The Ideal Ransomware Victim: What Attackers Are Looking For

ke-la.com/the-ideal-ransomware-victim-what-attackers-are-looking-for/

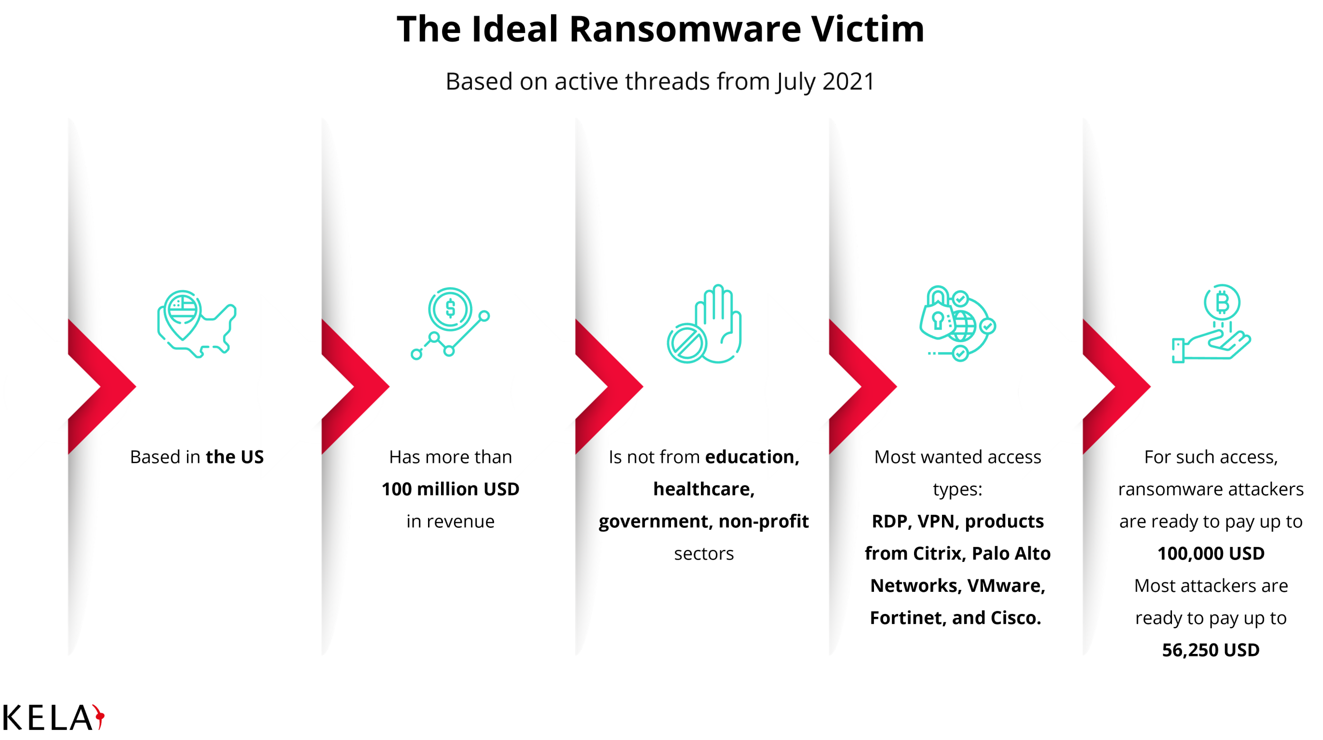
September 6, 2021

In July 2021, KELA observed threat actors creating multiple threads where they claimed they are ready to buy accesses and described their conditions. Some of them appear to use access for deploying info-stealing malware and carrying out other malicious activities. Others aim to plant ransomware and steal data. KELA explored what is valuable for threat actors buying accesses, especially ransomware attackers, and built a profile of an ideal ransomware victim.

Bottom line up front:

- **In July 2021, KELA found 48 active threads where actors claimed they are looking to buy different kinds of accesses.** 46% of them were created in that month, illustrating the demand for access listings.
- **40% of the actors who were looking to buy accesses were identified as active participants in the ransomware-as-a-service (RaaS) supply chain – operators, or affiliates, or middlemen.**

- Ransomware attackers appear to form “industry standards” defining an ideal victim based on its revenue and geography and excluding certain sectors and countries from the targets list. **On average, the actors active in July 2021 aimed to buy access to US companies with revenue of more than 100 million USD. Almost half of them refused to buy access to companies from the healthcare and education industries.**
- Ransomware attackers are ready to buy all kinds of network accesses, with RDP and VPN being the most basic requirement. **The most common products (enabling network access) mentioned were Citrix, Palo Alto Networks, VMware, Fortinet, and Cisco.**
- **Ransomware attackers are ready to pay for access up to 100,000 USD, with most actors setting the boundaries at half of that price – 56,250 USD.**
- The similarities between ransomware-related actors’ requirements for victims and access listings and conditions for IABs illustrate that RaaS operations act just like corporate enterprises.



