Criminal Market for Initial Access

ptsecurity.com

Information security is a priority area for companies, and a huge amount of resources, including money, are spent on maintaining an adequate standard of security. According to a Gartner study, global information security spending in 2020 increased by 6.4% compared to 2019, and 61% of more than 2,000 CIOs surveyed named investment in information security their top priority in planning the corporate budget. However, injecting large amounts of cash and hiring qualified personnel may not be enough.

Generally accepted approaches to threat assessment provide for classification of potential intruders and construction of a security system that considers the capabilities of certain intruder types. Some companies tend to believe that they are of no interest to large APT groups or other serious threat actors, and that less experienced attackers are not capable of causing damage to the business. If they make an inadequate assessment of the potential attacker's capabilities, their security will prove ineffective.

> Because the criminal market for initial access is well developed and popular, former distinction between experienced and low-skilled attackers has now been blurred.

We have already written about the initial access market. In the new study, we will assess how this market has evolved throughout 2020 and early 2021, and what the implications of this for businesses can be. We have analyzed ten most popular Russian and English forums on the dark web that offer access to corporate networks, and ads seeking hackers for hire or hacking partners. The boards have a total of more than eight million registered users, more than seven million threads have been started, and more than 80 million messages have been posted.

How the dark web access-for-sale market has transformed

The market for access to corporate networks has evolved for the past few years. It could be assessed as mature as early as the beginning of 2020. A factor that contributed to this level of development is an increase in ransomware attacks: members of ransomware partner programs often use offers available on the access-for-sale market.

Background

A decade ago, you could already buy access to individual users' computers on a dark web marketplace. Most lots went to fraudsters who engaged in carding, i.e. unauthorized use of bank cards without the owners' knowledge. They were followed by cybercriminals using ransomware against individual users. At some point, ransomware distributors acquired access to a corporate network, easily carried out an attack and received a ransom: this gave rise to a trend for using initial access in attacks on organizations.

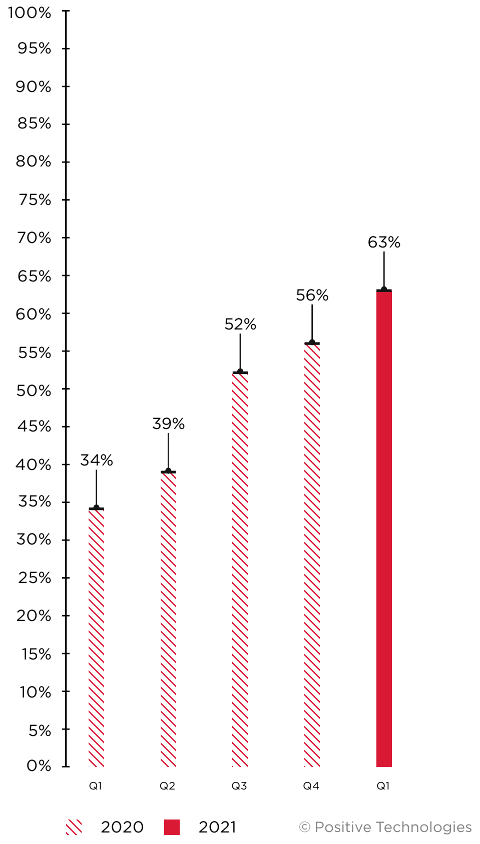


Figure 1. Percentage of ransomware attacks out of all malware attacks on organizations

The number of new ads for access on dark web forums increased with each quarter throughout the observed period. Most of these were ads for sale of access to corporate networks that have been breached. In 2020, we identified 707 new ads for sale of access. Compared with 2019, the number of new ads increased sevenfold. As many as 590 new offers were found in the first quarter of 2021 alone. The number of new ads seeking partners and hackers for hire also increased: it is safe to assume that this was due to the emergence of new ransomware partner programs and the expansion of existing groups that distribute this type of malware.

