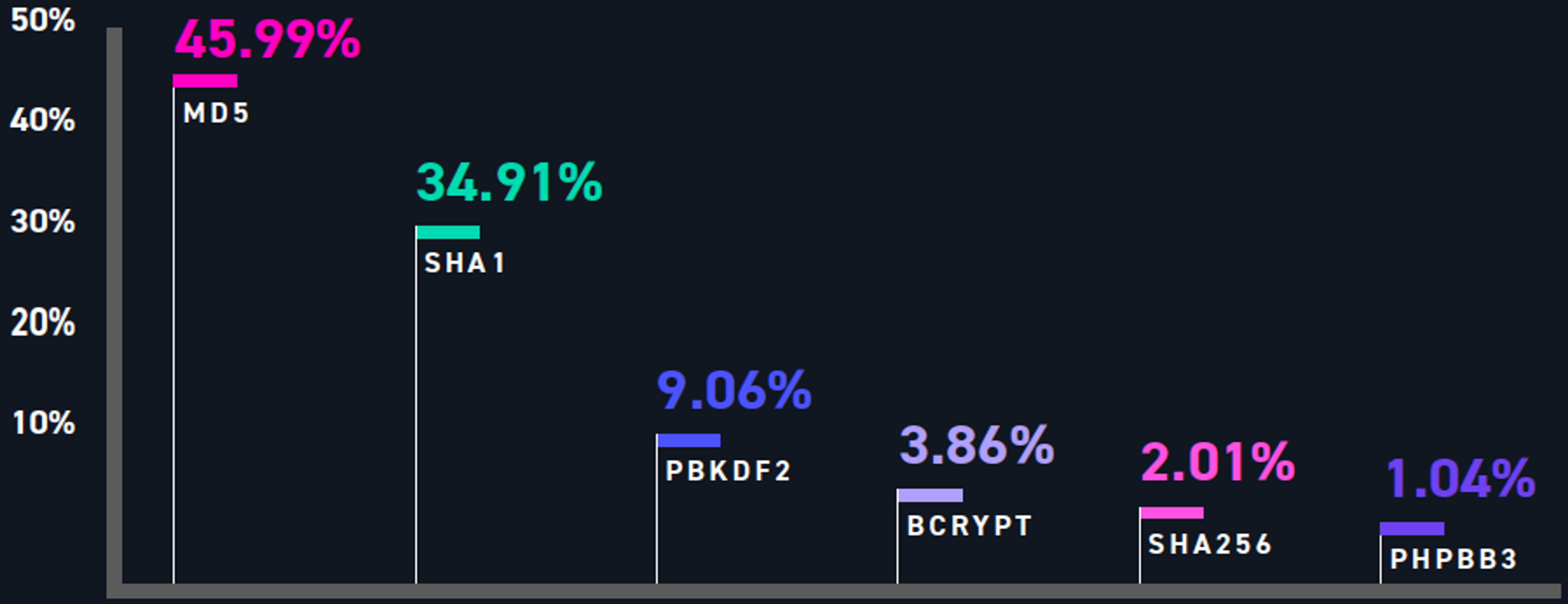


DID SOMEONE SAY
FREE STUFF?
memegenerator.net

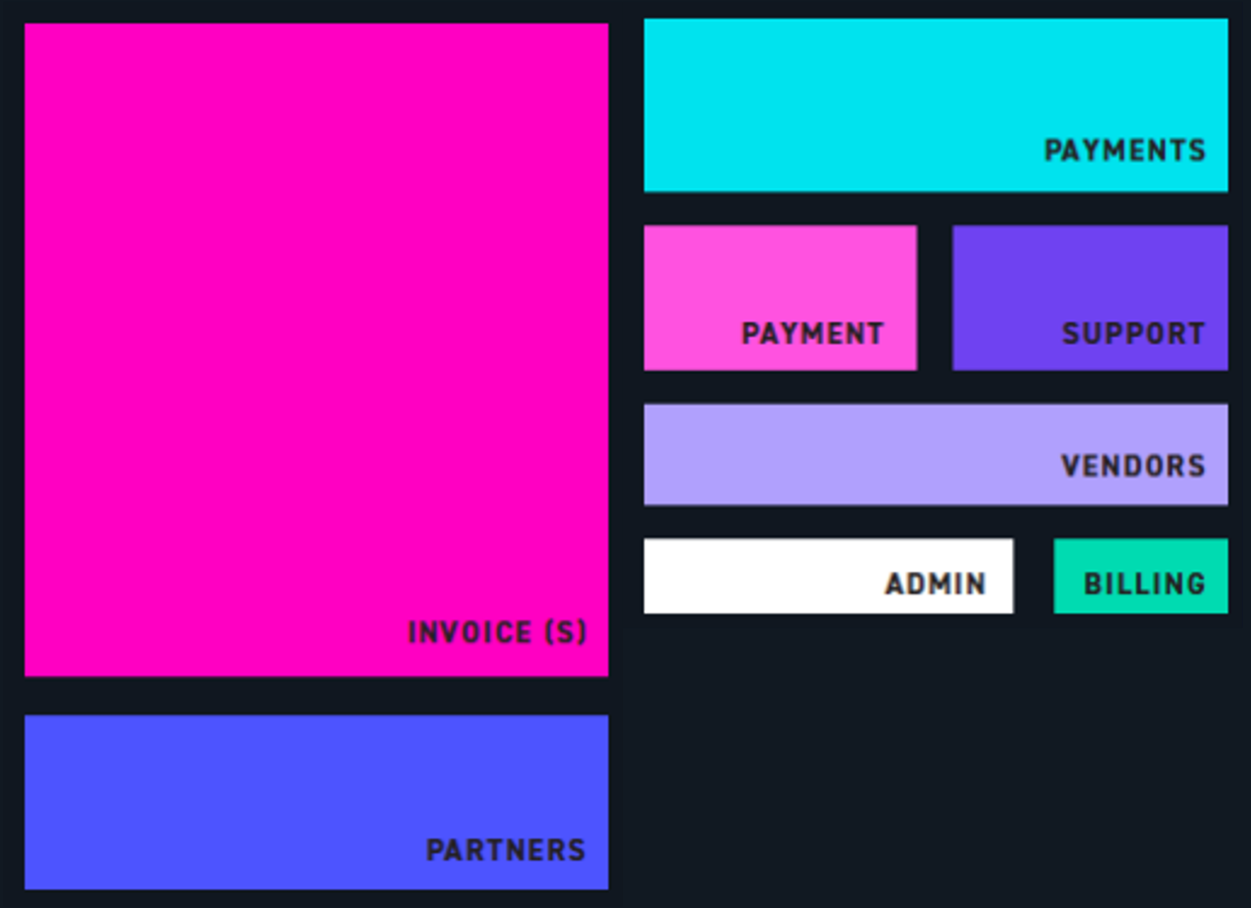
15,000,000,000

Credentials Exposed

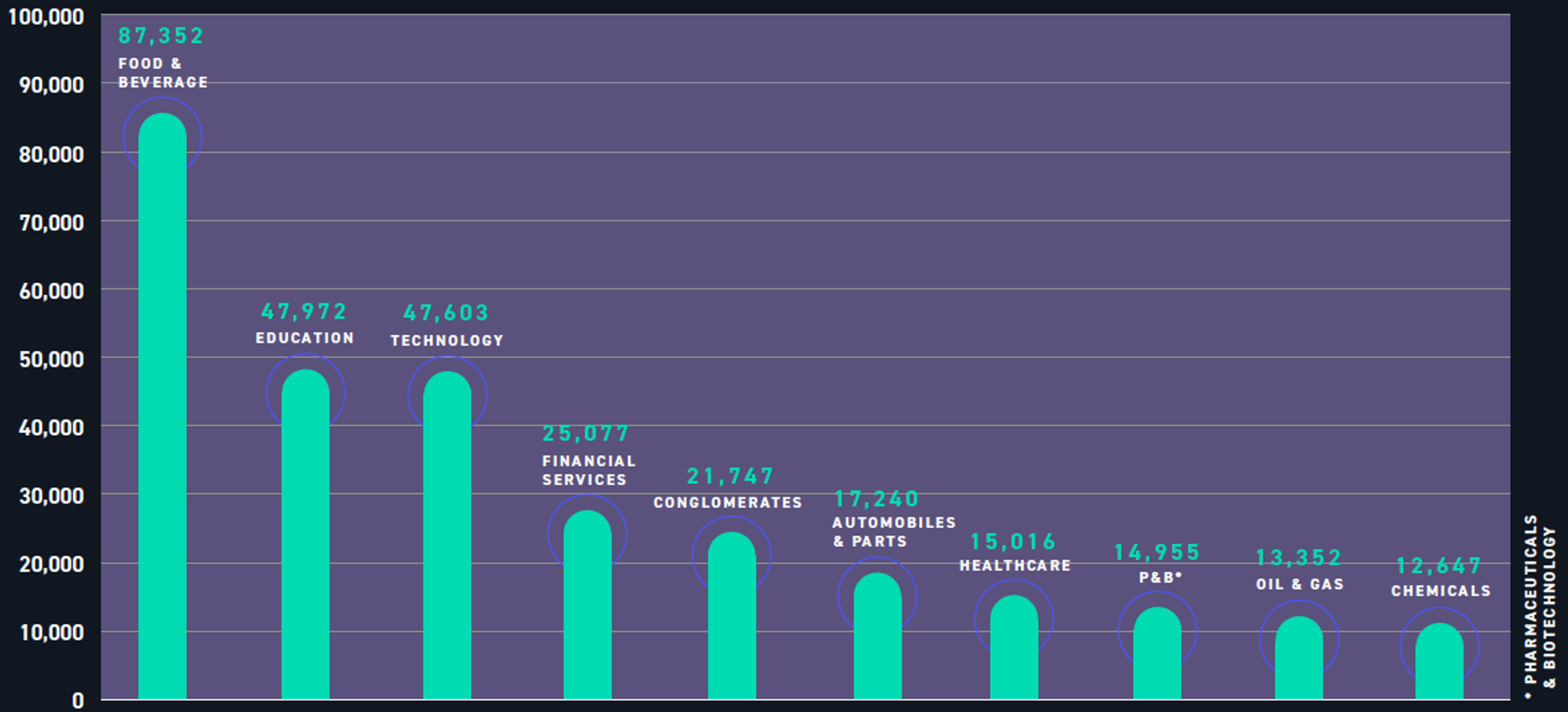
TYPES OF PASSWORD HASHES COLLECTED BY DIGITAL SHADOWS, EXCLUDING THOSE STORED IN PLAINTEXT.