The Ideal Ransomware Victim

Based on active threads from July 2021

Based in **the US**

Has more than **100 million USD** in revenue

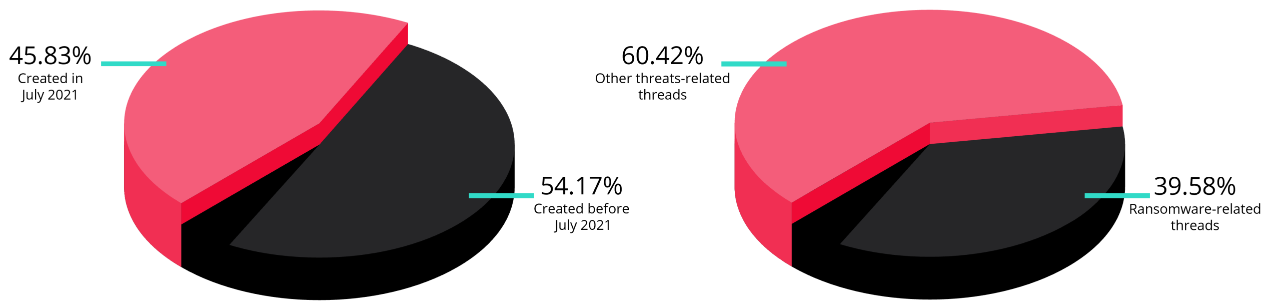
Is not from **education, healthcare, government, non-profit** sectors

Most wanted access types: **RDP, VPN, products from Citrix, Palo Alto Networks, VMware, Fortinet, and Cisco.**

For such access, ransomware attackers are ready to pay up to **100,000 USD** Most attackers are ready to pay up to **56,250 USD**

What Access Are Threat Actors Chasing

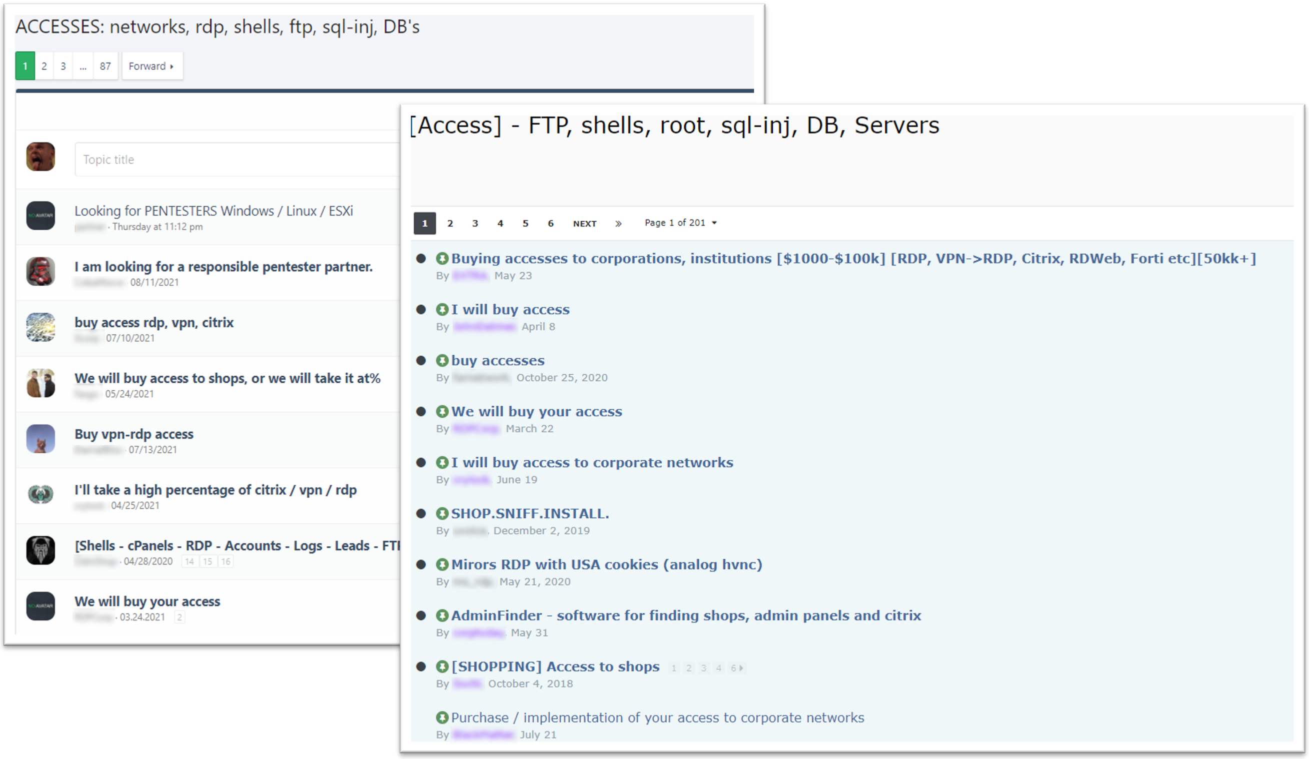
In total, KELA found 48 threads dedicated to buying accesses that were created or observed being active in July 2021. Almost half of them were created in July alone, showing an impressive pace and demand for access listings (with active meaning they had one or more updates from their creators in a thread). It begs the question – what access are the actors looking for and what is their ultimate goal?



Active Threads of Initial Access Buyers in July 2021

Based on active threads from July 2021

First of all, it is important to understand that threat actors behind the announcements do not necessarily mean network access when they say “access”. It is a term that is used in a very loose manner to describe multiple different vectors and entry points – from SQL injection and webshells to RDP- and VPN- based access. Analyzing the active threads dedicated to buying accesses, KELA found that in addition to initial network accesses sold by Initial Access Brokers (IABs), they included access to online shops’ panels, unprotected databases, Microsoft Exchange servers, and more. All these types of access are undoubtedly dangerous and can enable threat actors to perform various malicious actions, but they rarely provide access to a corporate network.



