Access for sale

ptsecurity.com

Cyberattacks are growing in number every year—by 19 percent in 2019 alone.[1] One of the main reasons is the low barrier to entry. The Internet's shadier side teems with illegal marketplaces for malware and services used to breach corporate networks. Low-skilled hackers have quickly learned how to put them to good (or rather, bad) use.

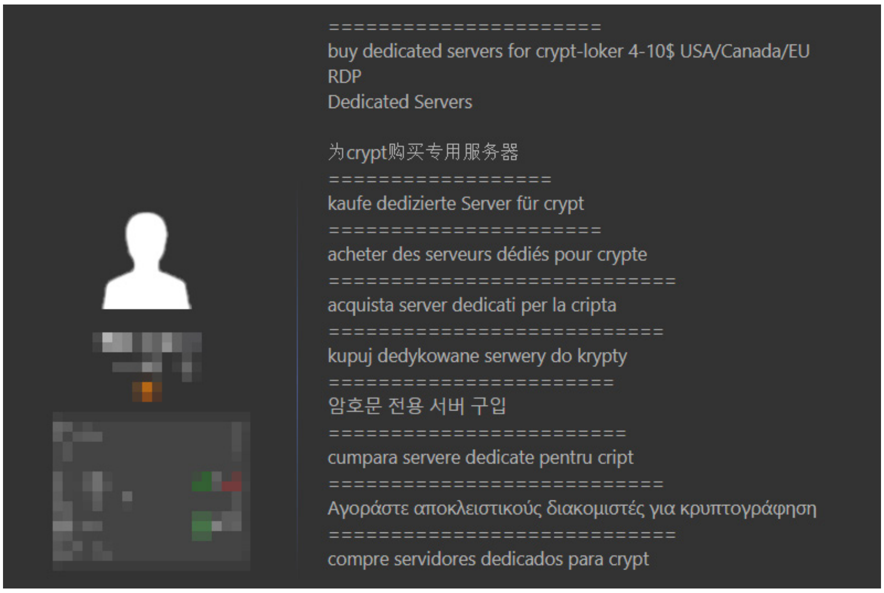
In this article, we will explain what "access for sale" and "ransomware partner program" mean, how dangerous these threats are, and the risks they pose for businesses.

Definition of access

"Access for sale" on the darkweb is a generic term, referring to software, exploits, credentials, or anything else that allows illicitly controlling one or more remote computers. Successfully hacking a website, web server, database, or workstation means that the attacker has access. This access can be transferred or sold to third parties, just like house keys. But for our purposes here, we will only cover access to servers and workstations.

Growing market

Only one or two years back, criminals seemed to be more interested in individual servers. Access to them was sold on the darkweb for up to $20 a pop.



```
======================
buy dedicated servers for crypt-loker 4-10$ USA/Canada/EU
RDP
Dedicated Servers

为crypt购买专用服务器
==================
kaufe dedizierte Server für crypt
======================
acheter des serveurs dédiés pour crypte
============================
acquista server dedicati per la cripta
===========================
kupuj dedykowane serwery do krypty
=======================
암호문 전용 서버 구입
========================
cumpara servere dedicate pentru cript
===========================
Αγοράστε αποκλειστικούς διακομιστές για κρυπτογράφηση
============================
compre servidores dedicados para crypt
```

Figure 1. Sale of ransomware access to remote PCs

However, starting in the second half of 2019, we have seen an increasing number of postings on hacker marketplaces[2] advertising access to local corporate networks.

[1] ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2019/

[2] We analyzed postings on 190 darkweb sites about purchase or sale of malicious tools, as well as custom malware development. We focused on forums, specialized marketplaces, and chat platforms with predominantly Russian- and English-speaking users. On average, over 70 million people visit them each month.