2 Million Accounting Usernames

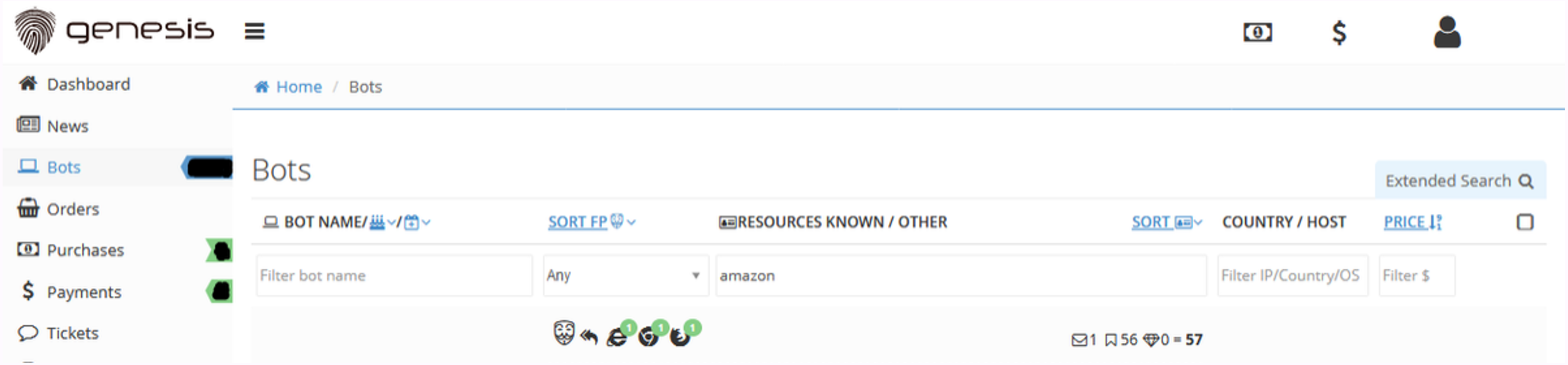


AVERAGE CREDENTIALS PER ONE ORGANIZATION PER SECTOR



ATO ATTACKER’S TOOLKIT

Rent Your Own



Bots

BOT NAME/ /	SORT FP	RESOURCES KNOWN / OTHER	SORT	COUNTRY / HOST	PRICE	□
Filter bot name	Any ▾	amazon		Filter IP/Country/OS	Filter $	
	1 1 1		1 56 0 = 57			

