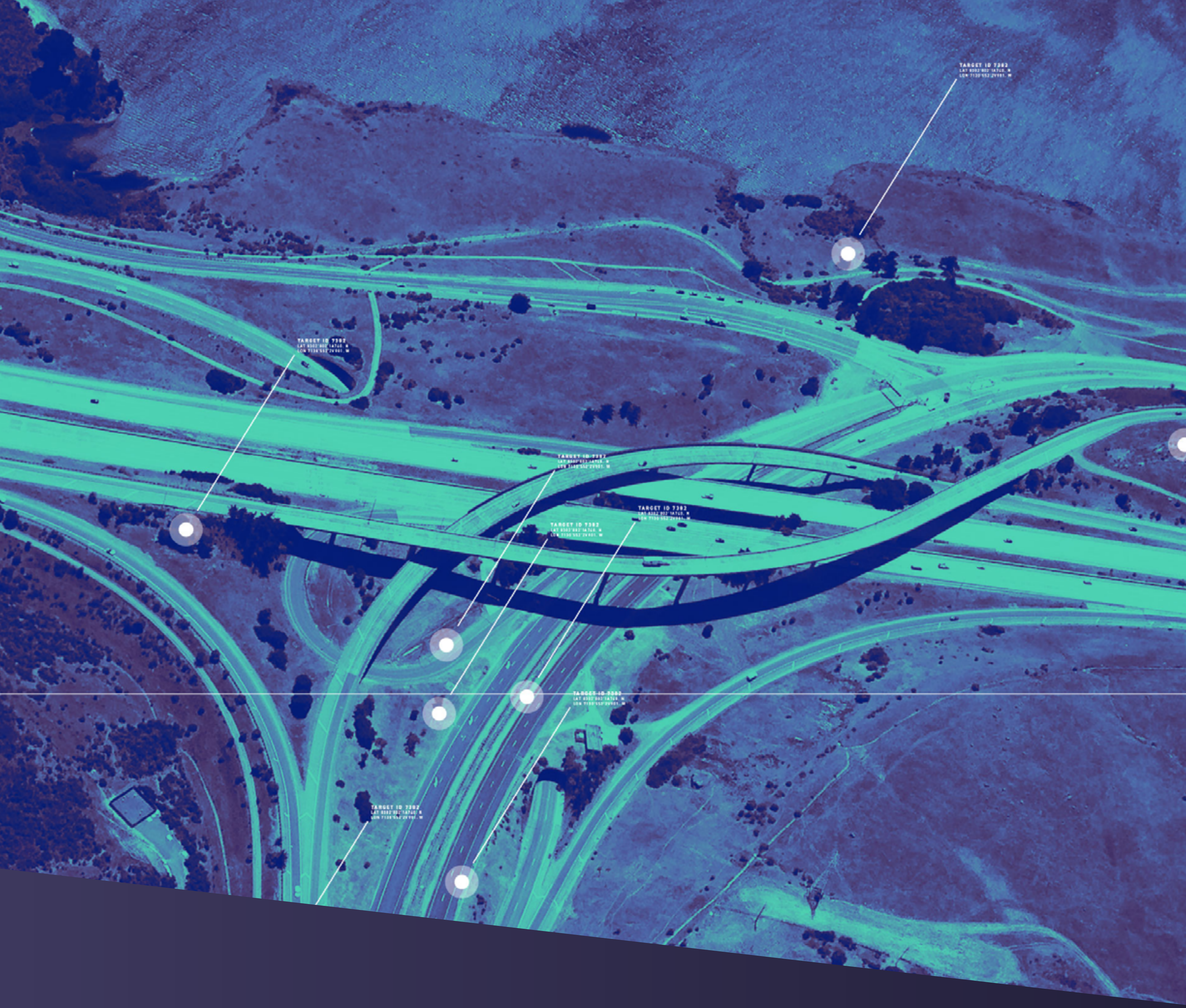


FROM EXPOSURE TO TAKEOVER

The 15 billion stolen credentials allowing account takeovers

Authors: Digital Shadows Photon Research Team

digital shadows_

EXECUTIVE SUMMARY

The average person uses some 191 services that require them to enter passwords or other credentials. That's a lot to keep on top of, and it presents a huge problem if compromise occurs, particularly if a person uses the same credentials across multiple services. Over the past 18 months the Digital Shadows Photon Research team has been analyzing how cybercriminals conspire to prey upon users of online services by "taking over" the accounts they all use on an everyday basis—for banks, to stream videos or music, for work—the list goes on.

For this paper we closely examine this ubiquitous problem, including how attackers approach account takeovers (ATO). Using the Digital Shadows SearchLight™ service, which maintains a database of breached credentials and scours criminal forums for attackers' trends, data dumps, advertisements and tools, we unearthed some insightful stats:

- **More than 15 billion** credentials are in circulation—up 300 percent since 2018 and coming from 100,000-plus discrete breaches.
- **5 billion** of those are "unique", without any repeated credential pairs.
- Most credentials belong to consumers, and cybercriminals give away many for free; **those that are sold go for an average of $15.43.**
- Unsurprisingly, **bank and other financial accounts are the most valuable, selling for an average of $70.91 apiece.** They account for 25 percent of all the advertisements we analyzed.
- Account accesses for **antivirus programs garner the second-highest prices:** around $21.67. Accounts for media streaming, social media, file sharing, virtual private networks (VPNs), and adult-content sites all trade for significantly under $10.
- **Access to organizations' key systems is being sold at a significant premium.** Dozens of advertisements offer domain administrator access through auctions, selling it to the highest bidder for up to $120,000 (with an average of $3,139).
- Cybercriminals are obviously going after the "purse strings" in organizations: We found **2 million accounting email addresses exposed.** Email addresses with "invoice" or "invoices" were, by far, the most commonly advertised.
- **Account takeover has never been easier (or cheaper)** for cybercriminals. Brute-force cracking tools and account checkers are available on criminal marketplaces for an average of $4. With recently launched options for ATO "as-a-service", a criminal can rent an identity for less than $10.
- Sentry MBA is the most popular credential stuffing tool, but the **newly emerged OpenBullet tool** has accounted for 35 percent of references across criminal forums so far in 2020.

- **Multi-factor authentication (MFA) is the best of a range of imperfect steps to mitigate.** Attackers are bypassing two-factor authentication (2FA)—and not just those that are SMS message based.

- **Initially compromised accounts can become pivot points** that lead to more sensitive accounts. Access to private GitHub repositories, for example, could provide additional application programming interface (API) keys and secrets.

THE ALLURE OF ATO: WHY CRIMINALS CAN'T RESIST

We rely on passwords to safeguard those precious accounts that allow us to conduct much of the business of life in cyberspace. Our finances, personal information, and sensitive documents are stored in the cloud, locked behind these sets of alphanumeric and special characters. They're prime targets for cybercriminals who conduct fraud and account takeover (ATO).

So it makes sense to secure these accounts as best we can. Since the early days of the Internet, standards for password complexity and encryption have come a long way, along with additional safeguards like MFA (more on that later). These days, many sites won't even let you set a password if it's shorter than a certain number of characters or doesn't mix uppercase with lowercase letters and special characters.

Password managers have also gained popularity, allowing us to generate unique passwords to combat attacks that rely on password reuse. Even still, your password's length or complexity won't matter too much if it's stored in plaintext, or if it's the only thing protecting your account.

According to Verizon's 2020 Data Breach Investigations Report, over 80 percent of breaches related to hacking involved brute-force cracking or the use of lost or stolen credentials. Credential lists are widely sold and traded on cybercriminal forums and marketplaces, and full accounts for various services can be bought for even a few dollars. Before we dig into the data on that concern, let's start off by setting the definition:

So, ATO: Literally, just what it sounds like. An attacker gains access to a user's account. Traditionally, this has meant an e-commerce or financial account, which is then used to conduct fraud. Of course such accounts are valuable to attackers (as seen in the next section), but a wide range of other online services are targeted, from streaming and cable TV subscriptions to VPNs and adult websites.

ACQUIRING CREDENTIALS: BEG, BORROW, OR STEAL

In most cases, a successful ATO requires first acquiring stolen credentials. Attackers can do this by hacking into a company and stealing a database containing credentials, but there are four slightly easier methods we explore in this section:

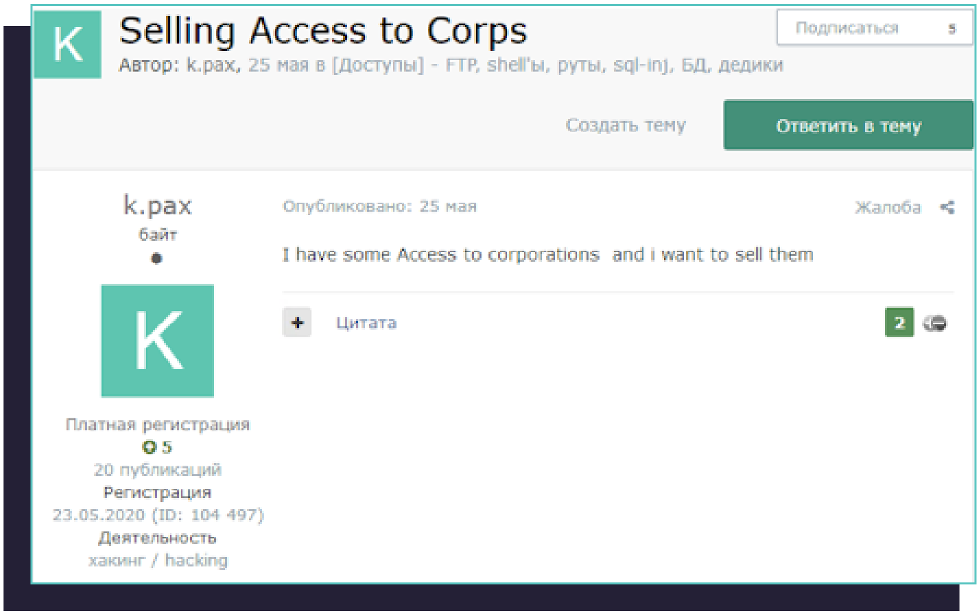
1. **Harvest your own**
2. **Buy credentials**
3. **Rent credentials**
4. **Use freebies**

Harvest your own: phishing, exploits, and malware

Credential-stealing malware and phishing campaigns are not the focus of this research, but we would be remiss not to mention them. Numerous types of trojans and keyloggers have this express purpose, and new pieces of malware surface regularly.

Many credential harvesters target banking credentials, in large volumes—they can be highly lucrative and are in high demand on underground marketplace sites. Credential harvesters use a combination of techniques to acquire victim's details, including man-in-the-browser attacks, which use code injection techniques to inject form fields into the user's banking website. These fields intercept the victim's credentials directly from their online banking portal. They're sent to the attackers, who monetize them directly (via fraudulent transactions) or, more commonly, sell them to other threat actors seeking freshly stolen credentials.

While we’re on the subject of stealing credentials: We’ve also seen some criminal advertisements for domain administrator accesses (login details, credentials or sensitive files from an organization or individual’s machine, used to access systems/infrastructure, data, bank accounts, and/or other accounts). This takes the conversation from “simple” account compromise to complete network compromise, and we’ve seen these accesses sold or auctioned for an average of $3,139 and up to $140,000. The data may not always be valid, but just the concept of a large corporation or government network administrator’s access being sold on criminal marketplaces is, to say the least, unnerving.