ACCESSES: networks, rdp, shells, ftp, sql-inj, DB's

Looking for PENTESTERS Windows / Linux / ESXi
[redacted] · Thursday at 11:12 pm

I am looking for a responsible pentester partner.
[redacted] · 08/11/2021

buy access rdp, vpn, citrix
[redacted] · 07/10/2021

We will buy access to shops, or we will take it at%
[redacted] · 05/24/2021

Buy vpn-rdp access
[redacted] · 07/13/2021

I'll take a high percentage of citrix / vpn / rdp
[redacted] · 04/25/2021

[Shells - cPanels - RDP - Accounts - Logs - Leads - FTI
[redacted] · 04/28/2020 14 15 16

We will buy your access
[redacted] · 03.24.2021 2

[Access] - FTP, shells, root, sql-inj, DB, Servers

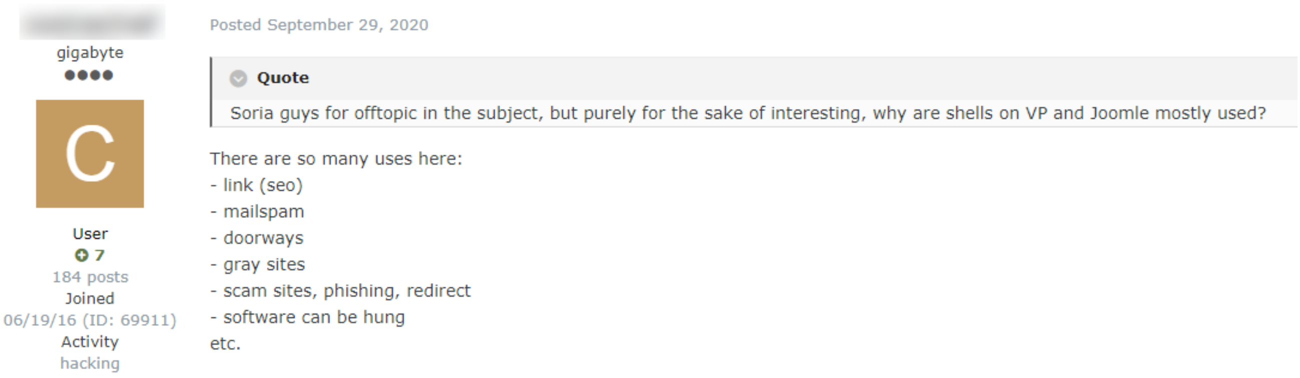
- Buying accesses to corporations, institutions [$1000-$100k] [RDP, VPN->RDP, Citrix, RDWeb, Forti etc][50kk+]
  By [redacted] May 23
- I will buy access
  By [redacted] April 8
- buy accesses
  By [redacted] October 25, 2020
- We will buy your access
  By [redacted] March 22
- I will buy access to corporate networks
  By [redacted] June 19
- SHOP.SNIFF.INSTALL.
  By [redacted] December 2, 2019
- Mirors RDP with USA cookies (analog hvnc)
  By [redacted] May 21, 2020
- AdminFinder - software for finding shops, admin panels and citrix
  By [redacted] May 31
- [SHOPPING] Access to shops 1 2 3 4 6 ▸
  By [redacted] October 4, 2018

Purchase / implementation of your access to corporate networks
By [redacted] July 21

Sections dedicated to accesses on XSS and Exploit cybercrime forums

---

Therefore, researching the actors' demands and their dark web activity, KELA determined that the actors behind the analyzed threads usually intended to exploit the access for all kinds of malicious activities, including information-stealing (from deploying info-stealing malware to injecting malicious scripts into websites), cryptocurrency mining, spam and phishing campaigns.



[redacted]
gigabyte
●●●●

User
7
184 posts
Joined
06/19/16 (ID: 69911)
Activity
hacking

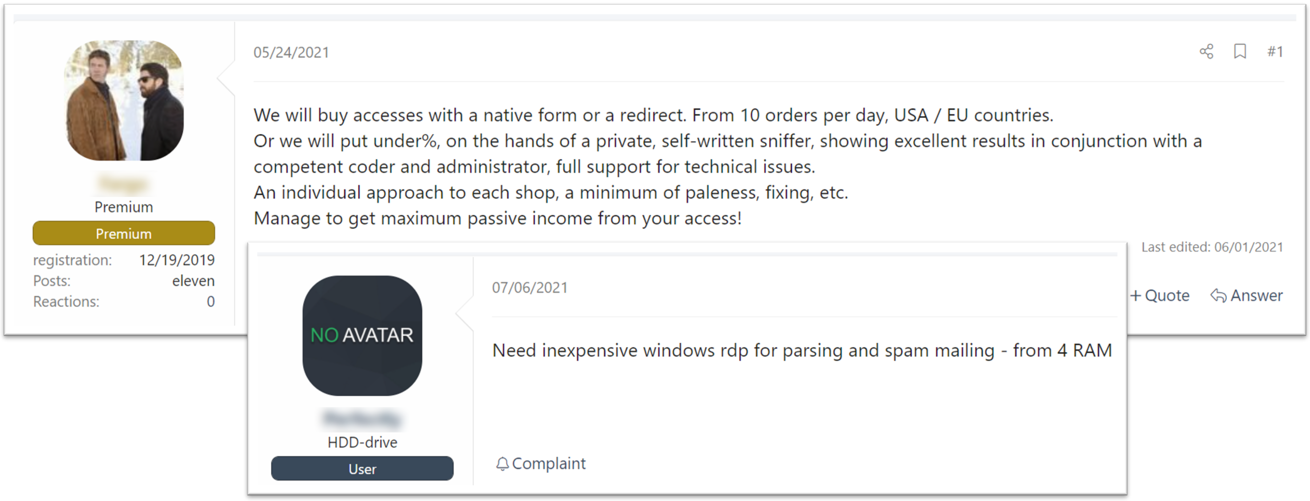
Posted September 29, 2020

> Quote
>
> Soria guys for offtopic in the subject, but purely for the sake of interesting, why are shells on VP and Joomle mostly used?

