INTSIGHTS
A RAPID7 COMPANY

Selling Breaches: The Transfer of Enterprise Network Access on Criminal Forums

Introduction

The sale and purchase of unauthorized access to compromised enterprise networks has become a significant enabler for criminal cyberattacks, particularly ransomware infections. Some cybercriminals specialize in network compromises and sell the access that they have obtained to third parties, rather than exploiting the networks themselves. By the same token, many criminals that exploit compromised networks — particularly ransomware operators — do not compromise those networks themselves but instead buy their access from other attackers.

These exchanges on underground criminal websites enable specialized actors with complementary skills and resources to increase the severity and impact of the underground criminal ecosystem and the threat actors' "kill chain." This specific variety of criminal market offerings is less well known than others, such as the sale of compromised payment cards from **retail and hospitality breaches**. This lesser-documented type of criminal market offering nonetheless deserves greater consideration because of the breadth and potential severity of its impact.

These sales of network access affect organizations in all industries and geographies. Technology and telecommunications companies are among the most common victims and often command higher prices. Criminals from around the world buy and sell network access, but, as in other aspects of the underground criminal ecosystem, Russian-speaking criminals are the market leaders. These offerings often include a combination of remote access into a network and administrator credentials or other highly privileged accounts. The shift to a remote workforce during the COVID-19 pandemic and the resulting increase in the use of remote access tools and services have given attackers more attack surface to exploit, which has significantly fueled the marked increase in these sales in the past 18 months. This phenomenon predates the pandemic, but it matured and took on a life of its own in 2020, with some underground criminal forums beginning to dedicate specific sections to this particular type of offering.

An Overview of the Criminal Underground

Underground criminal websites are "critical infrastructure" for the criminal ecosystem of cyber threat actors and fraudsters. These websites consist of both forums and marketplaces, the latter of which function like the criminal versions of e-commerce websites. Sales of compromised network access are available on both types of websites, but they are more common on forums. Perhaps the less structured thread format, which is more conducive to multilateral discussion and enables posters to "bump up" old posts, is more suitable for these sales than the more tightly formatted marketplaces. Both types of websites are most often on either the deep web, beyond the indexing of search engines, or the dark web, requiring the use of the Onion Router (Tor) or other specialized software to access them.

These underground criminal websites are key enablers for both buyers and sellers. On one hand, they enable buyers with fewer skills or resources to obtain "raw materials" with which to construct criminal enterprises, including malware, other malicious tools, illicit infrastructure, and compromised data, accounts, and payment card details. This accessibility lowers barriers to entry into the criminal ecosystem for actors who might otherwise lack necessary skills or resources but have the money to make investments. On the other hand, these websites enable actors with more skills and resources to monetize the fruits of their labor and convert their attacks or other malicious activities into profits.

These websites operate in a variety of languages, but the Russian-speaking criminal communities are the most important. The Russian-language forums tend to have the most unique and sophisticated offerings, and often display higher standards of professionalism. English-language forums include not only North American and other native Anglophone criminals but also non-native speakers of English from around the world, including former British colonies. Other language-specific forums serve geographically concentrated communities, such as the Romanian speakers of Romania and Moldavia and the Portuguese speakers of Brazil, both of which are also significant hubs for cybercrime. Forums also exist in other widely spoken languages, such as Spanish and German.

These criminal communities aim to establish a "circle of trust" that enables criminals to do business with each other with a reasonable degree of confidence. The risk that a buyer or vendor will rip off, cheat, or defraud a vendor or customer is a significant concern for them, as is the risk of unwittingly doing business with undercover law enforcement or security researchers. Users can vet prospective vendors or buyers by reviewing their history and status, and the feedback or ratings that they have received from other users, so as to develop confidence in them. Many of these communities use escrow systems to instill further confidence in large purchases by entrusting funds to website administrators as a transaction proceeds. The risk of receiving negative feedback or being reported to website administrators serves as an additional deterrent to misconduct. These "quality control" mechanisms also enable security researchers to vet the sources of human intelligence (HUMINT) that they collect from these communities (including data points for this paper) by reviewing users' track records. A user with a long history of satisfied customers is a more reliable source than a new user with no track record, as the former has invested in building a reputation and has financial incentives to maintain it.

Why Do Criminals Sell Their Network Access?

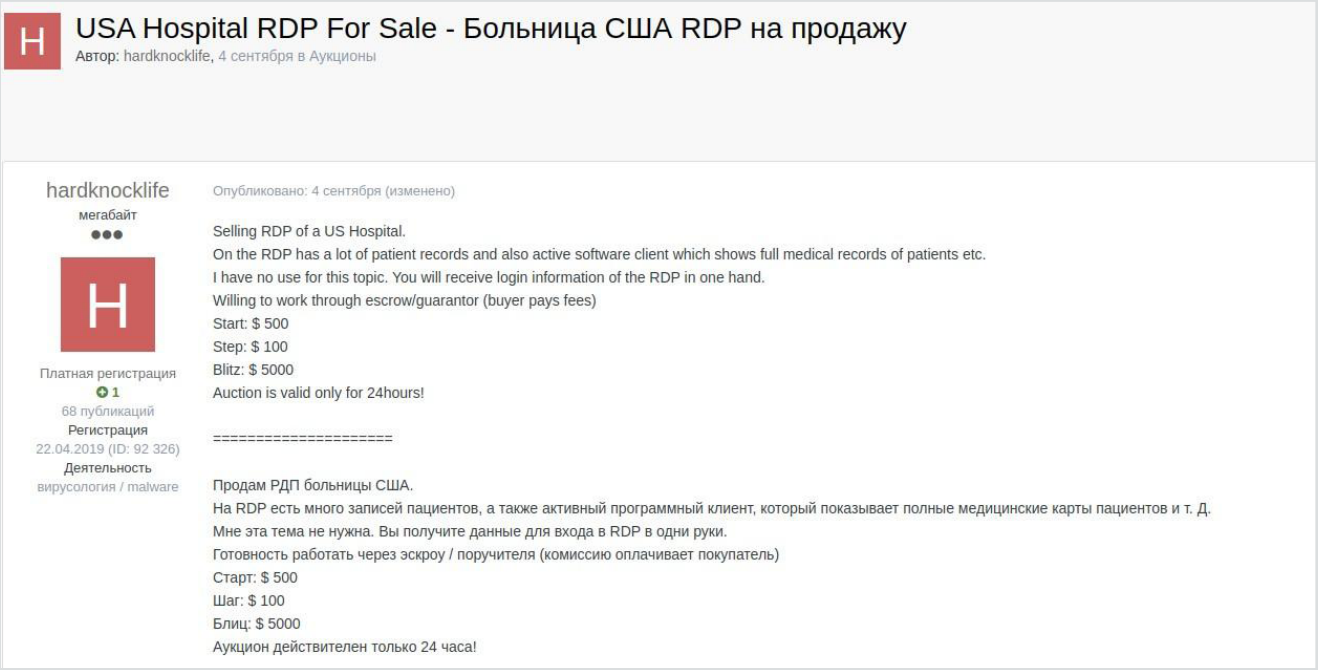
Users of these underground criminal forums and dark markets often specialize in certain sectors of the underground criminal economy. They often perform specific functions within that criminal ecosystem, perhaps with greater skill or ease. This specialization and division of labor increase the severity, impact, and cost-effectiveness of attacks and fraud by delegating or outsourcing various stages of an attack and the resulting exploitation of data or access to those that can perform it most optimally.

Indeed, very few cybercriminal enterprises have full "vertical integration" or achieve total operational self-sufficiency. Instead, most remain dependent on suppliers of "raw materials" for their attacks, such as malware payloads, hosting infrastructure, or access to compromised networks. They may also rely on customers that enable them to "fence" stolen information or otherwise monetize their labor.

For example, in the well-known case of compromised payment card sales, certain actors specialize in this particular function. These actors operate point-of-sale (PoS) malware or digital payment card skimmers that collect data from PoS terminals or e-commerce websites, respectively. These actors typically do not monetize compromised cards themselves, either because the sheer volume of data would prevent them from using the cards while they are still "fresh," or because they are less adept at fraud than carding specialists. It may thus be more optimal and cost-effective for them to sell cards to third-party carding specialists who have both the time and the skills to use them optimally.

A similar line of reasoning drives the sale of compromised network access. Attackers who specialize in initial compromises may not have the skills, time, labor resources, or work ethic to exploit and monetize their access most effectively. This factor is particularly applicable to compromises of specialized environments, such as those with operational technology (OT), industrial control systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, or other less common or less conventional technology that may be unfamiliar to many attackers.

