INITIAL ACCESS BROKERS

An Excess of Access

Digital Shadows Photon Research Team

digital shadows_

INITIAL ACCESS BROKERS: AN EXCESS OF ACCESS

EXECUTIVE SUMMARY

The past decade has thrown significant changes at our lives and work, partly propelled by technological advances. Remote-access software, virtual private networks (VPNs), and other innovations have steadily swelled the remote workforce, fostering a sense of trust in secure access to private networks—whether you're in a cottage in Croatia or a villa in the Maldives. With the onset of the COVID-19 pandemic, the adoption of those technologies jumped suddenly, exponentially, and threat actors have been quick to find ways to exploit network access tools.

Digital Shadows' Photon Team has been tracking these threat actors since 2016, and we're now witnessing a "perfect storm": a dramatic increase in remote working and an incredibly successful ransomware monetization model. Initial access brokers (IABs) are among the threat actors benefitting from this situation, which has elevated their status in the cybercriminal underground to critical.

IABs attempt to gain access to the networks of vulnerable organizations, often through remote desktop protocol (RDP) or compromised Citrix gateways. They attack organizations in all industry verticals and geographies, then sell the network "accesses" they've attained, predominantly on criminal forums. The buyers then have a conduit to unleash malicious activity on the victims' networks.

IABs' rise in popularity follows the trend of lowered barriers to entering the world of cybercrime; as brokers, they're doing the technical, dirty work for others. In 2020 we saw more listings, more threat actors, and higher prices than we've observed before. To better understand this phenomenon and what it means for security practitioners, we analyzed more than 500 access listings between 1 Jan 2020 and 31 Dec 2020, and made some useful discoveries:

Overview of Key Findings

- Listings for initial access increased during 2020 as the pandemic disrupted business processes, and particularly for VPN access, which flourished off the back of increased remote working trends.
- The market of IABs is reaching full potential as these threat actors are increasingly able to sell a substantial number of accesses, to all kinds of organizations—regardless of size, industry, country, or revenue.
- The average selling price of initial access to a network is $7,100. Price is based on the organization's revenue, type of access sold, and number of devices accessible.
- RDP access was the most common type listed (17 percent) and it commanded the highest average price ($9,800).
- The most targeted industries were retail (10 percent of IAB incidents), financial services (9 percent), and technology (7 percent). Average listings were worth $4,712; $6,619; and $13,607, respectively.
- North America was the most targeted geography, representing 39 percent of network access listings. Europe followed, with 15 percent, and then Asia and the Middle East with 9 percent each.

BEHIND THE BROKER: MARKETING INITIAL ACCESS

BROKERING BACK IN THE DAY

Digital Shadows has tracked the sale of access to systems since the practice first began making ripples in the cybercriminal underground. Initial access brokership isn't a business model spun off the COVID-19 pandemic; its popularity and profitability have simmered beneath the surface since the early days.

On popular Russian-language cybercriminal forum Exploit, accesses[1] for FTP servers, dedicated servers, and cPanel first started to be advertised in the Accesses section shortly after the site's founding, in 2005. On the widely used Russian-language forum XSS, references in the Accesses section sprung up the same year the site was founded. The English-language RaidForums was predominantly a database trading service when it emerged in 2015, but in 2020 its Leaks Market section became the primary place for initial access advertising and trading. With the growing prevalence of IAB activity in 2020, forum owners restructured their platforms to make these listings more prominent.

Accesses sections have become increasingly central areas of cybercriminal forums and marketplaces, flooded with a supply of high- and low-value access credentials. We've also seen accesses traded in the Auctions section of Exploit, possibly to maximize profit and make offerings stand out from the crowd.

These days, IABs are increasingly antsy about their operational security (OPSEC). Looking back at old access listings on cybercriminal forums, you see bold threat actors who named their victims outright; this boosted revenue potential, because buyers knew exactly what they were getting access to. Now OPSEC is discouraging IABs from mentioning their victims (see "OPSEC upsets").

On top of this, IABs have expanded their range of offerings, moving on from low-value accesses to small companies to include a few highly valuable targets. The market now seems mature enough to offer various sizes, values, and prices. This illustrates the professionalization and democratization of cybercrime, which is becoming a practice increasingly available to everyone.

[1] Accesses are login details, credentials, or sensitive files from a particular organization or individual's machine, used to access a victim's systems/infrastructure, data, bank accounts, and/or other accounts.

WHO'S DOING THE DIRTY WORK?

What makes IABs distinct is their broad spectrum of sophistication and technical expertise. At the lower end we have brokers who are incapable of using the access they have, or unsure how to use it. Some may have obtained access to a control panel by trying a default credential—sadly, an effective tactic. IABs in this category aren't readily capable of completing the final stages of the attack and decide to sell the access.

Their lack of technical expertise doesn't make these actors any less of a threat. Because they're also less specialized, they tend to be customer agnostic and sell their accesses to the highest bidder: ransomware affiliates, nation-state actors, or anyone interested in fully exploiting the access. This also means that any company is a potential target for network compromise, regardless of size and geography (see the later sections on affected industries and regions).

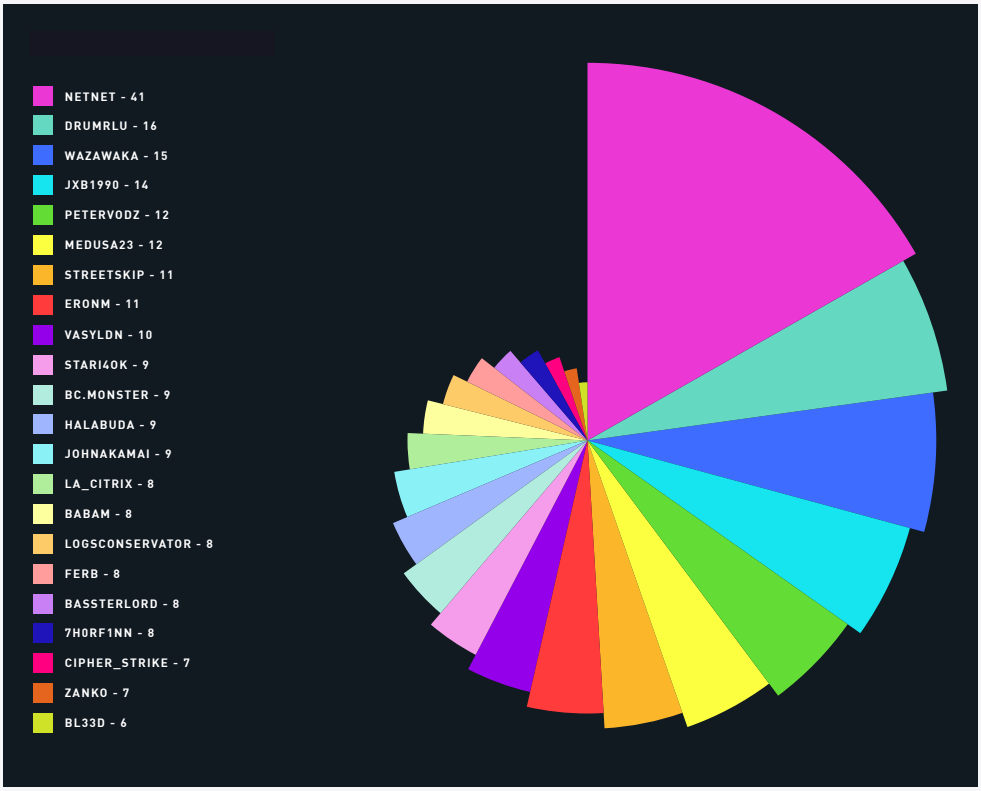

FIGURE 1: TOP ACTORS BY NUMBER OF LISTINGS (2020)

I am selling admin **access** to [redacted] dashboard, from a big Brazilian mining company. As you can see in the images below, you can use it to send e-mails, attach files, explore private documents and send whatever you want to board director members. It's a good option to distribute **ransomware**, I think.

Price: 1.25 BTC (escrow mandatory)
Details in PM.

FIGURE 2: EXAMPLE OF AN INITIAL ACCESS BROKER LISTING

EARNING TRUST AND SCREEN CRED

There's certainly no honor among thieves, which means reputations on criminal forums are vital. Weak trust in an IAB means they'll be less likely to orchestrate a successful sale of accesses at high prices, and will typically need to work through a guarantor. A single "downvote" can have considerable repercussions on an IAB's bottom line or long-term career viability.

To gain trust and credibility, IABs need to prove their reliability and value before they can advertise their goods or charge high prices.

Cybercrime may not seem rooted in integrity, but its markets mirror the real world. Just like you'd be skeptical of an anonymous user posting for the first time on Reddit or Quora, most criminal forum/marketplace users are skeptical of IABs who are completely new to the scene. Only those with a long history of reliable and valuable listings are considered trustworthy enough to do business with.

OPSEC UPSETS

IABs have the extremely difficult task of providing enough information to make a listing attractive, but not so much that it will tip off security researchers. It's relatively well known in the cybercriminal underground that security researchers maintain a presence on most forums, so IABs have adopted some OPSEC practices to make the identification of victims difficult.

Organization names are replaced with vague details, such as company revenue, industry, country, staff size, Alexa rankings of web domains, stock tickers with certain letters obscured, and number of hosts on the compromised network. It's up to the shopper to triangulate the details and determine the value of access before making an offer.

As an example of security-savvy forum users and their OPSEC practices, in September 2020, a forum user advertised an RCE[2] vulnerability affecting a large bank in Chile, but redacted the bank name; as a reason for their caution, they cited a Twitter account (@Bank_Security) they claimed was actively alerting named victims to accesses being traded on the forum. The seller noted that "there is no place for people with high knowledge to live," when referring to the forum being full of "script kiddies".

Although naming the targeted victim can result in higher revenue and more interested buyers, basic OPSEC practices have become widespread among IABs, and the market has ultimately adapted to this security trend.

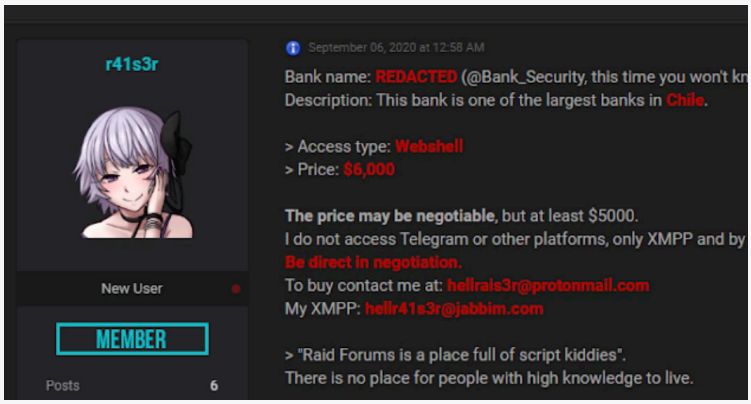

FIGURE 3: OBSCURING TARGET DETAILS

2020 VISION: THE RISE OF THE IAB

In the cyber-threat landscape, 2020 could be easily remembered as the year of ransomware. Not a single day passed without new ransomware operators and variants making headlines. Throughout the year, we also saw the emergence and widespread adoption of the "pay or get breached" model. This was characterized by attempts to turn the screw on ransomware victims to pay, by threatening to publish encrypted and exfiltrated data on data-leak dark-websites.

The ransomware gangs that formed (composed of tough competitors and partners) required a huge base of victims to infect. Enter the IAB in a starring role. Playing the middleman between targeted organizations and ransomware operators, the IAB worked hard to breach as many companies as possible and sell those access to the highest bidder.

Their part was so important to the ransomware business model that threat actors of all technical capabilities joined the effort to provide network accesses to ransomware operators. And by providing accesses to organizations of various sizes and industries, IABs greatly expanded the potential surface of attack for ransomware operators. The benefit for IABs? Profiting from highly lucrative ransomware operations without actually taking part in the extortion attempts. Take a look at their takings in 2020, below.

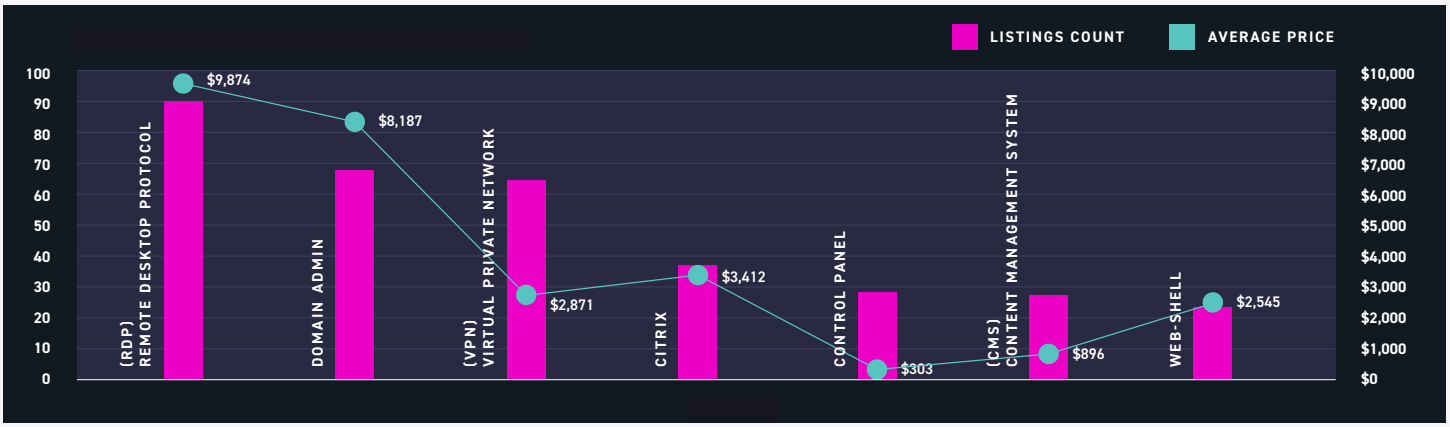

FIGURE 4: POPULAR ACCESS TYPES AND THEIR AVERAGE PRICES (2020)