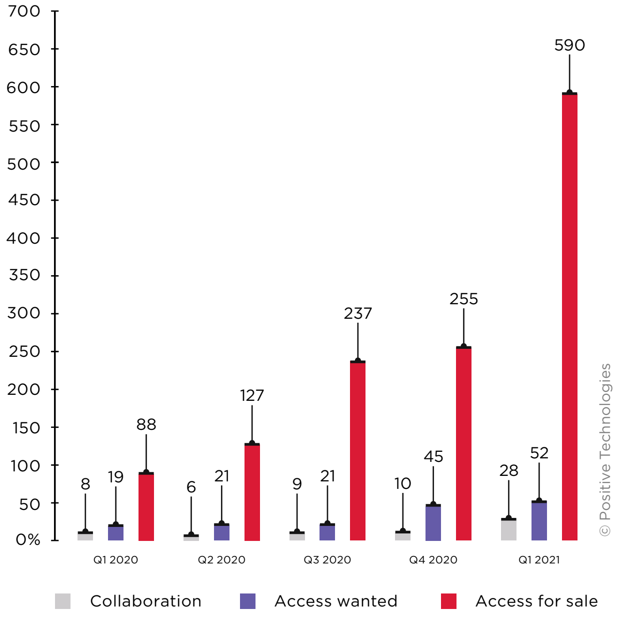


Figure 2. New ads on dark web forums for access to corporate networks

Another indication of interest in access is the number of users placing ads for buying access, selling access, or collaborating. The first quarter of 2021 saw the number of the users triple year on year.

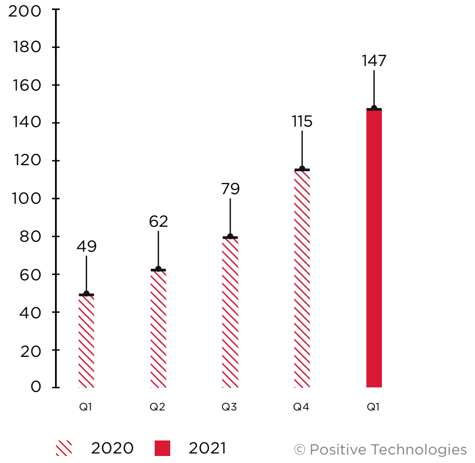
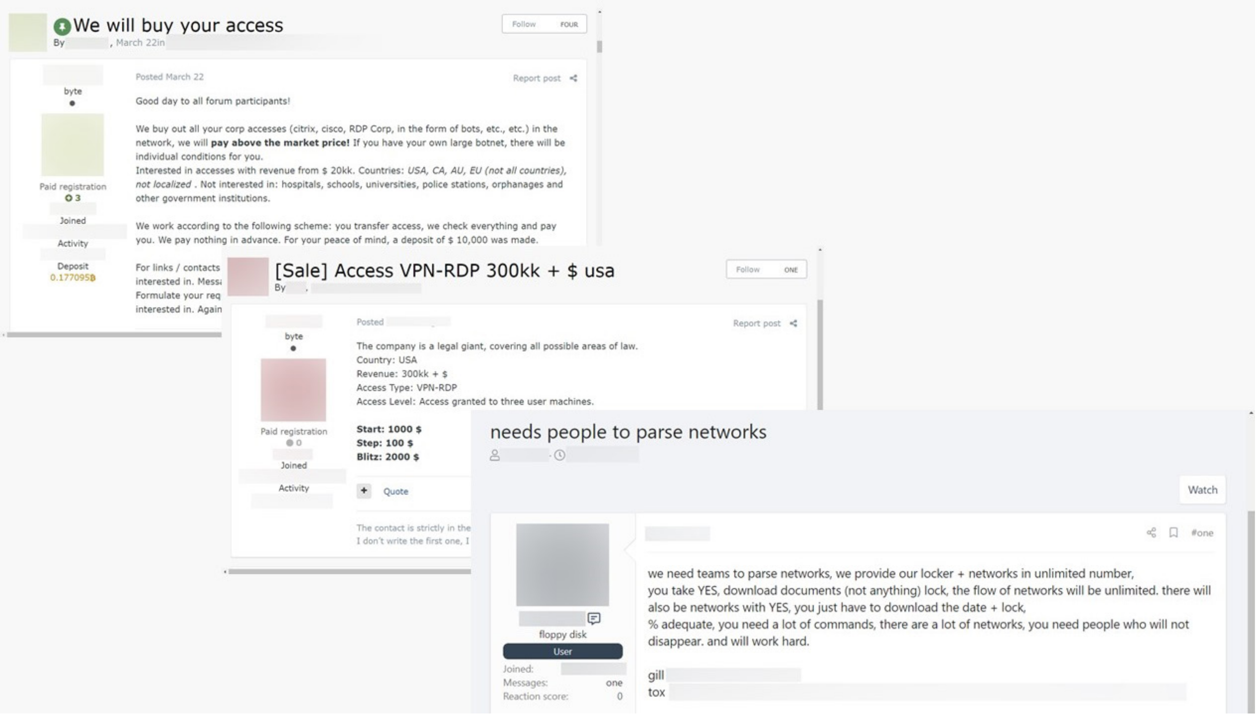