For example, in September 2020, Russian-speaking username "hardknocklife" auctioned off RDP access to a US hospital. He mentioned as a selling point that this RDP access yielded patient records, in which he reportedly had no interest. US patient records from healthcare organizations are a valuable resource for identity thieves and other fraudsters because they contain dates of birth, Social Security numbers, and other personal details that they can use for fraudulent credit applications and other malicious purposes. This seller could have mined or monetized that data himself but lacked interest in doing so, perhaps because he could be more productive as an intruder than a fraudster, or because he lacked the fraud or criminal business skills to do so. The low price of $500 USD at which he started his auction suggested that he simply wanted to move this inventory quickly, but his "buy now" price of $5,000 USD also recognized the high monetary value of US patient records (see Figure 1).



H

USA Hospital RDP For Sale - Больница США RDP на продажу

Автор: hardknocklife, 4 сентября в Аукционы

hardknocklife
мегабайт
●●●

H

Платная регистрация
1
68 публикаций
Регистрация
22.04.2019 (ID: 92 326)
Деятельность
вирусология / malware

Опубликовано: 4 сентября (изменено)

Selling RDP of a US Hospital.
On the RDP has a lot of patient records and also active software client which shows full medical records of patients etc.
I have no use for this topic. You will receive login information of the RDP in one hand.
Willing to work through escrow/guarantor (buyer pays fees)
Start: $ 500
Step: $ 100
Blitz: $ 5000
Auction is valid only for 24hours!

=====================

Продам РДП больницы США.
На RDP есть много записей пациентов, а также активный программный клиент, который показывает полные медицинские карты пациентов и т. Д.
Мне эта тема не нужна. Вы получите данные для входа в RDP в одни руки.
Готовность работать через эскроу / поручителя (комиссию оплачивает покупатель)
Старт: $ 500
Шаг: $ 100
Блиц: $ 5000
Аукцион действителен только 24 часа!

Figure 1

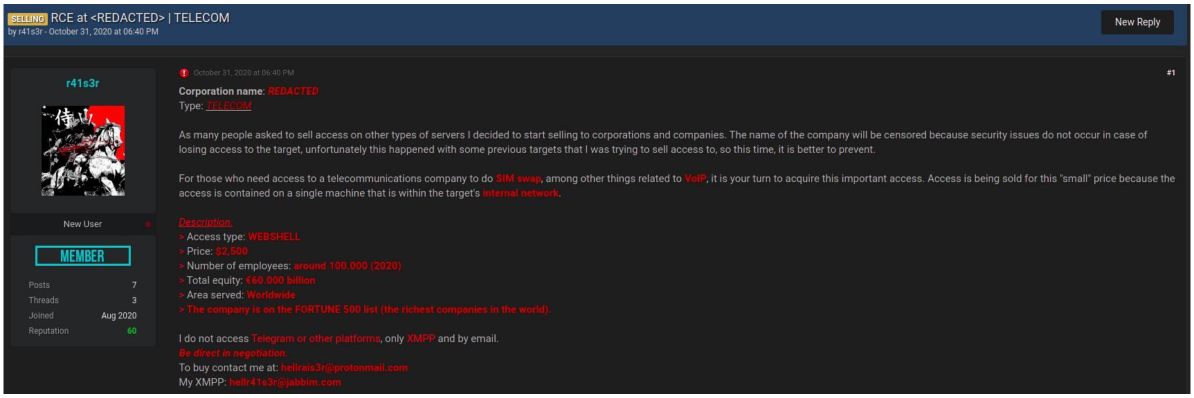
Another reason for attackers to sell access is when their reconnaissance indicates that the network contains little or no data of monetary value, in which case it would be more profitable for ransomware operators. The initial attacker can thus sell network access to ransomware operators who may not have the skills to compromise networks themselves. Sales of compromised network access are thus significant enablers for ransomware attacks. Such sales to ransomware operators also enable the initial intruders to reap profits from breaches that might have otherwise gone to waste and yielded no profits.

How Do Criminals Sell Their Network Access?

The typical way to advertise a sale of compromised network access is to start a thread in the appropriate section of an underground criminal forum. The originating post on that thread typically describes the victim, the form and level of access for sale, and the pricing and other transaction details.

These advertisements typically do not identify victims by name. Users of criminal forums and dark markets are keenly aware that security researchers and law enforcement monitor their communities. Thus the sellers usually (but not always) refrain from naming victims in these posts, which are typically viewable by all users, so as to avoid exposing their breaches. The minority of sellers that do disclose the names of their victims in public posts are usually on English-speaking forums, where some users may be less discreet than their Russian-speaking counterparts. They may, however, identify the victim by name in private message exchanges with prospective buyers who inquire about an offering. Some sellers are nonetheless reluctant to expose the names of their victims, even in private communications with prospective buyers, and may only offer proof of their access, which is often in the form of screenshots.

For example, in October 2020, English-speaking username “r41s3r” explained in one of his advertisements why he would not disclose the name of the victim. He claimed that previous disclosures of the names of victims had caused him to lose access to their networks, so he would not repeat that mistake in the future. Perhaps security researchers or law enforcement observed previous posts of his in which he identified a victim, whom they notified, enabling the victim to resolve the unauthorized access (see Figure 2).



RCE at <REDACTED> | TELECOM
by r41s3r - October 31, 2020 at 06:40 PM

October 31, 2020 at 06:40 PM

Corporation name: *REDACTED*
Type: *TELECOM*

As many people asked to sell access on other types of servers I decided to start selling to corporations and companies. The name of the company will be censored because security issues do not occur in case of losing access to the target, unfortunately this happened with some previous targets that I was trying to sell access to, so this time, it is better to prevent.

For those who need access to a telecommunications company to do SIM swap, among other things related to VoIP, it is your turn to acquire this important access. Access is being sold for this "small" price because the access is contained on a single machine that is within the target's internal network.

Description:
> Access type: WEBSHELL
> Price: $2,500
> Number of employees: around 100.000 (2020)
> Total equity: €60.000 billion
> Area served: Worldwide
> The company is on the FORTUNE 500 list (the richest companies in the world).

I do not access Telegram or other platforms, only XMPP and by email.
Be direct in negotiation.
To buy contact me at: hellrais3r@protonmail.com
My XMPP: hellr41s3r@jabbim.com

Figure 2

These public advertisements typically describe a victim by location, industry or sector, and revenue or market valuation. Also often included are broad descriptions of the compromised network, such as the number and types of machines on it and/or the types of files and data that it contains. If the seller believes that the network is a suitable candidate for a ransomware infection, the advertisement often specifies that selling point for ransomware operators in particular. Including revenue or market value figures enables ransomware operators to estimate the size of the ransom that they can hope to extract from the victim. The advertisement usually specifies the forms and points of access to the compromised network that the buyer will receive. These access points often involve remote access services and tools, such as RDP and VPNs, frequently in conjunction with elevated privileges. Pricing is typically fixed, but some sales take the form of auctions. Some buyers are more open to negotiating prices than others, particularly if an offering has gone unsold for an extended period of time. Typical pricing for these sales of compromised network access ranges from three to five figures in USD, with most prices in the four-figure range.

How Do Criminals Transfer Their Network Access to Buyers?

Sellers of compromised network access typically use credentials as persistence mechanisms to transfer their access to buyers. It is unclear if and when these persistence mechanisms might have also been the initial access vector for the compromises, or if and when the attackers gained initial access by other unidentified means and then established the separate persistence mechanisms that they sell.

One major gap in threat intelligence on these attacks is the initial access vector. These advertisements typically do not identify initial access vectors, as there is no need for prospective buyers to know those details. Nonetheless, some of the various types of persistence mechanisms on sale in these offerings are also so common as initial access vectors that it is reasonable to assume that, in many cases, they might have been the initial access vectors as well. Furthermore, in some cases, a review of a given forum user's previous posts may reveal their previously used tactics, techniques and procedures (TTPs), which could indicate initial access vectors that they might have used. For example, if a given user's offering includes RDP access, and that user also has a history of selling RDP brute force tools, then one can reasonably infer that he might have used one of those tools to compromise this network.

RDP credentials are a common feature of these sales. RDP is a common initial access vector, particularly for brute force attacks on networks and often in conjunction with ransomware. Many organizations fail to disable RDP services that they do not use, which gives attackers more chances to compromise targets. Even when there is a business reason to enable RDP access, many organizations fail to protect RDP credentials with two-factor authentication (2FA) or strong passwords, which leaves them vulnerable to brute force attacks. Increased use of RDP services due to the rise of remote work during the COVID-19 pandemic has also given attackers more RDP attack surface to exploit.