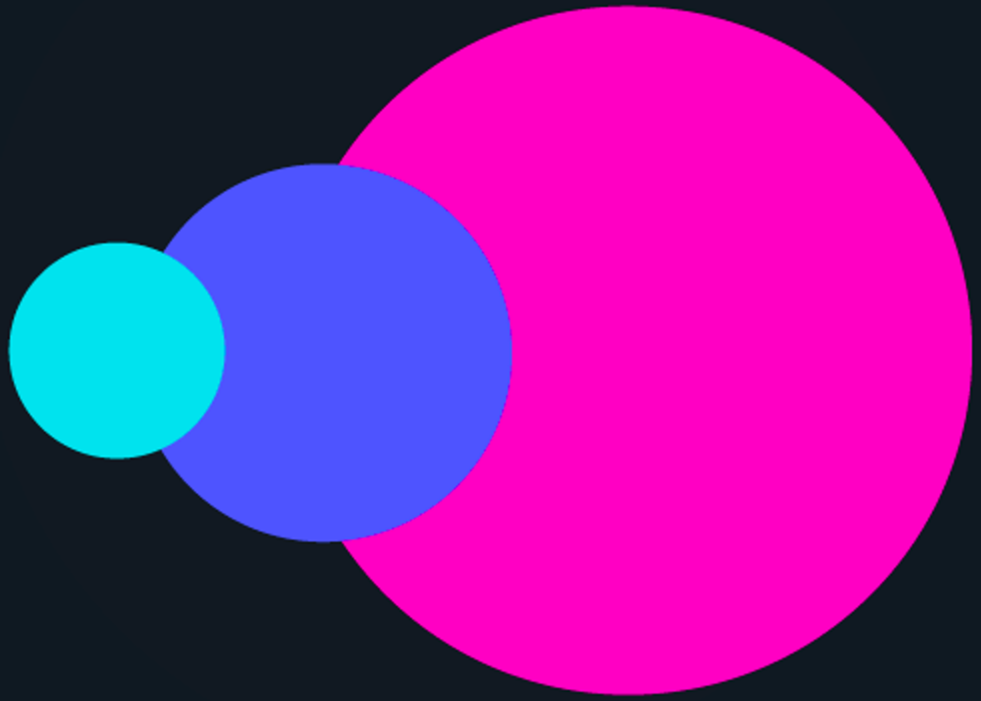
PREVALENCE OF DISCUSSIONS RELATED TO THREE FINGERPRINTING SERVICES BY TOTAL REFERENCES

JANUARY 2020-JUNE 2020

● 11.4% UNDERWORLD MARKET

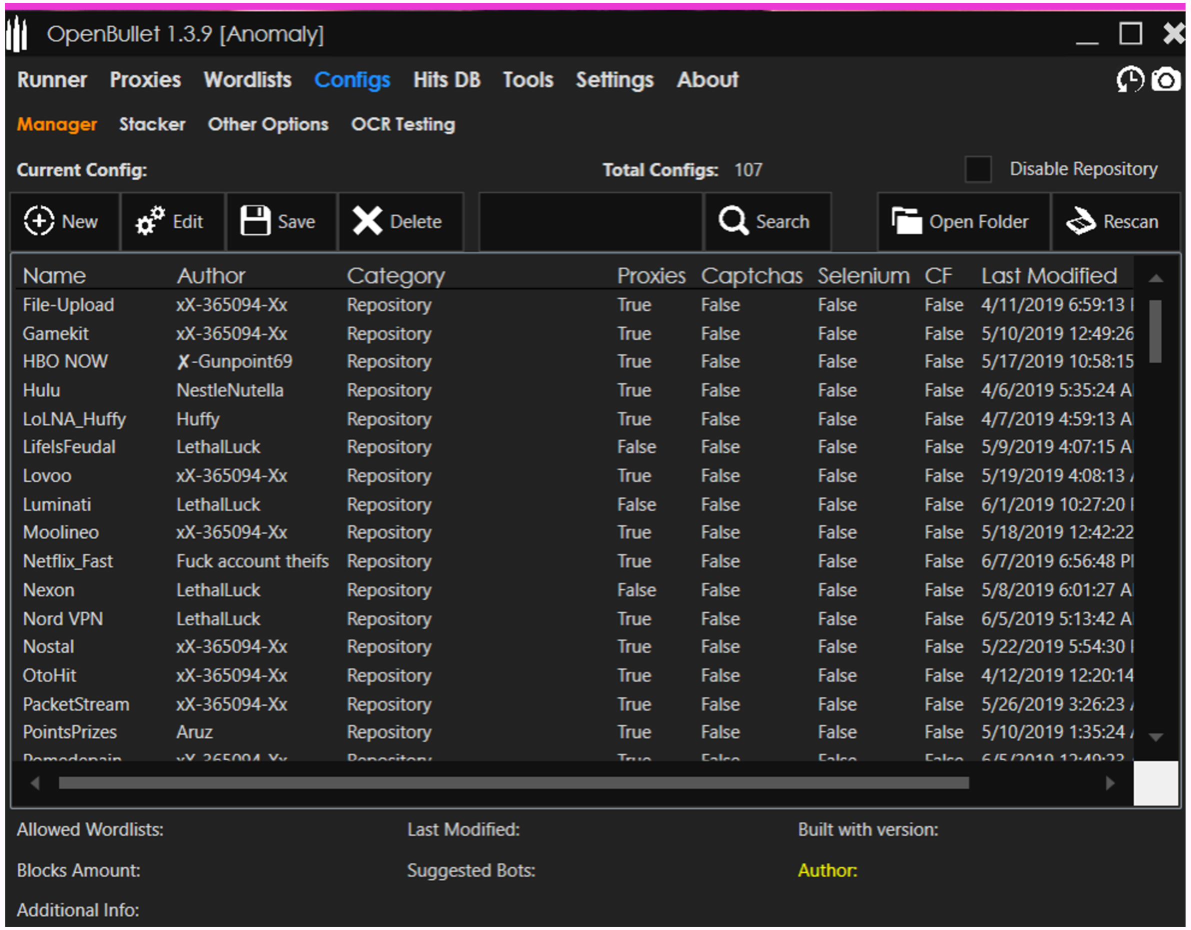
● 23.6% TENEBRIS

● 65% GENESIS



ATO ATTACKER'S TOOLKIT

- Brute-force tools
- Account checkers
- Credential stuffing tools
- SentryMBA
- Rising star: OpenBullet



OpenBullet 1.3.9 [Anomaly]

Current Config:

Total Configs: 107

□ Disable Repository

Name	Author	Category	Proxies	Captchas	Selenium	CF	Last Modified
File-Upload	xX-365094-Xx	Repository	True	False	False	False	4/11/2019 6:59:13
Gamekit	xX-365094-Xx	Repository	True	False	False	False	5/10/2019 12:49:26
HBO NOW	✗-Gunpoint69	Repository	True	False	False	False	5/17/2019 10:58:15
Hulu	NestleNutella	Repository	True	False	False	False	4/6/2019 5:35:24 A
LoLNA_Huffy	Huffy	Repository	True	False	False	False	4/7/2019 4:59:13 A
LifeIsFeudal	LethalLuck	Repository	False	False	False	False	5/9/2019 4:07:15 A
Lovoo	xX-365094-Xx	Repository	True	False	False	False	5/19/2019 4:08:13
Luminati	LethalLuck	Repository	False	False	False	False	6/1/2019 10:27:20
Moolineo	xX-365094-Xx	Repository	True	False	False	False	5/18/2019 12:42:22
Netflix_Fast	Fuck account theifs	Repository	True	False	False	False	6/7/2019 6:56:48 P
Nexon	LethalLuck	Repository	False	False	False	False	5/8/2019 6:01:27 A
Nord VPN	LethalLuck	Repository	True	False	False	False	6/5/2019 5:13:42 A
Nostal	xX-365094-Xx	Repository	True	False	False	False	5/22/2019 5:54:30
OtoHit	xX-365094-Xx	Repository	True	False	False	False	4/12/2019 12:20:14
PacketStream	xX-365094-Xx	Repository	True	False	False	False	5/26/2019 3:26:23
PointsPrizes	Aruz	Repository	True	False	False	False	5/10/2019 1:35:24
Pomodonain	xX-365094-Xx	Repository	True	False	False	False	6/5/2019 12:49:23