[2] Remote code execution

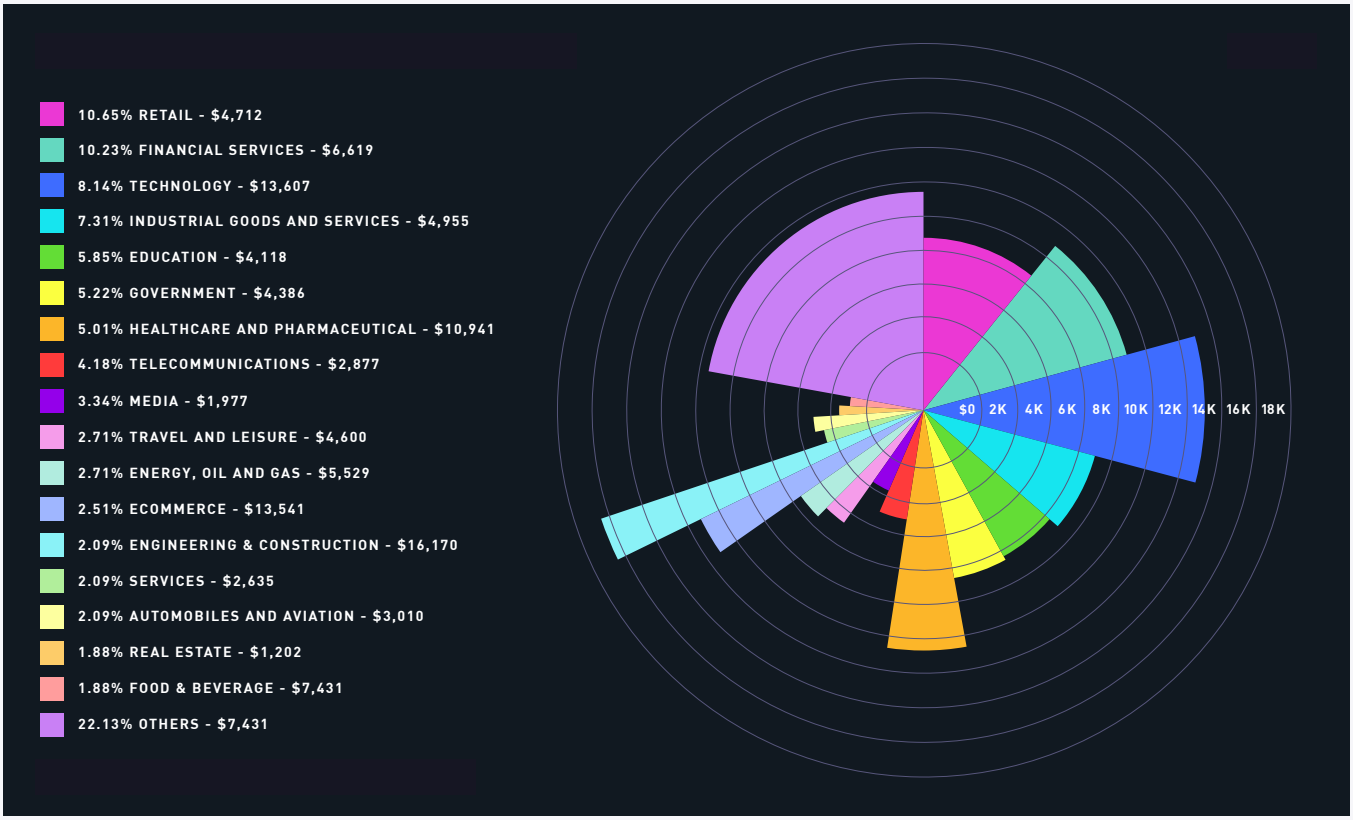

FIGURE 5: MOST TARGETED INDUSTRIES AND THE AVERAGE PRICES OF ACCESS (2020)

WHY SHOULD YOU CARE?

The professionalization of cybercrime has made ransomware operations extremely sophisticated and dangerous. Understanding the roles various actors play in the broad ransomware ecosystem is crucial to preventing and mitigating this serious threat, so we should all be striving for a deep knowledge of how IABs operate and how they interact with ransomware operators. Such insights can go a long way in avoiding the massive damages of a ransomware attack.

Since risk is calculated as the likelihood of an attack multiplied per its potential impact, it's frighteningly obvious that the risk posed by ransomware is more pressing than ever. Mitigation isn't easy, and having a dedicated in-house or outsourced cyber-threat intelligence (CTI) team can be extremely beneficial. They can set up monitoring programs across surface-, deep-, and dark-web forums and marketplaces, observing cybercriminal activity and quickly identifying relevant accesses. Those teams can then provide actionable and relevant information to the appropriate security teams, who will move on to patch and update the most sensitive assets at risk.

Detecting IAB offerings in a timely manner is crucial to buy time for prioritizing actions and preparing against potential attacks. And a useful tool here is one the IABs are using themselves: To sell accesses for a good price to ransomware operators, they often gather details (victim size, industry, revenue, country) from ZoomInfo, a company whose website features business-to-business data about global organizations. Those same details can also help CTI teams swiftly spot potential targets and mitigate threats.

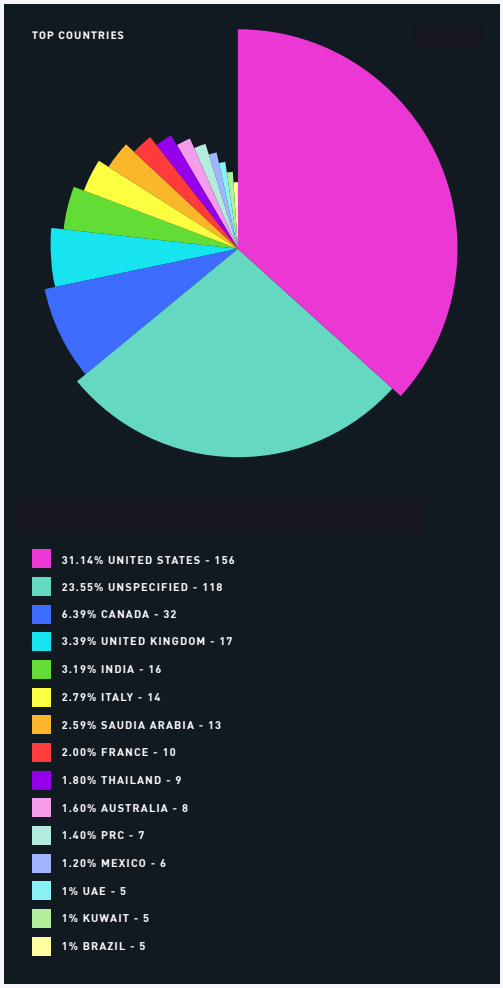

FIGURE 6: POPULAR REGIONS TARGETED BY INITIAL ACCESS BROKERS (2020)

2

MOST WANTED ACCESS TYPES

RDP

Average Price: $9,765
Popular Regions: North America, Europe
Popular Industries/Sectors: Education, healthcare and pharmaceuticals

What is it?

Remote desktop protocol is a popular protocol developed by Microsoft, which allows users to connect to a remote PC or server over the Internet or on a local network, granting full control over the accessed machine. In practice, RDP allows users to open and edit files, access tools, and control resources as if they were in front of the remote desktop computer.

In the age of COVID-19, RDP has become all too familiar to defenders and cybercriminals alike. Many organizations are using remote-access solutions to enable their employees to work effectively offsite, inviting cybercriminal RDP exploitation.

Selling RDP access is definitely not a new trend. RDP shops have sold RDP credentials for quite some time, but the move of ransomware operators from targeting individuals to targeting enterprises has enhanced RDP's value as an access type.

Actor SpotLight: bc.monster

"bc.monster" has been a consistent name in the IAB realm, offering various access types to organizations across a multitude of industry verticals. They joined the Exploit forum on 18 Jul 2019, and their early posts were brash, claiming to offer network access to US "companies with big data". bc.monster said they'd only work with forum members who had an existing presence in the threat landscape: no new or untrusted members.

Within the first month of purchasing their access to Exploit, bc.monster offered access to a water and wastewater company, a "new Energy Corporation", and a website belonging to a new airline. In 2020, bc.monster advertised RDP access to a Canada-based accountancy and business corporation, a US-based petroleum company, and a US-based engineering and construction company. Prices ranged from $1,400 to $4,000.

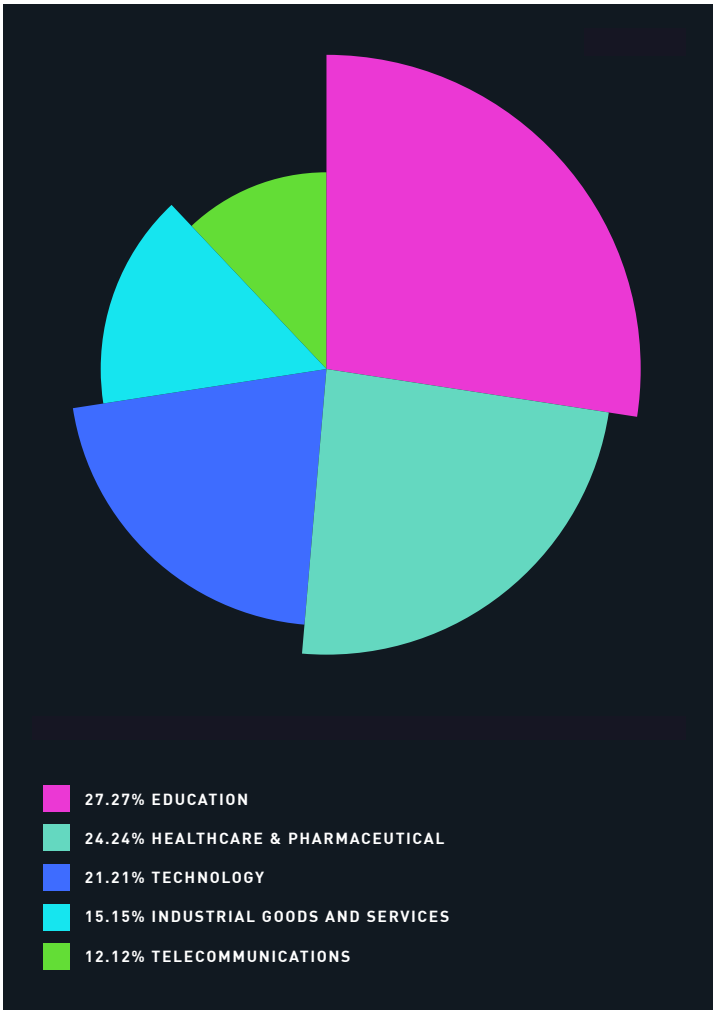

FIGURE 7: POPULAR INDUSTRIES TARGETED BY IABS SELLING RDP ACCESS (2020)

RDP

How do they get it?

RDP's exposure to the Internet is a recurring call of concern ringing through the security landscape. A quick search using publicly available tools can identify all the systems that are operating with RDP exposed to the Internet. Threat actors can then attempt to gain access through a brute-force attack that can bring success when weak credentials have been used—anyone heard the horror stories of RDP access being gained because the password was set to "admin" or "password"? IABs typically try such tactics first, as they require minimal effort and often prove effective[3].

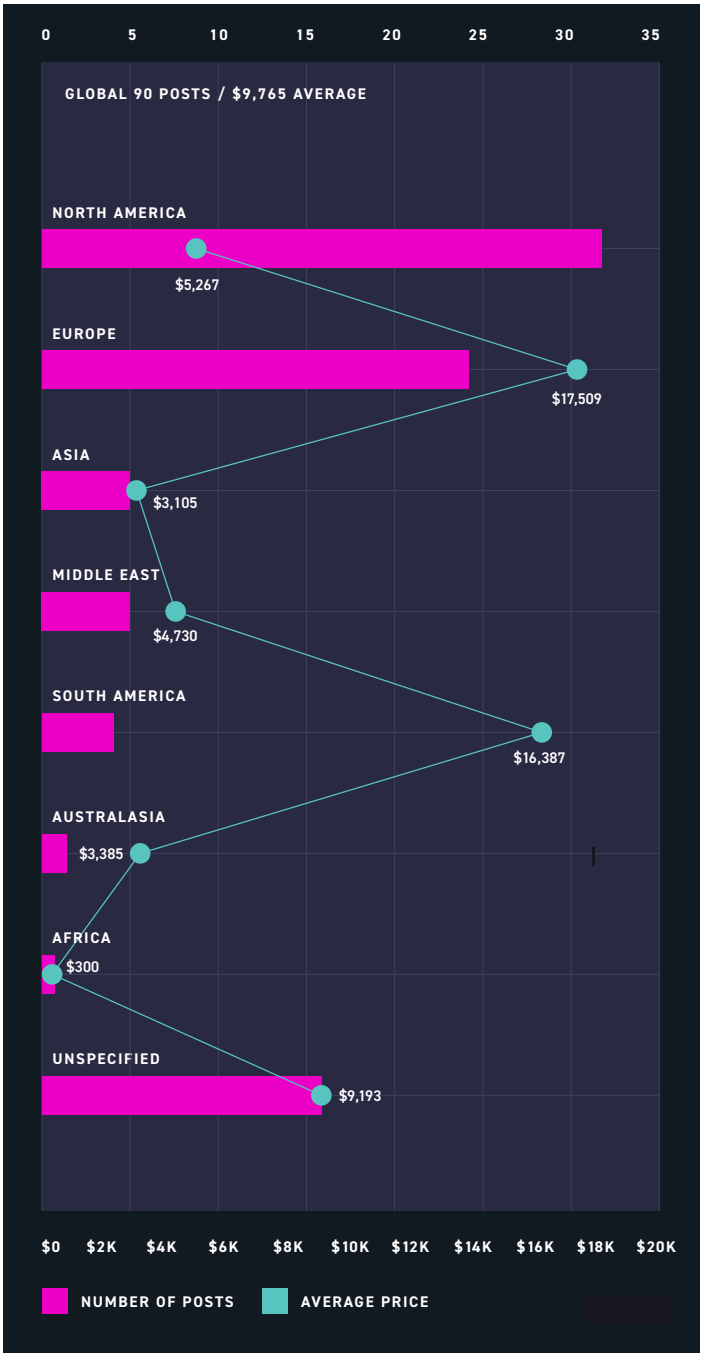

FIGURE 8: POPULAR REGIONS TARGETED BY IABS SELLING RDP ACCESS (2020)

How do threat actors use this access?

After buying RDP access from an IAB, a threat actor is blessed with a plethora of options. Ransomware actors are big RDP fans because it yields access to multiple hosts on a network, increasing the significance of a ransomware attack. According to FBI Special Agent Joel DeCapua, "RDP is still 70 to 80 percent of the initial foothold that ransomware actors use"—and he was only reflecting on the situation in early 2020. The pandemic has since opened up a treasure trove of new RDP opportunities.

A recent attack in the US state of Florida is the latest prominent real-world example of RDP weaponization. In an attack on the City of Oldsmar's water treatment system, the attacker reportedly gained control of the plant operator's computer. They manually edited the chemical levels of the water supply, briefly altering the plant's controls to change the water composition to toxic levels. Disaster was averted by the threat actor's technical unsophistication and the plant's water-composition controls, which immediately tipped off security teams.

[3] https://attack.mitre.org/techniques/T1021/001/, https://attack.mitre.org/techniques/T1563/002/, and https://attack.mitre.org/techniques/T1021/

VPN

Average Price: $3,389
Popular Regions: North America, Middle East
Popular Industries/Sectors: Retail, telecommunications

What is it?