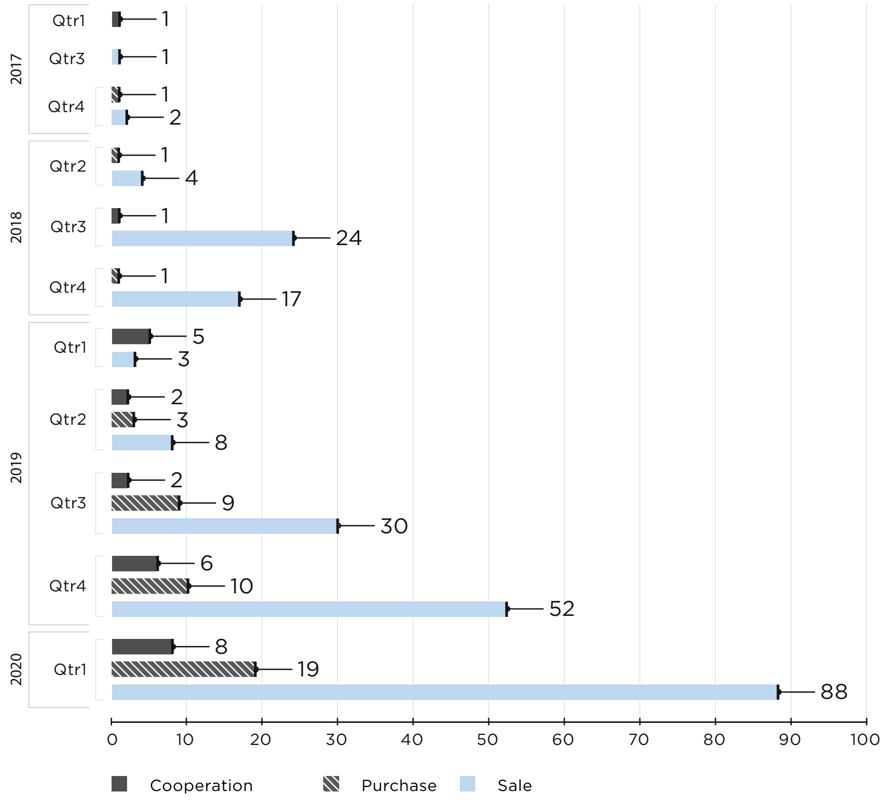
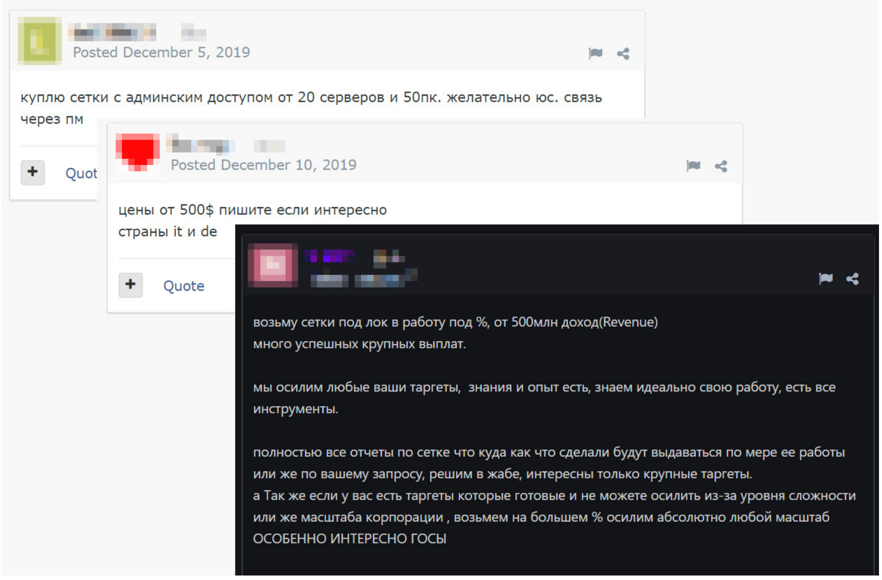


Figure 2. New threads on darkweb forums discussing access to corporate networks

Some buyers offer lucrative terms and an ongoing relationship. For example, they may pay out a commission of up to 30 percent of the potential profit for a hack of the infrastructure of a company with annual income exceeding $500 million.



[redacted]
Posted December 5, 2019

куплю сетки с админским доступом от 20 серверов и 50пк. желательно юс. связь через пм

[redacted]
Posted December 10, 2019

цены от 500$ пишите если интересно
страны it и de

[redacted]

возьму сетки под лок в работу под %, от 500млн доход(Revenue)
много успешных крупных выплат.

мы осилим любые ваши таргеты, знания и опыт есть, знаем идеально свою работу, есть все инструменты.

полностью все отчеты по сетке что куда как что сделали будут выдаваться по мере ее работы или же по вашему запросу, решим в жабе, интересны только крупные таргеты.
а Так же если у вас есть таргеты которые готовые и не можете осилить из-за уровня сложности или же масштаба корпорации , возьмем на большем % осилим абсолютно любой масштаб
ОСОБЕННО ИНТЕРЕСНО ГОСЫ

Figure 3. Purchase of access to corporate networks (posting in Russian)

Demand creates supply. At the end of 2019, over 50 accesses to the networks of major companies from all over the world were publicly available for sale. Among the victims were some rather large companies, with annual income running into the hundreds of millions or even billions of dollars.