Allowed Wordlists:

Last Modified:

Built with version:

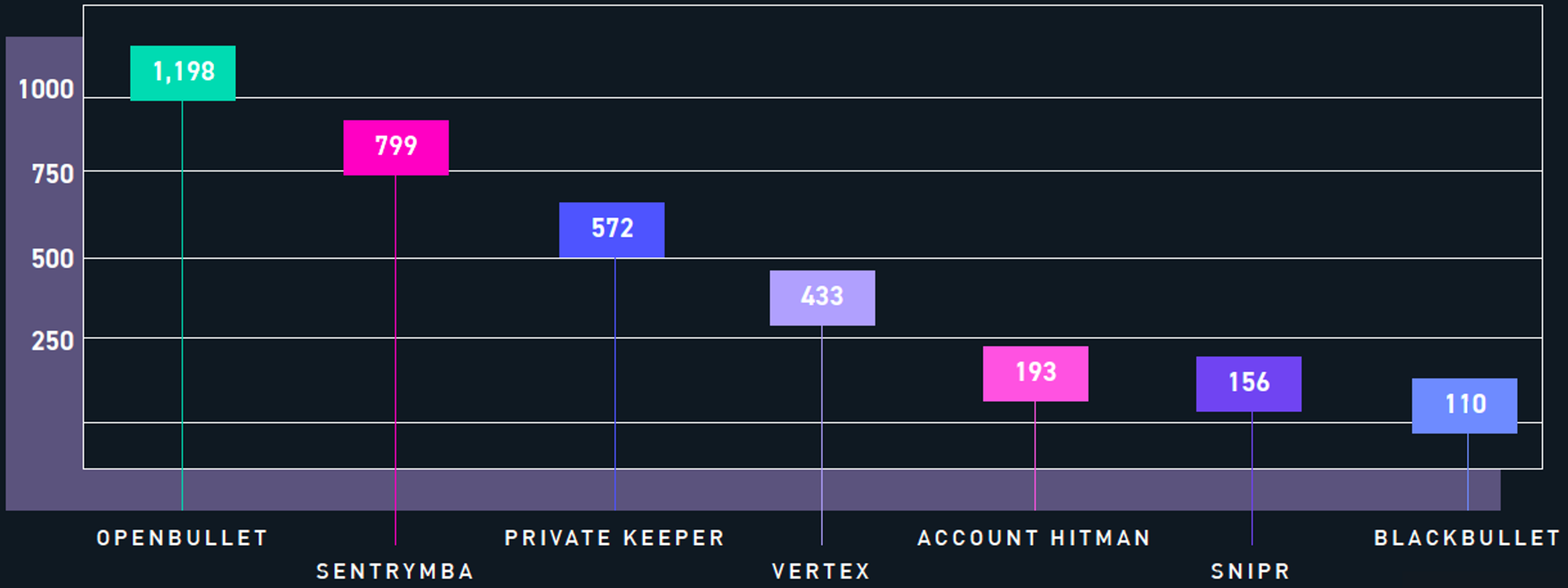
Blocks Amount:

Suggested Bots:

Author:

Additional Info:

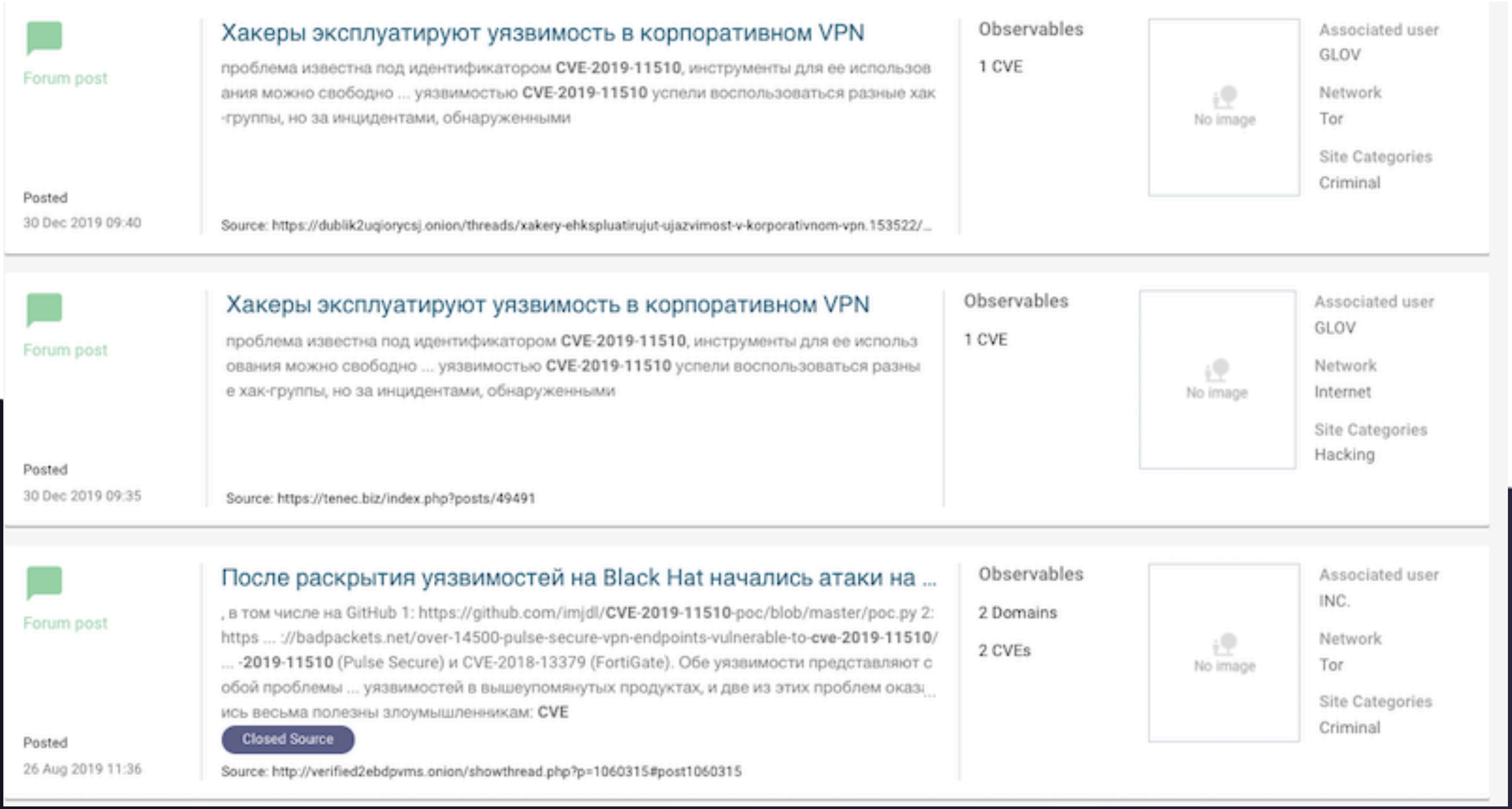
MENTIONS OF VARIOUS CREDENTIAL STUFFING TOOLS ACROSS CRIMINAL LOCATIONS IN 2020.