A virtual private network establishes a secure and encrypted connection for online privacy and anonymity. VPN users can hide their IP address and location by creating a private network from a public Internet connection.

VPNs are used by individuals or organizations, and the pandemic-fuelled shift to working from home has pushed most companies to adopt VPNs. By establishing that secure connection between business networks and remote employees' devices, employees can access network resources the same way they would if sitting in the company office.

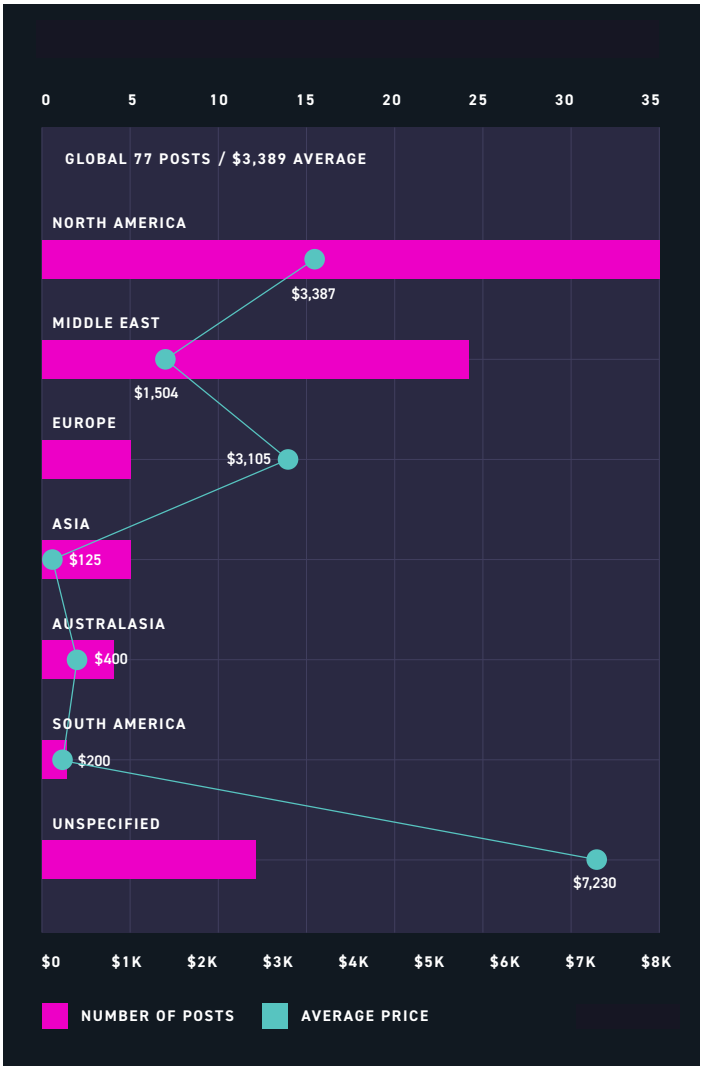

FIGURE 9: POPULAR REGIONS TARGETED BY IABS SELLING VPN ACCESS (2020)

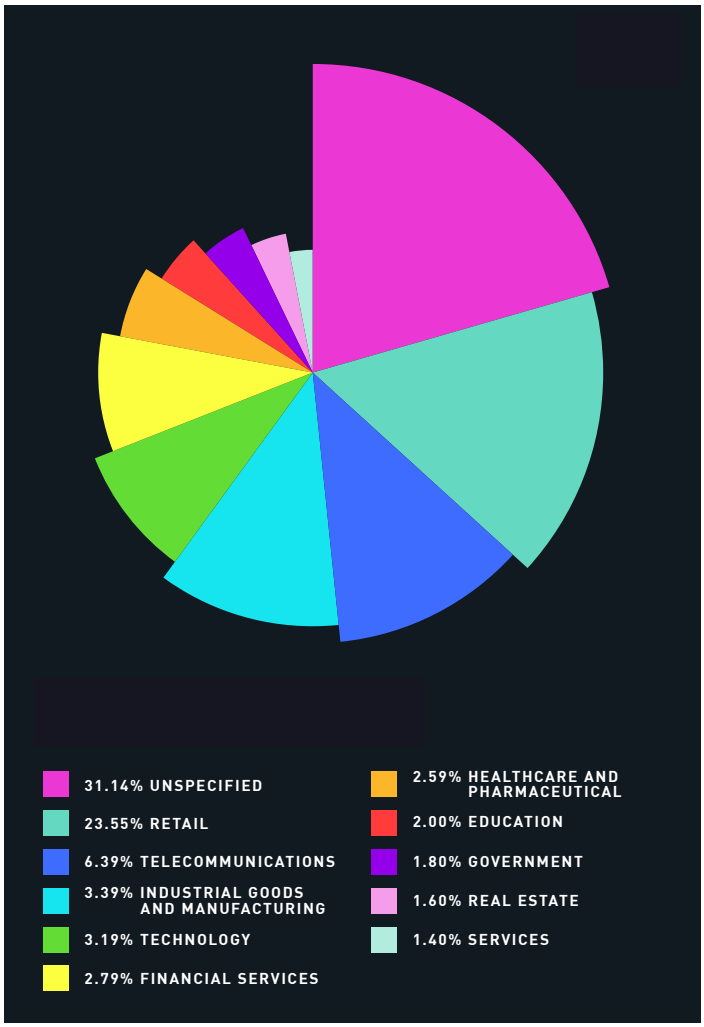

FIGURE 10: POPULAR INDUSTRIES TARGETED BY IABS SELLING VPN ACCESS (2020)

VPN

How do they get it?

Malicious actors are constantly scanning the Internet to find potential vulnerable targets. Most VPN providers have released patches for their products that, if not applied, leave organizations vulnerable to attackers retrieving files, such as authentication credentials.

These credentials can then be used to connect to the vulnerable VPN, change configuration settings, and connect to the organization's internal infrastructure.[4] What's more, unauthorized VPN access can also grant the attacker the necessary privileges to run additional exploits.

How do threat actors use this access?

Digital Shadows has observed cybercriminals and threat actors exploiting VPN accesses to engage in cyber espionage or financial crime, or to establish a persistent presence on corporate networks. Also, IABs are reselling VPN accesses to other criminal groups, such as ransomware operators. Over 2020, the use of VPNs as access points for ransomware operators and advanced persistent threats (APTs) skyrocketed, and again demonstrated the importance of patching critical software.

Actor SpotLight: NetNet

"NetNet" is a vendor of VPN network accesses on the Russian-language forums Exploit and XSS. The threat actor first appeared in September 2020, and initially offered limited information about their victims before changing tactics and providing more context.

NetNet seems to be indiscriminate in choosing victims, and has targeted a wide variety of sectors around the globe. They have received a small amount of entirely positive feedback from other forum users; this, coupled with the volume and frequency of their posts and evidence of successful transactions, indicates they are likely a credible and skilled threat actor.

[4] https://attack.mitre.org/techniques/T1133/, https://attack.mitre.org/techniques/T1078/, and https://attack.mitre.org/techniques/T1428/

CITRIX

Average Price: $3,826
Popular Regions: North America, Europe
Popular industries/sectors: Financial services, telecommunications, education

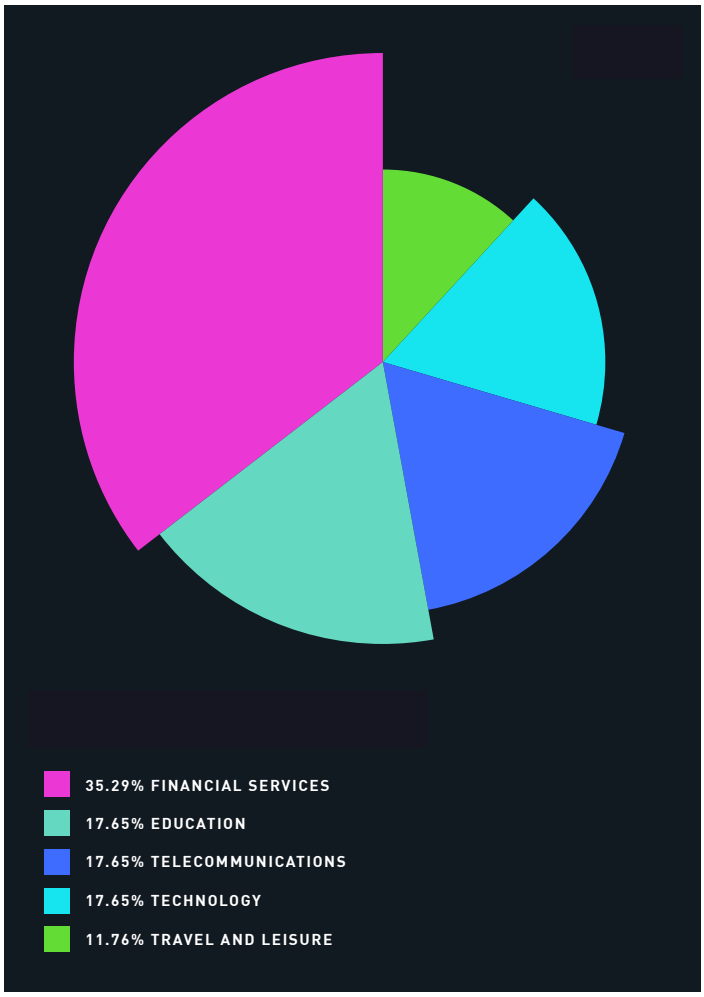

FIGURE 11: POPULAR INDUSTRIES TARGETED BY IABS SELLING CITRIX ACCESS (2020)

What is it?

Citrix Systems, Inc. is a US-based multinational software company, offering a multitude of enterprise solutions. These include server, application and desktop virtualization, networking, and cloud computing technologies. A Citrix blog explains their offerings with the analogy of a preschool child watching their favorite show on TV; someone pauses the show and the preschooler moves to watching on a mobile device. The expectation is that the show would pick up at the point last seen on the TV.

In more technical terms, Citrix helps enable remote work, helping employees access information that may be stored on systems in the office from external systems[5]. Similar to RDP, this can facilitate remote access to a terminal for use by the IT department.

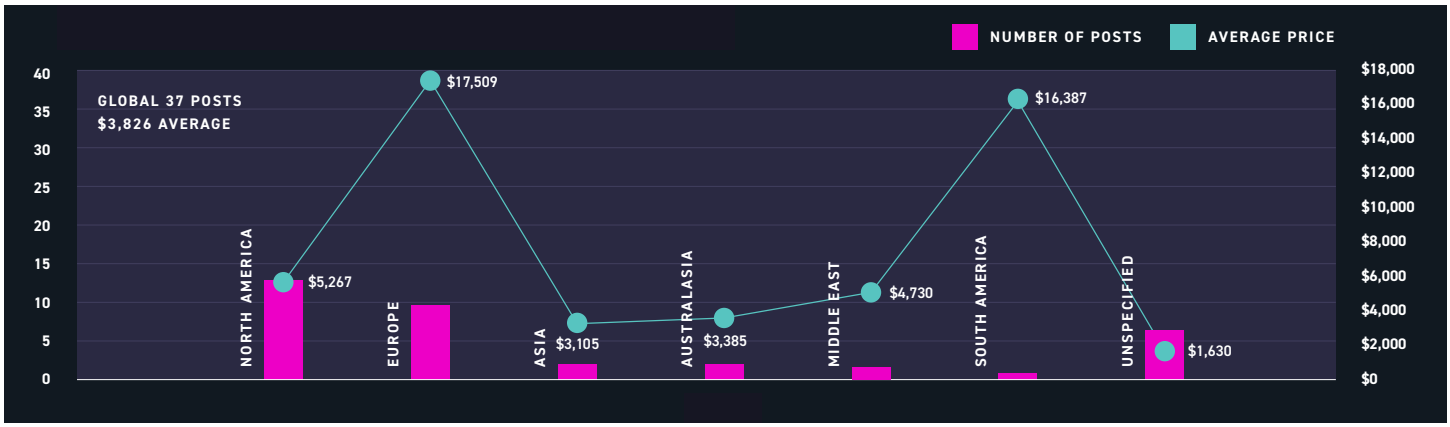

FIGURE 12: POPULAR REGIONS TARGETED BY IABS SELLING CITRIX ACCESS (2020)

5 https://attack.mitre.org/techniques/T1133/

CITRIX

How do they get it?

Most people will remember the critical Citrix vulnerability CVE-2019-19781, which could result in remote code execution (RCE) and directory traversal in Citrix Application Delivery Controllers. This product was very popular among businesses in healthcare, military, and critical infrastructure, and it left thousands of companies wide open to malicious exploits. That's why—one year after that vulnerability was patched—attackers still scan the Internet to spot insecure Citrix products that haven't been mitigated yet.

How do threat actors use this access?

Similar to RDP access, the implications of handing over remote access to an organization's network are implied. Ransomware operators, such as "Sodinokibi" (aka REvil), "Ragnarok", "Maze", "DoppelPaymer", and "Nefilim" have all been observed exploiting Citrix systems' vulnerability in 2020.

Actor SpotLight: Andreich_kms

"Andreich_kms" was a network access vendor, active on Exploit from February 2015 to October 2020. There is a realistic possibility that the threat actor will return to the forum after a hiatus. Many of the accesses Andreich_kms offered were low in value, and gave scant details about the victim organizations.

A large number of Andreich_kms's threads solicited advice on technical matters or commissioned coding work, from other users, suggesting a limit to their technical knowledge. Andreich_kms's threads also contained evidence of successful commercial transactions and that they have received good reviews from other forum members. This points to legitimate offerings from a credible user, albeit one lacking technical proficiency.

CONTROL PANELS

Average Price: $304
Popular Regions: North America, Asia
Popular industries/sectors: Technology, education

What is it?

Generally speaking, a software control panel lets a user configure an operating system and system applications. It can come in many different forms, and IABs advertise control panel access to various applications.

One example that was prominent in 2020 was the sale of cPanel access. cPanel is a control panel for web hosting accounts, simplifying website and server management. cPanel can be used to manage domains, create and maintain email networks, and store web files. Through cPanel, web hosting providers can manage the web server, and users can manage their websites.

It's easy to get the concerns about this type of control being compromised. cPanel includes information relevant to the users of the websites, and that can include payment-card details. IAB listings advertising cPanel access often include how many websites are active within the cPanel control, the sites' Alexa web rankings, and whether a payment portal exists on any of the sites.

Another example of control panels are Cloud Control Panels (CCP). These let users manage their cloud-based applications and include security aspects like Web Application Firewall (WAF) settings, domain backups, MySQL database tables, and domain controller (DC) access. An organization that finds its CCP compromised would be at the mercy of the attacker, with significant implications when it comes to data loss.