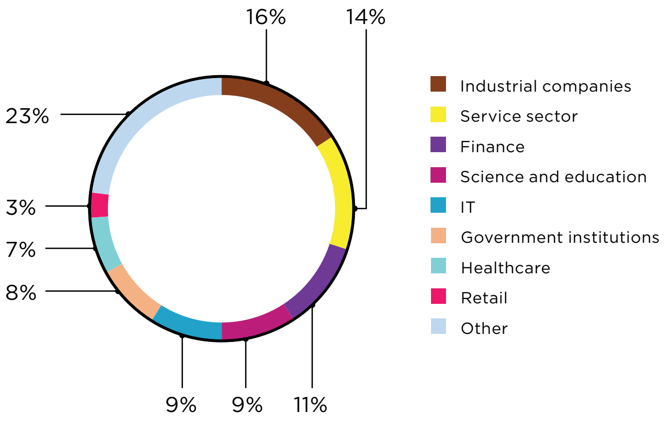


Figure 4. Hacked companies by industry

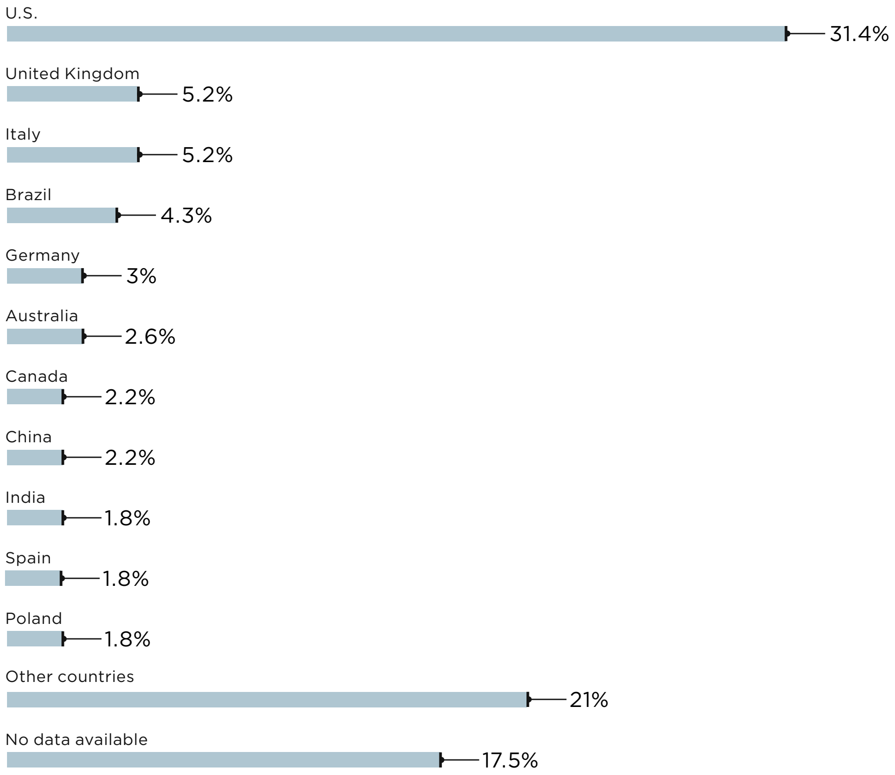
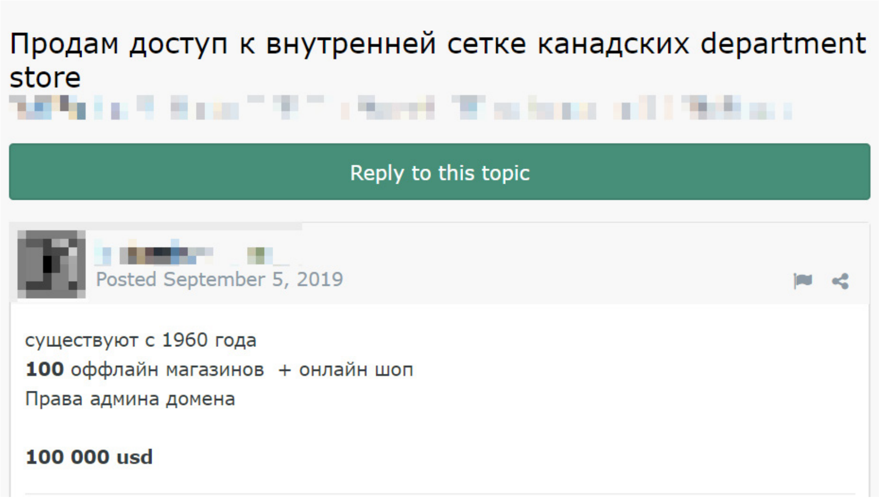