Selling Access to Corps

Автор: k.pax, 25 мая в [Доступы] - FTP, shell'ы, руты, sql-inj, БД, дедики

k.pax
байт
●
Платная регистрация
5
20 публикаций
Регистрация
23.05.2020 (ID: 104 497)
Деятельность
хакинг / hacking

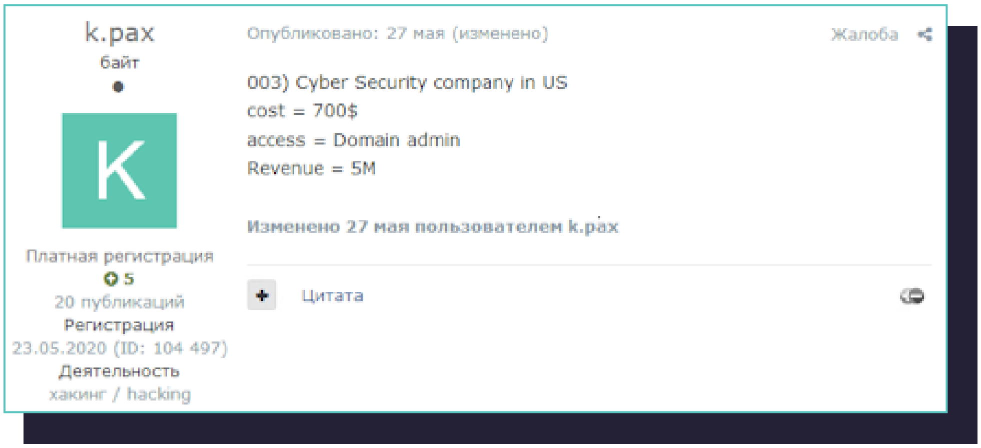
Опубликовано: 25 мая

I have some Access to corporations and i want to sell them

Figure 1: A user initiates the sale of corporate network data on Exploit

Privileged accounts, like administrator accounts, are considered extremely valuable in the criminal underworld. Not only do they give access to a network, but they feature the highest levels of control and trust, and their permissions are nigh unlimited. A person using a privileged account could change system configuration settings, read and modify sensitive data, or give other users access to critical assets.

We found domain administrator-access ads with descriptions including “petrochemical company,” “cybersecurity company,” “architecture and engineering company,” “petroleum company,” “big university,” and various state governments. Some vendors also mention the number of machines on the network, the number of employees, the site’s Alexa ranking,



k.pax
байт
●
Платная регистрация
5
20 публикаций
Регистрация
23.05.2020 (ID: 104 497)
Деятельность
хакинг / hacking

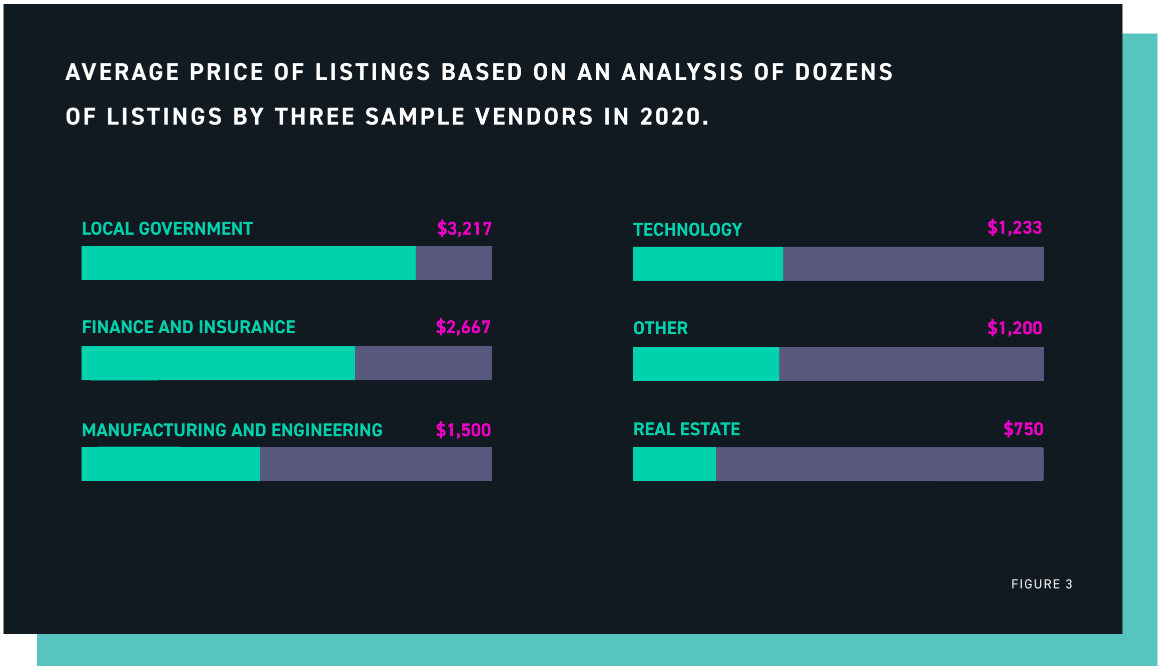
Опубликовано: 27 мая (изменено)

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

Изменено 27 мая пользователем k.pax

Figure 2: Advertisement for domain administrator access for a cyber-security company on Exploit

any intellectual property or sensitive documents on the system, and whether any trusts[1] are available, to give buyers an idea of the value of the access.



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

FIGURE 3

Going out to tender: account sales

Another, somewhat more straightforward, option to acquire credentials is just buy them on a cybercriminal marketplace. With Digital Shadows' Shadow Search™, we gathered hundreds of marketplace advertisements for accounts over the past two and a half years across nine active and defunct dark web marketplaces.

Across all these platforms, the average cost of a single account was $15.43. Unsurprisingly, banking/financial services accounts made up most of the listings and were, on average, the most expensive: $70.91. Account accesses for antivirus programs came a distant second place, averaging around $21.67. All other types of accounts were, on average, just under or significantly below $10. Some can even be had for under $2, like file-sharing or video-game accounts.

1. Authentication for a linked, trusted domain that also allows access to other linked, trusted domains

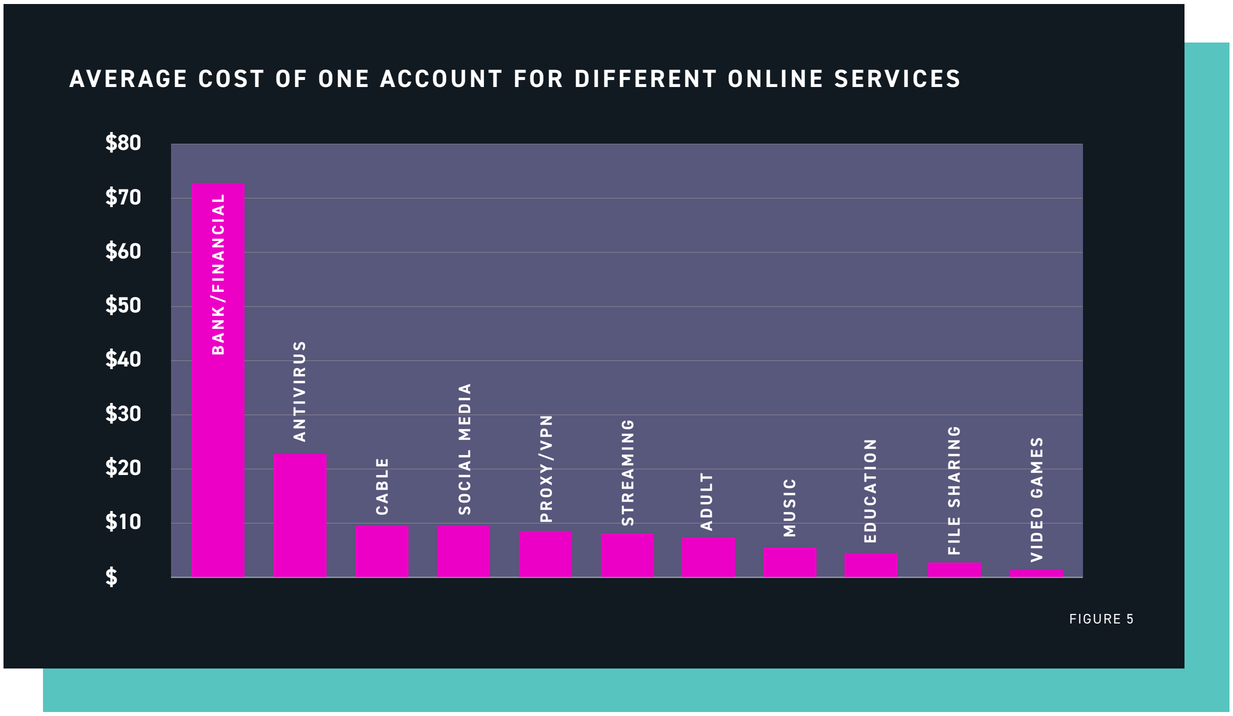


FIGURE 5

In addition to being expensive, banking and other financial accounts are rife—accounting for 25 percent of all the access advertisements we observed. This makes sense; when you compromise someone's bank account, you have direct access to all their funds, plus any sensitive personal information tied to that account. Many of the bank account listings we saw claimed to include the victim's United States social security number, their physical address, their birthdate, and answers to security questions.

Even though the average cost of one banking account was just under $71, we saw some going for upwards of $500. The price can be influenced by many factors: If it's confirmed to have a certain amount of funds, if it has personally identifiable information (PII) attached, and its age (older accounts tend to be cheaper).

Many higher-priced advertisements advertise "drop" accounts, meaning they can be used to facilitate money laundering or cash-out schemes.

In terms of geography, United States-based accounts were advertised most frequently on criminal forums and marketplaces, followed close behind by Canada, Australia, the United Kingdom, and Germany. Cybercriminals very likely perceive North American accounts as being the most profitable. And in terms of non-financial accounts, the second and third most advertised were for streaming and proxy or VPN accounts: comprising 13% and 12%, respectively.