There are so many uses here:
- link (seo)
- mailspam
- doorways
- gray sites
- scam sites, phishing, redirect
- software can be hung

etc.

A user explaining how to use access via shells for malicious purposes



[redacted]

Premium

Premium

registration: 12/19/2019

Posts: eleven

Reactions: 0

05/24/2021

We will buy accesses with a native form or a redirect. From 10 orders per day, USA / EU countries.
Or we will put under%, on the hands of a private, self-written sniffer, showing excellent results in conjunction with a competent coder and administrator, full support for technical issues.
An individual approach to each shop, a minimum of paleness, fixing, etc.
Manage to get maximum passive income from your access!

Last edited: 06/01/2021

[redacted]

HDD-drive

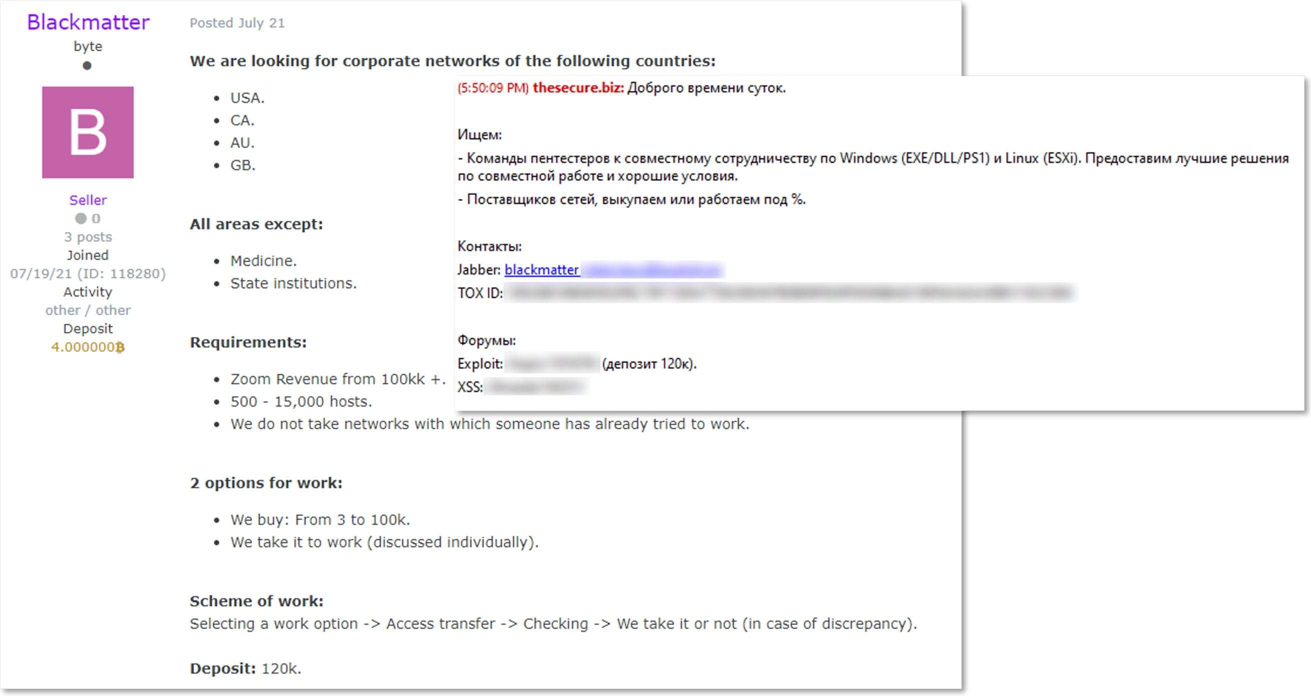
User

07/06/2021

Need inexpensive windows rdp for parsing and spam mailing - from 4 RAM

Threat actors looking for accesses to abuse them to deploy sniffers or send e-mail spam

However, one threat obviously stands out. Almost **40% of the analyzed threads were created by actors related to Raas supply chain – operators, affiliates, or middlemen.** As ransomware operations have been growing and maturing, KELA observed multiple ransomware gangs using the IABs' services. Announcements about buying accesses help them to find each other and cooperate further. Some gangs, like BlackMatter and Avos, even sent an advertisement about them buying accesses in Jabber – apparently to all users registered via XSS/Exploit Jabber services. Others, like Crylock ransomware representative, specifically mentioned they are looking for constant sellers.



Blackmatter
byte
●

Seller
● 0
3 posts
Joined
07/19/21 (ID: 118280)
Activity
other / other
Deposit
4.000000Ƀ

Posted July 21

We are looking for corporate networks of the following countries:

- USA.
- CA.
- AU.
- GB.

All areas except:

- Medicine.
- State institutions.

Requirements:

- Zoom Revenue from 100kk +.
- 500 - 15,000 hosts.
- We do not take networks with which someone has already tried to work.

2 options for work:

- We buy: From 3 to 100k.
- We take it to work (discussed individually).

Scheme of work:
Selecting a work option -> Access transfer -> Checking -> We take it or not (in case of discrepancy).

Deposit: 120k.

(5:50:09 PM) **thesecure.biz:** Доброго времени суток.

Ищем:

- Команды пентестеров к совместному сотрудничеству по Windows (EXE/DLL/PS1) и Linux (ESXi). Предоставим лучшие решения по совместной работе и хорошие условия.