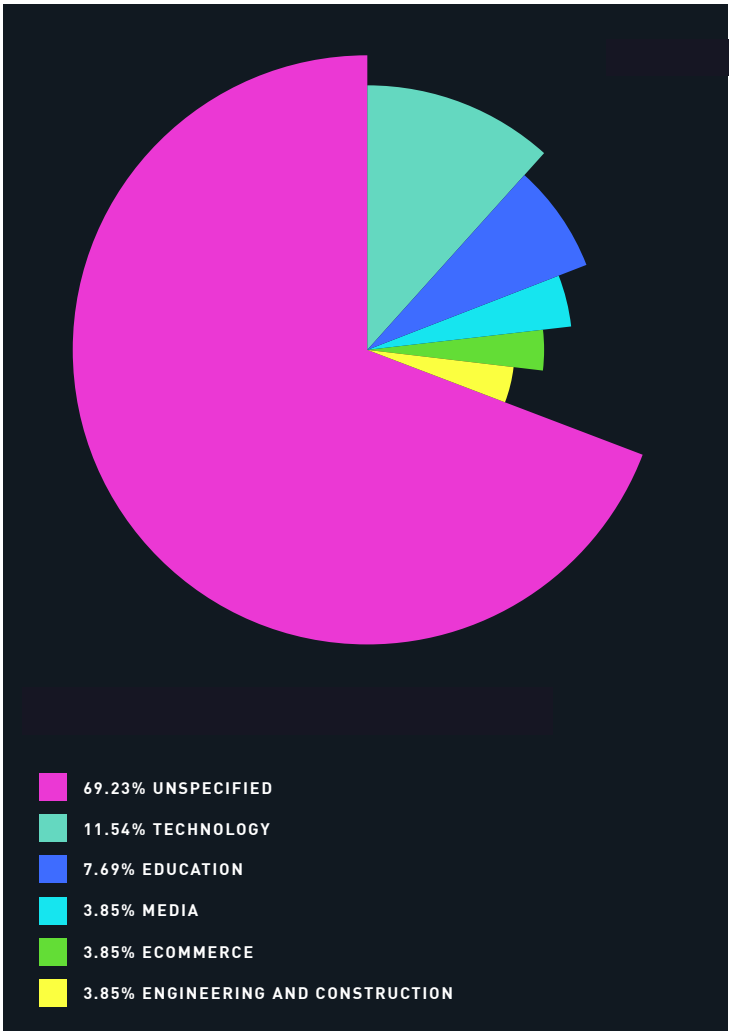

FIGURE 13: POPULAR INDUSTRIES TARGETED BY IABS SELLING CONTROL PANEL ACCESS (2020)

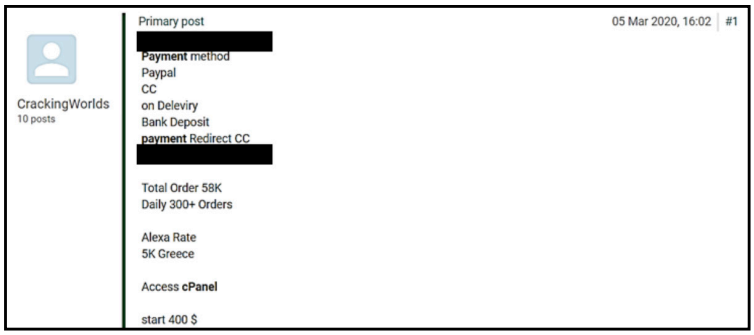

FIGURE 14: EXAMPLE OF AN IAB LISTING FOR A CONTROL PANEL

CONTROL PANELS

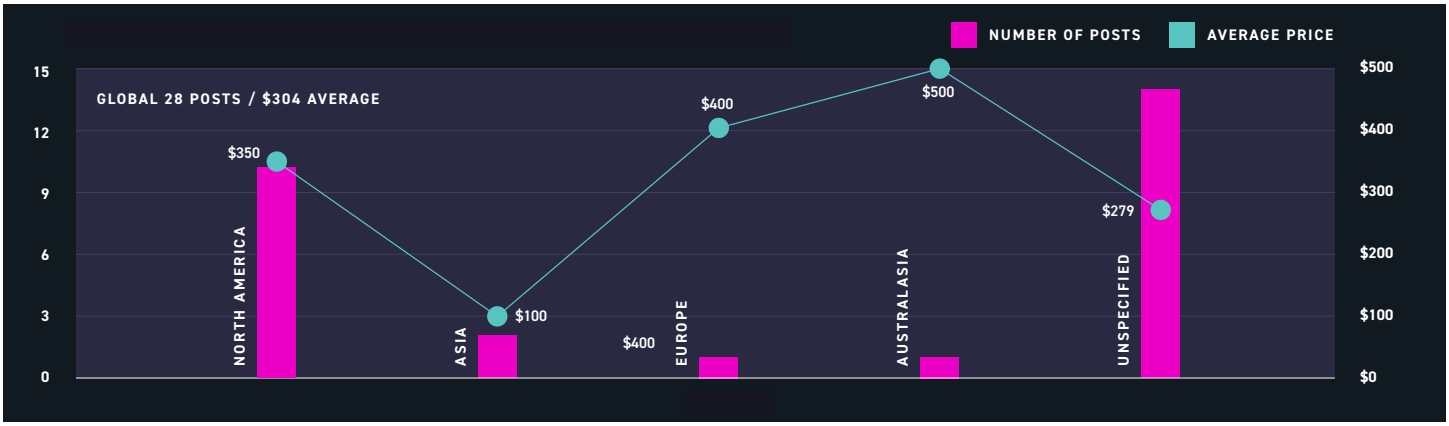

FIGURE 15: POPULAR REGIONS TARGETED BY IABS SELLING CONTROL PANEL ACCESS (2020)

How do threat actors use this access?

Control panel access can be used in a variety of ways, depending on what type of panel access is purchased. Consider cPanel access to an e-commerce site with hundreds of thousands of visitors and a payment platform: This can divulge visitor information—which might even be payment-card information or PII—which can be used for immediate financial gain or resold easily on criminal marketplaces.

CCP access can result in a range of problems for a victim organization; the threat actor can steal data or use DC access to distribute files that contain a ransomware payload. Realistically, if any of these accesses are purchased, the goal of any threat actor interested in more than a quick buck is to pivot, and see how far they can embed themselves in a victim network.

Actor SpotLight: Stari4ok

User "Stari4ok" is active on Exploit, where they mainly advertise listings of accesses to target systems/websites via the cPanel or web hosting manager (WHM) control panels. Stari4ok has also advertised credit-card dumps on several occasions. This threat actor is heavily involved in the forum community, commenting on other users' threads to offer help and advice, and contributing to arbitration cases.

Although many of their offerings seem unsold, at the time of writing, there is evidence to suggest that Stari4ok has successfully sold multiple offerings, and strong indications that they found buyers for many more. Stari4ok has received mixed comments from other users; feedback has been positive overall and reflects high quality in Stari4ok's offerings.

WEB-SHELL

Average Price: $2,845
Popular Regions: North America, Asia, South America
Popular industries/sectors: Technology, retail, government

What is it?

Web-shells are not inherently malicious and have legitimate uses, like many of the access types above. A web-shell is a piece of code or a script that enables remote administration of an Internet-facing web server.[6] Threat actors can inject a web-shell into a website vulnerable to any of the myriad of web security flaws, including SQL injection, cross-site scripting (XSS), Remote File Inclusion (RFI), or Local File Inclusion (LFI).

Once the web server is infected with the malicious web-shell, the threat actor creates a way to call back to the web-shell with commands. This facilitates man-in-the-middle (MITM) attacks, data exfiltration, and potential distribution of malicious attachments.

Actor SpotLight: 7h0rf1nn

"7h0rf1nn" is active on Exploit and RaidForums, where they have advertised multiple access offerings targeting victims working in education, military, government, and finance in Portugal, the US, Brazil, and Mexico.

There has been little public-forum interest in 7h0rf1nn's listings, but user feedback on RaidForums suggests that the threat actor has conducted some successful transactions with other forum members. There is no available forum evidence of 7h0rf1nn's level of technical proficiency, but their successful sales indicate that their listings are credible.

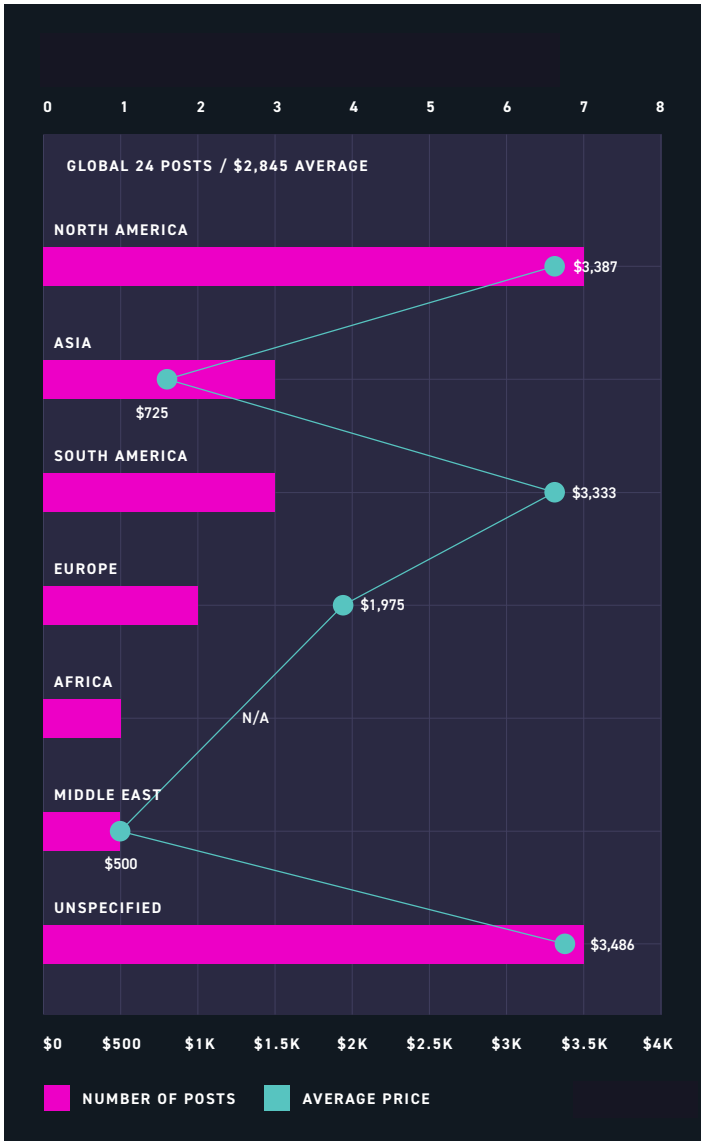

FIGURE 16: POPULAR REGIONS TARGETED BY IABS SELLING WEB-SHELL ACCESS (2020)

6 https://attack.mitre.org/techniques/T1505/003

WEB-SHELL

How do threat actors use this access?

There are some good real-world examples of how threat actors use malicious web-shell access. One of the most prominent web-shells is the notorious China Chopper, which has been wielded in multiple threat campaigns by nation-state threat actors and cybercriminals alike. The most obvious web-shell use case is espionage or data exfiltration, and China Chopper cropped up in a global espionage campaign against telecommunications organizations. China Chopper has also been used as a means to distribute the Sodinokibi and "GandCrab" ransomware variants against Lebanon-based organizations.

Given that IABs don't really care which customers they sell to, it isn't outside of the realm of possibility that they supply web-shell access to nation-state actors interested in cyber-espionage campaigns.

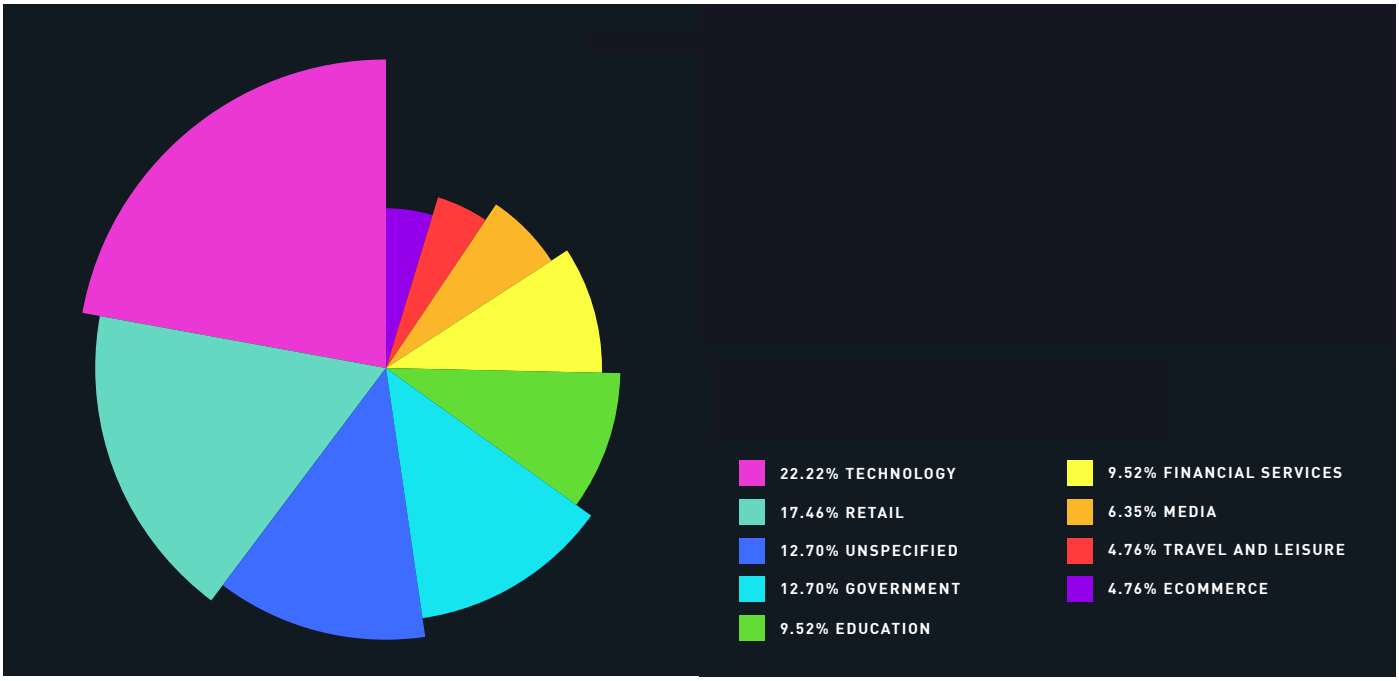

FIGURE 17: POPULAR INDUSTRIES TARGETED BY IABS SELLING WEB-SHELL ACCESS (2020)

3

EYEING ACCESS INDUSTRIES AT RISK

RETAIL

According to Digital Shadows' data, the retail sector is the unwilling winner of the most IAB mentions in 2020. The vast amount of sensitive information and transactions that can be monetized makes retail a prime target for cybercrime. Threat actors targeting this sector are primarily financially motivated, so cybercrime is much more prevalent than nation-state–linked threats.