Figure 3. Users on forums posting initial access ads

About $600,000 worth of corporate network access is sold on the dark web on a quarterly basis. Although the number of available offers is increasing, the cumulative worth is changing only slightly, indicating that the average price per access is going down. Cheap access typically carries no access privileges, and it is usually offered by inexperienced cybercriminals who are afraid of following through with the attack. In general, the cost of access usually depends on:

- Number of computers to be exposed
- Account privileges
- Company size
- Corporate revenue and other financial indicators
- Industry



We will buy your access

By , March 22in

Posted March 22

Good day to all forum participants!

We buy out all your corp accesses (citrix, cisco, RDP Corp, in the form of bots, etc., etc.) in the network, we will **pay above the market price!** If you have your own large botnet, there will be individual conditions for you.
Interested in accesses with revenue from $ 20kk. Countries: *USA, CA, AU, EU (not all countries), not localized* . Not interested in: hospitals, schools, universities, police stations, orphanages and other government institutions.

We work according to the following scheme: you transfer access, we check everything and pay you. We pay nothing in advance. For your peace of mind, a deposit of $ 10,000 was made.

For links / contacts
interested in. Messa
Formulate your req
interested in. Again

[Sale] Access VPN-RDP 300kk + $ usa

By ,

Posted

The company is a legal giant, covering all possible areas of law.
Country: USA
Revenue: 300kk + $
Access Type: VPN-RDP
Access Level: Access granted to three user machines.

Start: 1000 $
Step: 100 $
Blitz: 2000 $

The contact is strictly in the
I don't write the first one, I

needs people to parse networks

we need teams to parse networks, we provide our locker + networks in unlimited number,
you take YES, download documents (not anything) lock, the flow of networks will be unlimited. there will also be networks with YES, you just have to download the date + lock,
% adequate, you need a lot of commands, there are a lot of networks, you need people who will not disappear. and will work hard.

gill
tox

Figure 4. Sample dark web forum ads

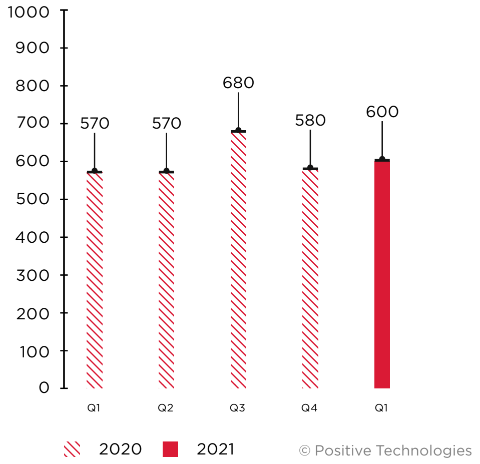
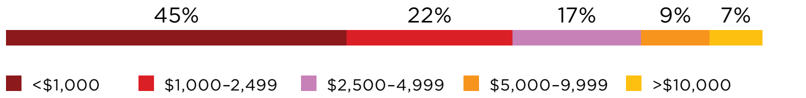