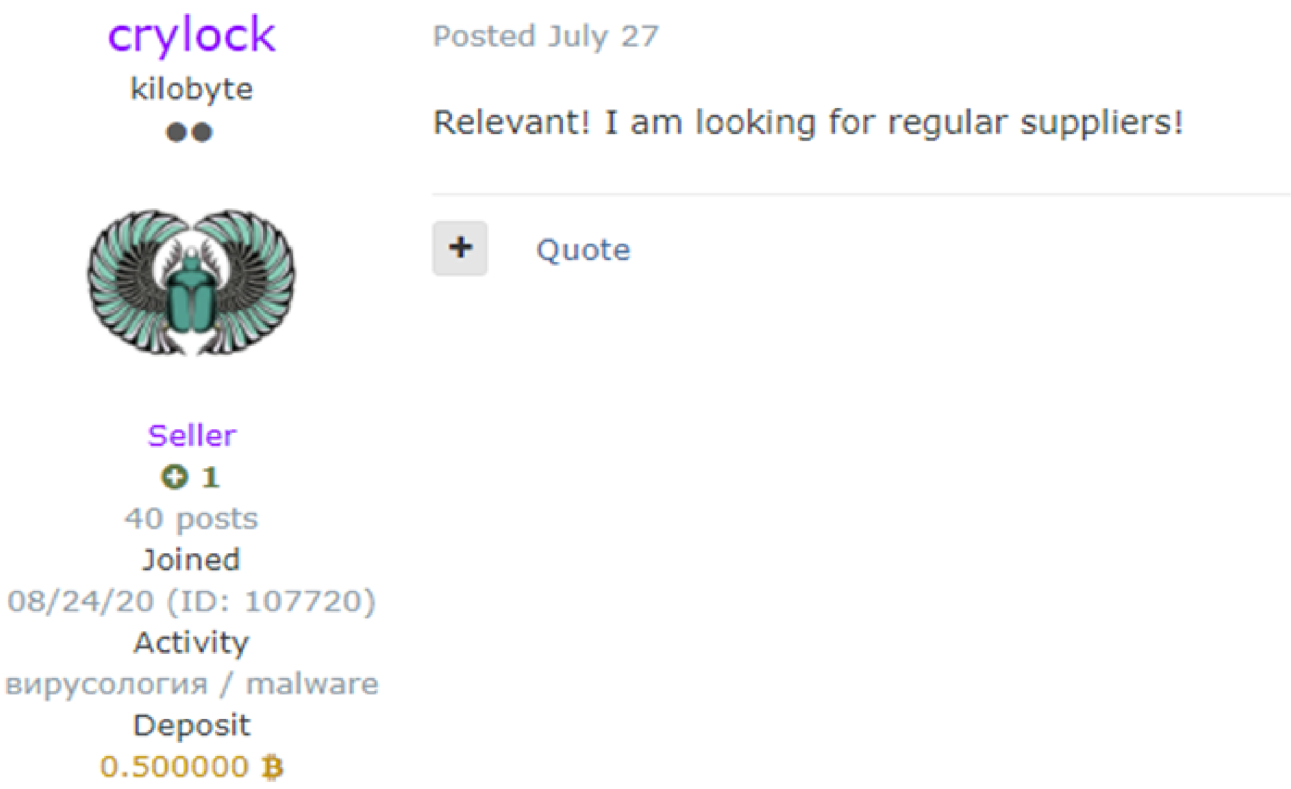
- Поставщиков сетей, выкупаем или работаем под %.

Контакты:
Jabber: blackmatter [redacted]
TOX ID: [redacted]

Форумы:
Exploit: [redacted] (депозит 120к).
XSS: [redacted]

BlackMatter ransomware gang is looking for Initial Access Brokers both on forums and via Jabber

---



crylock
kilobyte
●●

Seller
⊕ 1
40 posts
Joined
08/24/20 (ID: 107720)
Activity
вирусология / malware
Deposit
0.500000 Ƀ

Posted July 27

Relevant! I am looking for regular suppliers!

Crylock ransomware gang is looking for constant suppliers of access

Such posts are not new, though with the growth and diversification of the ransomware-as-a-service (RaaS) ecosystem they have become much more standardized. Instead of a simple "I'll buy access", threat actors now scrupulously list potential victims' characteristics and types of access, knowing exactly what they want – i.e. to ease the attack and eventually receive a ransom. KELA explored these metrics to find out what companies are in the ransomware attackers' target list.