VPN credentials are another common component of these sales of network access. As with RDP, the rise of remote work during the COVID-19 pandemic has given attackers more VPN attack surface to exploit. Furthermore, the sudden and often large-scale nature of the shift to remote work in March 2020 left many organizations and less technically literate employees more vulnerable to attack due to misconfigurations, unpatched versions of VPN software, a lack of 2FA for VPN credentials, and VPN-themed social engineering attacks. Even before the pandemic and the rise of remote work, VPNs were desirable targets, particularly with exploits for old, vulnerable versions of popular VPN software.

Some of these sales use web shells as persistence mechanisms to transfer access. Web shells on a web server can enable malicious activities against its public-facing services and provide a foothold for additional lateral movement into the non-public-facing segments of an enterprise network. Web server access can be particularly useful in compromises of enterprise victims whose potential profitability lies in their public-facing web services to customers, such as online banking or e-commerce. Other means of access to web infrastructure include WordPress credentials and credentials for SQL databases, often in conjunction with exploitable remote code execution (RCE) vulnerabilities.

Elevated privileges are a common feature of these sales, but not a universal one. Many types of malware, including ransomware, need elevated privileges in order to run. Higher privileges can also enable attackers to create their own accounts or take other measures to use as additional persistence mechanisms, providing redundancy for the access that they purchased. Domain administrator credentials are a common component of these sales, in conjunction with a form of remote access. Some forms of remote access for sale may also come with their own elevated privileges.

Applying the MITRE ATT&CK Framework

The MITRE ATT&CK framework can clarify the division of labor in a breach between the initial intruders and the buyers that later exploit this access. The initial intruders conduct the first ten stages of an attack: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, and Lateral Movement. The buyers focus on the final four stages of an attack: Collection, Command and Control, Exfiltration, and Impact (see Figure 3).

Forum advertisements provide varying degrees of insight into the specific tactics that the initial intruders and the buyers use at each stage of an attack. For example, the sellers do not typically disclose their Initial Access tactics, but, as referenced above, the use of Valid Accounts (T1078), External Remote Services (T1133), and Exploit Public-Facing Application (T1190) is probably common. The forum posts provide greater insight into the initial intruders' Persistence tactics, since the posts typically specify what persistence mechanisms they will transfer to buyers. Valid Accounts (T1078) are clearly the main form of persistence, since these offerings typically include credentials. Many of these credentials are for External Remote Services (T1133), such as RDP or VPNs. Web shells (T1505) also establish persistence on web servers. Web servers can provide access to a broader internal network, but they can also be targets of interest in their own right for the public-facing services that they provide.

Privilege Escalation is another key stage for the initial intruders, given the frequency with which these offerings include domain administrator accounts or other highly privileged credentials. These forum posts typically do not disclose the initial intruder's Privilege Escalation tactics either, but it is reasonable to presume that Valid Accounts (T1078) is among them, given the regularity with which these offerings include highly privileged accounts. This and earlier uses of Valid Accounts (T1078) depend in large part on Credential Access tactics. While the forum posts typically do not disclose these tactics either, the frequency with which these offerings include RDP credentials suggests the use of Brute Force (T1110), among others. Brute force is a preferred tactic for use against RDP credentials by criminals. It is reasonable to assume that initial intruders conduct internal network reconnaissance, or Discovery, on these networks before selling them. IntSights identified one access vendor who includes internal network reconnaissance details as part of his standardized offerings.

Security researchers have less insight into what buyers do with the access that they have purchased, as there is no business reason for them to disclose that information on the forums. The frequency with which ransomware operators in particular purchase these intrusions nonetheless suggests that Data Encrypted for Impact (T1486) is probably one of the most common Impact techniques. It is reasonable to assume that buyers, including ransomware operators, also engage in the Collection and Exfiltration of profitable data from compromised networks, but those techniques may vary considerably from one buyer to another. By the same token, Command and Control techniques may vary considerably, depending on which ransomware or other types of malware the buyers might deploy (if any).

Applying the MITRE ATT&CK Framework

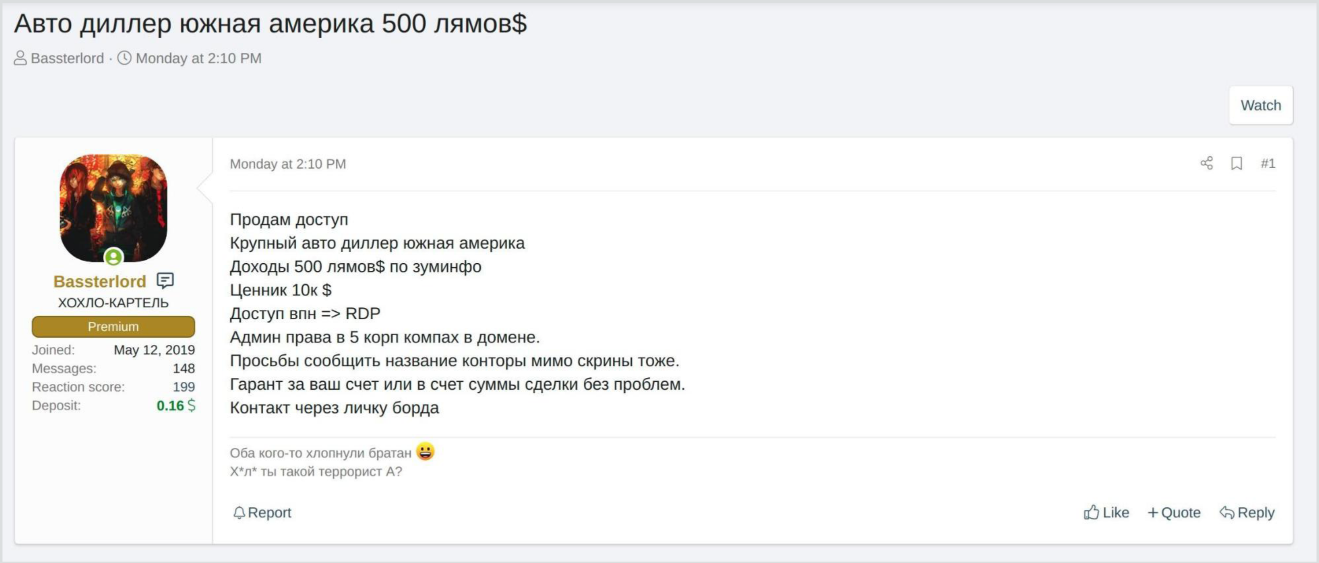
Sellers				Buyers
Initial Access	**Persistence**	**Privilege Escalation**	**Credential Access**	**Impact**
Valid Accounts (T1078)	Valid Accounts (T1078)	Valid Accounts (T1078)	Brute Force (T1110)	Data Encrypted For Impact (T1486)
External Remote Services (T1133)	External Remote Services (T1133)			
Exploit Public-Facing Application (T1190)	Web Shell (T1505.003)			

Figure 3

Quantitative and Qualitative Analysis of Underground Network Access Sales

IntSights conducted quantitative and qualitative analysis of a sample of 46 sales of network access on underground forums covered in alerts we provided to IntSights customers from September 2019 to May 2021. This analysis yielded the following observations about the sources and pricing of these compromises, as well as the distribution of their victims and perpetrators by industry and geography.

The sample includes 30 offerings from Russian-language forums (65%) and 16 offerings from English-language forums (35%). This predominance of offerings from Russian-language forums reflects the leading position of Russian-speaking criminals in the underground cybercrime economy. It is worth noting that there is no consistent English terminology for these sales, either among criminals or security researchers, although some researchers use the term "access brokers" to describe these sellers. Russian-speaking sellers do, however, frequently use the term "**продам доступ**," or, "I will sell access." This stock phrase occurs repeatedly in Russian-language advertisements for these sales, either in the title of the thread or at the very beginning of the initial post (see Figure 4). This more consistent terminology and labeling make these advertisements easier to search for with keywords, or to spot while skimming.



Авто диллер южная америка 500 лямов$

Bassterlord · Monday at 2:10 PM

Bassterlord
ХОХЛО-КАРТЕЛЬ
Premium
Joined: May 12, 2019
Messages: 148
Reaction score: 199
Deposit: 0.16 $

Monday at 2:10 PM #1

Продам доступ
Крупный авто диллер южная америка
Доходы 500 лямов$ по зуминфо
Ценник 10к $
Доступ впн => RDP
Админ права в 5 корп компах в домене.
Просьбы сообщить название конторы мимо скрины тоже.
Гарант за ваш счет или в счет суммы сделки без проблем.
Контакт через личку борда

Оба кого-то хлопнули братан 😀
Х*л* ты такой террорист А?