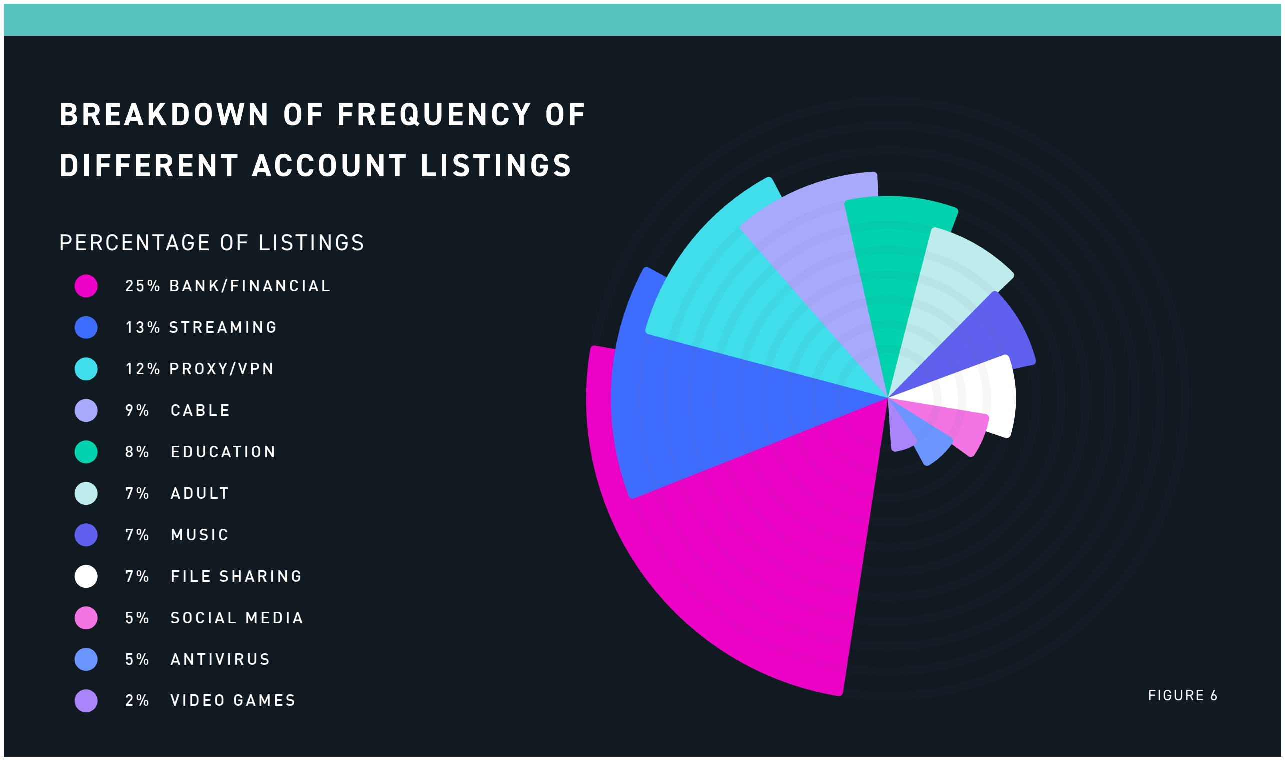

BREAKDOWN OF FREQUENCY OF DIFFERENT ACCOUNT LISTINGS

FIGURE 6

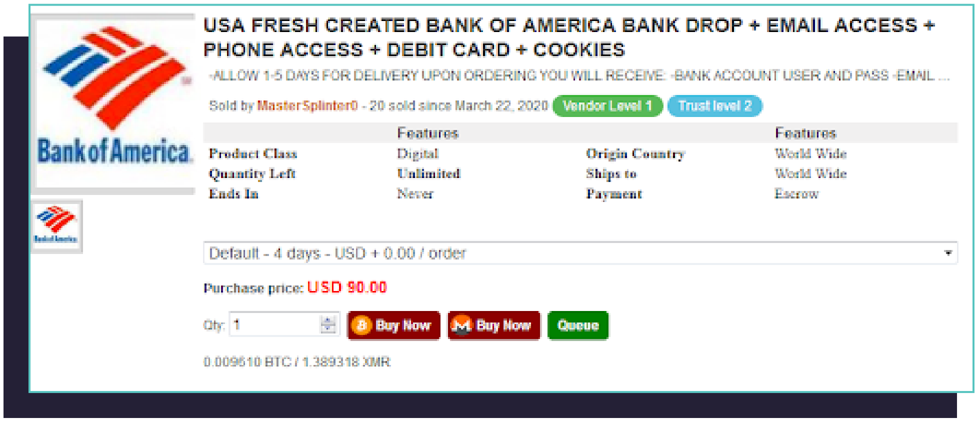
The listings we observed fit into the 11 categories shown in Figure 6. Many of the categories are for services that can be quite pricey if purchased legitimately. Would you rather pay $10 a month for yet another streaming service, or pay $5 for lifetime access? [2] Additionally, accounts for adult websites offer other added benefits, considering that buyers may not want their real names or financial information associated with these services.

In any case, account accesses are relatively cheap. This is probably, at least partly, because of two main factors:

1. Buyers have no guarantee that their purchase will grant them access in the long run; login details could become invalid at any point. Caveat emptor.
2. Vendors can obtain the account accesses cheaply and efficiently [3], so they can sell them at low prices. Typically, they're obtained using techniques such as credential stuffing (more on that later). But many are also byproducts of another crime, allowing them to be sold at low prices or even shared for free.

[2] By "lifetime" we actually just mean the time it takes for the account owner to realize their account has been compromised. This can be days, weeks, months, years, or never.

[3] And even via a u t o m a t i o n!


USA FRESH CREATED BANK OF AMERICA BANK DROP + EMAIL ACCESS + PHONE ACCESS + DEBIT CARD + COOKIES

-ALLOW 1-5 DAYS FOR DELIVERY UPON ORDERING YOU WILL RECEIVE: -BANK ACCOUNT USER AND PASS -EMAIL ...

Sold by MasterSplinter0 - 20 sold since March 22, 2020 Vendor Level 1 Trust level 2

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

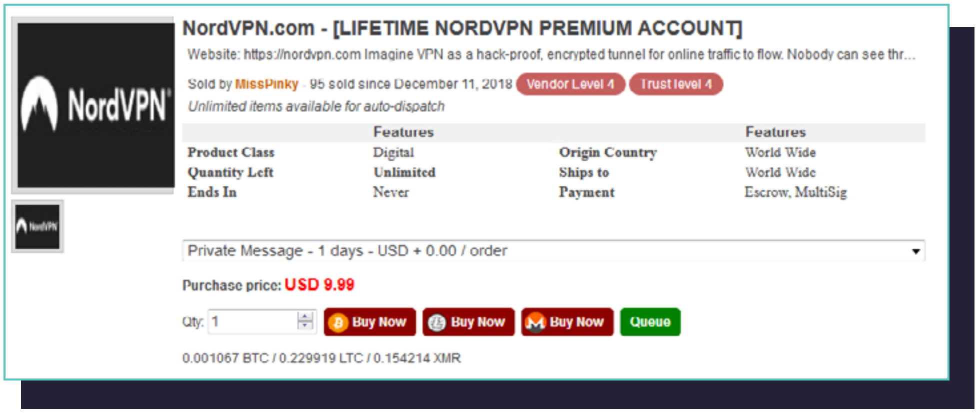
Default - 4 days - USD + 0.00 / order

Purchase price: USD 90.00

Qty: 1

0.009610 BTC / 1.389318 XMR

Figure 7: Bank account access advertised on Empire


NordVPN.com - [LIFETIME NORDVPN PREMIUM ACCOUNT]

Website: https://nordvpn.com Imagine VPN as a hack-proof, encrypted tunnel for online traffic to flow. Nobody can see thr...

Sold by MissPinky - 95 sold since December 11, 2018 Vendor Level 4 Trust level 4

Unlimited items available for auto-dispatch

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow, MultiSig

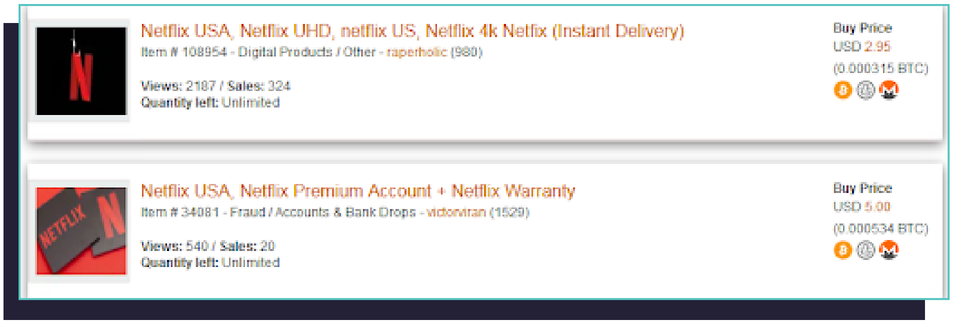
Private Message - 1 days - USD + 0.00 / order

Purchase price: USD 9.99

Qty: 1

0.001067 BTC / 0.229919 LTC / 0.154214 XMR

Figure 8: VPN account advertised on Empire


Netflix USA, Netflix UHD, netflix US, Netflix 4k Netfix (Instant Delivery)

Item # 108954 - Digital Products / Other - raperholic (980)

Views: 2187 / Sales: 324
Quantity left: Unlimited

Buy Price
USD 2.95
(0.000315 BTC)

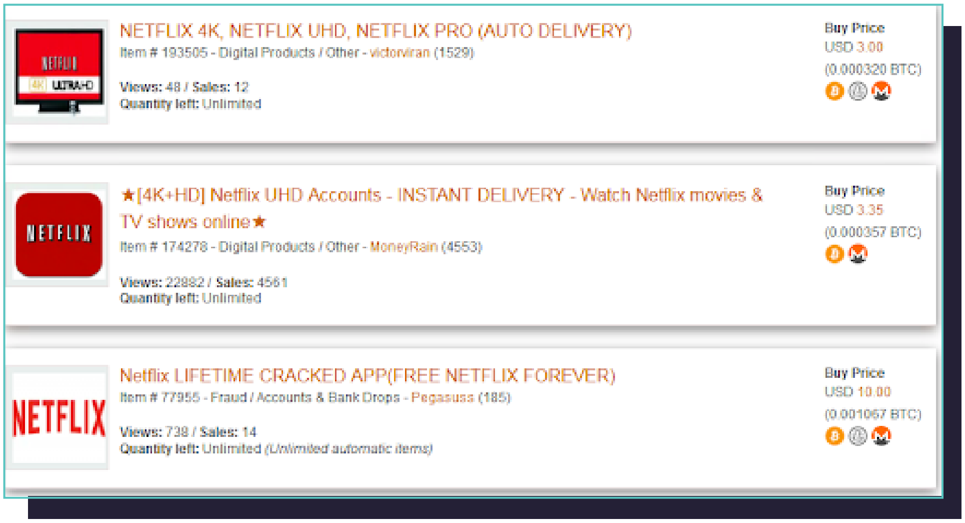
Netflix USA, Netflix Premium Account + Netflix Warranty

Item # 34081 - Fraud / Accounts & Bank Drops - victorviran (1529)

Views: 540 / Sales: 20
Quantity left: Unlimited

Buy Price
USD 5.00
(0.000534 BTC)

Figure 9.1: Streaming access advertised on Empire


NETFLIX 4K, NETFLIX UHD, NETFLIX PRO (AUTO DELIVERY)

Item # 193505 - Digital Products / Other - victorviran (1529)

Views: 48 / Sales: 12
Quantity left: Unlimited

Buy Price
USD 3.00
(0.000320 BTC)

★[4K+HD] Netflix UHD Accounts - INSTANT DELIVERY - Watch Netflix movies & TV shows online★

Item # 174278 - Digital Products / Other - MoneyRain (4553)

Views: 22882 / Sales: 4561
Quantity left: Unlimited

Buy Price
USD 3.35
(0.000357 BTC)

Netflix LIFETIME CRACKED APP(FREE NETFLIX FOREVER)

Item # 77955 - Fraud / Accounts & Bank Drops - Pegasuss (185)

Views: 738 / Sales: 14
Quantity left: Unlimited *(Unlimited automatic items)*

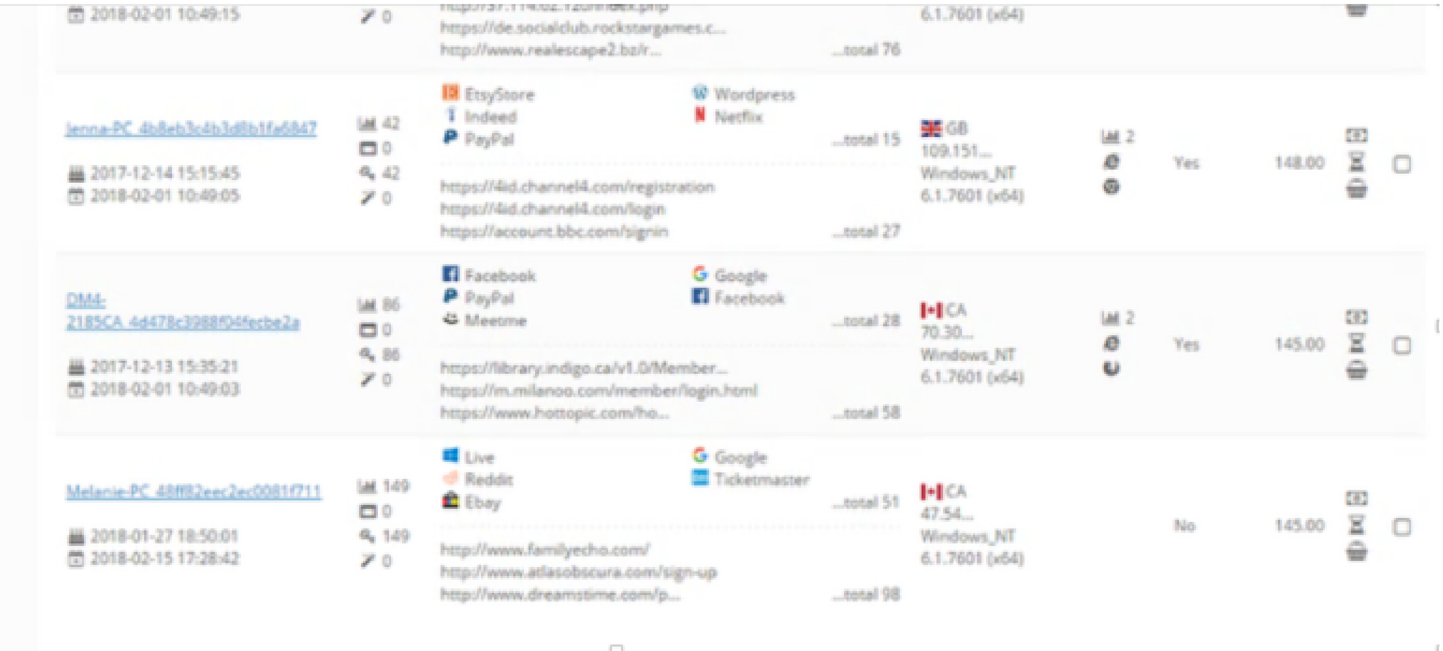
Buy Price
USD 10.00
(0.001067 BTC)