Figure 5. Geographic location of hacked companies

In the U.S., criminals mostly sell access to service sector companies (20%), industrial companies (18%), and government institutions (14%). In Italy, the order was reversed: industrial companies (25%) are followed by service sector companies (17%). In the United Kingdom, the service sector accounts for 33 percent, science and education for 25 percent, and finance for 17 percent. Government institutions (20%) and healthcare (10%) lead in Brazil. In Germany, IT and services each account for 29 percent of accesses for sale. In number six position is Australia, for which most offers involve access to government or science and education. However, by their nature these statistics give a limited picture: in 17 percent of cases, the sellers do not indicate any country in their posts. Many sellers may not advertise their wares at all.

In general, the asking price is in the range of $500 to $100,000. The average cost of privileged access to a single local network is on the order of $5,000.



Продам доступ к внутренней сетке канадских department store

[redacted]

Reply to this topic

[redacted]

Posted September 5, 2019

существуют с 1960 года
100 оффлайн магазинов + онлайн шоп
Права админа домена

100 000 usd

Figure 6. Access can cost as much as $100,000 (posting in Russian)

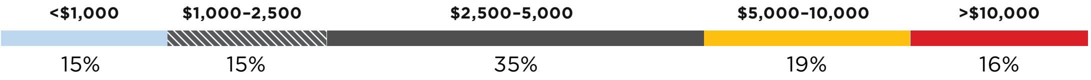
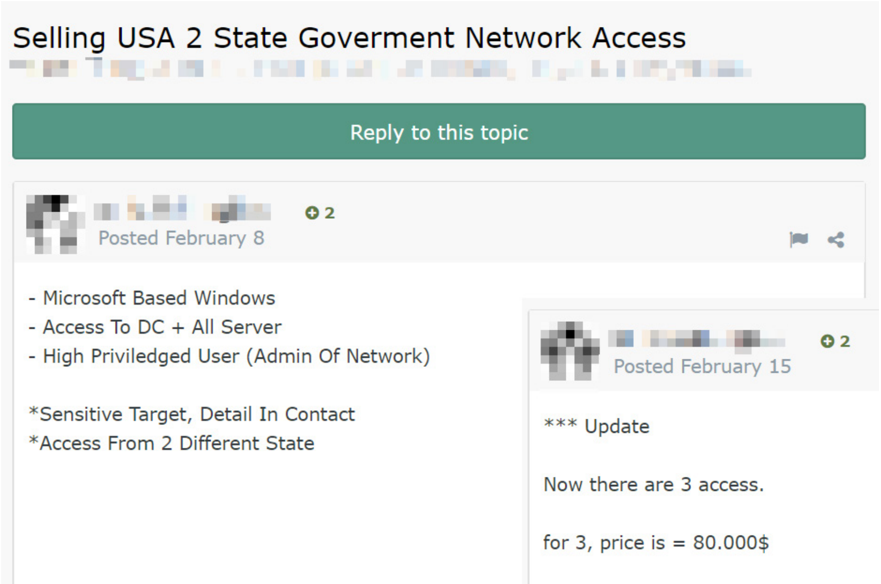


Figure 7. Selling network access on the darkweb

In the past, middling hackers had a hard time monetizing attacks: they did not have the skills to pursue an attack to the point of obtaining a payoff or valuable data. But with the current market demand, they can make a steady income by selling to other criminals.

Buyers can then develop an attack on business systems or hire a team of more skilled hackers who can quickly obtain domain administrator privileges and infect critical servers with malware.



Selling USA 2 State Goverment Network Access

[redacted]

[redacted] 2

Posted February 8

- Microsoft Based Windows
- Access To DC + All Server
- High Priviledged User (Admin Of Network)