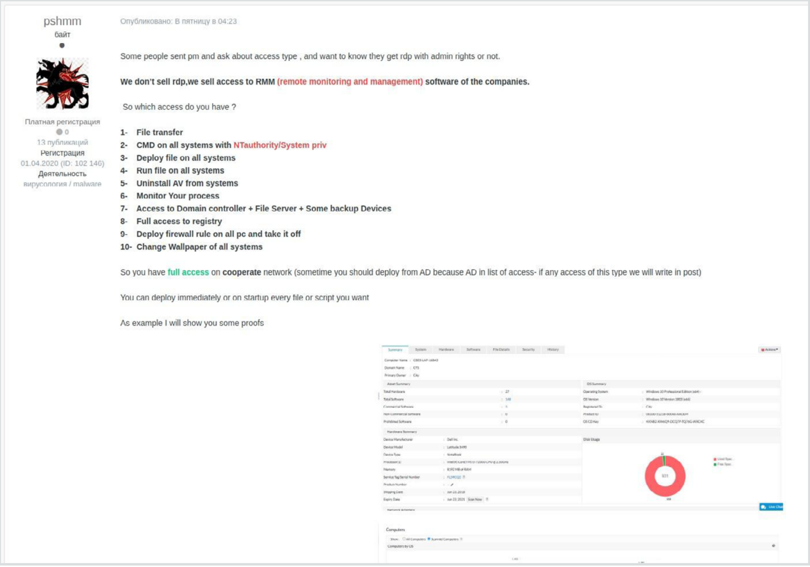
Figure 4

Vendor Analysis

Equally clear is the predominance of a handful of specialized access vendors. Just seven individuals were the source of the majority of these offerings (26 out of 46, or 56.5%): usernames "pshmm" (8), "drumrlu" (5), "7h0rf1nn" (4), "Cipher_Strike" (3), "iannker" (2), "Sheriff" (2), and "mont4na" (2). This concentration of inventory among a relatively small number of specialized vendors highlights the degree to which the division of labor drives the supply of compromised networks for this niche market.

The two most prolific vendors have refined and standardized their advertisements more than their counterparts. For example, "pshmm" explained that their standard offerings enable access to networks via remote monitoring and management (RMM) software, rather than the more common use of RDP. They also provided a detailed list of capabilities that a buyer will receive as part of their standard access packages, including the ability to: transfer, deliver, and execute files; run commands; disable or uninstall anti-virus software and firewalls; and access Active Directory and registries (see Figure 5).

The second-most prolific vendor, "drumrlu," also has a standard format for their offerings, as in this case of an Italian e-commerce company. Their access packages include domain administrator access, access to Windows NT Directory Services (for Active Directory), and full network reconnaissance details (see Figure 6). The inclusion of network reconnaissance is not a common feature of most access offerings, yet it is appealing to buyers because these details significantly facilitate buyer exploitation of a compromised network by familiarizing them with its architecture and the various machines on it.



pshmm
байт
●
Платная регистрация
● 0
13 публикаций
Регистрация
01.04.2020 (ID: 102 146)
Деятельность
вирусология / malware

Опубликовано: В пятницу в 04:23

Some people sent pm and ask about access type , and want to know they get rdp with admin rights or not.

We don't sell rdp,we sell access to RMM (remote monitoring and management) software of the companies.

So which access do you have ?

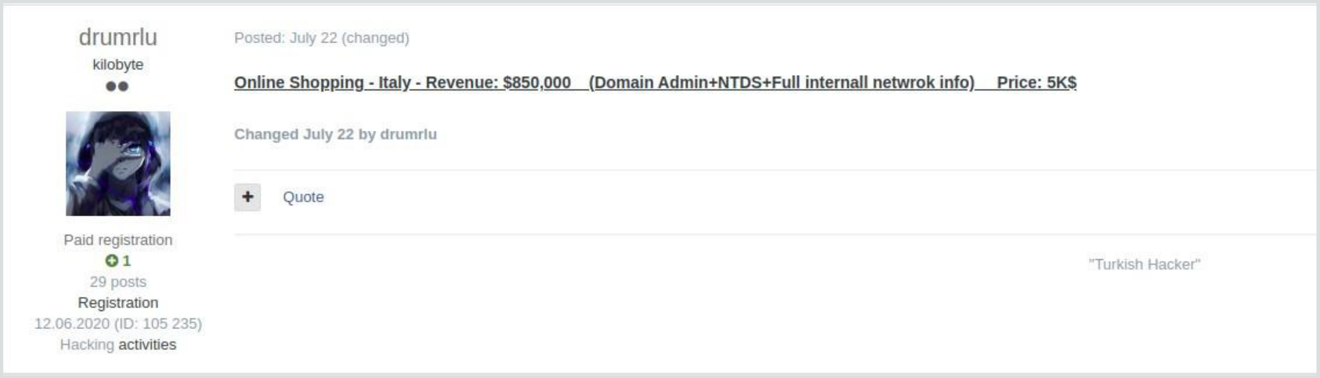
1- File transfer
2- CMD on all systems with NTauthority/System priv
3- Deploy file on all systems
4- Run file on all systems
5- Uninstall AV from systems
6- Monitor Your process
7- Access to Domain controller + File Server + Some backup Devices
8- Full access to registry
9- Deploy firewall rule on all pc and take it off
10- Change Wallpaper of all systems

So you have **full access** on **cooperate** network (sometime you should deploy from AD because AD in list of access- if any access of this type we will write in post)

You can deploy immediately or on startup every file or script you want

As example I will show you some proofs

Figure 5



drumrlu
kilobyte
●●
Paid registration
● 1
29 posts
Registration
12.06.2020 (ID: 105 235)
Hacking activities

Posted: July 22 (changed)

Online Shopping - Italy - Revenue: $850,000 (Domain Admin+NTDS+Full internall netwrok info) Price: 5K$

Changed July 22 by drumrlu

"Turkish Hacker"

Figure 6

Victim Geography

The geographic concentration of victims (see Figure 7) fits broader trends in underground criminal activity. Nearly all (40) of the 46 offerings in this sample specified the locations of their victims, and 15 of those 40 offerings (37.5%) were in North America (either the US or Canada). This disproportionate emphasis on North America reflects the preference of these criminals for both wealthy economies and English-speaking victims. Victims in wealthier countries are generally more lucrative, and English-speaking victims are often easier to compromise because they speak the world's leading *lingua franca.*

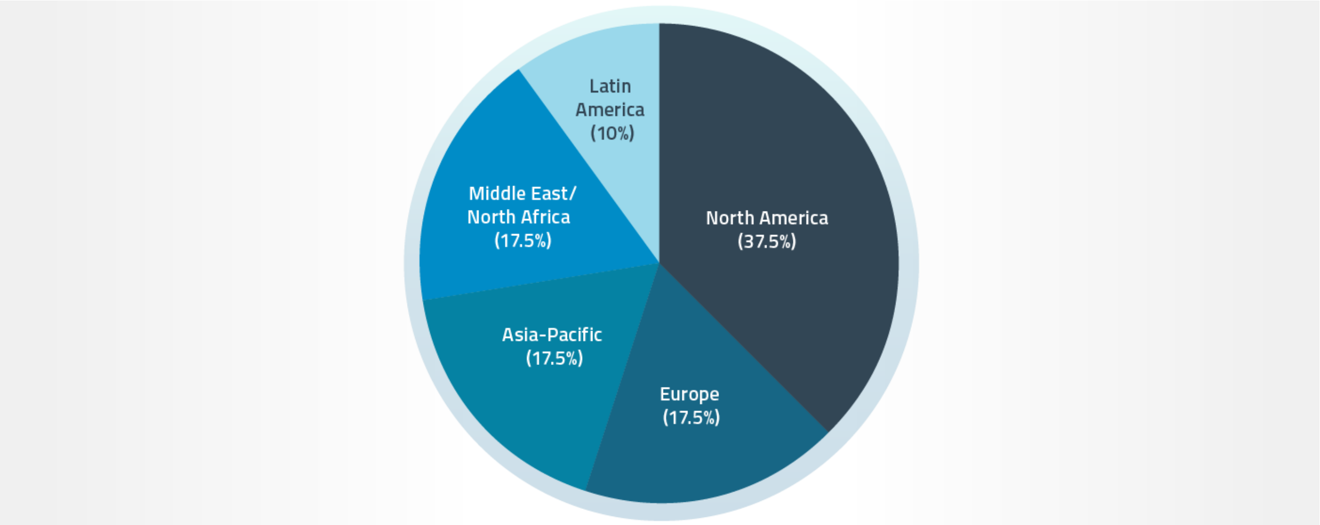
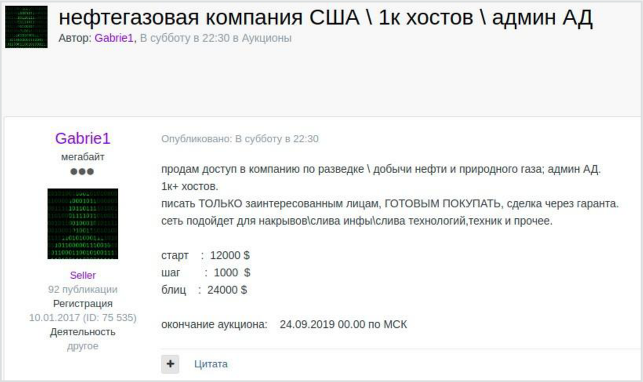


Figure 7

There was no clear geographic focus beyond the disproportionate emphasis on North America. There were seven victims each (17.5%) in Europe, Asia-Pacific, and the Middle East and North Africa. European targets are also desirable victims because of the relative wealth of European economies. The Asia-Pacific region has both large and wealthy economies as well, but four of the seven victims in this region were in India. Indian organizations are desirable targets for criminals due to the widespread use of English in India, and the outsourcing of many Western business operations to India.