Figure 9.2: Streaming access advertised on Empire

Renting tools: The rise of fingerprint markets

A happy medium between harvesting your own credentials and purchasing stolen credentials is renting account access. We've been closely following the emergence and subsequent rise of certain markets for this kind of service, like Genesis Market, which we first identified in April 2018.[4]

These markets have their own injects and botnets harvesting credentials. But rather than buying a credential, you can rent an identity for a given period for less than $10 (with prices increasing depending on the type of access). The market also collects browser fingerprint data (such as cookies, IP addresses, time zones) from victims, making it considerably easy to perform ATO and transactions that go unnoticed.



2018-02-01 10:49:15	0	https://de.socialclub.rockstargames.c... http://www.realescape2.bz/r... ...total 76	6.1.7601 (x64)				
Jenna-PC_4b8eb3c4b3d8b1fa6847 2017-12-14 15:15:45 2018-02-01 10:49:05	42 0 42 0	EtsyStore Indeed PayPal Wordpress Netflix ...total 15 https://4id.channel4.com/registration https://4id.channel4.com/login https://account.bbc.com/signin ...total 27	GB 109.151... Windows_NT 6.1.7601 (x64)	2	Yes	148.00	☐
DM4-2185CA_4d478c3988f04fecbe2a 2017-12-13 15:35:21 2018-02-01 10:49:03	86 0 86 0	Facebook PayPal Meetme Google Facebook ...total 28 https://library.indigo.ca/v1.0/Member... https://m.milanoo.com/member/login.html https://www.hottopic.com/ho... ...total 58	CA 70.30... Windows_NT 6.1.7601 (x64)	2	Yes	145.00	☐
Melanie-PC_48ff82eec2ec0081f711 2018-01-27 18:50:01 2018-02-15 17:28:42	149 0 149 0	Live Reddit Ebay Google Ticketmaster ...total 51 http://www.familyecho.com/ http://www.atlasobscura.com/sign-up http://www.dreamstime.com/p... ...total 98	CA 47.54... Windows_NT 6.1.7601 (x64)		No	145.00	☐

Figure 10: Genesis Market listings to rent account identities

Although other markets have since emerged as contenders, such as UnderWorld Market (formerly RichLogs) and Tenebris, Genesis Market retains its crown, being the most popular. In Figure 11 you can see how it dominates discussions about fingerprinting, with 65 percent of references across criminal markets. Such discussions have exploded since early January 2018, and forum users are desperate to acquire invite codes to Genesis Market.

[4] https://www.digitalshadows.com/blog-and-research/genesis-botnet-the-market-claiming-to-sell-bots-that-bypass-fingerprinting-controls/

PREVALENCE OF DISCUSSIONS RELATED TO THREE FINGERPRINTING SERVICES BY TOTAL REFERENCES

JANUARY 2020-JUNE 2020

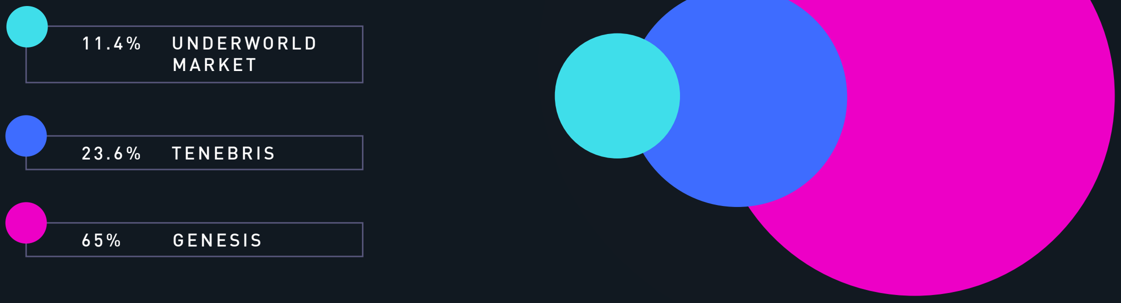


FIGURE 11

REFERENCES TO THE GENESIS MARKET JAN 2018 - DEC 2019

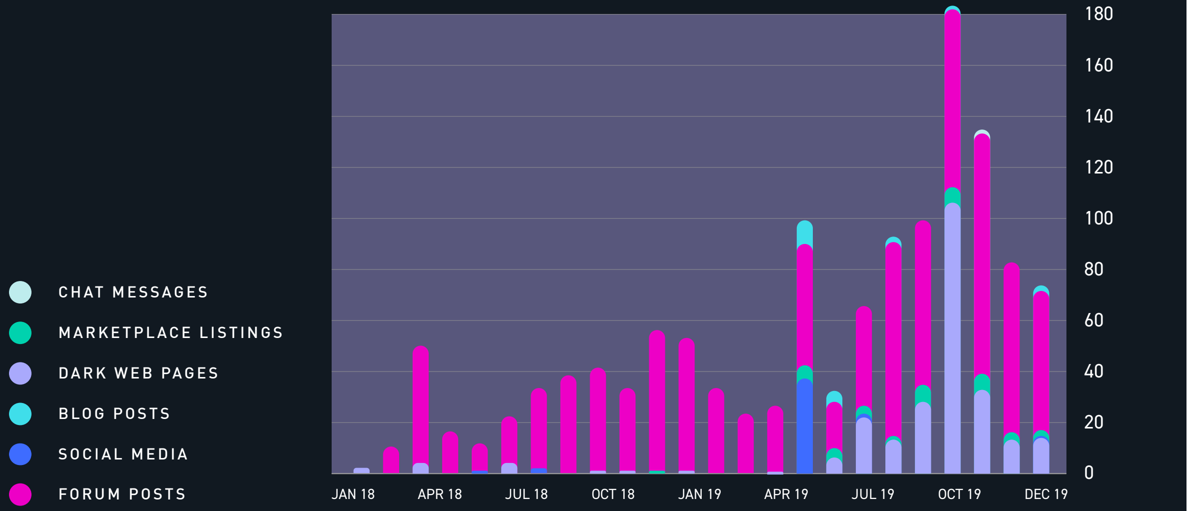


FIGURE 12

Making use of free: Sharing is caring

Although a threat actor could buy or rent account access, they'd be passing up an awful lot of credentials being shared for free on certain cybercriminal forums. A significant amount of Digital Shadows' technology and closed-sources resources are devoted to finding these credentials, so you don't have to. Databases of breached credentials are commonly shared for free on these forums; after someone posts a hashed data set, other forum users work on dehashing it and then post the plaintext passwords as a database.

To date, we've discovered 15 billion-plus credentials, stemming from more than 100,000 discrete breaches. Of these credentials, more than 5 billion are unique.

15,000,000,000

exposed credentials collected by Digital Shadows

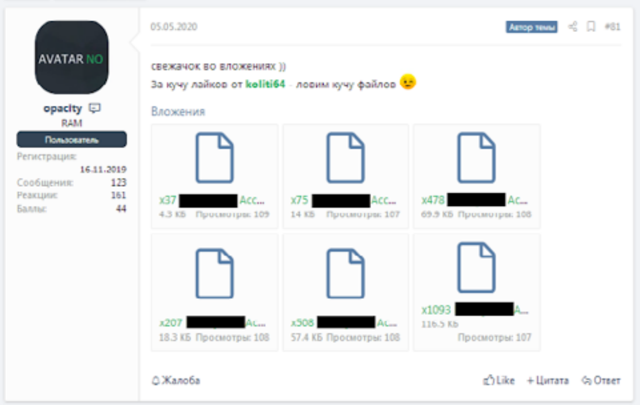
Users of Russian-language cybercriminal forums like Exploit and XSS often freely share credentials for entertainment services with other forum members. These can range from individual credential pairs to files containing thousands of valid accounts.

These free accounts are typically limited to music and video streaming services, because:

1. Cybercriminals don't want to pay for their own streaming, and/or

2. Cybercriminals obtain many accounts as byproducts, so they may sell the valuable goods (e.g. an expensive set of banking credentials) and share any leftovers for free (e.g. streaming credentials).

How very thoughtful.

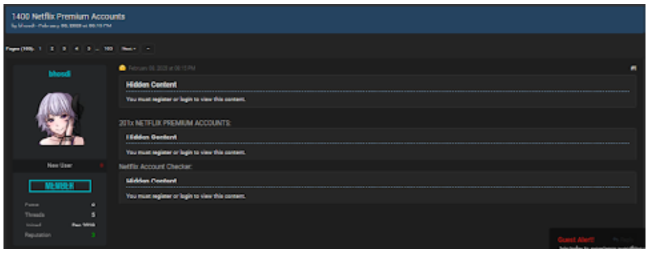

05.05.2020 Автор темы #81

свежачок во вложениях))
За кучу лайков от koliti64 - ловим кучу файлов

Вложения

x37 [redacted] Acc... 4.3 КБ Просмотры: 109
x75 [redacted] Acc... 14 КБ Просмотры: 107
x478 [redacted] Ac... 69.9 КБ Просмотры: 108
x207 [redacted] Ac... 18.3 КБ Просмотры: 108
x508 [redacted] Ac... 57.4 КБ Просмотры: 108
x1093 [redacted] A... 116.5 Кb Просмотры: 107

Figure 13: XSS user shares account credentials for popular streaming service, free of charge


1400 Netflix Premium Accounts

Hidden Content
You must register or login to view this content.

201x NETFLIX PREMIUM ACCOUNTS:

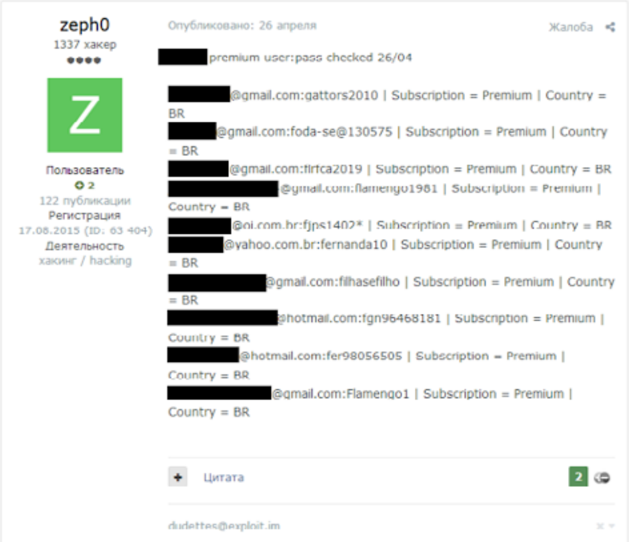
Hidden Content
You must register or login to view this content.

