

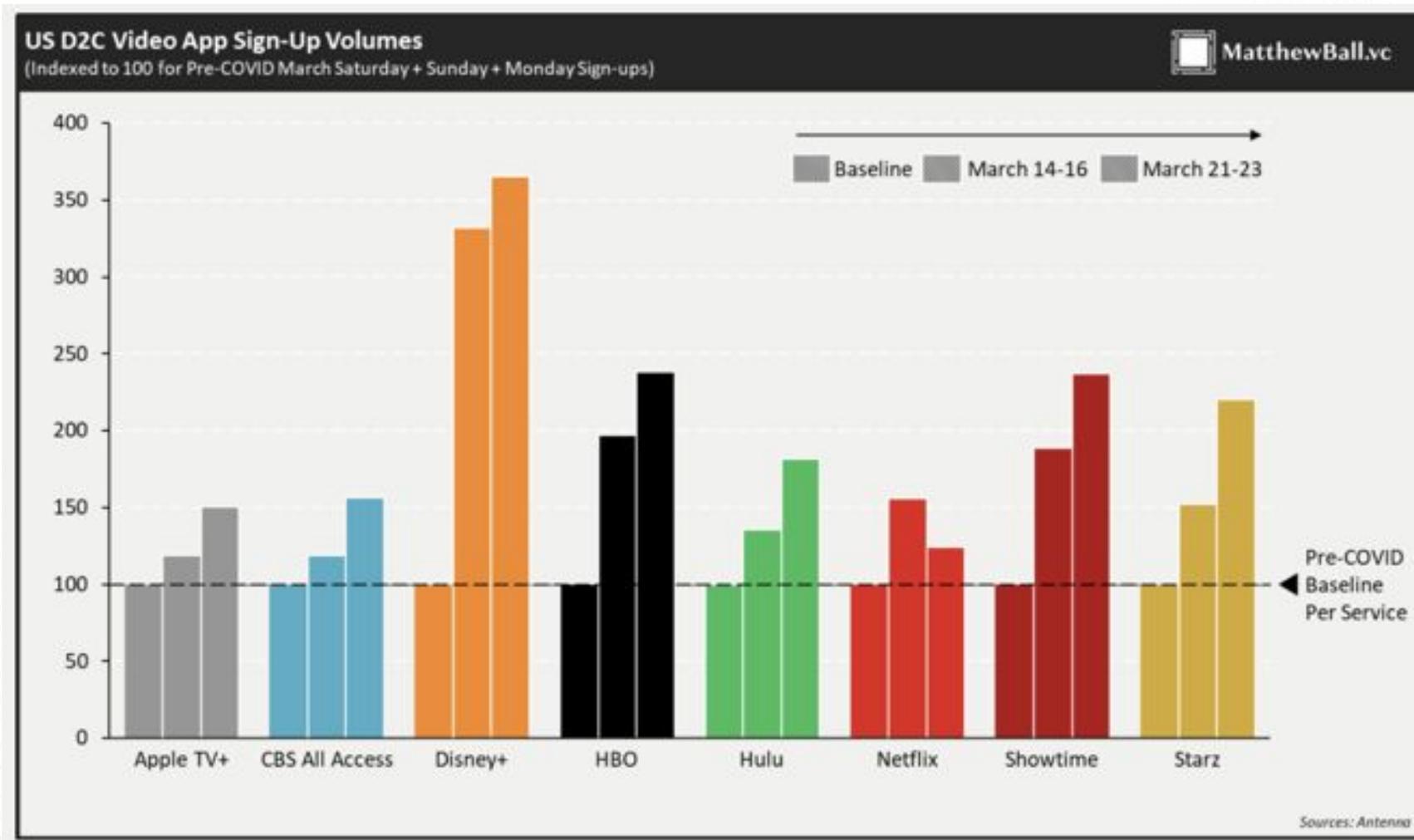
Data Doesn't Lie

Media Industry Full of Credential Stuffing Attacks

Patrick Sullivan,
Chief Technology Officer Security Strategy



OTT Consumption is Surging as People Stay Home



Peak Traffic on Akamai's Edge Platform Doubled Y/Y

82 Tbps

March 2019

167 Tbps

March 2020

WANTED BY THE FBI

BANK ROBBERY

UNLAWFUL FLIGHT TO AVOID CONFINEMENT - ARMED ROBBERY

Photograph taken October 24, 1945

Photograph taken April 3, 1945



WILLIAM FRANCIS SUTTON

Piracy Targeting OTT Monetization

The Account Takeover Kill Chain

Credential Supply Chain
Acquire credentials



- Breach or skim site to steal credentials
- Phish website users
- Purchase list of stolen credentials on dark web