The Middle East is of interest to criminals to a degree disproportionate to the size of its population and geographic area due to the hydrocarbon-based wealth of Saudi Arabia, the UAE, and other affluent monarchies in the Arabian Peninsula. A majority (5) of the seven Middle Eastern victims were in these wealthier countries, but, surprisingly, none of them were oil and gas organizations; indeed, the only energy-related organization among them was an electric utility in Jordan, which is neither an affluent country nor a major energy producer. All of the other six Middle Eastern victims were either healthcare or technology and telecommunications organizations. Indeed, all but one of the other oil and gas or energy victims with specified locations were in either North America or Europe. For example, username "Gabrie1" auctioned access to a US oil and gas company (see Figure 8). The United States is also a leading oil and gas producer.



нефтегазовая компания США \ 1к хостов \ админ АД

Автор: Gabrie1, В субботу в 22:30 в Аукционы

Gabrie1
мегабайт
●●●

Seller
92 публикации
Регистрация
10.01.2017 (ID: 75 535)
Деятельность
другое

Опубликовано: В субботу в 22:30

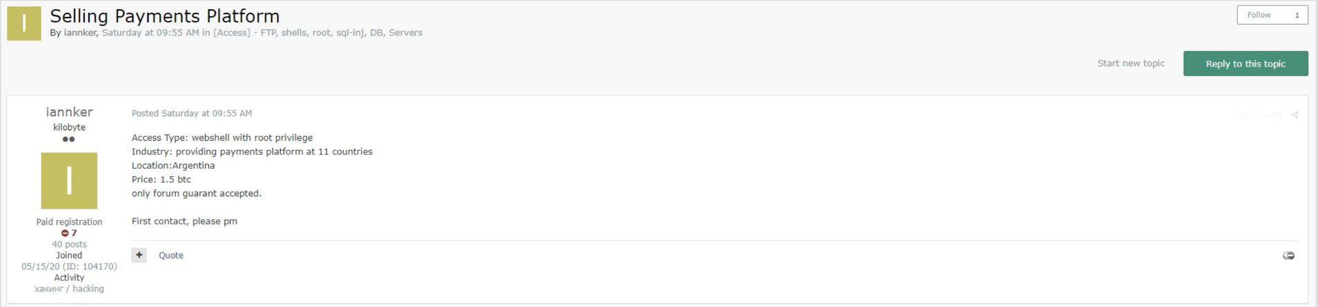
продам доступ в компанию по разведке \ добычи нефти и природного газа; админ АД.
1к+ хостов.
писать ТОЛЬКО заинтересованным лицам, ГОТОВЫМ ПОКУПАТЬ, сделка через гаранта.
сеть подойдет для накрывов\слива инфы\слива технологий,техник и прочее.

старт : 12000 $
шаг : 1000 $
блиц : 24000 $

окончание аукциона: 24.09.2019 00.00 по МСК

Figure 8

In our sample, Latin America had the smallest number of victims, with only four compromised networks for sale. This lower level of interest in developing countries is consistent with broader trends in these underground criminal communities. Nonetheless, this lower level of interest evidently did not deter some access vendors from asking for high prices for access to Latin American targets. For example, in December 2020, username “iannker” asked for the equivalent of approximately $27,000 USD in Bitcoin in exchange for a web shell with root privileges on an Argentina-based payments platform operating in 11 countries (see Figure 9). In this case, it would appear that the main factor in his pricing was the potentially lucrative opportunity to compromise a financial services organization, rather than geography.



Selling Payments Platform
By iannker, Saturday at 09:55 AM in [Access] - FTP, shells, root, sql-inj, DB, Servers

iannker
kilobyte
Paid registration
7
40 posts
Joined
05/15/20 (ID: 104170)
Activity
хакинг / hacking

Posted Saturday at 09:55 AM

Access Type: webshell with root privilege
Industry: providing payments platform at 11 countries
Location:Argentina
Price: 1.5 btc
only forum guarant accepted.

First contact, please pm

Figure 9

Industry Analysis

The sales of network access are a cross-industry phenomenon. In our sample, technology and telecommunications was the most frequently affected industry, representing 10 of the 46 victims (22%). Three other industries tied for a close second place, with nine victims each: financial services, healthcare and pharmaceuticals, and energy and industrials (19.5% each). Other affected industries included automotive (4, or 9%), retail and hospitality (3, or 6.5%), and professional services (2, or 4%) (see Figure 10).

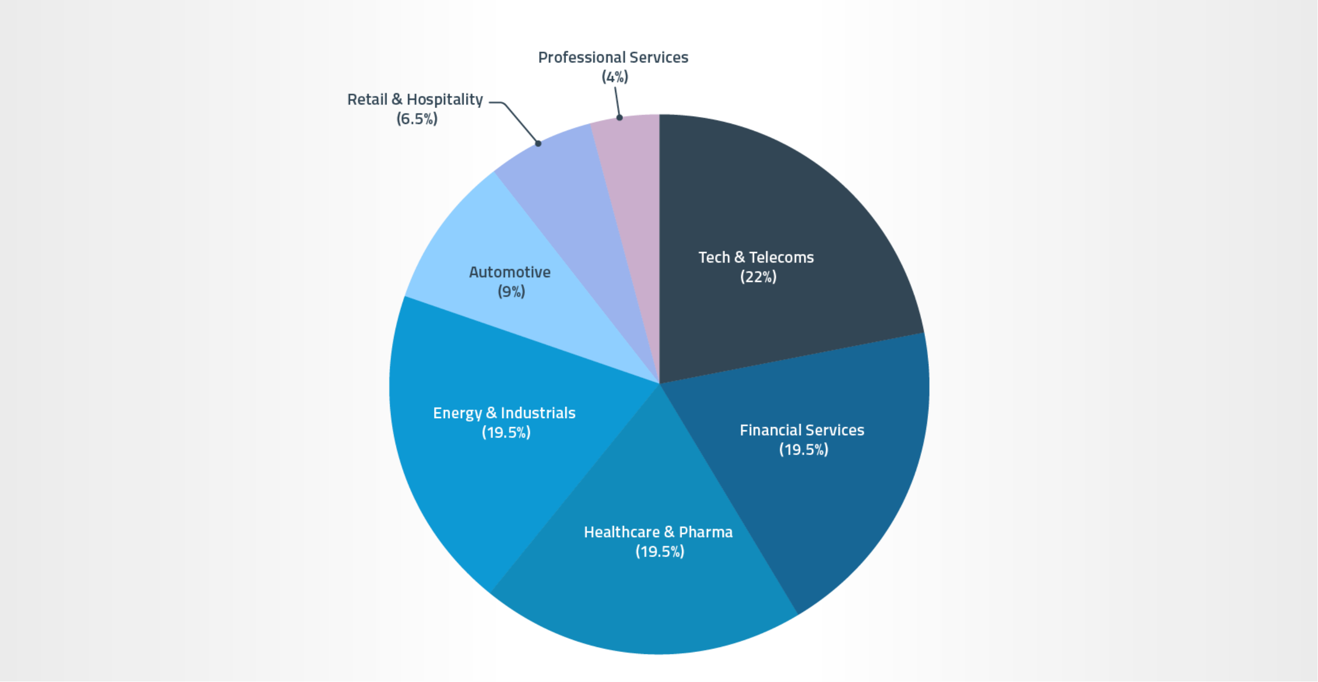


Figure 10

The proportion of retail and hospitality victims for sale is surprisingly low, given the popularity of that industry as a target for members of these underground criminal communities. Ransomware operators are among the main customers of these access brokers, but a ransomware infection may not be the most optimal way to monetize access to a retail and hospitality business. Deployments of PoS malware on physical payment terminals or digital payment card skimmers on e-commerce websites and online payment forms may be more lucrative or reliable ways to monetize such retail and hospitality breaches. Deploying ransomware while payment card collection is in progress would be counterproductive; it would disrupt the flow of payment card data and alert the victim to the presence of an intruder, and thus "kill the goose that lays the golden eggs."