Moving to a Proactive Stance

Prioritize Patching

digital shadows_



Forum post

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://dublik2uqiorycsj.onion/threads/xakery-ehkspluatirujut-ujazvimost-v-korporativnom-vpn.153522/...

Posted
30 Dec 2019 09:40

Observables
1 CVE

Associated user
GLOV

Network
Tor

Site Categories
Criminal

Forum post

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

Posted
30 Dec 2019 09:35

Observables
1 CVE

Associated user
GLOV

Network
Internet

Site Categories
Hacking

Forum post

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

, в том числе на GitHub 1: https://github.com/imjdl/**CVE-2019-11510**-poc/blob/master/poc.py 2: https ... ://badpackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-**cve-2019-11510**/ ... -**2019-11510** (Pulse Secure) и CVE-2018-13379 (FortiGate). Обе уязвимости представляют собой проблемы ... уязвимостей в вышеупомянутых продуктах, и две из этих проблем оказ... ись весьма полезны злоумышленникам: **CVE**

Closed Source

Source: http://verified2ebdpvms.onion/showthread.php?p=1060315#post1060315

Posted
26 Aug 2019 11:36

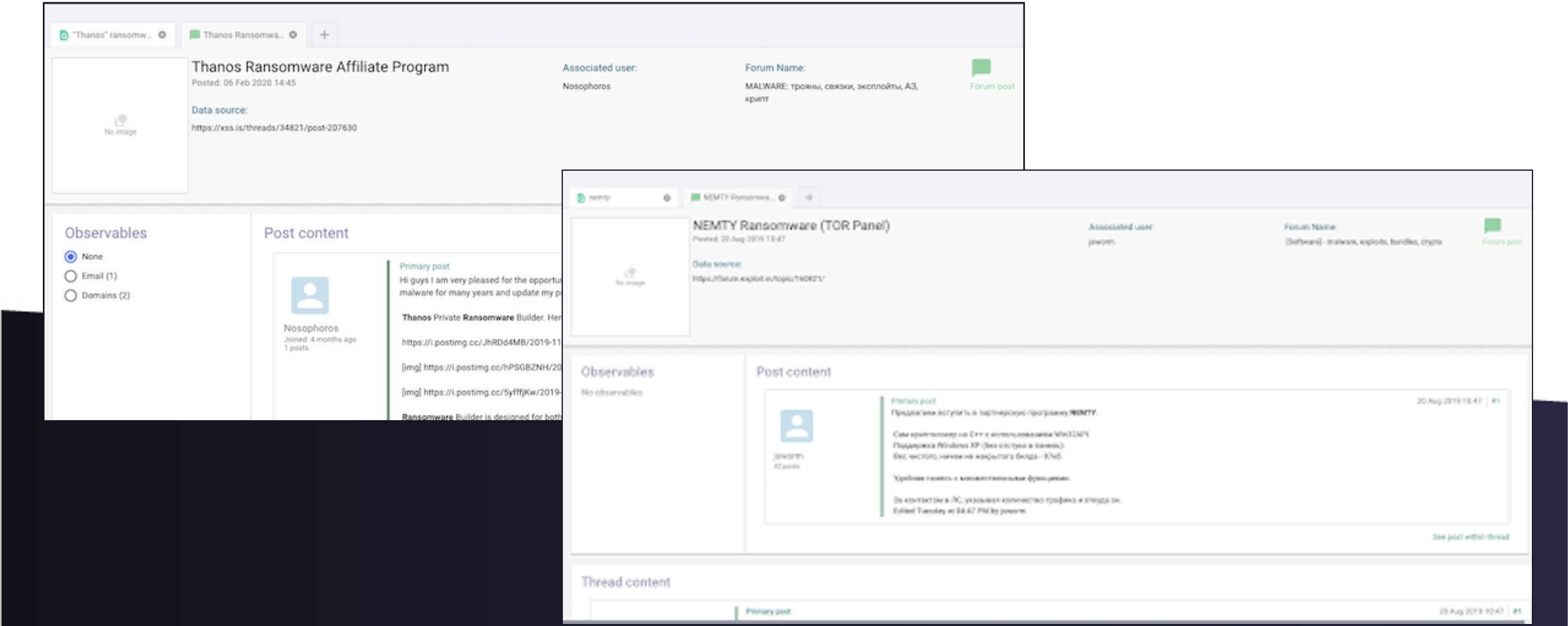
Observables
2 Domains
2 CVEs

Associated user
INC.

Network
Tor

Site Categories
Criminal

ID Early Discussions and Advertisements



"Thanos" ransomw... | Thanos Ransomwa... | +

Thanos Ransomware Affiliate Program
Posted: 06 Feb 2020 14:45

Data source:
https://xss.is/threads/34821/post-207630

Associated user:
Nosophoros

Forum Name:
MALWARE: трояны, связки, эксплойты, АЗ, крипт

Forum post

No image

Observables

● None
○ Email (1)
○ Domains (2)

Post content

Nosophoros
Joined: 4 months ago
1 posts

Primary post
Hi guys I am very pleased for the opportu
malware for many years and update my p

Thanos Private **Ransomware** Builder. Her

https://i.postimg.cc/JhRDd4MB/2019-11

[img] https://i.postimg.cc/hPSGBZNH/20

[img] https://i.postimg.cc/5yfffjKw/2019-

Ransomware Builder is designed for both

nemty | NEMTY Ransomwa... | +

NEMTY Ransomware (TOR Panel)
Posted: 20 Aug 2019 18:47

Data source:
https://forum.exploit.in/topic/160821/

Associated user:
jsworm

Forum Name:
[Software] - malware, exploits, bundles, crypts

Forum post

No image

Observables
No observables

Post content

jsworm
32 posts

Primary post — 20 Aug 2019 18:47 | #1
Предлагаем вступить в партнерскую программу **NEMTY**.

Сам криптолокер на C++ с использованием WinAPI.
Поддержка Windows XP (без доступа в панель).
Вес чистого, ничем не накрытого билда - 87кб.

Удобная панель с множественным функционалом.