Credential Acquisition

Bot
Threats taking advantage of automation to perform large scale **Credential Stuffing**



- Leverage a botnet to automate validation

Weaponization



- Validate credentials against target website

Delivery

Human
Threats from human fraudsters performing targeted **Account Take Over** attacks



- Use compromised account credentials to login

Exploitation

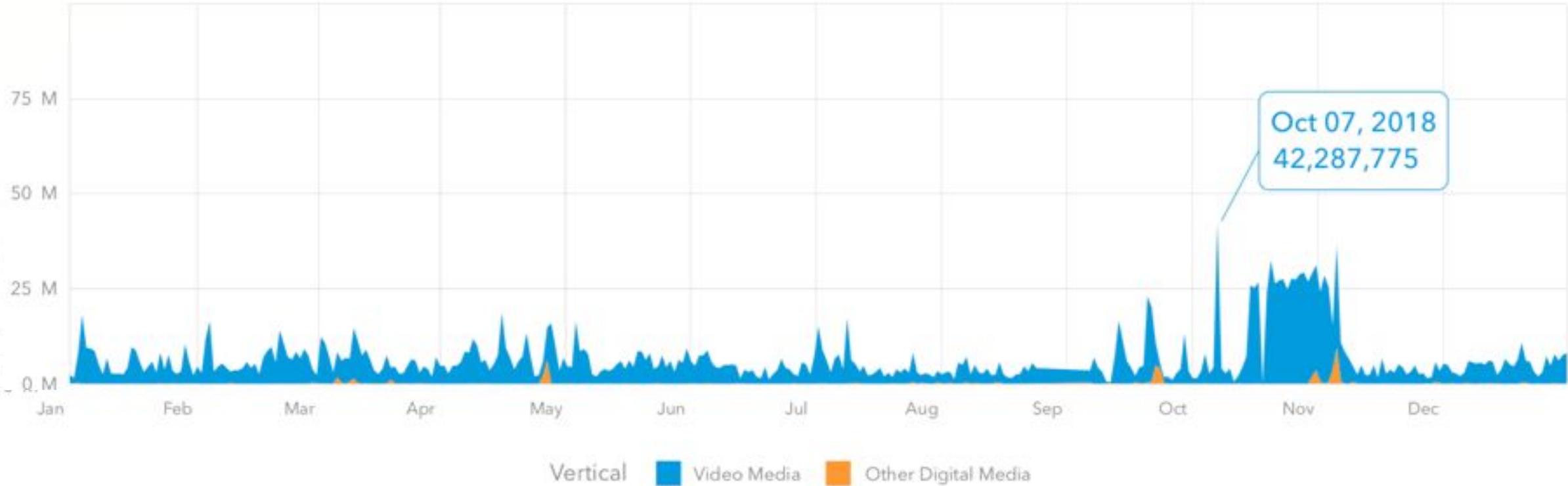


- Perform fraudulent actions using compromised account

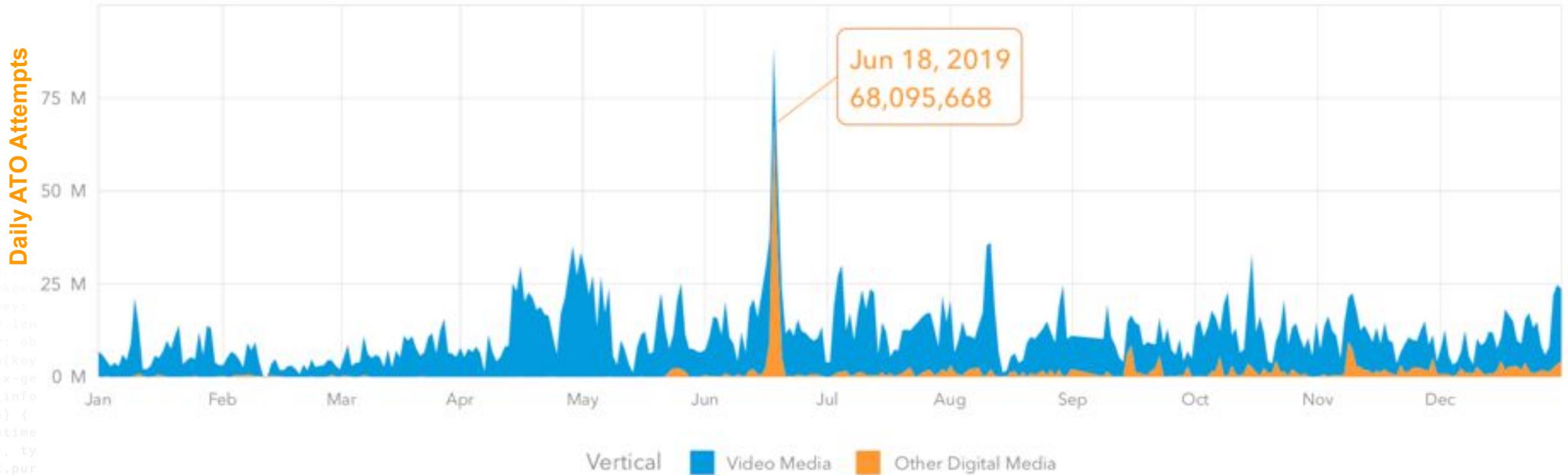
Action

2018: Video Media Sees More Attacks than FiServe

Daily ATO Attempts



2019: Video Media Attacks Jump 63% YoY



Why is Media so Attractive to Attackers?

★All in 1★ Netflix+ 2 Sling +2 Hbo+ 2 Hulu + 2 Xfinity+ 2 Nord vpn+ 2 Ipvnish + 30Best Porn sit

Sold by **excellence** - 2706 sold since April 22, 2019 **Vendor Level 5** **Trust level 5** **D** 671 (4.95)

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

All in1 Netflix Sling Hbo Hulu Xfinity Nord vpn Ipvnish 30 Best Porn Plus Bonuses - 1 days - USD + 8.99 / order

Purchase price: **USD 0.99**

Qty: [Buy Now](#) [Buy Now](#) [Buy Now](#) [Queue](#)

0.000113 BTC / 0.021167 LTC / 0.015539 XMR

▶ 2 X ▶ ★ XFINITY COMCAST PREMIUM + 2 X Nord vpn + Bonus ★ Premium Account ▶ Insta