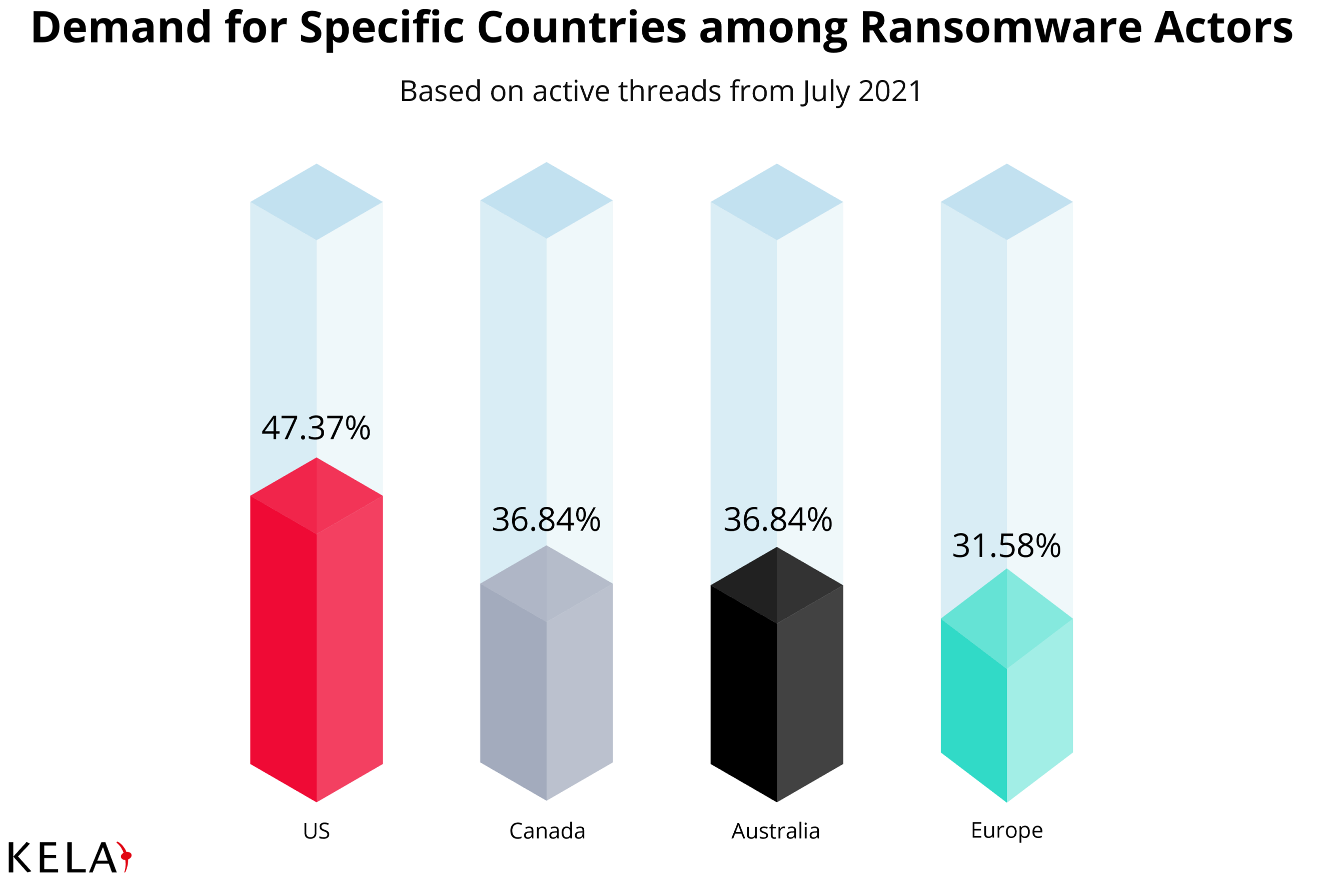
Ransomware Attackers' Requirements to IABs

When describing the pricing model formed by IABs, KELA determined that it mainly depends on the revenue and the size of the affected company, though geography sometimes plays a certain role. The level of privileges in the compromised network also influences the prices (for example, a domain administrator account costs at least 10 times more than access to a machine with user rights). Logically, the same metrics are important to ransomware actors since IABs have always followed the needs of their customers.

A typical ransomware actors' advertisement includes the following characteristics of the victim:

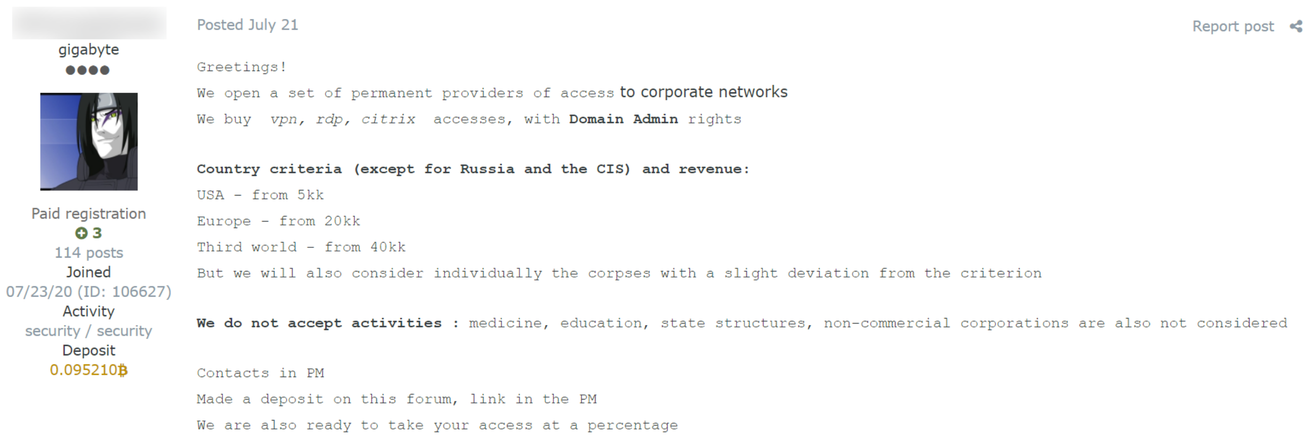
Geography

The majority of requests mentioned the desired location of victims, with **the US being the most popular choice – 47% of the actors mentioned it. Other top locations included Canada (37%), Australia (37%), and European countries (31%).** Most of the advertisements included a call for multiple countries. The reason behind this geographical focus is that actors choose the most wealthy companies which are expected to be located in the biggest and the most developed countries. For example, the LockBit 2.0 ransomware representative said in his recent interview: "The bigger the company's capitalization is – the better. <..> It does not matter where the target is situated, we attack everyone."