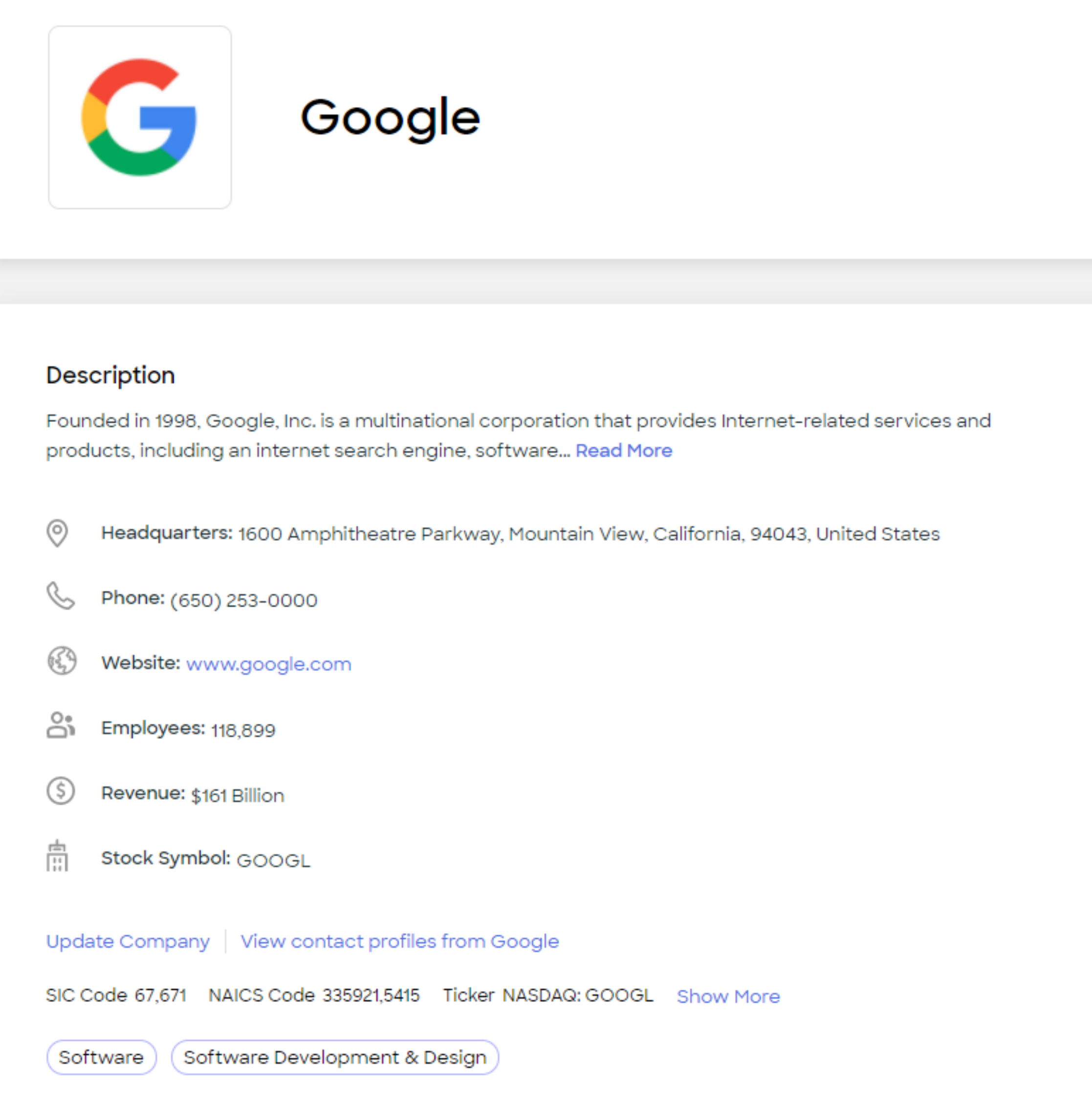
За контактом в ЛС, указывая количество трафика и откуда он.
Edited Tuesday at 04:47 PM by jsworm

See post within thread

Thread content

Primary post — 20 Aug 2019 10:47 | #1

ZoomInfo



Google

Description

Founded in 1998, Google, Inc. is a multinational corporation that provides Internet-related services and products, including an internet search engine, software... 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

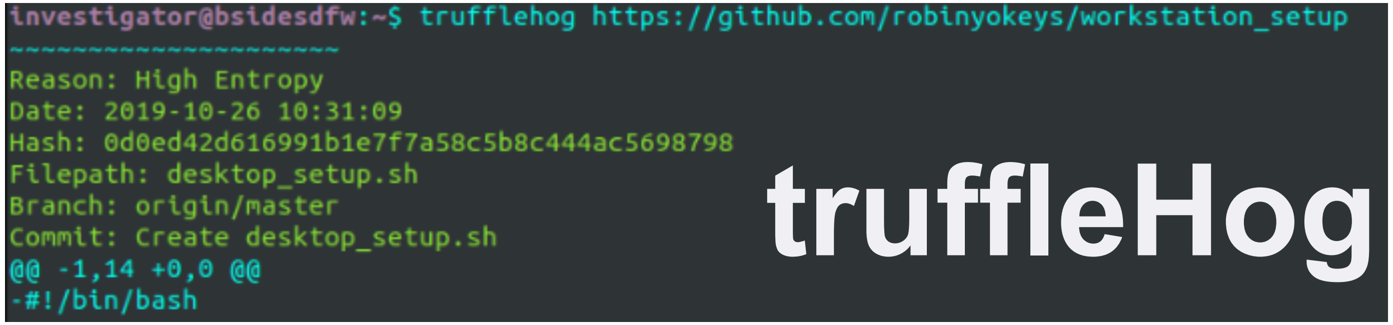
Stock Symbol: GOOGL

Update Company | View contact profiles from Google

SIC Code 67,671 NAICS Code 335921,5415 Ticker NASDAQ: GOOGL Show More

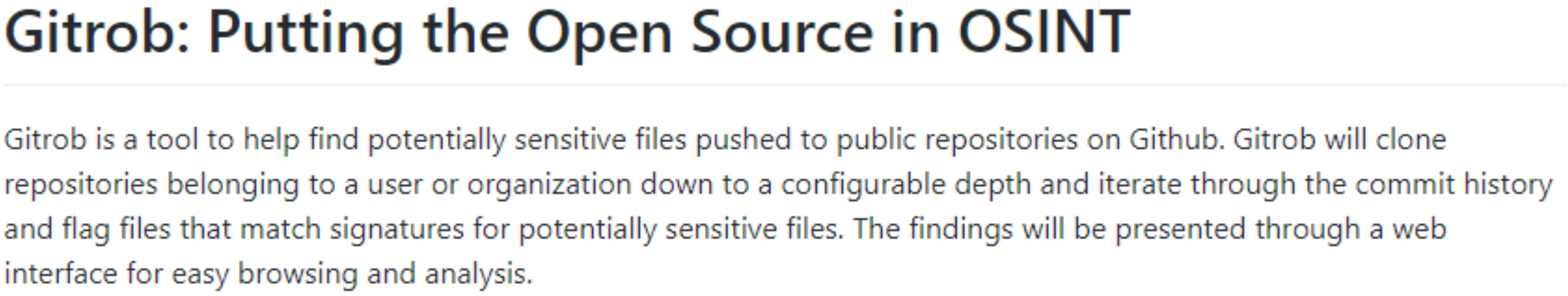
Software | Software Development & Design