Sold by **excellence** - 779 sold since April 22, 2019 **Vendor Level 5** **Trust level 5** **D** 671 (4.95)

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

Internet only X 2 nord vpn - 1 days - USD + 0.75 / order

Internet only X 2 nord vpn - 1 days - USD + 0.75 / order

2 x Internet only x1 100 to 140 channels and internet plus 5 x nord vpn - 1 days - USD + 1.25 / order

2 x Internet only x1 140 channels and internet plus 5 nord vpn - 1 days - USD + 1.75 / order

2 x Internet only x1 210 channels and internet plus 5 nord vpn - 1 days - USD + 2.25 / order

2 x Internet only x1 125 to 260 channels voice and internet plus 5 nord vpn - 1 days - USD + 2.75 / order

[Description](#) [Feedback](#) [Refund policy](#)

NETFLIX Netflix HD 1 Year \$786	twitch Prime Twitch Prime + Amazon Prime \$3.00	NETFLIX NETFLIX WITH LIFETIME WARRANTY \$35.00	NETFLIX Netflix Premium x10 \$4.00
amazon prime video Amazon Prime 1 Month \$1.78	hulu Hulu Premium \$6.00	hotstar Hotstar Premium \$8.00	HBO NOW HBO Now \$7.00
NETFLIX Netflix UHD 1 Year \$1115	Disney+ Disney+ (US) \$2.05	SONY LIV Sony Liv Premium Account Sony Liv Premium [1 Year Subscription] \$5.00	ALT BALAJI AltBalaji Premium [YEAR] \$5.00