Revenue

Typically, the actors stated only the minimum desired revenue in attempts to cut off victims that are unlikely to pay a significant ransom. **The average minimum revenue wanted by ransomware attackers is 100 million USD, with some of them stating that the desired revenue depends on the location.** For example, one of the actors described the following formula: revenue should be more than 5 million USD for US victims, more than 20 million USD for European victims, and more than 40 million USD for “the third world” countries.



[redacted]
gigabyte
●●●●

Paid registration
3
114 posts
Joined
07/23/20 (ID: 106627)
Activity
security / security
Deposit
0.095210฿

Posted July 21

Greetings!
We open a set of permanent providers of access to corporate networks
We buy *vpn, rdp, citrix* accesses, with **Domain Admin** rights

Country criteria (except for Russia and the CIS) and revenue:
USA - from 5kk
Europe - from 20kk
Third world - from 40kk
But we will also consider individually the corpses with a slight deviation from the criterion

We do not accept activities : medicine, education, state structures, non-commercial corporations are also not considered

Contacts in PM
Made a deposit on this forum, link in the PM
We are also ready to take your access at a percentage

A threat actor sets prices for accesses depending on the revenue of potential victims

---

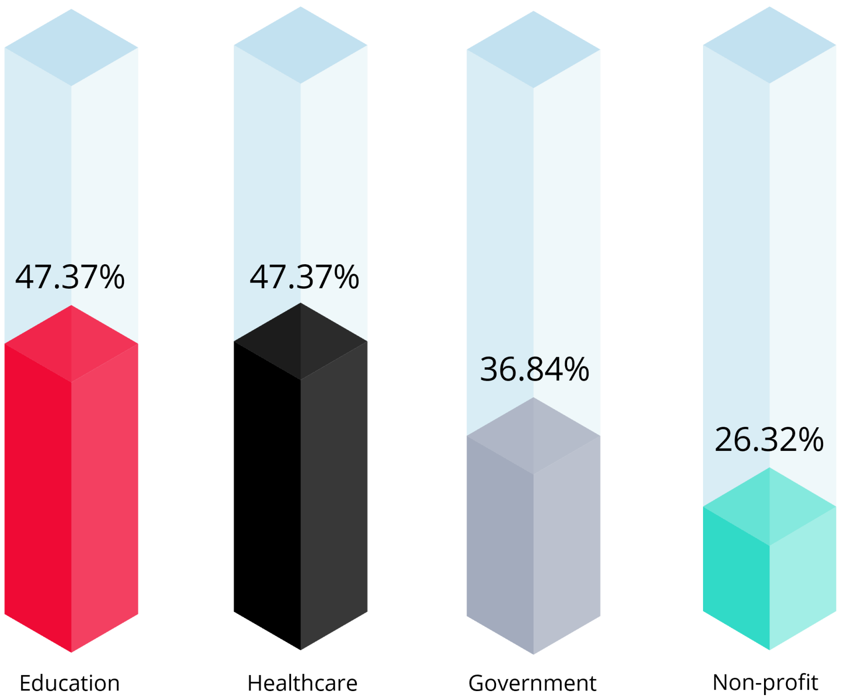
Blacklist of sectors

A significant difference can be spotted between the advertisement of threat actors buying access for ransomware attacks and cybercriminals with other specializations. Almost a half of ransomware-related threads included a blacklist of sectors, meaning that the actors are not ready to buy access to companies from specific industries.

47% of ransomware attackers refused to buy access to companies from the healthcare and education industries. 37% prohibited compromising the government sector, while 26% claimed they will not purchase access related to non-profit organizations. When actors prohibit healthcare or non-profit industries offers, it is more likely due to the moral code of the actors. When the education sector is off the table, the reason is the same or the fact that education victims simply cannot afford to pay much. Finally, when actors refuse to target government companies, it is a precaution measure and an attempt to avoid unwanted attention from law enforcement.