Our data showed that North America and Europe were the most impacted regions, with an average access price of $6,107 and $6,108, respectively. The most prevalent access type is the CMS—software used to organize the creation and modification of digital content—whose most popular platform was (unsurprisingly) Magento.

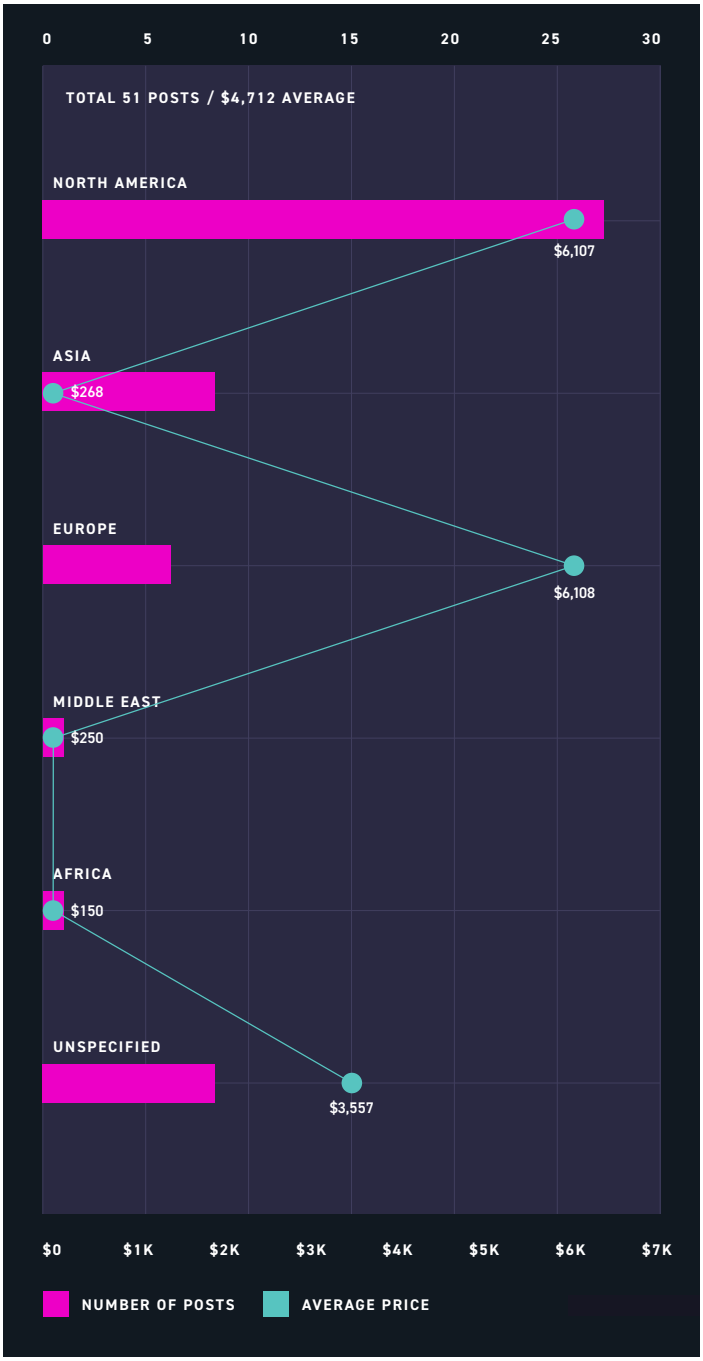

FIGURE 18: TOP REGIONS AND THEIR PRICES FOR IAB RETAIL TARGETS (2020)

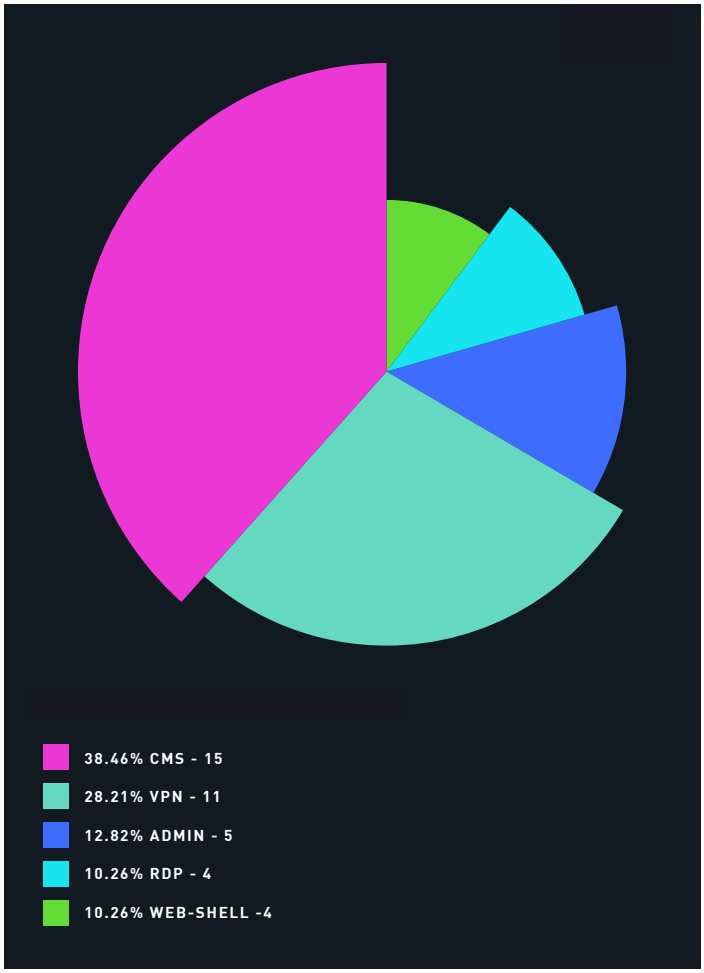

FIGURE 19: TOP ACCESS TYPES FOR IAB RETAIL TARGETS (2020)

FINANCIAL SERVICES

Organizations in the financial services sector are increasingly desirable to cybercriminals and threat actors, given the potential for a big pay-out. Cybercrime campaigns against the sector generally increased in 2020, aligning with the transition to a remote workforce.

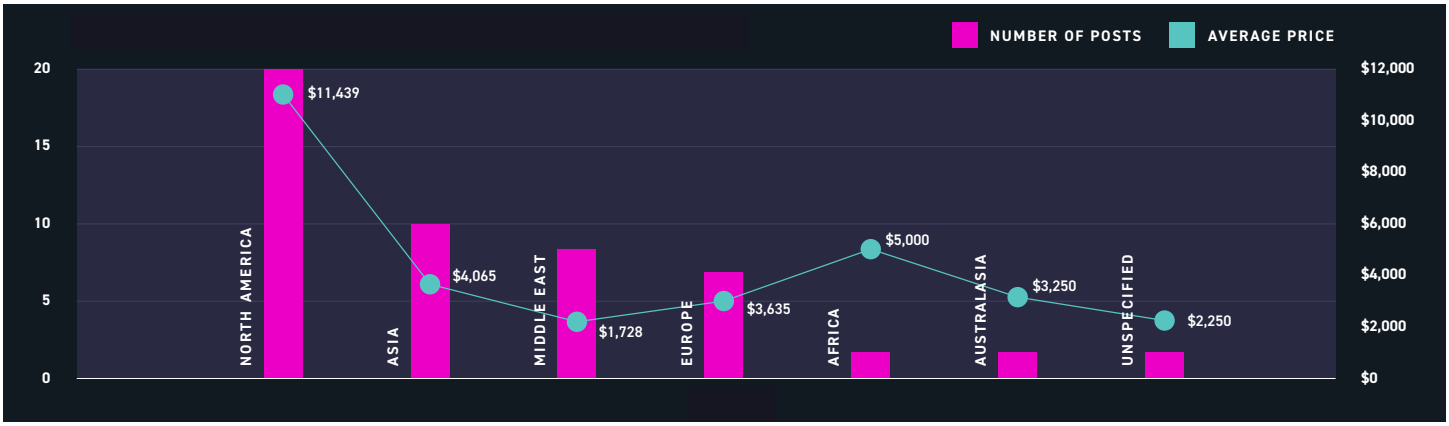

FIGURE 20: TOP REGIONS AND THEIR PRICES FOR IAB FINANCIAL SERVICES TARGETS

Extortion-based attacks, such as involving ransomware, remained a consistent threat. Groups such as “Egregor”, “NetWalker”, “Conti”, and Sodinokibi were widely reported targeting financial services. The risk they pose is compounded by the use of data leak and auction sites, likely increasing the potential for cybercriminals to obtain ransom payments.

Threat actors also frequently advertised access to banks and asset management companies on highly trafficked cybercriminal forums. Our data shows that IABs have been focusing particularly on North America, Asia, and the Middle East, and mainly offering domain access, VPN, and Citrix.

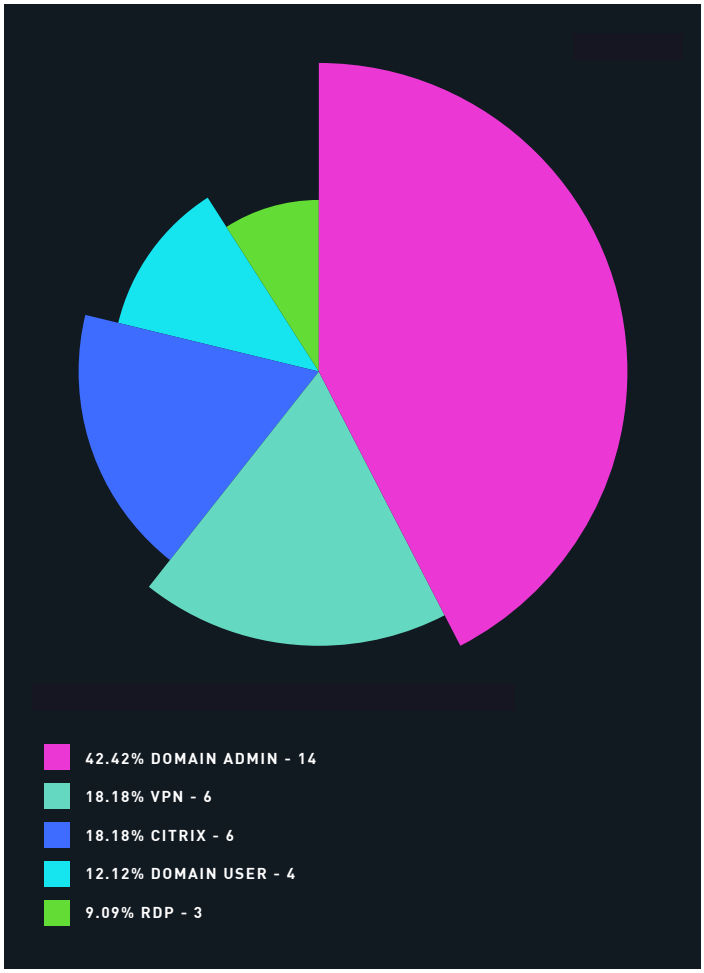

FIGURE 21: POPULAR ACCESS TYPES FOR IAB FINANCIAL SERVICES TARGETS

TECHNOLOGY

Organizations working in technology often hold valuable information that can be sold on cybercriminal forums. Our data shows that access to tech companies is sold for $13,607, on average, making this one of the most rewarding sectors for IABs.

Access can be used for a variety of reasons, including acquiring sensitive data and springboarding to an organization by compromising a third-party service provider. However, ransomware operations are generally the most financially gratifying for malicious actors. Egregor, Conti, and DoppelPaymer were ransomware variants frequently observed targeting the technology sector.

FIGURE 22: TOP REGIONS AND THEIR PRICES FOR IAB TECHNOLOGY TARGETS

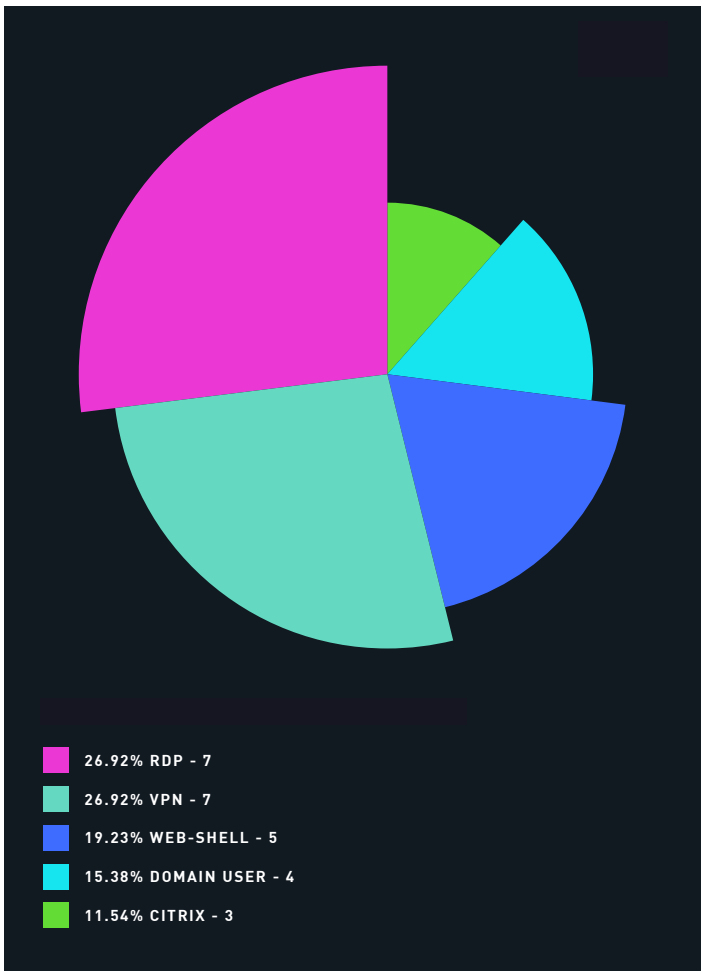

FIGURE 23: TOP ACCESS TYPES FOR IAB TECHNOLOGY TARGETS

HEALTHCARE & PHARMACEUTICAL

It shouldn't come as a surprise that the healthcare and pharmaceutical sector was one of the most profitable and sought-after targets for cybercrime in 2020. COVID-19 stretched the already-scarce cyber-security resources in this sector, leaving plenty of room for cybercriminal activity. Cyber-espionage actors frequently went after information related to vaccine development, in operations usually linked to nation-states.