Despite the relatively small number of retail and hospitality victims, the second-most expensive offering in this sample, with an asking price of approximately $66,000 USD worth of Bitcoin at the time, was for access to an organization supporting hundreds of retail and hospitality businesses. The victim was a third-party operator of customer loyalty and rewards programs. The seller highlighted the various ways in which a buyer could monetize this access, including: review and manipulation of source code; access to the accounts and points of loyalty program members; and spam and phishing attacks, including ransomware campaigns against loyalty program members via legitimate communication channels. Customer loyalty programs, such as airline frequent flier programs, are desirable targets for many criminals due to their typically less extensive anti-fraud measures, compared to payment cards.

Pricing Characteristics

Pricing varies considerably from one sale to another. Factors that can influence pricing include: the extent and the privilege level of the access; the size and value of the victim as a source of criminal revenue; the industry and location of the victim; and the sales strategies of the various sellers. Of the 46 offers, six did not specify a price and allowed prospective buyers to make their own offers and name their own prices. Another six of these sales took the form of auctions; for this statistical analysis, IntSights used an average of the opening bid and the "buy now" price as if it were a fixed price.

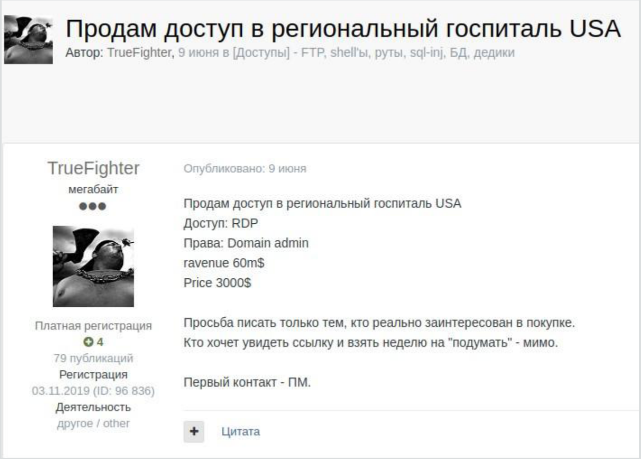
The average price for those 40 sales was approximately $9,640 USD, and the median price was $3,000 USD. The large discrepancy between the average price and the median price is attributable in large part to a few unusually high prices among the most expensive offerings. IntSights researchers view the median price of $3,000 USD as a more representative example of typical pricing for these sales. Indeed, $3,000 USD was not just the median price but also the single most common price; five of the 40 offerings with some form of specified pricing, or 12.5%, had exactly that price. IntSights researchers view the average price of $9,640 USD as a better indicator of the higher end of the typical price range. When ranked in ascending order, the list of these 40 prices only met or exceeded the average of $9,640 USD in the top quartile, or among the 10 highest prices of these 40. This higher end of the price range began at $10,000 USD, with three offerings at exactly that price. In the lowest quartile (the 10 lowest prices among these 40 offerings), all but the highest one were just three figures in USD.

These figures support the following anecdotal observations of IntSights researchers: a majority of these offerings are in the four-figure range in USD; the more expensive offerings have five-figure prices in USD; and the cheapest offerings have three-figure prices in USD.

An examination of the higher and lower prices sheds light on the factors that influence pricing. For example, the single lowest price of $240 USD was for access to a healthcare organization in Colombia. Criminals typically prefer victims in wealthier countries with advanced economies, as they are generally more lucrative. Prices for access to healthcare organizations also trend lower due to the perception that they are easier to compromise (which may have an element of truth to it) and due to the balance or imbalance of supply and demand. Healthcare organizations were the victims of nine of the 46 offerings in this sample, or 19.5% of the total. Healthcare pricing also trends significantly lower than other industries, with an average price of $4,860 USD and a median price of $700 USD in this sample. Healthcare organizations have long been popular targets for ransomware operators, well before these sales of access matured. The lower cost of buying access to healthcare organizations has probably made them an even more desirable target for those ransomware operators that depend on these sellers.

This July 2020 healthcare offering from username "TrueFighter" was practically a textbook example of network access sales. The post features the easily spotted Russian "I will sell access" label in both the title of the thread and at the beginning of the initial post on that thread. The unnamed victim was a US regional hospital network with $60 million USD in revenue. The seller offered a combination of RDP access and domain administrator credentials for $3,000 USD. Hospitals are popular targets for ransomware attacks, which probably made this offering attractive to many ransomware operators. RDP is a common form of remote access in these sales, and domain administrator credentials give buyers high privileges with which to execute ransomware payloads or achieve other malicious goals. A thorough and efficient criminal would also probably exfiltrate patient records before deploying ransomware, as patient data is of high value to identity thieves in particular. The figure of $3,000 USD for this offering is the median price for this sample (see Figure 11).

The second-lowest price, $300, was for access to an automotive manufacturing organization in India. As in the above example, a location in a developing country often pushes pricing downward. The offering includes only local administrative privileges within the domain, rather than domain controller privileges, which many actors prefer. The network has a relatively small number of hosts. The variety of ways to monetize access to industrial or manufacturing organizations may also be less obvious to some criminals than the more well-established targets in financial services, retail and hospitality, and healthcare. Ransomware would be an obvious choice, particularly in the wake of the May 2021 Colonial pipeline incident, but the monetization of intellectual property, customer records, or other data from these organizations may be less readily apparent to many criminal consumers (see Figure 12). For an overview of threats to industrial organizations, please consult the recent **IntSights Energy, Utilities, and Industrials Threat Landscape Report.**



Продам доступ в региональный госпиталь USA
Автор: TrueFighter, 9 июня в [Доступы] - FTP, shell'ы, руты, sql-inj, БД, дедики

TrueFighter
мегабайт
●●●
Платная регистрация
4
79 публикаций
Регистрация
03.11.2019 (ID: 96 836)
Деятельность
другое / other

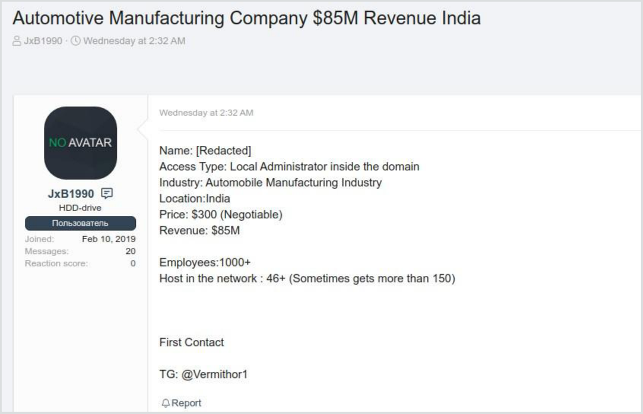
Опубликовано: 9 июня

Продам доступ в региональный госпиталь USA
Доступ: RDP
Права: Domain admin
ravenue 60m$
Price 3000$

Просьба писать только тем, кто реально заинтересован в покупке.
Кто хочет увидеть ссылку и взять неделю на "подумать" - мимо.

Первый контакт - ПМ.