Blacklist of Sectors among Ransomware Actors

Based on active threads from July 2021

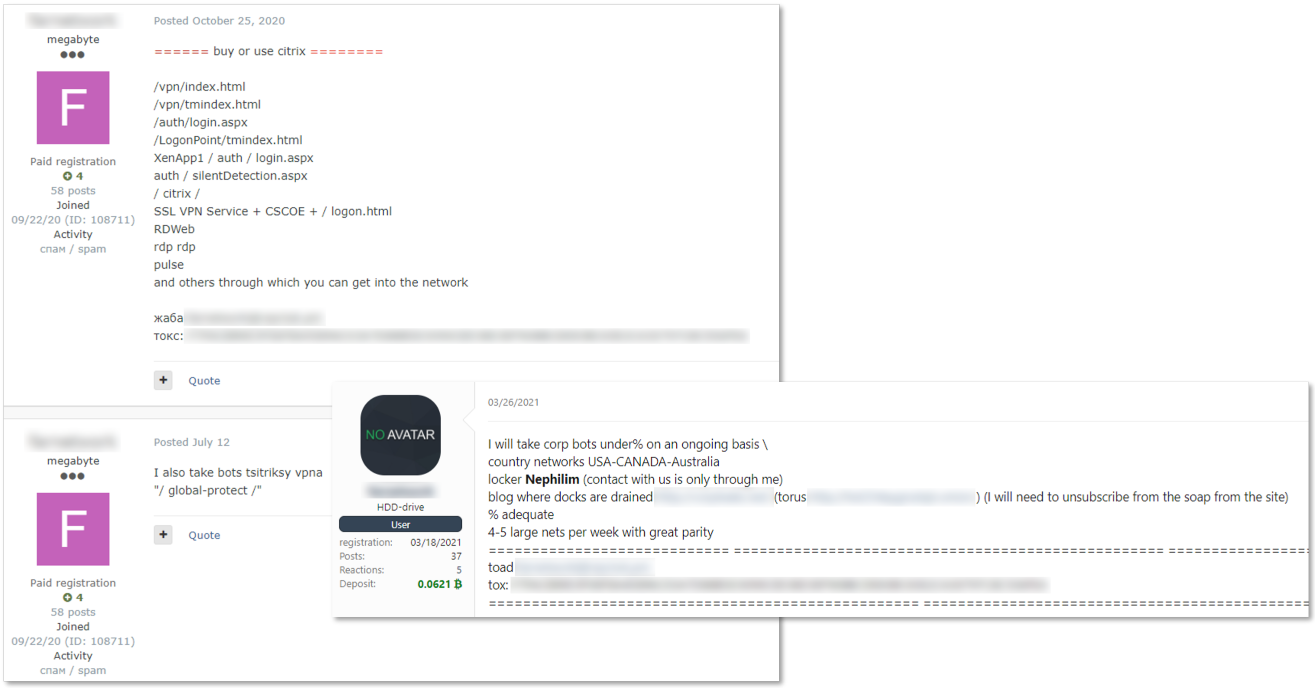


Blacklist of countries

Finally, some countries are out of ransomware attackers' interests. Not surprisingly, it's CIS, according to the old Russian-speaking hackers' rule "do not work in Ru" [in Russian speaking countries – KELA]. The actors based in CIS suppose that if they will not target these countries, local authorities will not hunt them. Other countries mentioned as "unwanted" included South America and third world countries – most likely due to low chances of getting a financial gain.

Ransomware Attackers Budget for Accesses

For suitable victims, ransomware attackers are ready to buy all kinds of network accesses, with RDP and VPN being the most basic requirement. **Among wanted products (enabling network access) they listed Citrix, Palo Alto Networks (specifically GlobalProtect VPN), VMware (specifically ESXi), Fortinet, and Cisco.** As for the level of privileges, some attackers stated they prefer domain admin rights, though it does not seem to be critical.



[redacted]

megabyte

●●●

Paid registration

4

58 posts

Joined

09/22/20 (ID: 108711)

Activity

спам / spam

Posted October 25, 2020

```
====== buy or use citrix ========

/vpn/index.html
/vpn/tmindex.html
/auth/login.aspx
/LogonPoint/tmindex.html
XenApp1 / auth / login.aspx
auth / silentDetection.aspx
/ citrix /
SSL VPN Service + CSCOE + / logon.html
RDWeb
rdp rdp
pulse
and others through which you can get into the network

жаба [redacted]
токс: [redacted]
```

[redacted]

megabyte

●●●

Paid registration

4

58 posts

Joined

09/22/20 (ID: 108711)

Activity

спам / spam

Posted July 12

I also take bots tsitriksy vpna "/ global-protect /"

[redacted]

HDD-drive

User

registration:	03/18/2021
Posts:	37
Reactions:	5
Deposit:	0.0621 ฿

03/26/2021

```
I will take corp bots under% on an ongoing basis \
country networks USA-CANADA-Australia
locker Nephilim (contact with us is only through me)
blog where docks are drained [redacted] (torus [redacted] ) (I will need to unsubscribe from the soap from the site)
% adequate
4-5 large nets per week with great parity
========================= ============================================================ ================
toad [redacted]
tox: [redacted]
======================================================================== ==========================================
```

An actor associated with the Nefilim ransomware operation looks for various types of access

---

How much are ransomware attackers ready to pay for such access to defined companies? The range really varies, starting from 100 and ending with 100,000 USD. The average minimum and maximum prices for access are 1600 – 56,250 USD. In addition, 32% of ransomware attackers are ready to pay a share of a ransom. As KELA determined earlier, IABs can get around 10% of a ransom.

The similarities between ransomware-related actors' requirements for victims and access listings and conditions for IABs illustrate that RaaS operations act just like corporate enterprises. They form " industry standards" with a blacklist of sectors and countries, define their "clients" revenue and geography, and offer a competitive price for threat actors supplying them the desired "goods." Confronting such organized cybercrime requires more effort and visibility into the sources where ransomware-related actors look for outsourcing services and recruit partners and employees.

Mitigation measures for enterprise defenders

Demand for access listings on cybercrime forums is growing, with more actors advertising they are ready to buy entry points to networks, sites, storage, and more. This is another proof of continuing servitization of cybercrime, especially ransomware-as-a-service (RaaS) operations that rely on different specialists to perform their attacks. However, **it is crucial to remember that access to a company in the wrong hands may be exploited not only for deploying ransomware and stealing data but also for other malicious campaigns.**

Confronting various threats require enterprise defenders to invest in:

1. Cybersecurity awareness and training for all key stakeholders and employees to ensure that key individuals know how to safely use their credentials and personal information online. This cyber training should include specifying how to identify suspicious activities, such as possible scam emails, or unusual requests from unauthorized individuals or email addresses.
2. Regular vulnerability monitoring and patching to continually protect their entire network infrastructure and prevent any unauthorized access by Initial Access Brokers or other network intruders.
3. Targeted and automated monitoring of key assets to immediately detect threats emerging from the cybercrime underground ecosystem. Constant automated and scalable monitoring of an organization's assets could significantly improve maintaining a reduced attack surface, ultimately helping organizations thwart possible attempts of cyberattacks against them.

Visit lumint.ke-la.com to stay up to date with more insights on recent ransomware attacks as well as compromised network accesses listed for sale and leaked databases and data dumps.