Netflix Account Checker:

Hidden Content
You must register or login to view this content.

Figure 14: Streaming-account credentials shared for free on RaidForums

Whatever the motive for their "philanthropy", cybercriminals are building a sense of community on the forums they use—which is one of the critical determiners of a forum's overall success. The more forum users feel an element of camaraderie with their fellow users, the more likely they are to stick around, if not just for the free streaming accounts. We wrote about this in greater detail in our research paper The Modern Cybercriminal Forum.


Опубликовано: 26 апреля

[redacted] premium user:pass checked 26/04

[redacted]@gmail.com:gattors2010 | Subscription = Premium | Country = BR
[redacted]@gmail.com:foda-se@130575 | Subscription = Premium | Country = BR
[redacted]@gmail.com:tirtca2019 | Subscription = Premium | Country = BR
[redacted]@gmail.com:flamengo1981 | Subscription = Premium | Country = BR
[redacted]@oi.com.br:fjps1402* | Subscription = Premium | Country = BR
[redacted]@yahoo.com.br:fernanda10 | Subscription = Premium | Country = BR
[redacted]@gmail.com:filhasefilho | Subscription = Premium | Country = BR
[redacted]@hotmail.com:fgn96468181 | Subscription = Premium | Country = BR
[redacted]@hotmail.com:fer98056505 | Subscription = Premium | Country = BR
[redacted]@gmail.com:Flamengo1 | Subscription = Premium | Country = BR

dudettes@exploit.im

Figure 15: Exploit user shares free account credentials for a popular streaming service

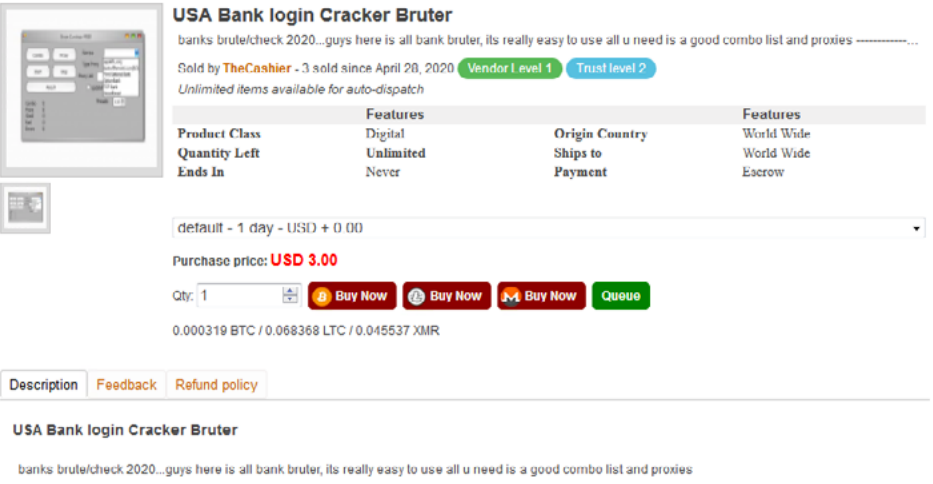
OVERTAKING THE BASICS WITH THE ATO ATTACKER'S TOOLKIT

For every cybercriminal sourcing credentials using any of the four easy ways discussed, there is another employing less obvious means to take over accounts. Let's lift the lid on the sophisticated ATO attacker's toolkit and see what you should worry about.

Brute-force cracking tools, account checkers

Brute-force cracking tools and account checkers are the cornerstones of many account compromise operations, reliably enabling attackers to get their hands on even more of your data. They're automated scripts or programs applied to a login system—whether it's associated with an API or website—to gain access to a user's account. Although some attack campaigns using these tools may be subtle and hard to detect, others resemble distributed denial of service campaigns.

Criminal operations using brute-force cracking tools or account checkers may also take advantage of IP addresses, VPN services, botnets, or proxies to maintain anonymity or improve the likelihood of accessing an account. Once they're in, they can use the account for malicious purposes or extract all of its data (potentially including payment-card details or PII) to monetize it.



USA Bank login Cracker Bruter

banks brute/check 2020...guys here is all bank bruter, its really easy to use all u need is a good combo list and proxies ------------...

Sold by TheCashier - 3 sold since April 28, 2020 Vendor Level 1 Trust level 2

Unlimited items available for auto-dispatch

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

default - 1 day - USD + 0.00

Purchase price: USD 3.00

Qty: 1

0.000319 BTC / 0.068368 LTC / 0.045537 XMR

USA Bank login Cracker Bruter

banks brute/check 2020...guys here is all bank bruter, its really easy to use all u need is a good combo list and proxies

Figure 16: Advertisement for a bank login brute-force cracking tool on Empire

The Photon team found a myriad of brute-force cracking tools and account checkers available on criminal marketplaces for an average of $4. Some advertisements were super vague—"USA Bank login Cracker Bruter"—but others were obviously targeting a specific service, like Hulu, Minecraft, or Spotify. Most of the tools didn't seem to be named, but some listings claimed to include the Burp Suite Professional application security testing software, Hydra login cracker, Zeus and WarBot botnets, and Sentry MBA account cracker.

Based on their descriptions, these tools can "crack" accounts associated with banking, video games, e-commerce services, social media, streaming, VPN accounts, and proxy services. Really, the only items required to wage an ATO attack with these tools are a proxy and an email address or username and password combo list—which, as we said above, can be easily purchased or acquired for free on a criminal marketplace.

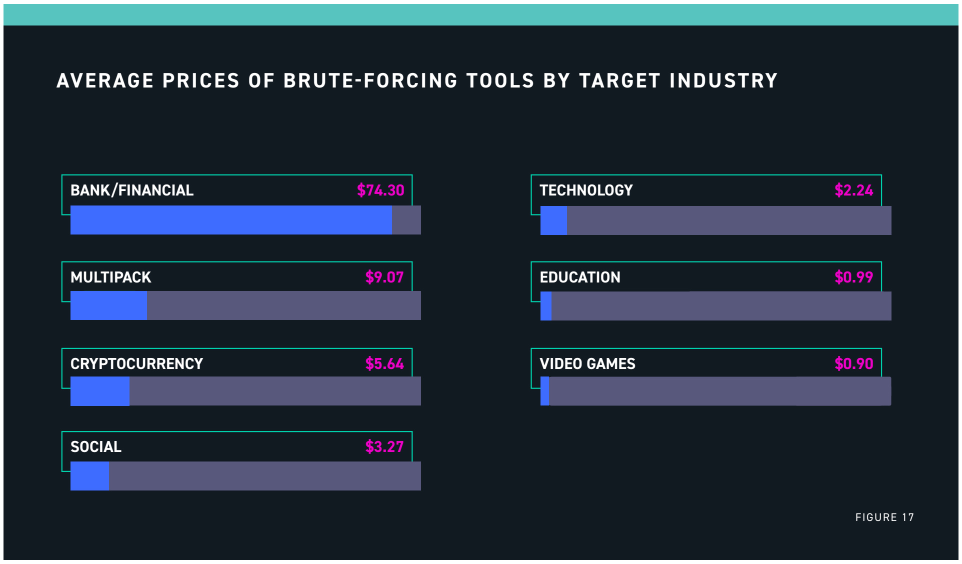

AVERAGE PRICES OF BRUTE-FORCING TOOLS BY TARGET INDUSTRY

FIGURE 17

* "Multipack" (figure 17 and 18) *represents tools used to access accounts spanning multiple industries.*

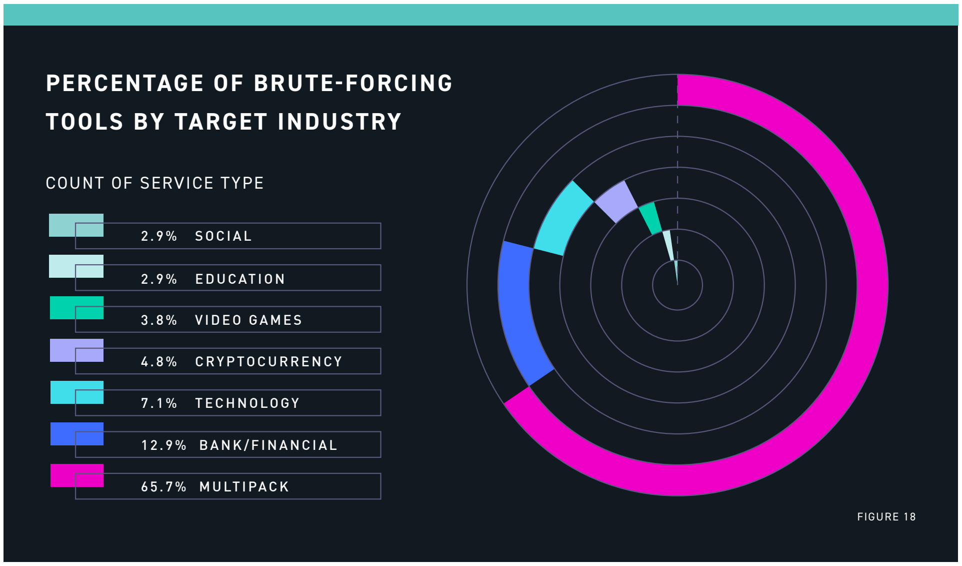
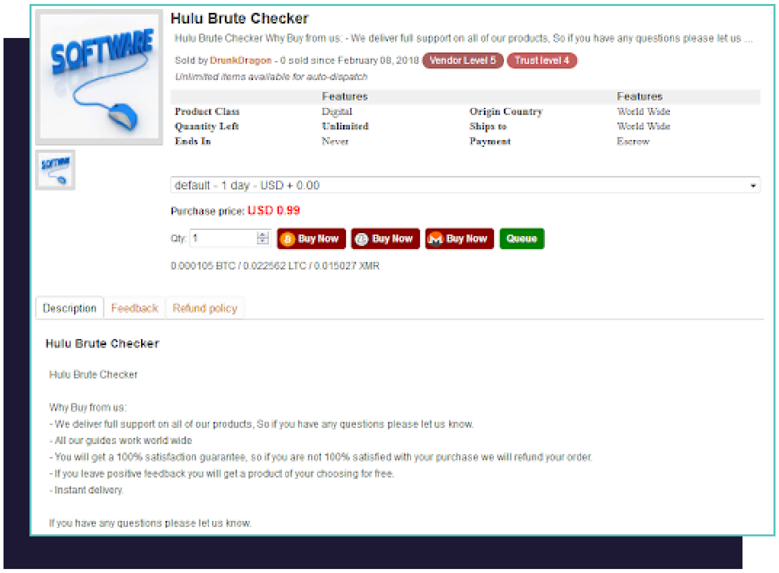

PERCENTAGE OF BRUTE-FORCING TOOLS BY TARGET INDUSTRY

FIGURE 18


Hulu Brute Checker

Hulu Brute Checker Why Buy from us: - We deliver full support on all of our products, So if you have any questions please let us ...

Sold by DrunkDragon - 0 sold since February 08, 2018 Vendor Level 5 Trust level 4

Unlimited items available for auto-dispatch

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

default - 1 day - USD + 0.00

Purchase price: USD 0.99

Qty: 1

0.000105 BTC / 0.022562 LTC / 0.015027 XMR

Hulu Brute Checker

Hulu Brute Checker

Why Buy from us:
- We deliver full support on all of our products, So if you have any questions please let us know.
- All our guides work world wide
- You will get a 100% satisfaction guarantee, so if you are not 100% satisfied with your purchase we will refund your order.
- If you leave positive feedback you will get a product of your choosing for free.
- Instant delivery.