*Sensitive Target, Detail In Contact
*Access From 2 Different State

[redacted] 2

Posted February 15

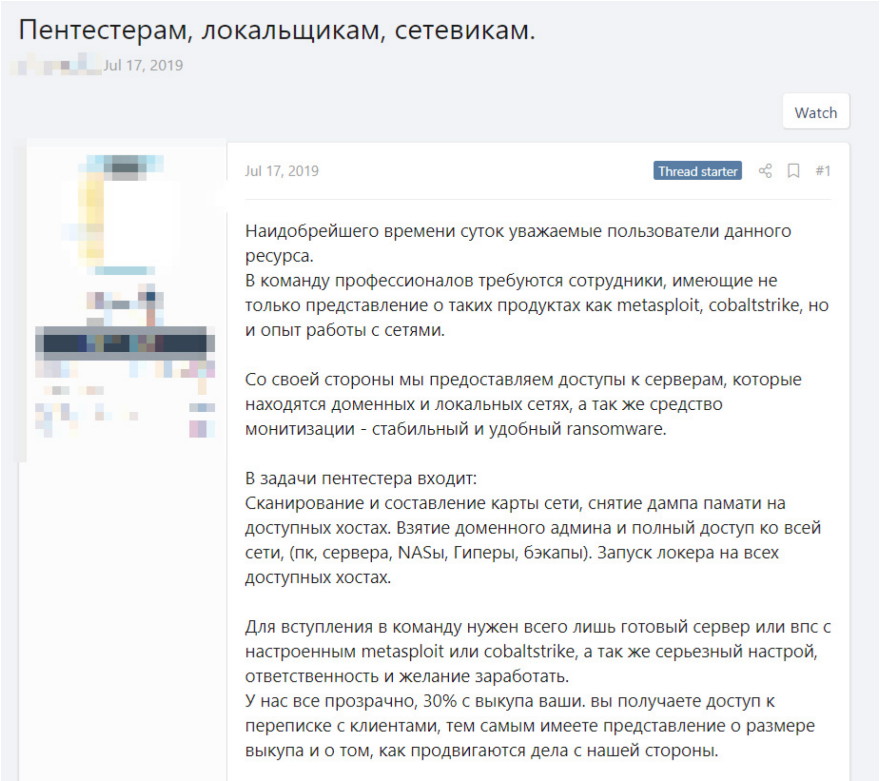
*** Update

Now there are 3 access.

for 3, price is = 80.000$

Figure 8. Advertising domain administrator rights on a government network

The first ones to use this scheme were ransomware operators, who bought access for a fixed price from one set of criminals and then hired other criminals to infect local networks with malware in return for a large percentage of the victim's ransom. On darkweb forums, this setup is known as a "ransomware affiliate program."



Пентестерам, локальщикам, сетевикам.

[redacted] Jul 17, 2019

Jul 17, 2019 Thread starter #1

Наидобрейшего времени суток уважаемые пользователи данного ресурса.
В команду профессионалов требуются сотрудники, имеющие не только представление о таких продуктах как metasploit, cobaltstrike, но и опыт работы с сетями.

Со своей стороны мы предоставляем доступы к серверам, которые находятся доменных и локальных сетях, а так же средство монитизации - стабильный и удобный ransomware.

В задачи пентестера входит:
Сканирование и составление карты сети, снятие дампа памати на доступных хостах. Взятие доменного админа и полный доступ ко всей сети, (пк, сервера, NASы, Гиперы, бэкапы). Запуск локера на всех доступных хостах.

Для вступления в команду нужен всего лишь готовый сервер или впс с настроенным metasploit или cobaltstrike, а так же серьезный настрой, ответственность и желание заработать.
У нас все прозрачно, 30% с выкупа ваши. вы получаете доступ к переписке с клиентами, тем самым имеете представление о размере выкупа и о том, как продвигаются дела с нашей стороны.

Figure 9. Hiring hackers for post-exploitation (posting in Russian)

Consequences for companies

Large companies stand to become a source of easy money for low-skilled hackers. External attacks on corporate infrastructures will increase significantly. This issue is especially acute now that so many employees are working from home. Hackers will look for any and all security lapses on the network perimeter, such as an unprotected web application, non-updated software, or incorrectly configured server with a weak administrator password. The larger the hacked company is, and the higher the obtained privileges, the more profitable the attack becomes.

Small and medium-sized companies are commonly believed to be at greater risk from script kiddies[3] due to smaller investments in network security. Being able to spend more, large companies should be better protected. But penetration tests by our experts prove that even the largest companies are vulnerable. Our testers find easy ways to penetrate local networks that do not require particular skill on the part of potential attackers. All the same, small and medium-sized companies have less money available to put into security and, therefore, are at even greater risk.

Companies should ensure comprehensive infrastructure protection, both on the network perimeter and within the local network. Make sure that all services on the perimeter are protected and security events on the local network are properly monitored to detect intruders in time. Regular retrospective analysis of security events allows discovering previously undetected attacks and addressing threats before criminals can steal data or disrupt business processes.

[3] Those who use other people's software to attack computer systems and networks or deface websites. The prototypical script kiddie is a teenager, unable to write their own complex programs or exploits, who seeks to impress friends or fellow computer enthusiasts. Age is not the defining feature, however.

About
Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

ptsecurity.com
info@ptsecurity.com