Figure 11



Automotive Manufacturing Company $85M Revenue India
JxB1990 · Wednesday at 2:32 AM

JxB1990
HDD-drive
Пользователь
Joined: Feb 10, 2019
Messages: 20
Reaction score: 0

Wednesday at 2:32 AM

Name: [Redacted]
Access Type: Local Administrator inside the domain
Industry: Automobile Manufacturing Industry
Location:India
Price: $300 (Negotiable)
Revenue: $85M

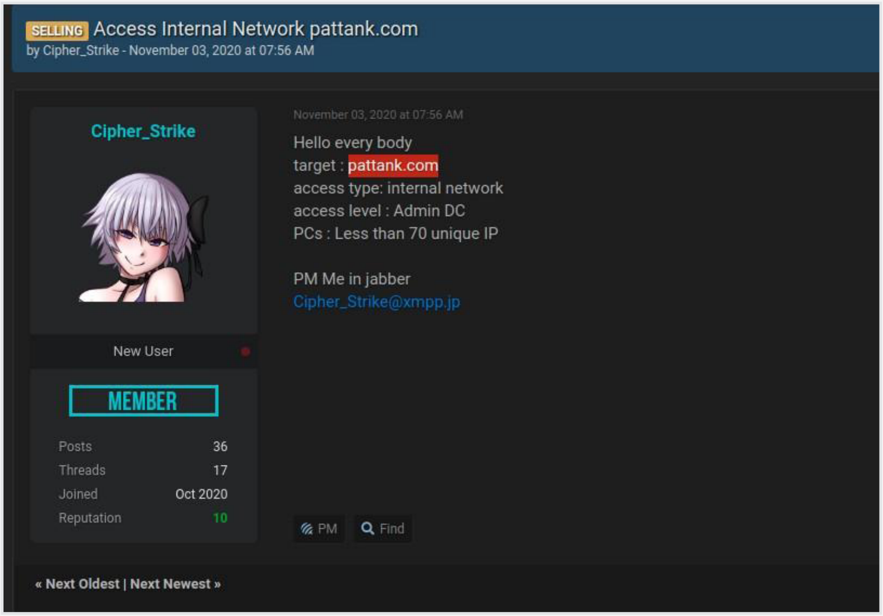
Employees:1000+
Host in the network : 46+ (Sometimes gets more than 150)

First Contact

TG: @Vermithor1

Figure 12

Another one of the cheapest offers, at $700 USD, is also for a manufacturing/industrial organization: a Texas-based company specializing in the construction and repair of above-ground storage tanks for oil and gas, power, chemical, and agricultural companies. This offering commands a somewhat higher price than the above automotive manufacturer, given its US location, the larger number of hosts on the network, and its higher domain controller privileges. Nonetheless, the organization may be a less desirable target and thus command a lower price due to the nature of its business. Many criminals may not see or take interest in the various ways of monetizing access to it, besides ransomware (see Figure 13).



SELLING Access Internal Network pattank.com
by Cipher_Strike - November 03, 2020 at 07:56 AM

Cipher_Strike

New User

MEMBER

Posts	36
Threads	17
Joined	Oct 2020
Reputation	10

November 03, 2020 at 07:56 AM

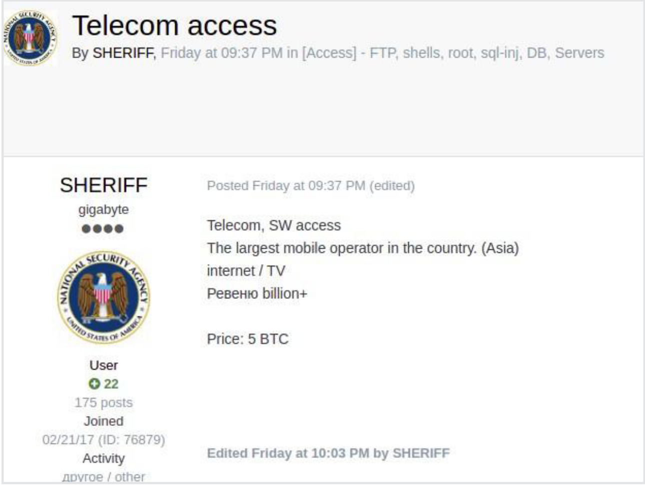
Hello every body
target : pattank.com
access type: internal network
access level : Admin DC
PCs : Less than 70 unique IP

PM Me in jabber
Cipher_Strike@xmpp.jp

Figure 13

At the opposite, higher end of the price range, the technology and telecommunications industry stands out as the most common target. Out of the 10 most expensive offerings in this sample, four of them were for telecommunications or technology companies. Beyond those four, there were only two technology and telecommunications offerings in this sample with specified prices below $10,000 USD, which we have used as the cutoff point for the higher price range. The single most expensive offering in this sample by far, with a price of approximately $95,000 USD worth of Bitcoin (at the exchange rates current at the time), was for a telecommunications service provider. The seller described it as the largest mobile service provider in an unspecified Asian country, with over $1 billion USD in revenue (see Figure 14).

IntSights researchers believe that both the high value and high number of technology and telecommunications companies as breach victims stem from their usefulness for enabling further attacks on other targets. For example, as IntSights highlighted in its [Cyber Threat Landscape of the Telecommunications Industry Report](), criminals seek access to mobile service providers in order to conduct SIM swapping attacks on online banking customers who use two-factor authentication (2FA) via SMS. Their goal is to reassign those customer phone numbers to SIM cards that they control in order to receive 2FA codes for their online banking credentials, enabling them to compromise those accounts. Many cybercriminals conduct these attacks via networks of malicious insiders that advertise their services on these



Telecom access
By SHERIFF, Friday at 09:37 PM in [Access] - FTP, shells, root, sql-inj, DB, Servers

SHERIFF
gigabyte
●●●●

User
22
175 posts
Joined
02/21/17 (ID: 76879)
Activity
другое / other

Posted Friday at 09:37 PM (edited)

Telecom, SW access
The largest mobile operator in the country. (Asia)
internet / TV
Ревеню billion+

Price: 5 BTC

Edited Friday at 10:03 PM by SHERIFF

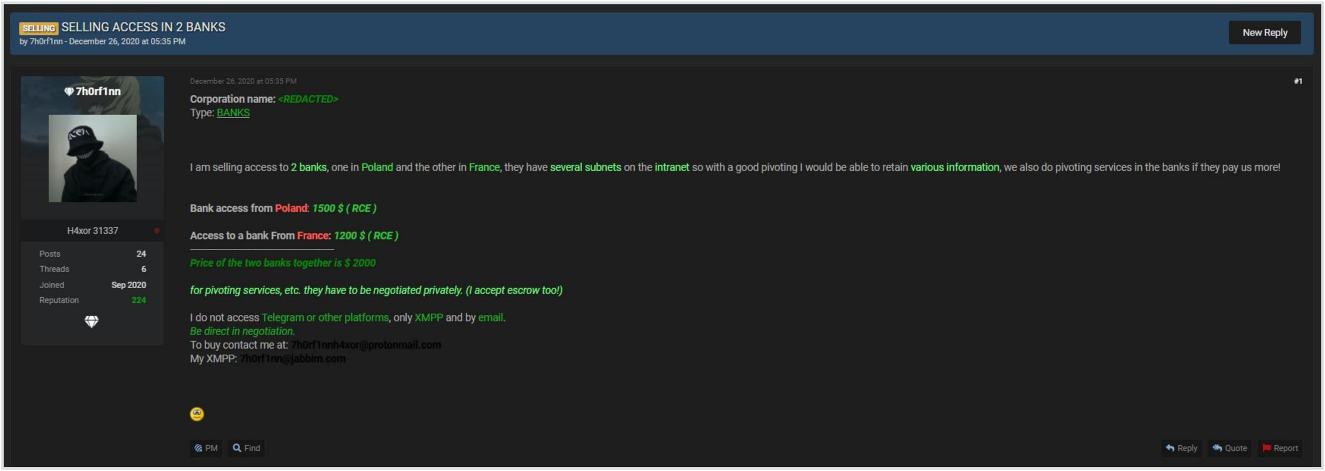
Figure 14

criminal forums. Some of these services charge anywhere from $200 to $400 USD per phone number, which is expensive by the pricing standards of these forums. Buying access to a mobile service provider might cost more up front but could save money for a prolific fraudster in the long term.

Similarly, unauthorized access to technology companies can enable supply chain attacks on those companies' customers, as IntSights highlighted in its **2021 Technology Industry Cyber Threat Landscape Report.** Attackers can compromise software updates or alter source code in order to deliver malicious code to users of a compromised company's software. Even without altering source code, attackers can review it for previously unknown vulnerabilities for them to exploit. Technology company code signing certificates are valuable additions to malware payloads, increasing the chances of evading detection.

The only other industry with more than one representative among the 10 most expensive offerings in this sample is the financial services industry. Banks and other financial services organizations are a top target for cybercriminals because they are among the most direct sources of the money that they seek to acquire, as IntSights highlighted in its **2021 Banking and Financial Services Industry Cyber Threat Landscape Report.**

By the same token and for the same reasons, banks are among the most difficult targets to compromise due to their typically extensive security measures. Indeed, it appears that the financial services offerings in this sample reflect the greater difficulty of compromising these targets. Not a single one of them mentioned any domain administrator or other credentials with similarly high privileges across a network. In many cases, it is unclear if or how much the unauthorized access that is for sale extends beyond public-facing web server infrastructure. The persistence mechanisms for the financial services offerings include a disproportionate number of web shells and WordPress credentials. The web shells often come with root privileges, and the WordPress credentials often have administrative privileges, but it is unclear what if any lateral movement into back-end infrastructure they could enable, with or without privileges. Only one seller, username "7h0rf1nn," specified that enabling such further lateral movement would cost extra (see Figure 15). Prices for such limited access to banks are nonetheless notably higher than other offerings with similarly limited access to businesses in other industries.