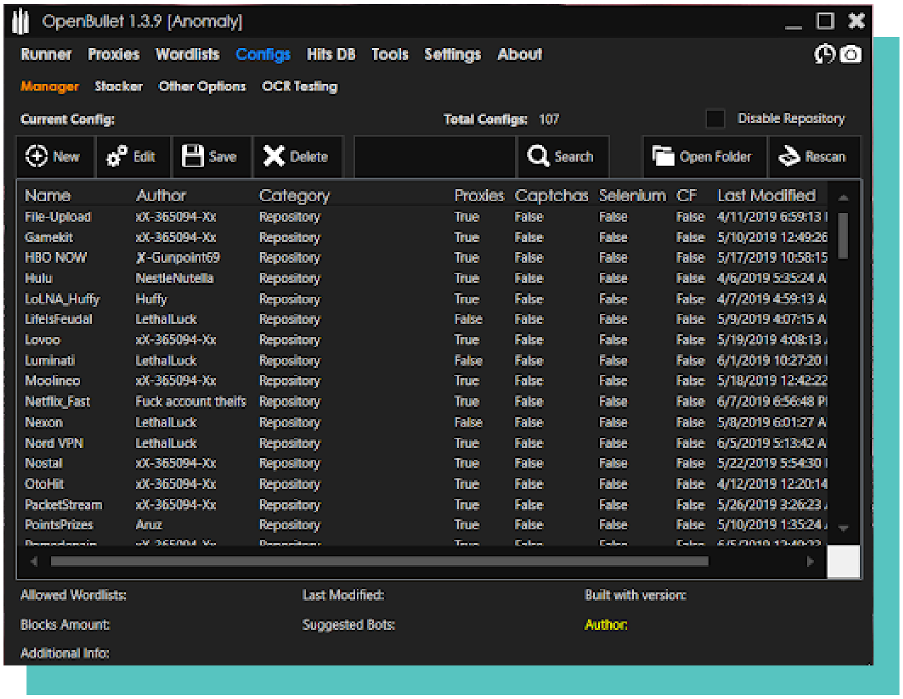
If you have any questions please let us know.

Figure 19: Advertisement for a brute-force cracking tool on Empire

CREDENTIAL STUFFING TOOLS

If an attacker acquires a list of credentials that have been exposed in breaches, what do they do next? Well, credential stuffing attacks are undeniably popular, and push the ATO to the next stage by opportunistically providing initial access to accounts. These attacks are typically automated login attempts that use a predetermined list of access credentials—often, combinations of usernames or email addresses and plaintext passwords—sourced from previous data breaches or leaks. Credential stuffing differs from brute-force cracking, which uses password lists or other resources to guess a successful match.

For many years, Sentry MBA has been one of the most widely used tools, and the most recognizable, in credential stuffing attacks. Like most tools of its type, it has a user interface that allows the uploading of base credential lists and proxies, and a screen where results are logged.



OpenBullet 1.3.9 [Anomaly]
Runner Proxies Wordlists Configs Hits DB Tools Settings About
Manager Stacker Other Options OCR Testing
New Edit Save Delete Search Open Folder Rescan

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	X-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

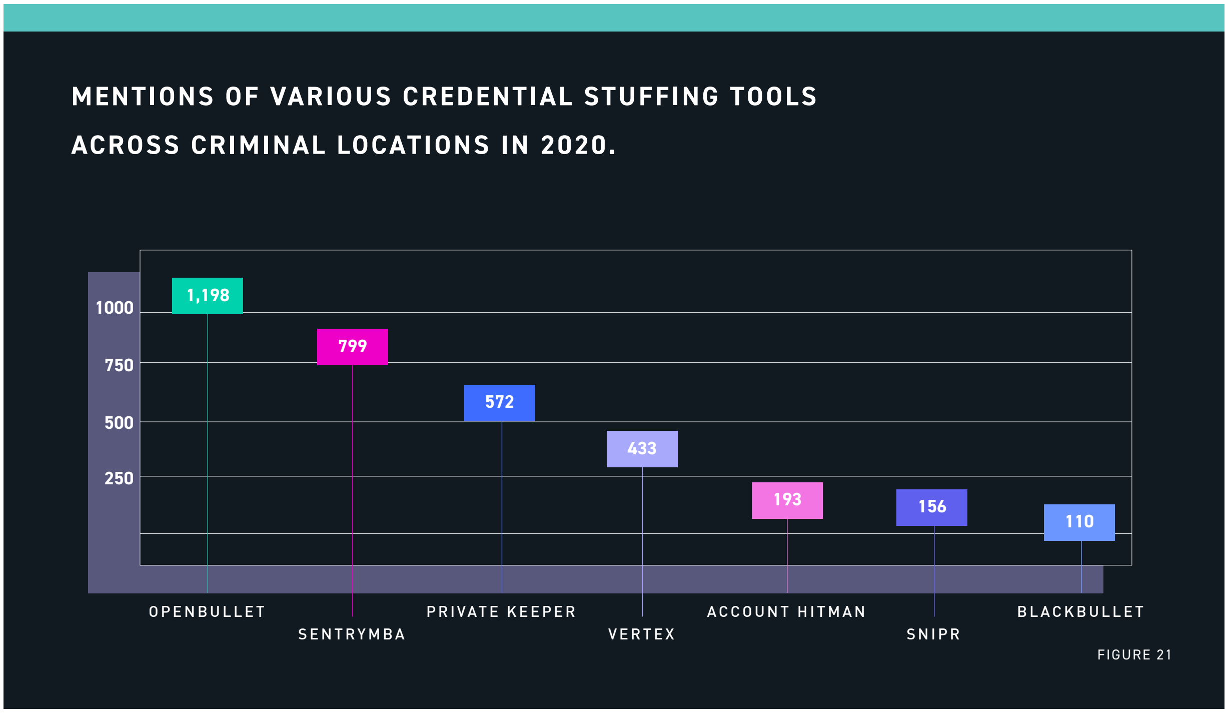
Allowed Wordlists: Last Modified: Built with version:

Blocks Amount: Suggested Bots: Author:

Additional Info:

Figure 20: Configuration Manager view in OpenBullet

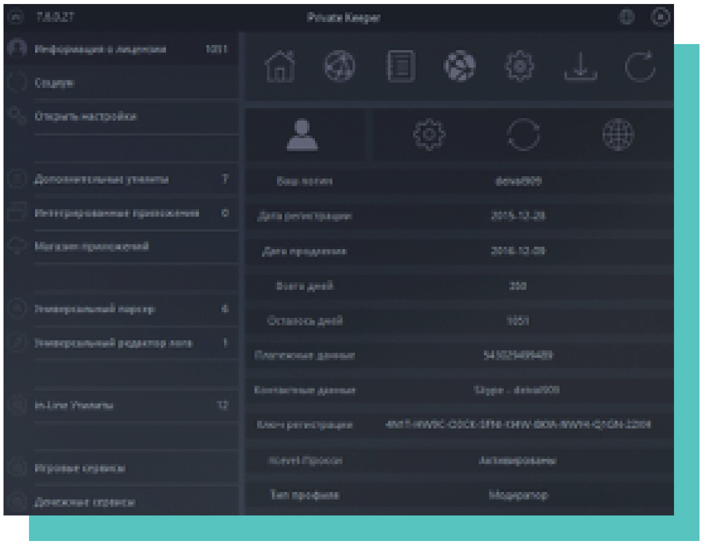
Sentry MBA still attracts significant interest, but a new player has entered the Thunderdome: OpenBullet. It's a website testing suite of software that allows users to perform requests on a target web application, and it's been gaining interest since early April 2019. Ostensibly created for legitimate purposes, OpenBullet includes multiple tools that can be used for scraping and parsing data, automated penetration testing, and unit testing with Selenium. Based on this tool's open-source format, continuously updated features, ability to customize configurations, and lower CPU usage, it's gaining popularity among cybercriminal forum users.



MORE CREDENTIAL-REUSE TOOLS

Threat actors are always advertising new tools across criminal locations—dark-webpages, forums, chat platforms—to dig up and reuse credentials. Here are some of those trending in 2020:

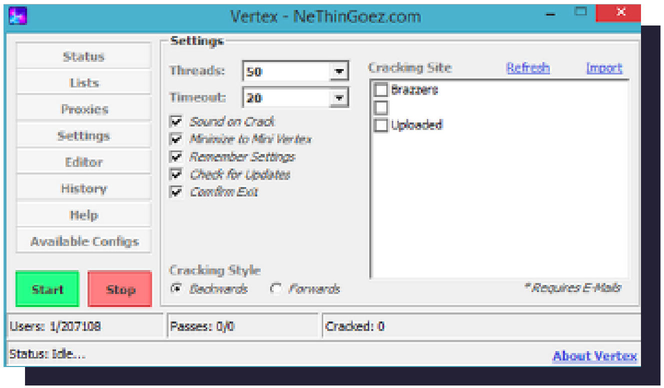
- **Private Keeper** is a tool used across Russian-language cybercriminal platforms, developed by a threat actor who goes by "deival909". Initially created as a brute-force cracking tool, the software underwent several changes during development, which enables users to create and configure their own brute-force crackers and utilities with the help of in-line technology. Private Keeper contains a utility for collecting private proxies from other private services, and provides access to multiple finished projects in an application store. Online tutorials explain how to use Private Keeper to target specific victims, such as banks and other financial organizations.



Ваш логин	deival909
Дата регистрации	2015-12-28
Дата продления	2016-12-09
Всего дней	350
Осталось дней	1051
Платежные данные	[illegible]
Контактные данные	Skype - deival909
Ключ регистрации	[illegible]
Kevel Прокси	Активированы
Тип профиля	Модератор

Figure 22: Private Keeper tool user interface

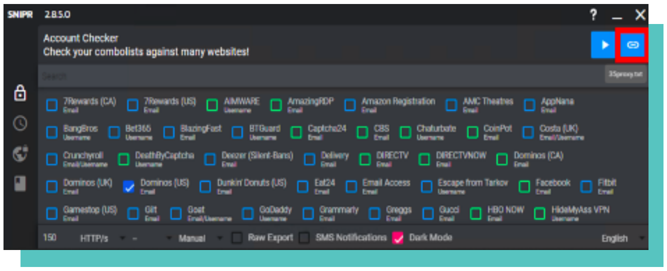
- **Vertex** requires users to supply a list of credentials and proxy servers, similar to Sentry MBA. Although the software is apparently still regularly used and advertised on carding and cracking sites, it's not as popular as Sentry MBA, and has different functionality.



Threads: 50
Timeout: 20
☑ Sound on Crack
☑ Minimize to Mini Vertex
☑ Remember Settings
☑ Check for Updates
☑ Confirm Exit
□ Brazzers
□
□ Uploaded
● Backwards ○ Forwards
*Requires E-Mails
Users: 1/207108
Passes: 0/0
Cracked: 0
Status: Idle...

Figure 23: Vertex tool user interface

- **Account Hitman** is not specifically a credential validation tool, but the software requires credential lists and proxy server lists to attack website login portals, similar to Sentry MBA and Vertex. The help guide, built into the program, likely appeals to less-technically advanced users; Account Hitman will probably continue to be a predictable choice for novice threat actors.