STREAMING SERVICES ACCOUNTS

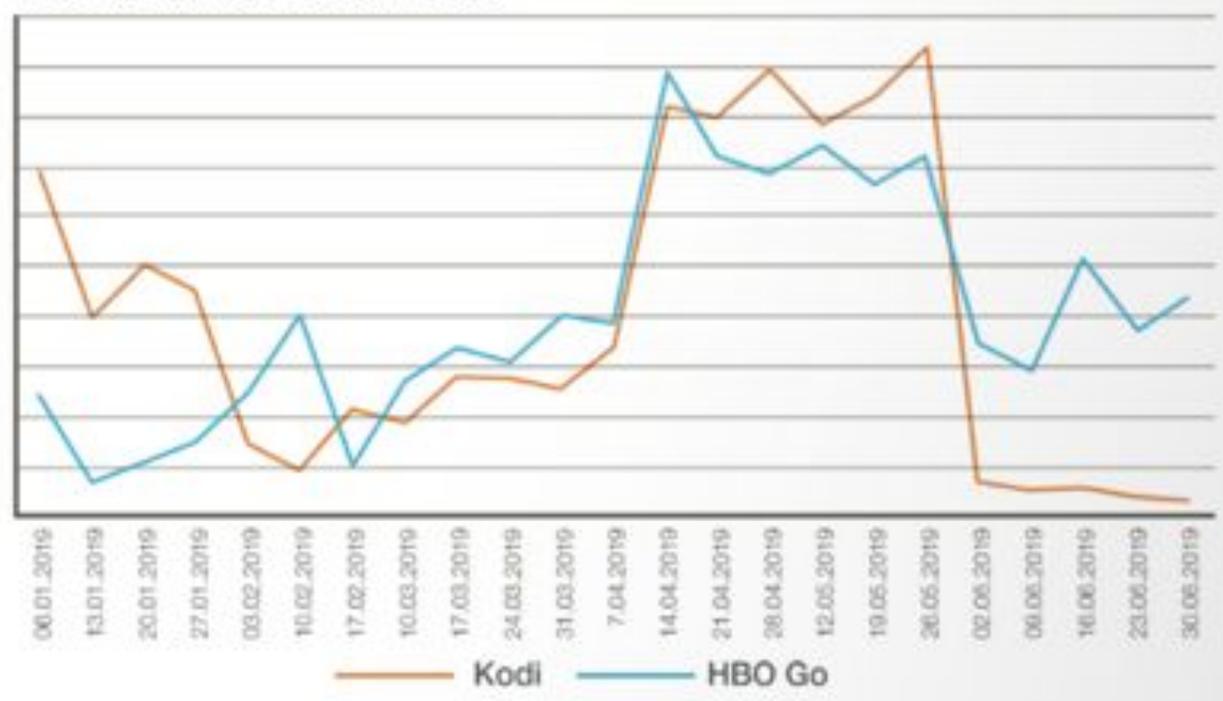
Disney+ Paid Account Remaining accounts: 8 0.001 BTC Buy	HBO Paid Account Remaining accounts: 4 0.001 BTC Buy	Netflix Premium Plan Remaining accounts: 3 0.001 BTC Buy	HULU (No ads) + Live TV Remaining accounts: 12 0.001 BTC Buy	Spotify Premium Account Remaining accounts: 2 0.001 BTC Buy	Apple TV+ Paid Account Remaining accounts: 10 0.001 BTC Buy	All services Remaining accounts: 2 6-PACK 0.005 BTC Buy
--	--	--	--	---	---	---

All accounts are 3 years paid
We send you a complete NEW account for the service selected
0% problems, all our accounts are legal, you can use it FOREVER
Guaranteed | ©2020

How Common is it?