Several government agencies issued security advisories that warned of a surge in ransomware attacks on healthcare and pharmaceutical organizations. Accesses were highly rewarding for cybercriminals involved in ransomware attacks, and IABs managed to sell them for an average of $10,941. RDP, domain administrator, and VPNs were the most mentioned types on cybercriminal forums.

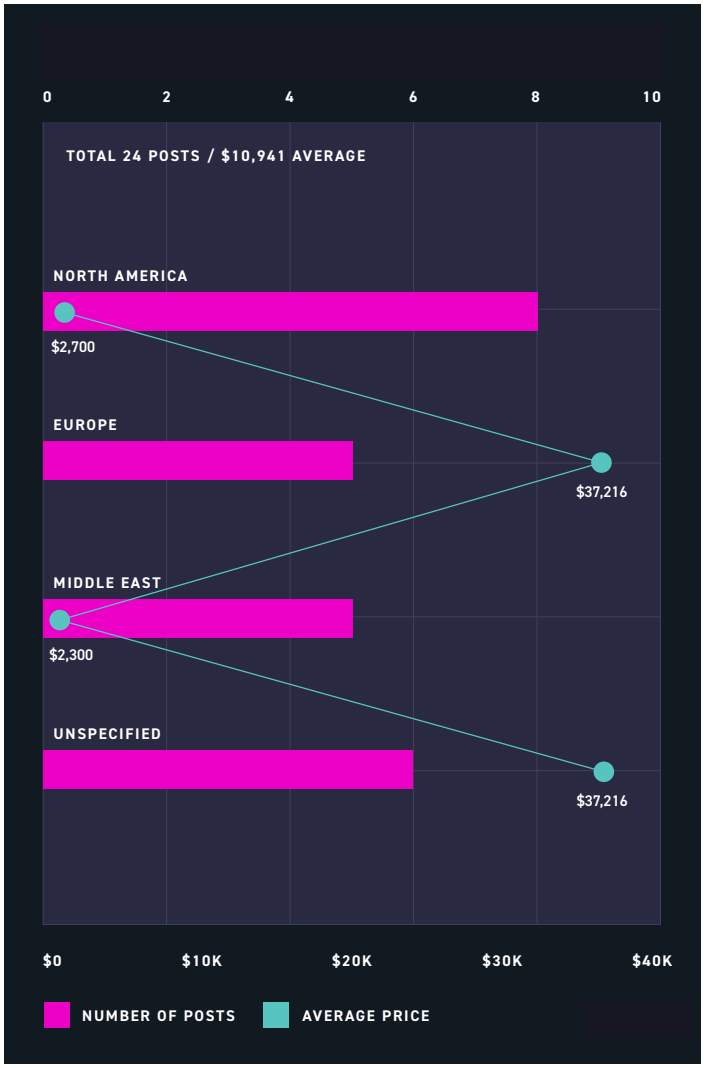

FIGURE 24: TOP REGIONS FOR IAB HEALTHCARE TARGETS

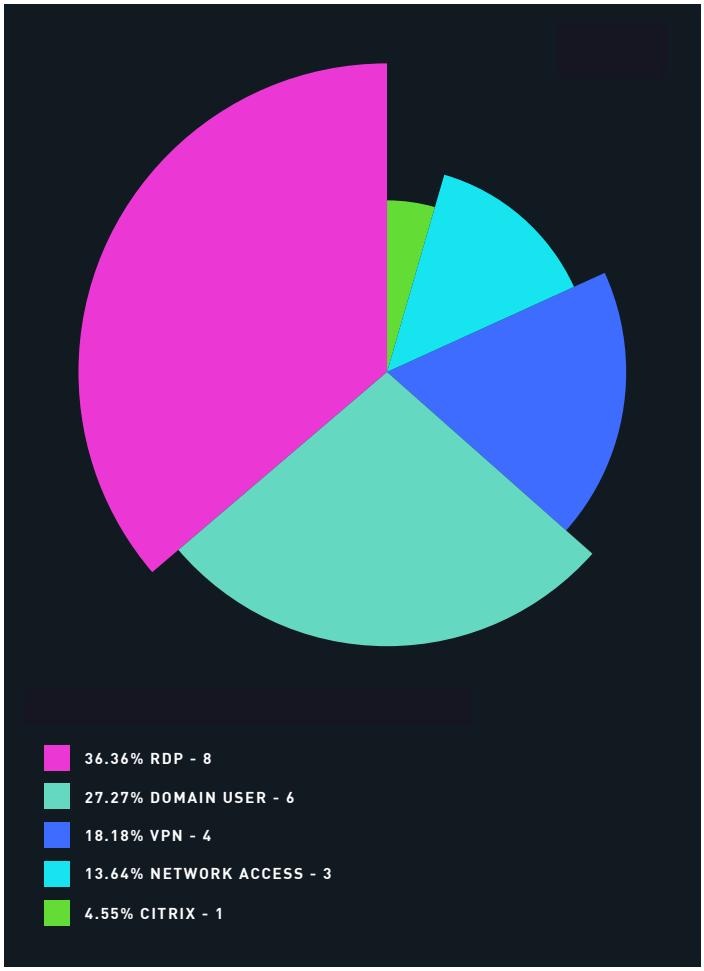

FIGURE 25: TOP ACCESS TYPES FOR IAB HEALTHCARE TARGETS

4

EYEING ACCESS
REGIONS AT RISK

NORTH AMERICA

A stunning majority of attack targets are located in North America, and 80 percent in the US. Companies in this region often command high-value networks that can be accessed for relatively low prices—starting at an average of about $5,000 for American; $2,000 for Canadian; and $1,000 for Mexican. These networks are usually accessed remotely or via a compromised Citrix gateway, and use of both bumped up during the COVID-19 pandemic.

The February 2021 attack on the Florida-based water treatment facility using RDP access shows that, although certain systems and infrastructure are critical, many American organizations have not invested enough in proper cyber-security protection. Ransomware operators can stand to earn higher amounts when taking control of critical systems (industrial goods and manufacturing attacks were the second most-targeted sector in this region) or accessing customer information (retail was the most targeted).

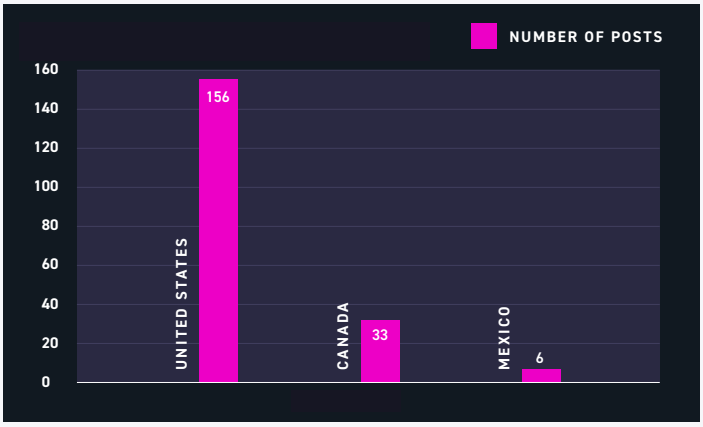

FIGURE 26: TOP COUNTRIES TARGETED IN NORTH AMERICA (2020)

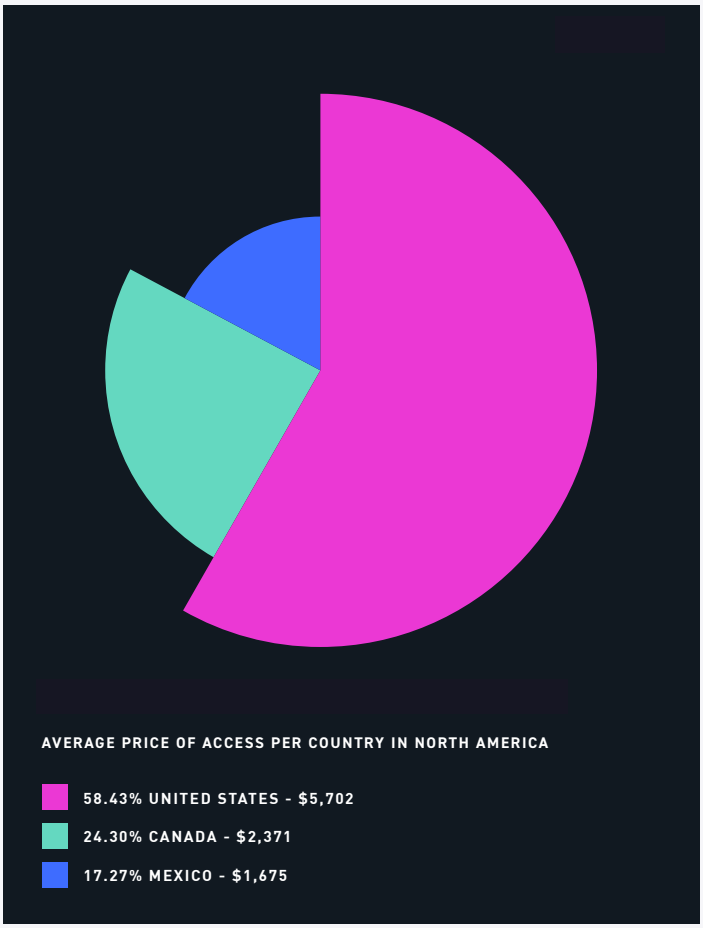

FIGURE 27: AVERAGE PRICE OF ACCESSES IN NORTH AMERICA (2020)

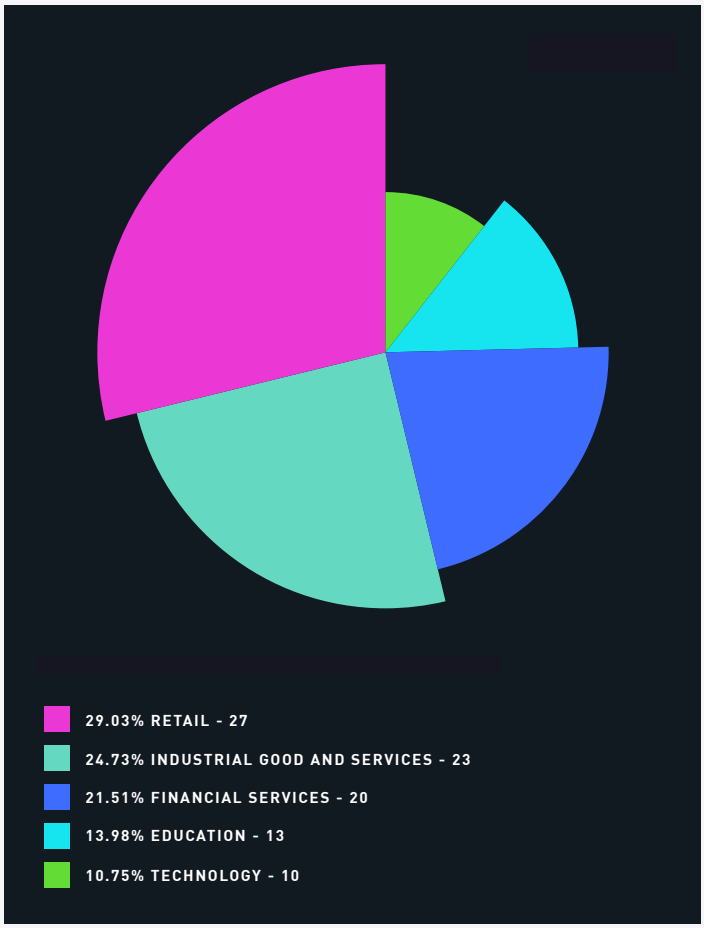

FIGURE 28: TOP INDUSTRIES TARGETED IN NORTH AMERICA (2020)

EUROPE

The European region is especially attractive to IABs for its several economic powerhouse countries, plus a workforce that has largely shifted to remote work practices as COVID-19 measures took hold. The UK, which has maintained Europe's longest lockdown, sustained the most IAB incidents (18) in 2020. Italy, which was the first EU country to institute strict stay-at-home measures, had the second-most IAB incidents (14).

The average price for access hovered around $3,000–7,000 in most countries, but Switzerland and France stood as outliers, with prices of approximately $101,000 and $904, respectively.

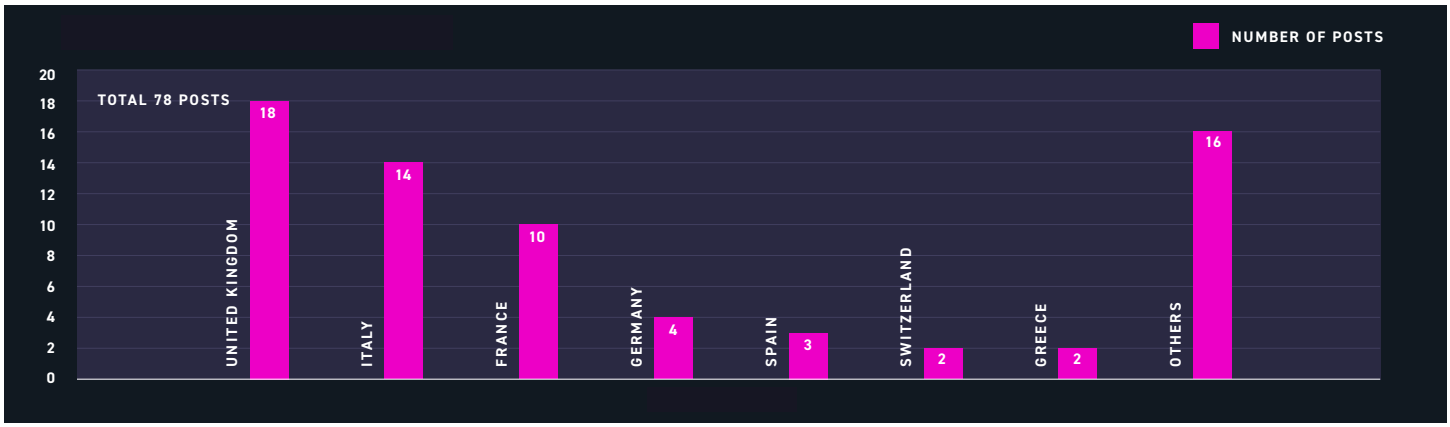

FIGURE 29: TOP COUNTRIES TARGETED IN EUROPE (2020)