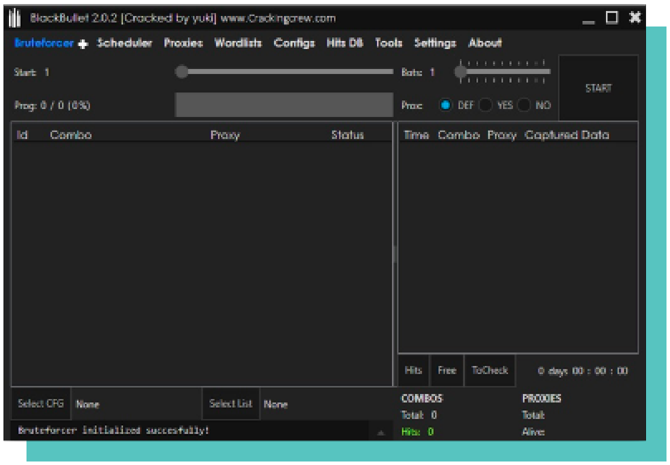


Account Checker
Check your combolists against many websites!

□ 7Rewards (CA) Email □ 7Rewards (US) Email □ AIMWARE Username □ AmazingRDP Email □ Amazon Registration Email □ AMC Theatres Email □ AppNana Email
□ BangBros Username □ Bet365 Username □ BlazingFast Email □ BTGuard Username □ Captcha24 Email □ CBS Email □ Chaturbate Username □ CoinPot Email □ Costa (UK) Email/Username
□ Crunchyroll Email/Username □ DeathByCaptcha Username □ Deezer (Silent-Bans) Email □ Delivery Email □ DIRECTV Email □ DIRECTVNOW Email □ Dominos (CA) Email
□ Dominos (UK) Email ☑ Dominos (US) Email □ Dunkin' Donuts (US) Email □ Eat24 Email □ Email Access Email □ Escape from Tarkov Username □ Facebook Email □ Fitbit Email
□ Gamestop (US) Email □ Gilt Email □ Goat Email/Username □ GoDaddy Username □ Grammarly Email □ Greggs Email □ Gucci Email □ HBO NOW Email □ HideMyAss VPN Username
150 HTTP/s - Manual □ Raw Export □ SMS Notifications ☑ Dark Mode English

Figure 24: SNIPR tool user interface

- **SNIPR** was created by a threat actor known as PRAGMA. The tool has been around since April 2017, functioning similarly to Sentry MBA. SNIPR is installed with a variety of pre-built configurations for popular sites, including requested URLs, user agent strings, data capturing form requests, and the correct order of authentication. There's also an in-built mechanism for public proxy scraping or the ability to import specified lists.



Start: 1
Bots: 1
Prog: 0 / 0 (0%)
Prox: ● DEF ○ YES ○ NO
0 days 00 : 00 : 00
Select CFG None
Select List None
COMBOS Total: 0 Hits: 0
PROXIES Total: Alive:

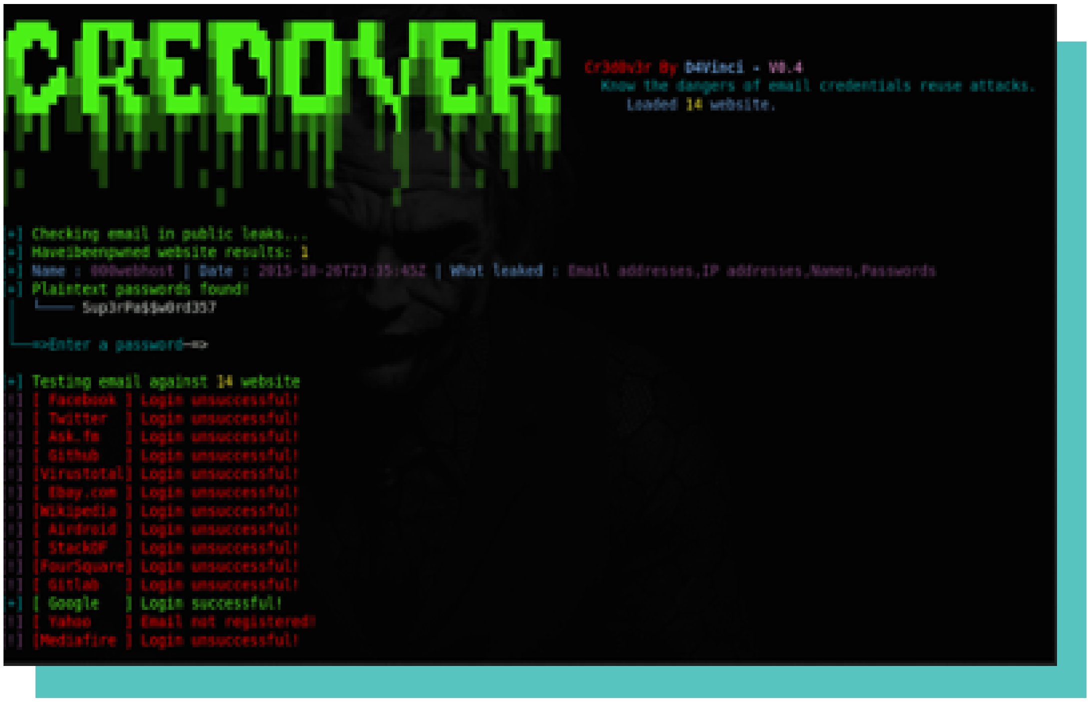
```
Bruteforcer initialized succesfully!
```

Figure 25: Brute-force user interface in BlackBullet

- **BlackBullet** is an increasingly popular tool, created by the threat actor "Ruri" and, later, released as a cracked version by "Yuki" and "Crank." A BlackBullet user is required to list username and password combinations to try on a web application and a list of proxy servers. This counters organizations' attempts to deter credential stuffing when they limit the number of attempts an IP address can make to automate account validation.

TOOLS OF ANOTHER TYPE

Just gaining access to accounts that have reused credentials is not always the end goal. These accesses can be used as pivot points to access even more sensitive information. Take, for example, the Cre3dov3r tool, which searches for public leaks related to any specified email address; if passwords are identified, the tool checks seven popular websites—including GitHub and Stackoverflow—to see if the credentials are valid or whether CAPTCHA is blocking access.



```
CREDOVER        Cr3d0v3r By D4Vinci - V0.4
                  Know the dangers of email credentials reuse attacks.
                     Loaded 14 website.

[+] Checking email in public leaks...
[+] Haveibeenpwned website results: 1
[+] Name : 000webhost | Date : 2015-10-26T23:35:45Z | What leaked : Email addresses,IP addresses,Names,Passwords
[+] Plaintext passwords found!
 │  └──── Sup3rPa$$w0rd357
 │
 └──=>Enter a password=>

[+] Testing email against 14 website
[!] [ Facebook ] Login unsuccessful!
[!] [ Twitter  ] Login unsuccessful!
[!] [ Ask.fm   ] Login unsuccessful!
[!] [ Github   ] Login unsuccessful!
[!] [Virustotal] Login unsuccessful!
[!] [ Ebay.com ] Login unsuccessful!
[!] [Wikipedia ] Login unsuccessful!
[!] [ Airdroid ] Login unsuccessful!
[!] [ StackOF  ] Login unsuccessful!
[!] [FourSquare] Login unsuccessful!
[!] [ Gitlab   ] Login unsuccessful!
[+] [ Google   ] Login successful!
[!] [ Yahoo    ] Email not registered!
[!] [Mediafire ] Login unsuccessful!
```

Figure 26: Cr3dOv3r screenshot of the tool in use posted on blog article (Source: kitploit[.]com)

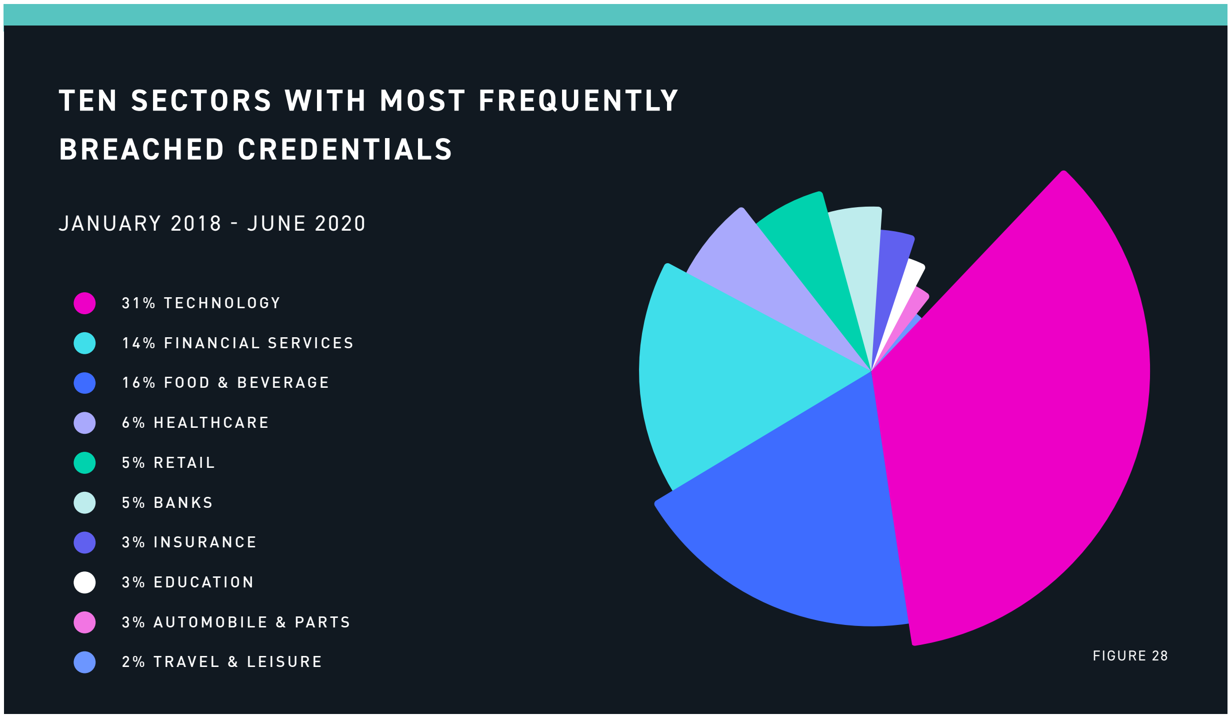
Although not a tool by itself, a code repository can be a particularly lucrative way to kick off ATO, if it contains access keys or other secrets that can provide access to accounts holding even more sensitive data. As outlined in the book *Hunting Cyber Criminals* [6] , several high-profile breaches have resulted from attackers brute-force cracking developer accounts on GitHub. Back in November 2019, the Photon team actually did a capture the flag (CTF) workshop that focused on this very topic: How an attacker can use open-source tools to take advantage of sensitive information inadvertently exposed on code-sharing repositories. (A recap of that event can be found here, and we also have a GitHub repository here.)

[6] Vinny Troia, Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques, Indianapolis: John Wiley & Sons, Inc, 2020.

HITTING WHERE IT HURTS: ATO AND ORGANIZATIONS

Of the 15 billion credentials in our repository, most belong to consumer accounts. We've given plenty of examples already: banking, streaming, personal VPNs. But of course, consumers aren't the only casualties when it comes to ATO. We performed some analysis of the types of alerts we've sent to our clients, to better understand the impact on organizations.

Just over the past 1.5 years, we've identified and alerted organizations to more than 27 million credentials being exposed; 27,339,059, to be exact. This includes usernames with passwords, and usernames on their own. As you can see in Figure 28, technology companies' credentials represented 31 percent of the top ten sectors, followed by food-and-beverage and financial services, at 16 percent and 14 percent, respectively.



TEN SECTORS WITH MOST FREQUENTLY BREACHED CREDENTIALS

JANUARY 2018 - JUNE 2020

FIGURE 28

We used this data to break down the average number of exposed credentials per organization, and found that a single food and beverage organization, on average, had a whopping 87,352 credentials exposed. Education and technology organizations came in a respective second and third, with an average of just under 48,000 exposed credentials per organization.