HBO Go: Kodi traffic > legal traffic

HBO Go and Kodi Traffic 1H 2019

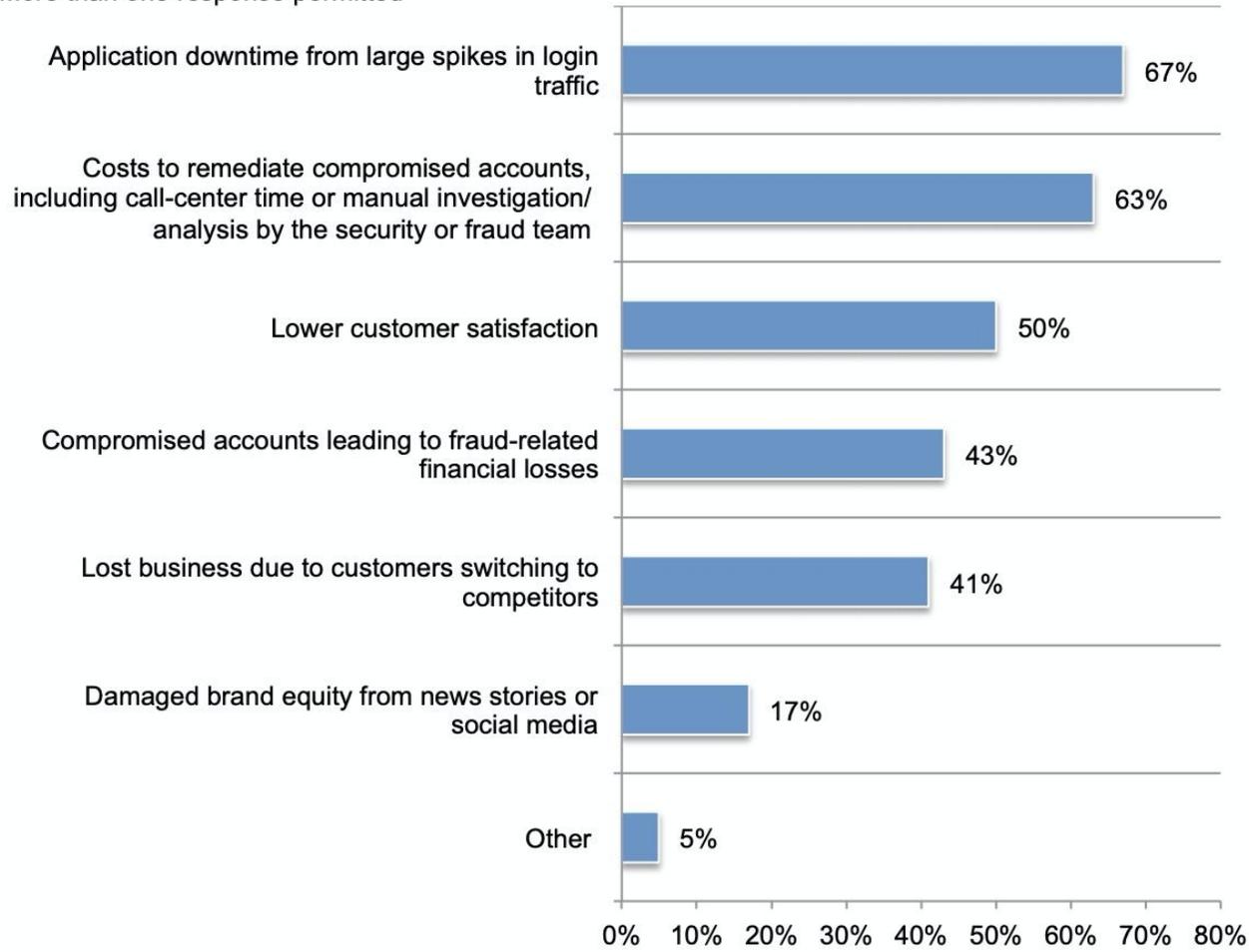


<https://www.sandvine.com/blog/the-state-of-affairs-a-spotlight-on-video-and-television-piracy-worldwide>

Impact of Credential Stuffing on the Business

Figure 13. Negative consequences resulting from a credential stuffing attack

More than one response permitted



Source: Ponemon Institute Total Business Impact of Credential Stuffing

Top Attack Sources by Country

SOURCE AREA	2019 TOTAL	YOY CHANGE 2018 TO 2019
United States	1,106,075,259	162%
France	393,053,557	407%
Russia	242,801,831	67%
Netherlands	215,858,077	217%
Germany	181,107,515	128%
Brazil	152,389,083	71%
India	150,954,578	-37%
Singapore	137,037,227	142%
United Kingdom	131,931,328	42%
Indonesia	97,448,973	234%

Top Attack Targets by Country

TARGET AREA	2019 TOTAL	YOY CHANGE 2018 TO 2019
India	2,394,309,395	114%
United States	1,421,345,721	22%
United Kingdom	124,273,711	49,185%
France	75,797,079	3,965%
Germany	66,864,153	561%
Italy	38,248,972	2,870%
Australia	29,949,976	-10%
Finland	6,557,245	606%
Switzerland	2,268,087	162%
China	1,248,276	-95%

Piracy Targeting Monetization Phase

The Account Takeover Kill Chain

Credential Supply Chain
Acquire credentials



- Breach or skim site to steal credentials
- Phish website users
- Purchase list of stolen credentials on dark web

Credential Acquisition

Bot
Threats taking advantage of automation to perform large scale **Credential Stuffing**



- Leverage a botnet to automate validation

Weaponization



- Validate credentials against target website

Delivery

Human
Threats from human fraudsters performing targeted **Account Take Over** attacks