SELLING ACCESS IN 2 BANKS
by 7h0rf1nn - December 26, 2020 at 05:35 PM

December 26, 2020 at 05:35 PM

Corporation name: <REDACTED>
Type: BANKS

I am selling access to 2 banks, one in Poland and the other in France, they have several subnets on the intranet so with a good pivoting I would be able to retain various information, we also do pivoting services in the banks if they pay us more!

Bank access from Poland: *1500 $ (RCE)*

Access to a bank From France: *1200 $ (RCE)*

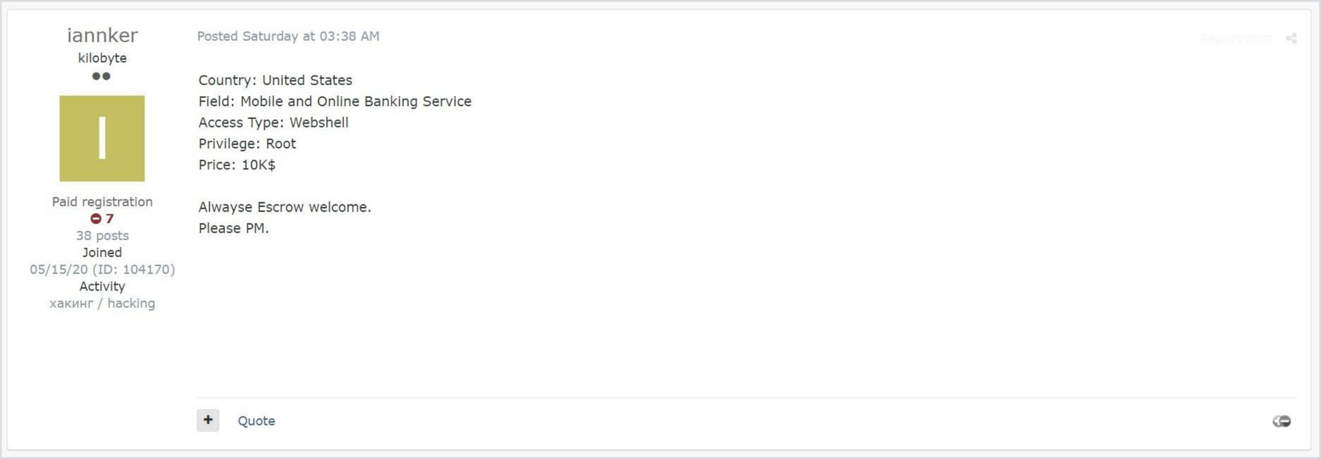
Price of the two banks together is $ 2000

for pivoting services, etc. they have to be negotiated privately. (I accept escrow too!)

I do not access Telegram or other platforms, only XMPP and by email.
Be direct in negotiation.
To buy contact me at: [redacted]
My XMPP: [redacted]

Figure 15

For example, username "iannker" quoted a price of $10,000 USD for a web shell with root privileges at a US online bank in October 2020. It is unclear if the offering includes lateral movement into the bank's internal network as well or merely access to public-facing web servers. Such web server access could enable fraud or other malicious actions against that bank's customers, which would still make this access a lucrative investment even without lateral movement across the network (see Figure 16).



Country: United States
Field: Mobile and Online Banking Service
Access Type: Webshell
Privilege: Root
Price: 10K$

Alwayse Escrow welcome.
Please PM.

Figure 16

The dates of these offerings are consistent with the anecdotal observations of security researchers that the COVID-19 pandemic and the associated rise of the remote workforce contributed to the increase in these sales. The sudden and widespread adoption of remote access services, such as RDP and VPNs, served as significant enablers for breaches, including those that attackers ended up selling to other criminals. There was a dramatic spike in these offerings in July 2020, after the initial lockdowns and the shift to remote work had time to impact organizations on a longer-term basis and attackers had time to adapt to “the new normal.” There was a steady stream of new offerings over the course of October, November, and December 2020, as the United States and Europe experienced subsequent infection waves.

How Can We Use Intelligence to Detect and Respond to Compromises?

These sales are significant enablers for criminal threats, but they also present opportunities for security professionals to detect and thwart attacks. The types of credentials and persistence mechanisms that these sellers transfer most frequently should be higher-priority targets for security teams. For example, audits or other scrutiny of these types of credentials and persistence mechanisms could be useful for threat hunters. By the same token, organizations that receive notifications of the sale of unauthorized access to their networks on these forums should begin their incident response by reviewing logs for the types of credentials and persistence mechanisms identified in the advertisement for that sale.

Other intelligence derived from these advertisements should also inform incident response teams. Many incident response teams or other security professionals may assume that there is continuity over the course of all stages of a breach, from initial access to the exfiltration of compromised data. The very existence of these sales on criminal forums demonstrates that this assumption is often false, and it could lead incident response teams to flawed conclusions about a breach. The tools, tactics, and infrastructure of the initial intruders may vary significantly from those of the subsequent buyers who exploit that access. Observed changes or discontinuities in indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) may reflect and result from these transfers of access. For example, an investigation may indicate that the initial intruders used IP addresses resolving to a specific ISP or geographic area. The subsequent disappearance of those IOCs from network logs could lead investigators to the false conclusion that the attack ended, when in fact it merely changed hands and transitioned to a new group of actors using different infrastructure.

The amount of time that it takes to sell network access may give security teams more time to detect a breach before a buyer monetizes it or does anything else with it that could cause significant harm. The amount of time needed to find a buyer varies considerably, ranging from hours to months, but a time frame of days or weeks is more typical. If security teams discover an intruder who has had access for a significant period of time but has not yet begun to monetize it, e.g., by exfiltrating profitable files or deploying ransomware, then that delay could indicate that the initial intruder is still waiting for a buyer.

Security researchers can often identify the victims of these sales by posing as prospective buyers in order to elicit more information. Sellers typically do not give the names of victims in their public advertisements, but they may be willing to name victims privately with prospective buyers that they deem credible and trustworthy. Even if a seller is unwilling to identify a victim by name, he may be willing to share screenshots or other details that can enable identification of the victim for notification.

Recommendations

Prevention

Observing the following best practices checklist can help prevent the network compromise events that lead to access sales in the criminal underground:

- Require the use of strong, unique, and frequently changed passwords.
- Require the use of 2FA, particularly for RDP, VPNs, and other remote access services.
- Use mobile authenticator apps, rather than SMS, for 2FA.
- Use rate limiting to defend against brute force attacks, particularly on RDP.
- Monitor credential dumps for email addresses from your organization’s domain.
- Update VPN software to ensure that it has the latest security patches.
- Disable remote access services that employees no longer need as they return to the office.
- Urge remote employees to change default passwords and update firmware on home routers.
- Issue devices with endpoint and network security monitoring for long-term remote employees. Ensure that they receive regular security updates and comply with other security policies.
- Establish a system of frequent, segmented, and redundant backups from which to restore encrypted files in the event of a ransomware infection.

Mitigation

The following are best practices for mitigation, should you find that access to your network is up for sale:

- If you receive a report that access to your network is for sale on a criminal forum, contact the security researcher that reported it. The security researcher may be able to elicit additional useful details about the breach from the seller by posing as a prospective buyer.
- If the advertisement for access to your network specifies the persistence mechanism or privileged accounts for sale, conduct an audit of those types of accounts for suspicious activity.
- Consult with an attorney before considering the possibility of buying back the unauthorized access to your organization's network, which may have legal implications.
- In the event of a ransomware infection, incident response teams should determine the full scope of the breach culminating in the encryption of files. Ransomware operators typically conduct other malicious activities, such as the exfiltration of profitable data, before encrypting files.
- Refrain from paying ransoms to ransomware operators. Many ransom payments do not result in file restoration due to technical errors or deceptive ransomware operators. Ransom payments encourage further extortion attempts and give criminals more resources for future attacks.

About IntSights

IntSights, **a Rapid7 company**, enables organizations of any type or size to gain the full benefits of external threat intelligence, no matter the size or sophistication of their threat intelligence programs. Unlike any other solution on the market, IntSights takes the complexity out of threat intelligence and delivers instant value without the heavy lift or sizable resource allocation that traditional threat intelligence solutions require. Designed to scale, IntSights is for any company, and frictionless integration of our real-time cyber threat intelligence with existing security infrastructure allows enterprises to maximize return on investment.

IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo. To learn more, visit **intsights.com** or connect with us on **LinkedIn**, **Twitter**, and **Facebook**.