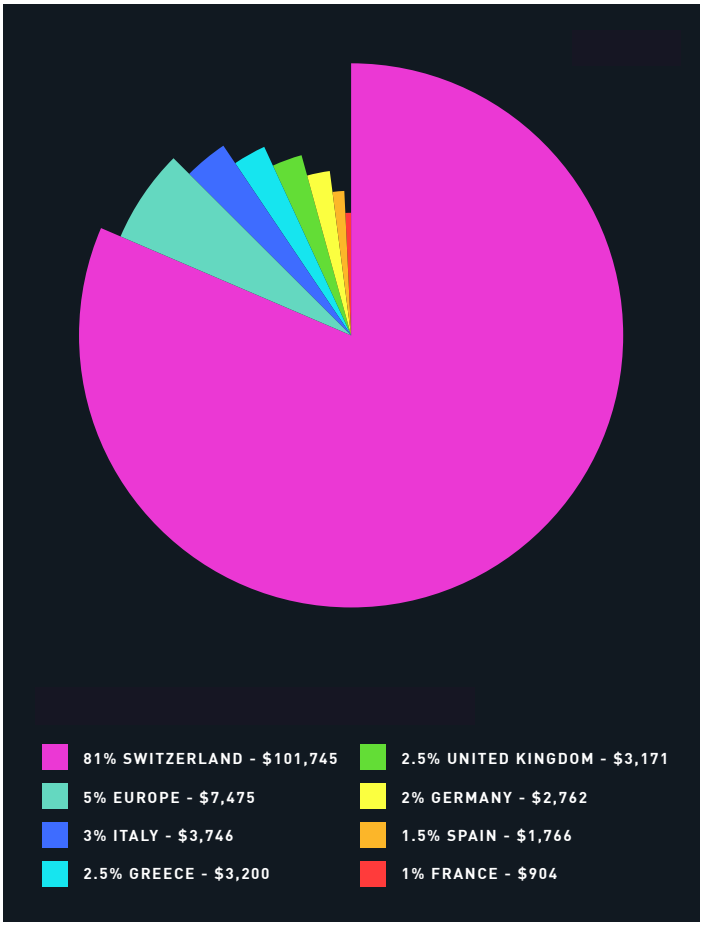

FIGURE 30: AVERAGE PRICE OF ACCESSES IN EUROPE (2020)

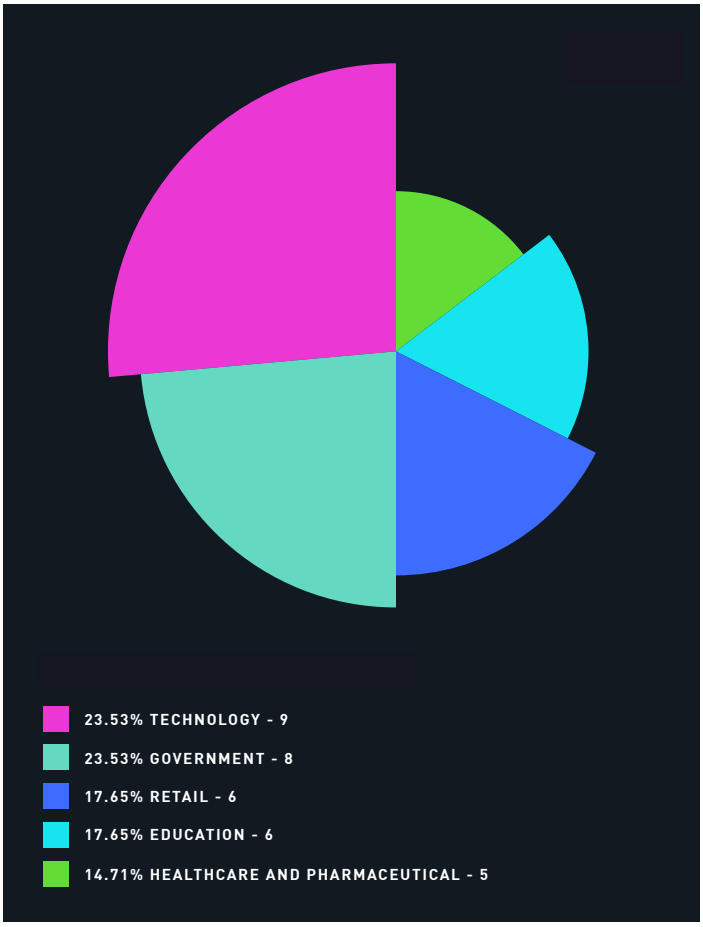

FIGURE 31: TOP INDUSTRIES TARGETED IN EUROPE (2020)

MIDDLE EAST

Due to its economic success, the Middle East is an increasingly popular region to target for data breaches—most often in the form of account takeover (ATO) via exposed credentials or IABs. Saudia Arabia was hit heavily in 2020, sustaining 13 reported IAB incidents with credentials averaging $1,173.

The telecommunications sector was hit the hardest (10 incidents); often that sector and similar ones are targeted because they have invested less in the depth and sophistication of their cyber-security teams. The financial services (7) and healthcare (5) industries were also heavily targeted as financially motivated threat actors sought to profit from remote work practices and pandemic panic.

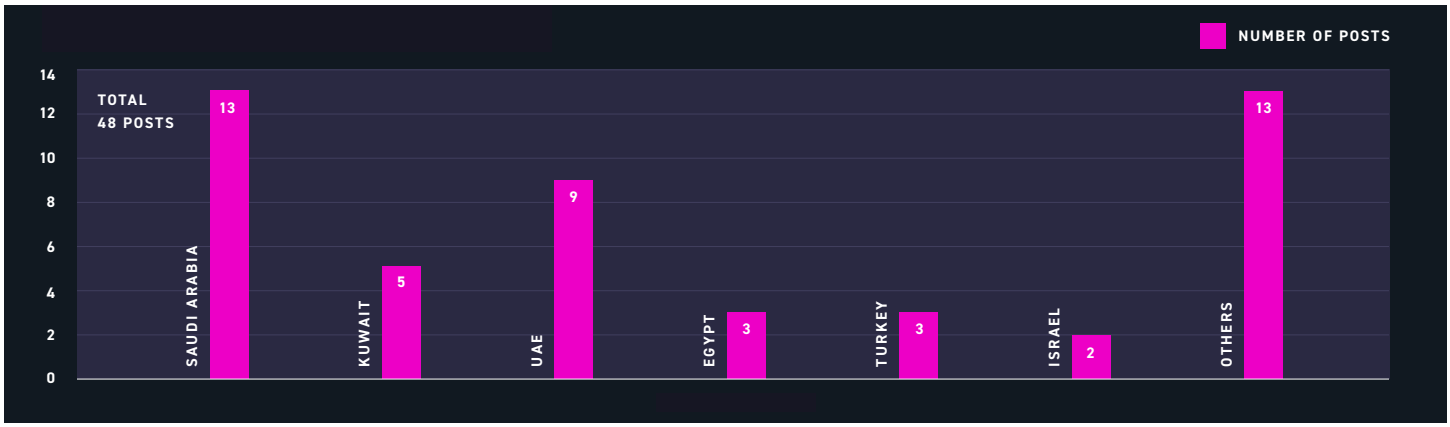

FIGURE 32: TOP COUNTRIES TARGETED IN MIDDLE EAST (2020)

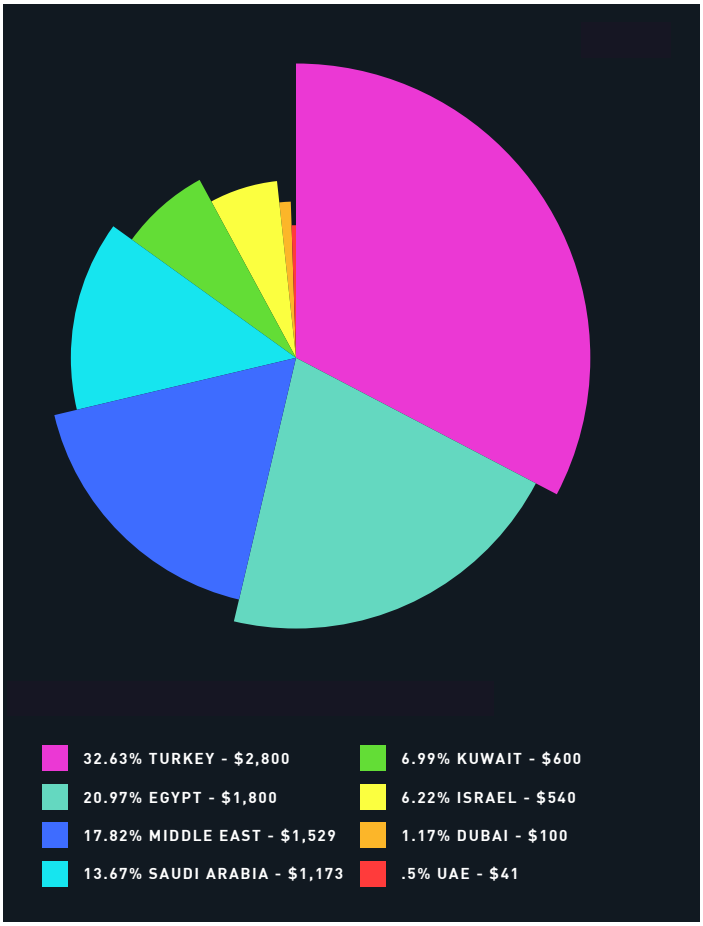

FIGURE 33: AVERAGE PRICES OF ACCESSES IN MIDDLE EAST (2020)

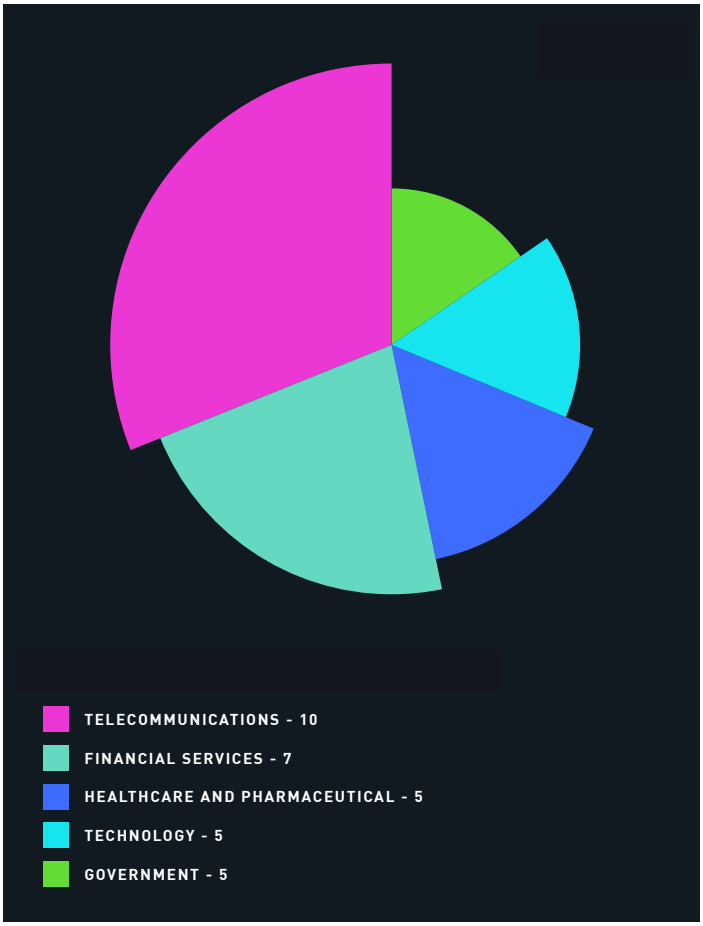

FIGURE 34: TOP INDUSTRIES TARGETED IN THE MIDDLE EAST (2020)

ASIA

IABs took a big interest in the Asian region in 2020; India weathered 16 incidents, followed by Thailand with 8 and the People's Republic of China (PRC) with 7. Cyber-security attacks in India jumped as much as 500 percent since pandemic lockdown measures were announced in March 2020, with the most common tactic reported as phishing to harvest login credentials.

Financial services, retail, and technology sector companies felt the biggest impact of IAB attacks. Credentials in these sectors tend to collect premium prices for the valuable customer PII, financial data, and intellectual property they may provide access to.

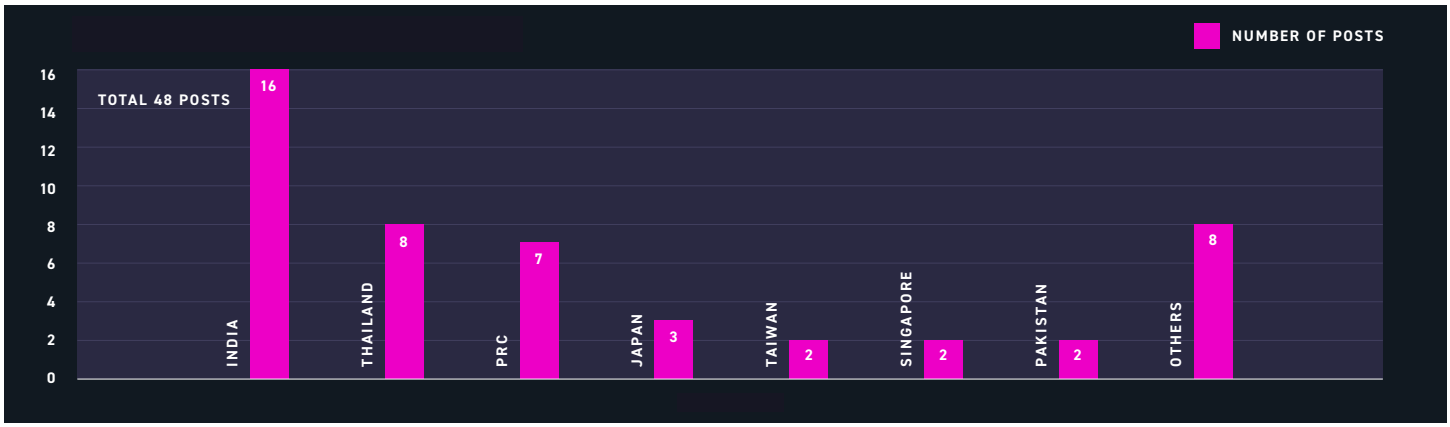

FIGURE 35: TOP COUNTRIES TARGETED IN ASIA (2020)