Figure 5. Total worth of access available on dark web forums (Thous. USD)

From 2017 until Q1 2020, the share of ads with a price below $1,000 for access to one company was 15%, and in the period between Q2 2020 and Q1 2021, it increased by 30 percentage points, reaching 45%. The share of expensive access lots priced above $5,000 almost halved in the same period. These changes may reflect mass entry into the market by novice cybercriminals.



© Positive Technologies

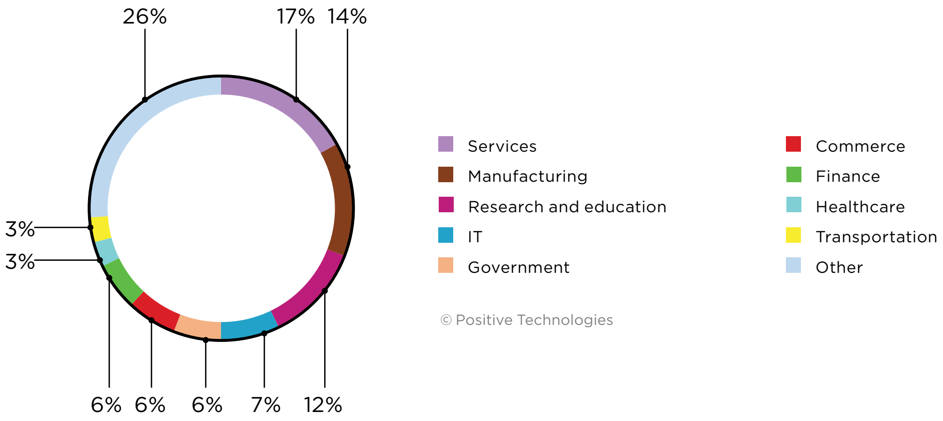
Figure 6. Distribution of offers for sale of access to corporate networks by value

Our forecast has been confirmed: cybercrime now offers a new job, "access miners", which attracts newcomers with the prospects of making a quick buck. Their main goal is to get initial access to a corporate network and then sell it on the dark web.

Can a company find out that someone has sold access to its network?

Credential compromise can be detected, for example, when the seller verifies access prior to sale, or when the buyer verifies access upon purchase. This requires configuring security, such as SIEM systems and network traffic analysis tools, to detect abnormal connections to the infrastructure.

Most companies who had access to their networks put up for sale by cybercriminals belonged to services (17%), manufacturing (14%), and research and education (12%). In the previous review period, the three most common sectors were manufacturing (16%), services (14%) and finance (11%). Research and educational institutions were the fourth most-targeted category, their share of access for sale being 9%. Note that the share of industrial companies and financial institutions, whose networks are typically more expensive to hack, decreased somewhat. This can be attributed to the fact that the access market is filled with low-skilled players who prefer easier victims.



© Positive Technologies

Figure 7. Hacked companies by industry

Business implications

As we can see, the attacker model is changing: an outside intruder who gains initial access to a corporate network and a criminal who follows through with the attack once inside are completely different in terms of skills. Even if the perimeter is hacked by a novice, the local network will be attacked by professionals. They have all the resources to achieve their goal: triggering the most dangerous events for the company, from theft of account funds to complete and lasting disruption of business operations. This means that a system for protection against cyberattacks must be built with these new realities in mind.

About Positive Technologies

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

For 19 years, Positive Technologies has been creating innovative solutions for information security. We develop products and services to detect, verify, and neutralize the real-world business risks associated with corporate IT infrastructure. Our technologies are backed by years of research experience and the expertise of world-class cybersecurity experts.

Over 2,000 companies in 30 countries trust us to keep them safe.

Follow us on social media (LinkedIn, Twitter) and the News section at ptsecurity.com.