- Use compromised account credentials to login

Exploitation

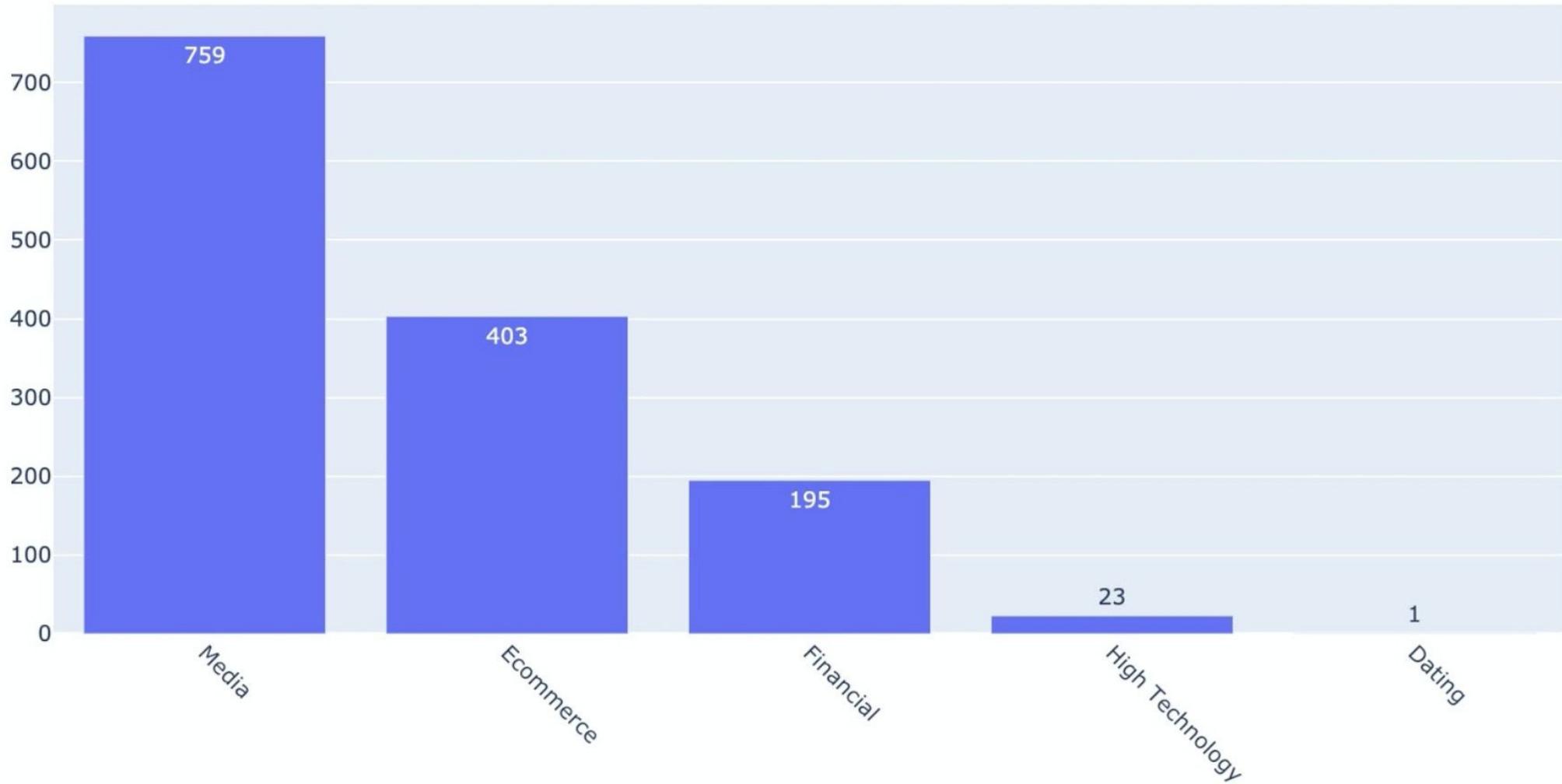


- Perform fraudulent actions using compromised account

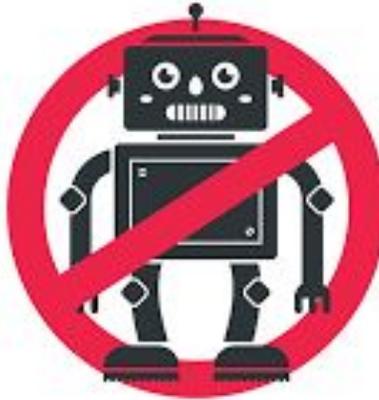
Action

CDN-Scale View of Phishing for Customer Creds

of Detected Phishing URLs



Summary



Draft (2nd) NIST Special Publication 800-207

Zero Trust Architecture