Sure, those numbers are huge, but it's important to remember that they don't all represent legitimate, active credentials. It's inevitable that a substantial portion are expired, or belong to former employees or legacy systems. Regardless, this gives you a sense of the sheer impact that data breaches can have on just one organization. It's unlikely that many of an organization’s exposed credentials will lead to actual ATO, but each exposure ups the chances, and the ramifications can be serious.

The fallout from a credential breach extends beyond an organization, to its customers. The relevant accounts can hold (or have access to) incredibly sensitive information. Going back to our 15-billion credential repository, we found that more than 2 million of them contained email addresses and usernames related to departments that deal with sensitive information—think addresses like invoice@companyname.com or billing@companyname.com.

AVERAGE CREDENTIALS PER ONE ORGANIZATION PER SECTOR

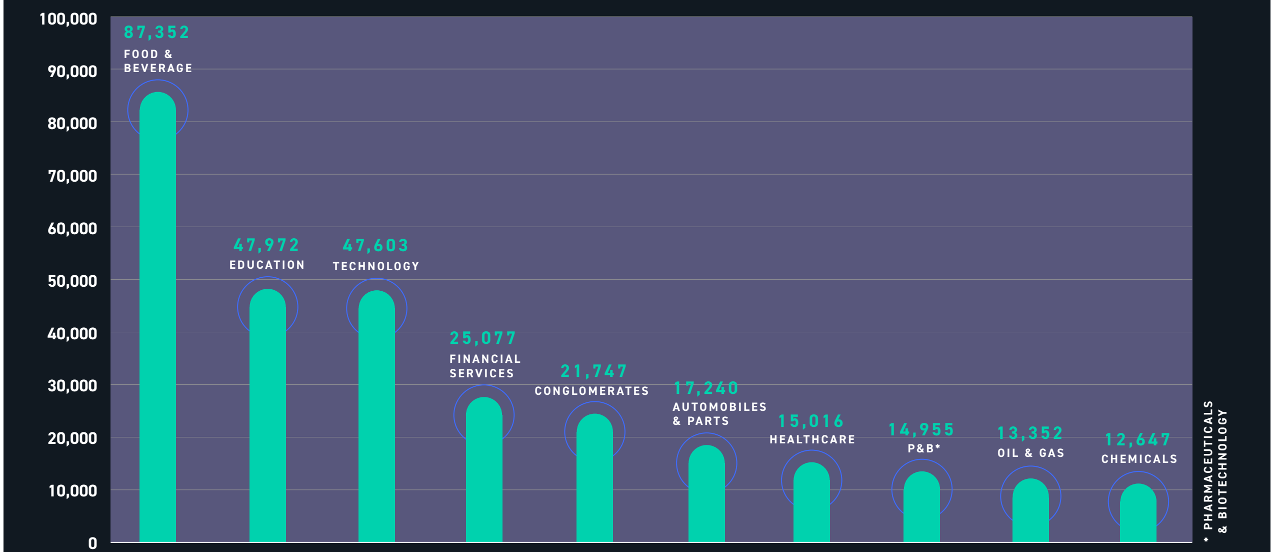


FIGURE 29

Email addresses containing “invoice” or “invoices” were by far the most common, accounting for 66 percent of those 2 million credentials. “Partners” and “payments”were tied for second place, both with 10 percent. Just imagine the type of data sitting in accounting inboxes! An attacker who gets their hands on credentials for valid accounts could inflict untold damage: logging in to internal databases, exfiltrating sensitive data or launching social-engineering attacks (e.g. business email compromise).

Of course, not all credentials are alike. We had a look at the various types of password hashes that have been exposed, to understand how they had been stored. The most popular two were MD5 and SHA1, contributing more than 80 percent of the hashed passwords. Although MD5 and SHA1 hashing algorithms provide more security than plaintext (aka unencrypted) passwords, cybercriminals can still find ways to convert hashed passwords to plaintext by using pre-computed hashes of large word lists or rainbow tables.

This risk can be circumvented by implementing a salt: a random string of characters that can be used in conjunction with the user's password before applying the hashing function. By deploying a dynamic salt, where a random string of characters is generated for each user and concatenated with the user's password, the chance of attackers being able to reverse the hash becomes significantly lower.

However, the vast majority of collected credentials (between 80 and 90 percent) weren't even hashed. This means they were either:

1. Initially stored in plaintext
2. Subsequently cracked by threat actors

With a (un)healthy circulation of plaintext and easy-to-crack hashed passwords, attackers will find brute-force cracking and credential stuffing a virtual cakewalk.

FREQUENCY OF MOST COMMON SENSITIVE TERMS IN BREACHED USERNAMES

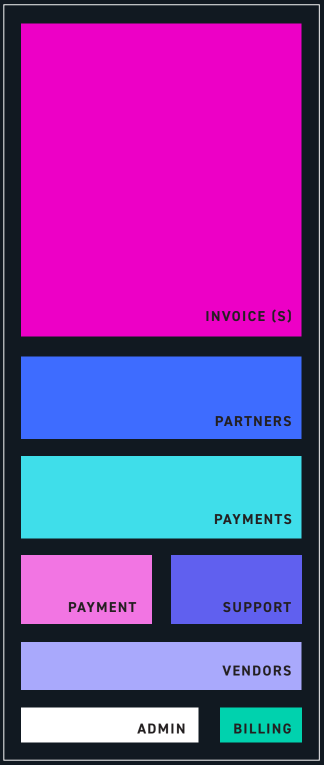


FIGURE 30

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

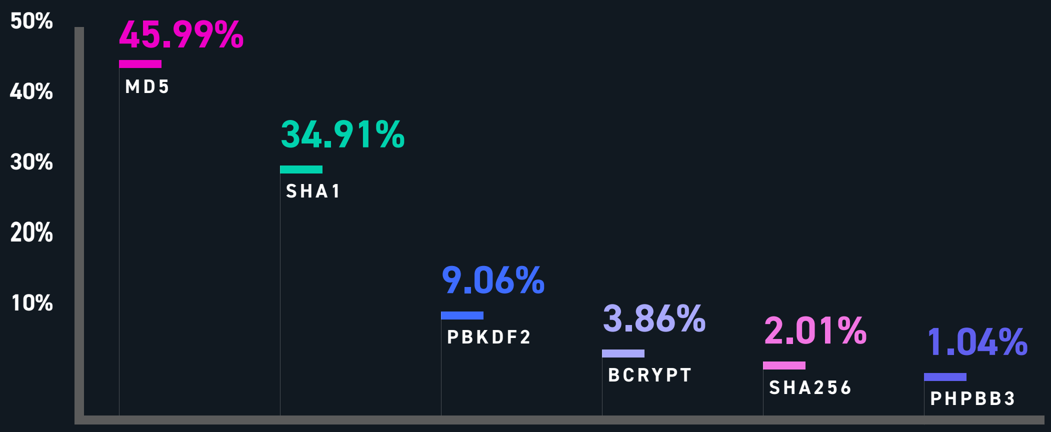


FIGURE 31

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.

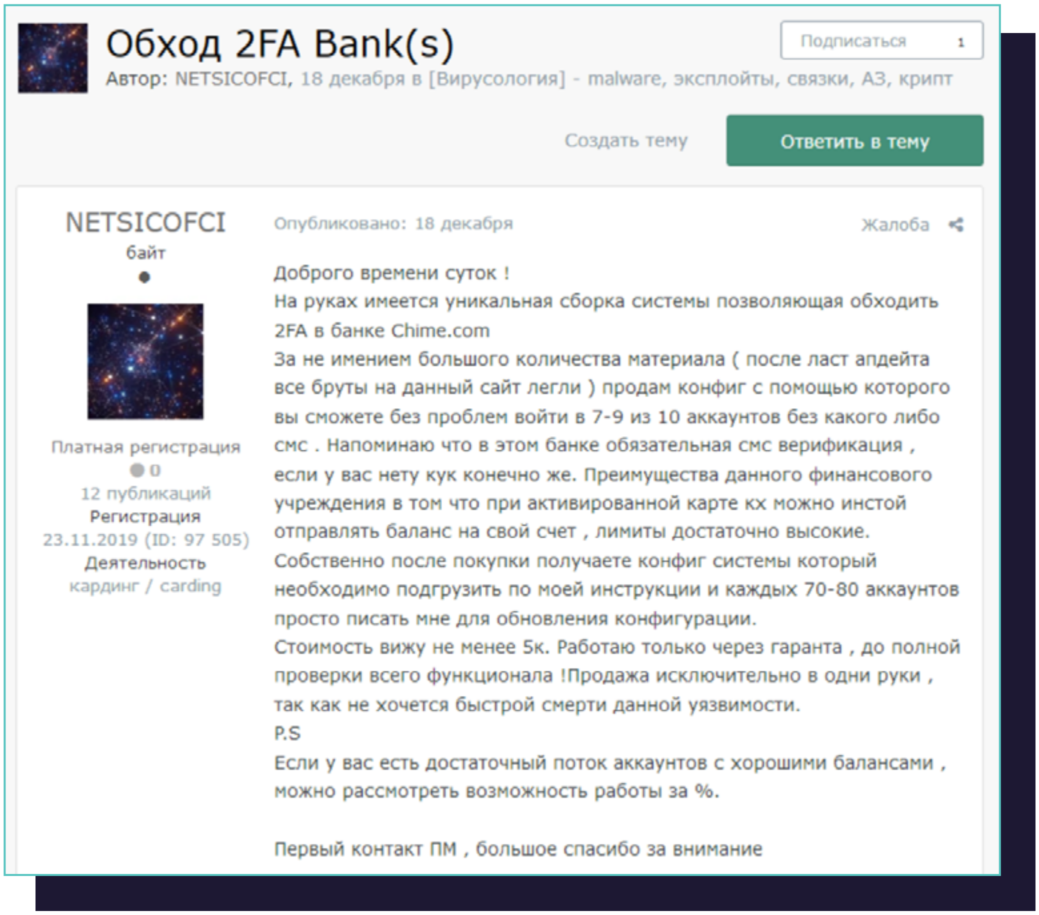
Other attacks that target SMS-based authentication include SS7 hijacking, which involves exploiting a weakness in Signaling System No 7, allowing attackers to intercept and eavesdrop on data, texts, and locations of a mobile device, perform man-in-the-middle attacks, and use tools like "Mureana". It's 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/



Обход 2FA Bank(s)

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

NETSICOFCI
байт
●
Платная регистрация
● 0
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 кх 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.

- Monitor for leaked credentials of your customers, which can enable you to respond proactively. Consider alerting any customers that have been involved in a breach, and prompting them to reset their password/s if they've reused credentials.

- Deploy an inline Web Application Firewall. Commercial and open-source web application firewalls, like ModSecurity, can identify and block credential stuffing attacks.

- Increase user awareness. Educate your staff and consumers about the dangers of using corporate email addresses for personal accounts, as well as reusing passwords.

- Maintain awareness of credential stuffing tools. Keep an eye on the development of OpenBullet and others, and monitor how your security solutions are protecting against evolving capabilities (such as bypassing CAPTCHA).

- Implement multi-factor authentication that doesn't use SMS messages. This can help reduce ATO, but should be balanced against the friction (and cost) it can cause. The Photon Research team's report Two-Factor In Review: A technical assessment of the most popular mitigation for account takeover attacks details the technologies involved with 2FA, attacks against the solution, and ways to mitigate.

About Digital Shadows

Digital Shadows minimizes digital risk by identifying unwanted exposure and protecting against external threat. Organizations can suffer regulatory fines, loss of intellectual property, and reputational damage when digital risk is left unmanaged. Digital Shadows SearchLight™ helps you minimize these risks by detecting data loss, securing your online brand, and reducing your attack surface.

To learn more and get free access to SearchLight™, visit
www.digitalshadows.com

London, UK **San Francisco, CA** **Dallas, TX**

Authors: Digital Shadows Photon Research Team

digital shadows_