Monitor for Leaked Access Keys



```
investigator@bsidesdfw:~$ trufflehog https://github.com/robinyokeys/workstation_setup
~~~~~~~~~~~~~~~~~~~~~
Reason: High Entropy
Date: 2019-10-26 10:31:09
Hash: 0d0ed42d616991b1e7f7a58c5b8c444ac5698798
Filepath: desktop_setup.sh
Branch: origin/master
Commit: Create desktop_setup.sh
@@ -1,14 +0,0 @@
-#!/bin/bash
```

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

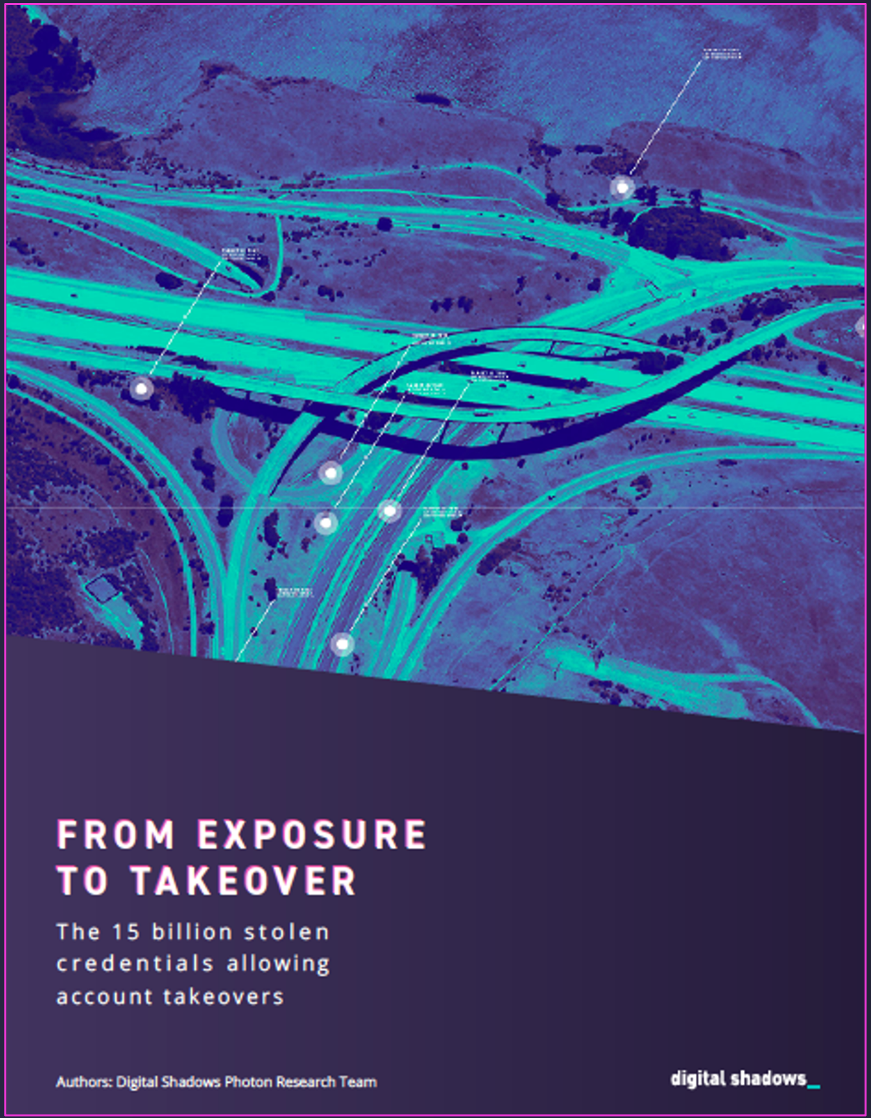
Monitor for Potentially Malicious Domains

Buy domains similar to yours

Monitor domain registration activity

Resources & Shameless Plug

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

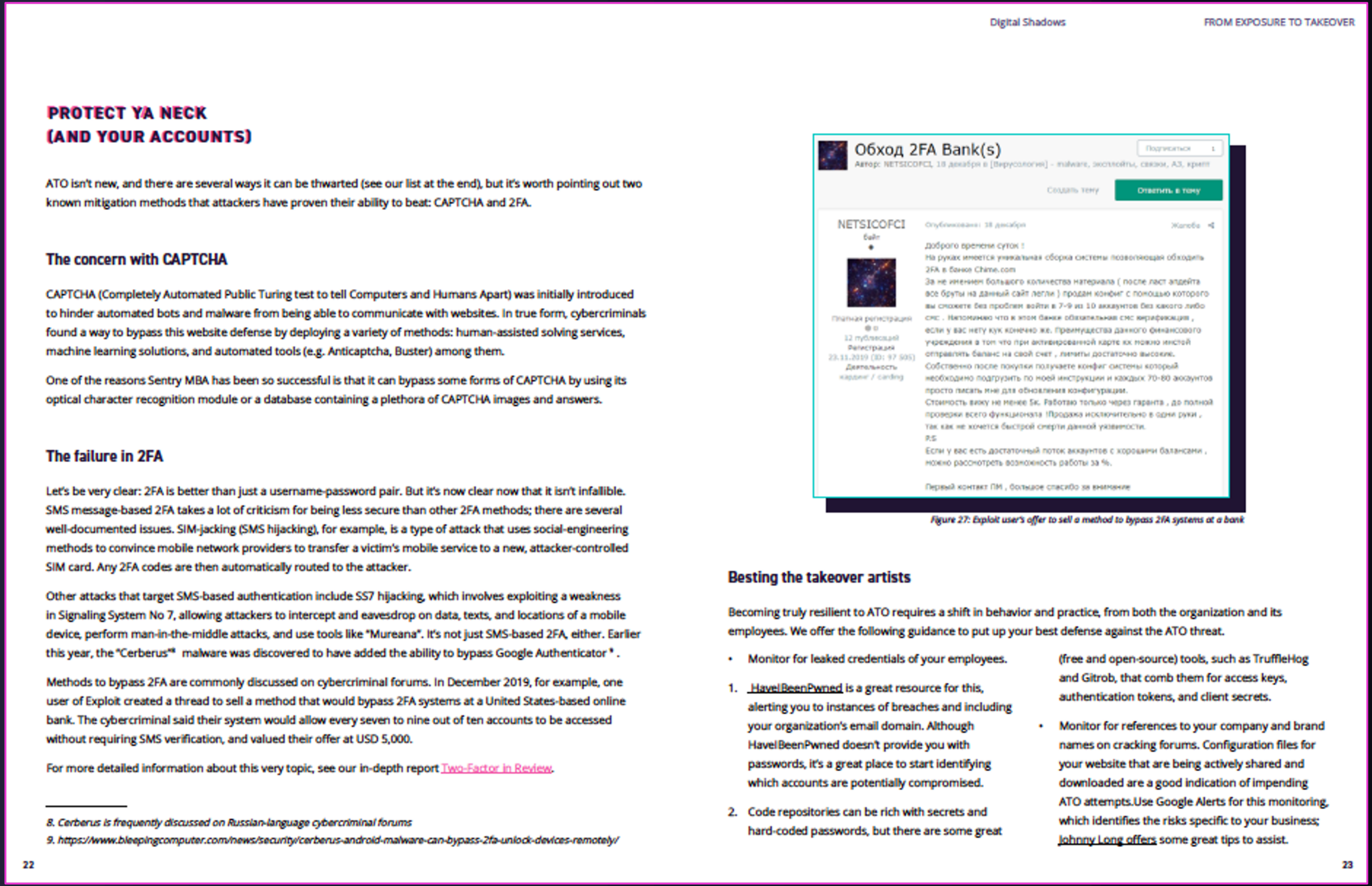


FROM EXPOSURE TO TAKEOVER

The 15 billion stolen credentials allowing account takeovers

Authors: Digital Shadows Photon Research Team

digital shadows_



Digital Shadows FROM EXPOSURE TO TAKEOVER

PROTECT YA NECK (AND YOUR ACCOUNTS)

ATO isn't new, and there are several ways it can be thwarted (see our list at the end), but it's worth pointing out two known mitigation methods that attackers have proven their ability to beat: CAPTCHA and 2FA.

The concern with CAPTCHA

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) was initially introduced to hinder automated bots and malware from being able to communicate with websites. In true form, cybercriminals found a way to bypass this website defense by deploying a variety of methods: human-assisted solving services, machine learning solutions, and automated tools (e.g. Anticaptcha, Buster) among them.

One of the reasons Sentry MBA has been so successful is that it can bypass some forms of CAPTCHA by using its optical character recognition module or a database containing a plethora of CAPTCHA images and answers.

The failure in 2FA

Let's be very clear: 2FA is better than just a username-password pair. But it's now clear now that it isn't infallible. SMS message-based 2FA takes a lot of criticism for being less secure than other 2FA methods; there are several well-documented issues. SIM-jacking (SMS hijacking), for example, is a type of attack that uses social-engineering methods to convince mobile network providers to transfer a victim's mobile service to a new, attacker-controlled SIM card. Any 2FA codes are then automatically routed to the attacker.

Other attacks that target SMS-based authentication include SS7 hijacking, which involves exploiting a weakness in Signaling System No 7, allowing attackers to intercept and eavesdrop on data, texts, and locations of a mobile device, perform man-in-the-middle attacks, and use tools like "Mureana". It's not just SMS-based 2FA, either. Earlier this year, the "Cerberus"[8] malware was discovered to have added the ability to bypass Google Authenticator [9] .

Methods to bypass 2FA are commonly discussed on cybercriminal forums. In December 2019, for example, one user of Exploit created a thread to sell a method that would bypass 2FA systems at a United States-based online bank. The cybercriminal said their system would allow every seven to nine out of ten accounts to be accessed without requiring SMS verification, and valued their offer at USD 5,000.

For more detailed information about this very topic, see our in-depth report Two-Factor in Review.