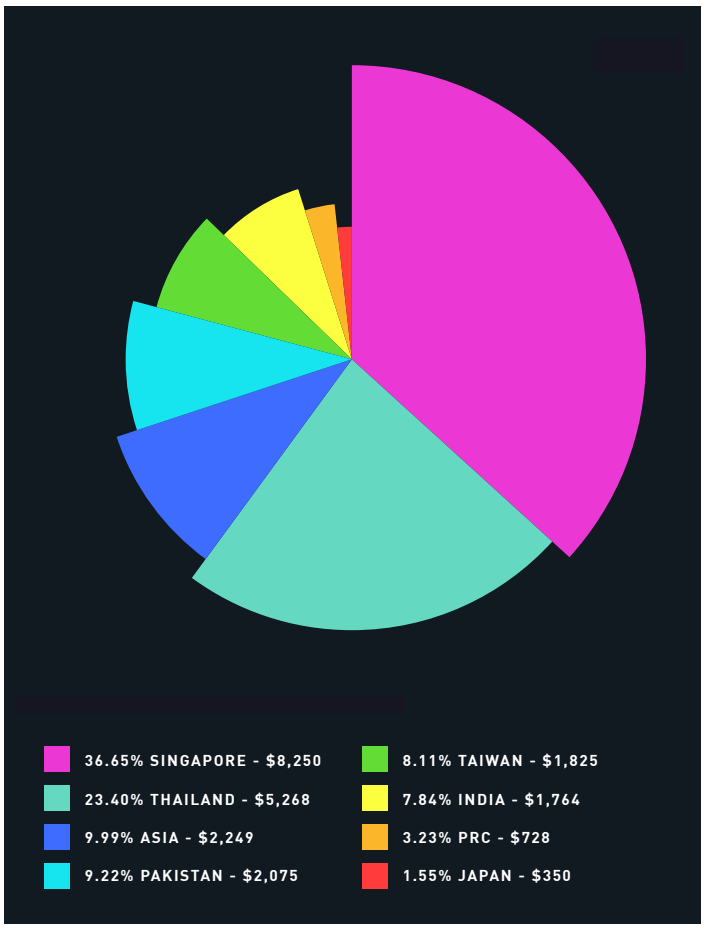

FIGURE 36: TOP COUNTRIES TARGETED IN ASIA (2020)

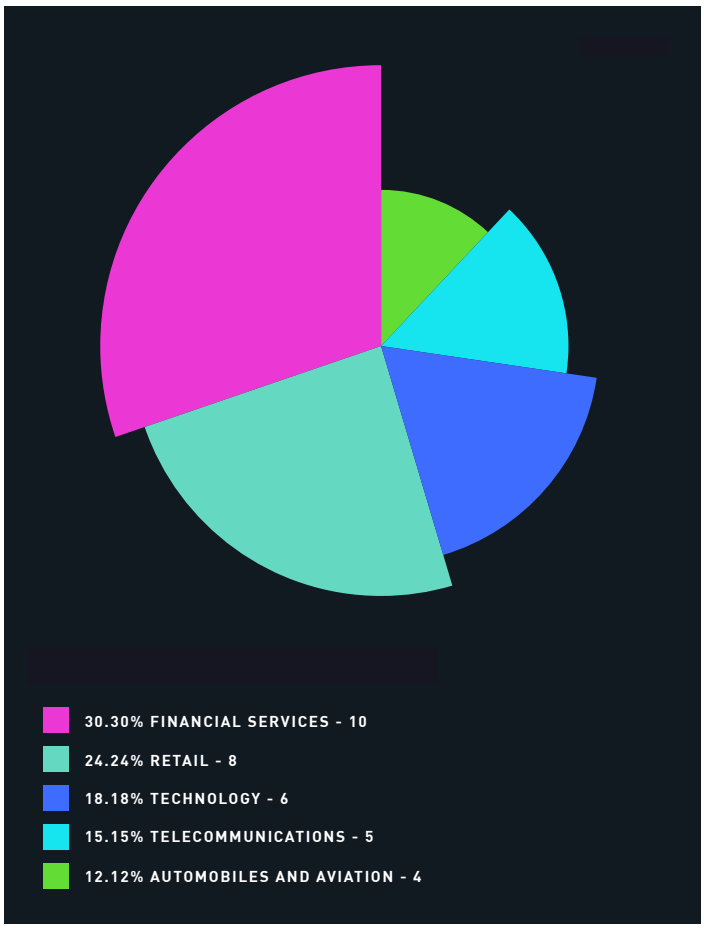

FIGURE 37: TOP INDUSTRIES TARGETED IN ASIA (2020)

AUSTRALASIA

Not to be neglected, Australia and New Zealand were key targets for IABs in 2020. With a stunning average price of $66,446 for Australian access and $1,500 for New Zealand, respectively, broker listings for Australasia were at the higher end, although representing a smaller data sample.

The primary sector for IAB data breaches was financial services, closely followed by engineering and construction, education, government, and insurance.

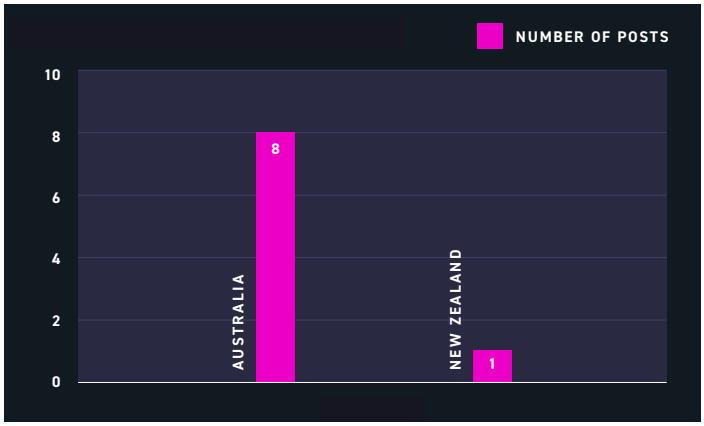

FIGURE 38: TOP COUNTRIES TARGETED IN AUSTRALASIA (2020)

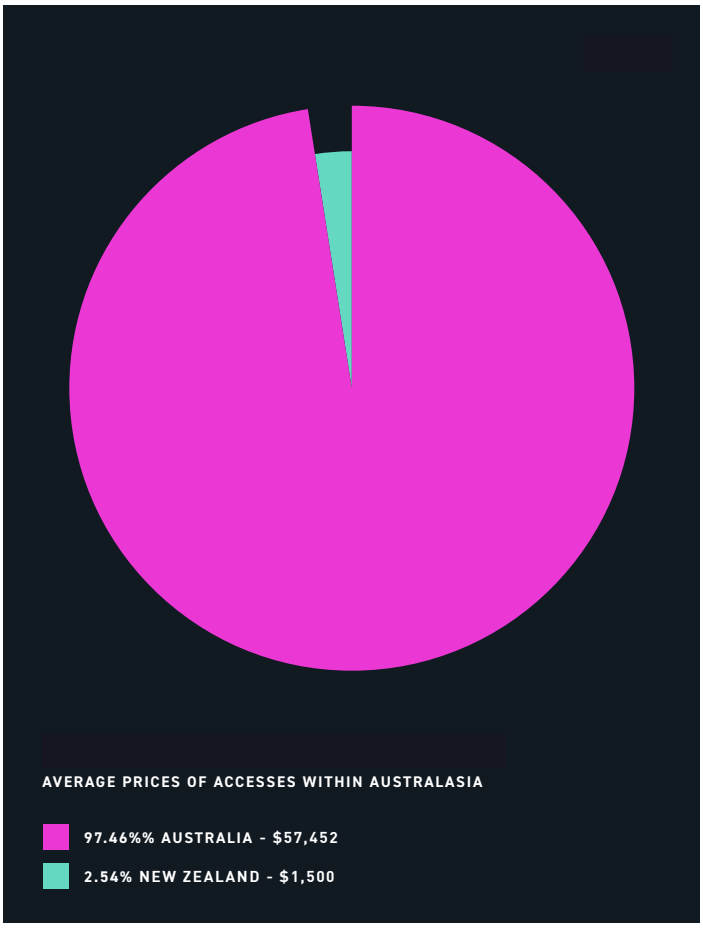

FIGURE 39: AVERAGE PRICE OF ACCESSES IN AUSTRALASIA

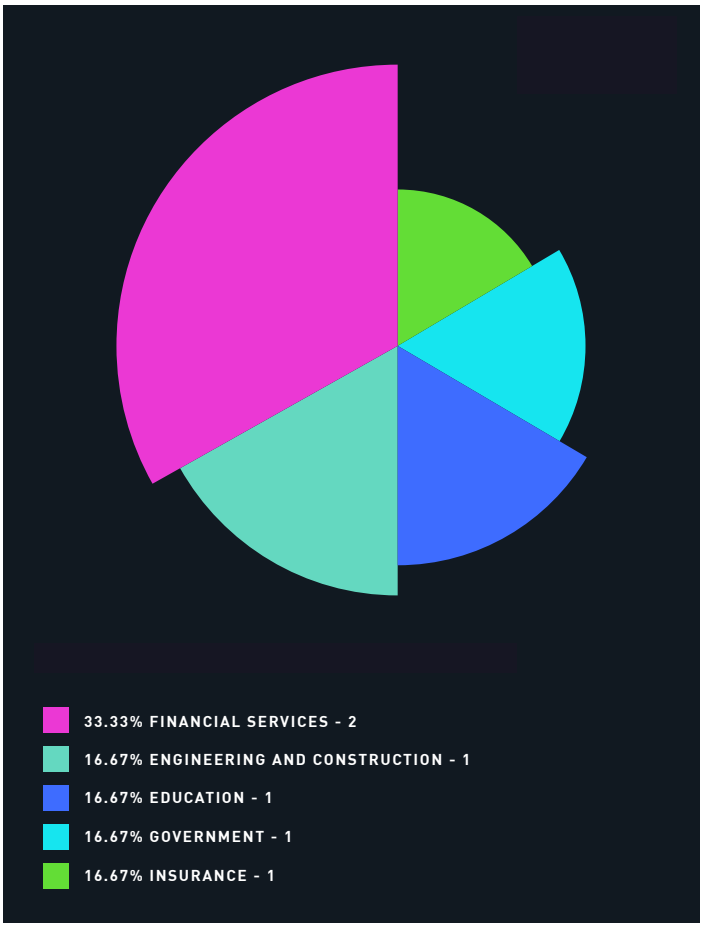

FIGURE 39: TOP INDUSTRIES TARGETED IN AUSTRALASIA (2020)

NO DEAL

MITIGATION STEPS TO BLOCK IAB ATTACKS

Given the prominence of IABs in the attack chain, they provide an opportunity for defenders to thwart potential attacks. Although not a foolproof measure, identifying an IAB listing that clearly affects your organization may open up a door to stopping an attack before it happens. Below we offer two areas for action; the first sees you preventing IAB from gaining access in the first place, and the second sees you keeping a close eye on IAB listings and deciphering listings to determine potential victims.

IABs are opportunistic, like many financially motivated threat actors—they'll often target the "low-hanging fruit" that require less work and offer a quicker route to their ultimate goal of being paid. So, proactive defenses involve making yourself a difficult target. We've broken down recommendations by access listing below.

RDP (https://attack.mitre.org/techniques/T1133/)

- Don't allow RDP connections over the open Internet. RDP instances can easily be found using search engines like Shodan.
- Use Network Level Authentication (NLA).
- Ensure password management policies include RDP accounts, enforcing complex and strong passwords, and password expiration. (Threat actors typically take over accounts with RDP access through brute-force password attacks against RDP accounts with weak or non existent passwords.)
- Utilize RDP gateways with support for 2FA.
- When possible utilize IP whitelisting to reduce attack surface.
- Tunnel RDP connections through SSH or IPSec.
- Minimize local administration and domain administration accounts, and control account permissions by implementing a role-based access control (RBAC) system.
- Routinely update devices with the latest patches, as vulnerabilities are regularly identified affecting RDP.
- Lock out users and block or time-out IP addresses that have too many failed login attempts.
- Consider using an account-naming convention that doesn't reveal organizational information.

NO DEAL

MITIGATION STEPS TO BLOCK IAB ATTACKS

VPN (https://attack.mitre.org/techniques/T1133/)

- Use the most secure encryption and authentication methods; this will depend on network infrastructure and VPN devices in use.
- Utilize VPN clients with 2FA enabled.
- Gateway and client software patching.
- Consider implementing compliance and posture checks when devices connect. This can help to ensure only compliant corporate devices can connect.
- Have administrators prioritise keeping VPN devices updated with the latest patches. (2020 saw several credible threat actors exploiting vulnerabilities affecting numerous VPN devices, including nation-state groups and ransomware actors.)
- Consider a 'zero trust' security model, which doesn't allow users access to data by default, and requires them to be consistently authenticated and verified. (Although threat actors cannot monitor VPN-encrypted traffic from outside the VPN, if they are able to connect to the VPN, they gain access to any resources connected to that network. It only takes one compromised account or device for an attacker to gain access to VPN-gated data.)

Web-Shell (https://attack.mitre.org/techniques/T1505/003)

- Patch web security vulnerabilities and maintain a strong vulnerability response plan as new exploits are identified and developed. (A web-shell depends on the injection of a malicious code or file, which is usually done through a web security vulnerability like cross-site scripting, SQL injection, RFI, or LFI.)
- Utilize intrusion prevention systems and web application firewalls to help prevent malicious activity.
- Follow secure design principles when building web applications.
- To potentially identify web-shells, compare existing web application code to a "known-good". (Detecting web-shells is fairly difficult as they are developed with obfuscation in mind. The goal is to maintain access for as long as possible and doing that means blending in within the environment.)

NO DEAL

MITIGATION STEPS TO BLOCK IAB ATTACKS

Citrix (https://attack.mitre.org/techniques/T1133/)

- Reduce the attack surface in a Citrix environment by disabling unnecessary features, virtual channels
- Configure Citrix policies to restrict redirections
- Where possible separate key components into individual virtual machines
- As with everything, maintain consistent operating system (OS) and firmware patch strategies
- Isolate critical resources from high-risk activities like web browsing and email access
- Use a process to just justify and approve new accounts
- Audit accounts and account permissions periodically
- Enforce policy settings consistent with intended security posture
- Encrypt all sensitive traffic flows

Control Panel (https://attack.mitre.org/techniques/T1133/)

- Utilize strong password standards
- Where possible, enable 2FA
- Maintain consistent operating system (OS) and firmware patch
- Update SSH packages to the latest stable version
- Disable password authentication and allow SSH access only by key-based authentication
- Enable brute-force protections that block IP addresses associated to multiple password attempts
- Utilize cPanel security plugins like RKHunter and ConfigServer eXploit Scanner (CXS)
- To the extent that is possible, prevent session breakouts

CATCHING THE SALE

MONITORING INITIAL ACCESS LISTINGS

IABs can often provide too much information and tip their hand on the victim organization that they have compromised. This can provide defenders an interesting opportunity to remove access to their system before it is sold to a threat actor with more malicious intent.

- **Monitor Access Trends:** Having insight into IAB listings can reveal trends targeting organizations in a similar sector or of a similar size. This will help you prioritize security efforts that combat the biggest threats.

- **Find Relevant Listings:** Initial access listings are put up for sale continually, with new listings almost hourly. You should monitor for listings that allude to your organization, remembering that IABs use clues like Alexa web rankings, sector, publicly stated revenue amounts, and staff size. Such details are often copied and pasted from business-to-business (B2B) databases. Craft your monitoring to reveal matching listings.

Although the emphasis should be placed on preventing access in the first place, monitoring the initial access listing landscape can provide defenders just another chance to avoid a more impactful incident.

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_