[8] Cerberus is frequently discussed on Russian-language cybercriminal forums

[9] https://www.bleepingcomputer.com/news/security/cerberus-android-malware-can-bypass-2fa-unlock-devices-remotely/

22

Обход 2FA Bank(s)

Автор: NETSICOFCI, 18 декабря в [Вирусология] - malware, эксплойты, связки, АЗ, крипт

NETSICOFCI
байт

Платная регистрация
12 публикаций
Регистрация
23.11.2019 (ID: 97 505)
Деятельность
кардинг / carding

Опубликовано: 18 декабря

Доброго времени суток !
На руках имеется уникальная сборка системы позволяющая обходить 2FA в банке Chime.com
За не имением большого количества материала (после ласт апдейта все бруты на данный сайт легли) продам конфиг с помощью которого вы сможете без проблем войти в 7-9 из 10 аккаунтов без какого либо смс . Напоминаю что в этом банке обязательная смс верификация , если у вас нету кук конечно же. Преимущества данного финансового учреждения в том что при активированной карте их можно инстой отправлять баланс на свой счет , лимиты достаточно высокие.
Собственно после покупки получаете конфиг системы который необходимо подгрузить по моей инструкции и каждых 70-80 аккаунтов просто писать мне для обновления конфигурации.
Стоимость вижу не менее 5к. Работаю только через гаранта , до полной проверки всего функционала !Продажа исключительно в одни руки , так как не хочется быстрой смерти данной уязвимости.
P.S
Если у вас есть достаточный поток аккаунтов с хорошими балансами , можно рассмотреть возможность работы за %.

Первый контакт ПМ , большое спасибо за внимание

Figure 27: Exploit user's offer to sell a method to bypass 2FA systems at a bank

Besting the takeover artists

Becoming truly resilient to ATO requires a shift in behavior and practice, from both the organization and its employees. We offer the following guidance to put up your best defense against the ATO threat.

- Monitor for leaked credentials of your employees.

1. HaveIBeenPwned is a great resource for this, alerting you to instances of breaches and including your organization's email domain. Although HaveIBeenPwned doesn't provide you with passwords, it's a great place to start identifying which accounts are potentially compromised.
2. Code repositories can be rich with secrets and hard-coded passwords, but there are some great (free and open-source) tools, such as TruffleHog and Gitrob, that comb them for access keys, authentication tokens, and client secrets.

- Monitor for references to your company and brand names on cracking forums. Configuration files for your website that are being actively shared and downloaded are a good indication of impending ATO attempts.Use Google Alerts for this monitoring, which identifies the risks specific to your business; Johnny Long offers some great tips to assist.

23

Blogs as Far as the Eye can See

ATO Part 1: https://www.digitalshadows.com/blog-and-research/from-exposure-to-takeover-part-1-beg-borrow-and-steal-your-way-in/

ATO Part 2: https://www.digitalshadows.com/blog-and-research/the-rise-of-openbullet-a-deep-dive-in-the-attackers-ato-toolkit/

ATO Part 3: https://www.digitalshadows.com/blog-and-research/account-takeover-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/

Shameless Plug

Kacey Clark
@sudosu_kacey

threat researcher @digitalshadows 🖤 @photon_research 👾 #ShadowTalk threat intelligence podcast 🎙 privacy advocate 🔎

Questions