The Secret Life of an Initial Access Broker

August 6, 2020

Bottom Line Up Front

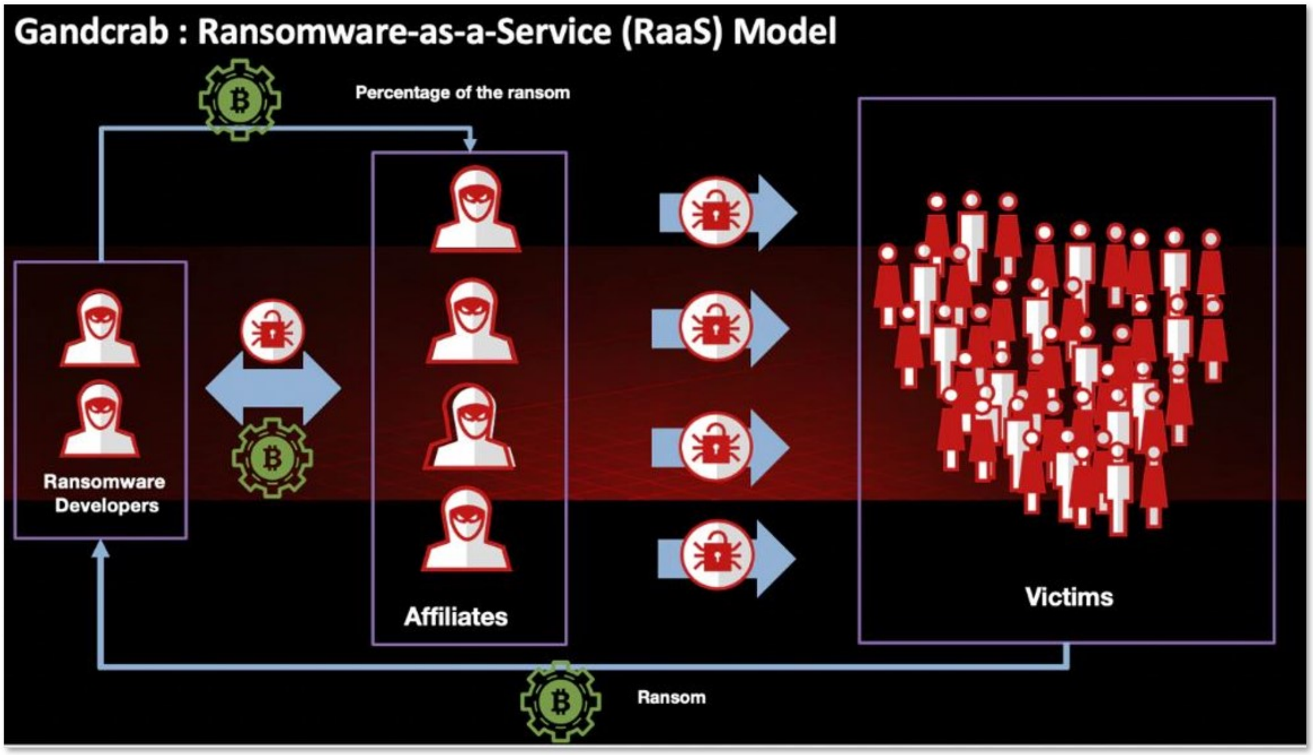
- Recently, ZDNet exclusively reported a **leak posted on a cybercrime community containing details and credentials of over 900 enterprise Secure Pulse servers** exploited by threat actors
- Since this leak represents an ever-growing ransomware risk, **KELA delved into both the leak's content and the actors** who were involved in its inception and circulation
- This short research targets a specific tier of cybercriminal actors – **Initial Access Brokers**. These are **mid-tier actors who specialize in obtaining initial network access from a variety of sources, curating and grooming it into a wider network compromise** – and then selling them off to ransomware affiliates
- With the affiliate ransomware network becoming more and more popular and affecting huge enterprises as well as smaller ones, **initial access brokers are rapidly becoming an important part of the affiliate ransomware supply chain**
- **The list leak mentioned above seems to have been circulating between several initial access brokers in cybercrime forums**, and have been exposed by a LockBit affiliate who regarded the actors as unprofessional
- This event showcases the breadth of information that's exchanged on cybercrime communities and, in KELA's eyes, **emphasizes the need for scalable and targeted monitoring of underground communities**

RaaS Ecosystem 101

For the past year or so, the threat intelligence community has been closely tracking the ongoing changes to the ransomware landscape – noting the shift in business models and TTPs employed by ransom actors. While vendors may choose different terms – "human-operated", "multi-stage", "targeted" and more – they all carry the same meaning: ransomware actors are opting to go for targets that have more means and more incentive for payment, so they can demand higher ransom amounts.

One major aspect of this trend, commonly mentioned in the media for its inherent flare and optics, is the naming-and-shaming leveraging tactics used to further push ransomware victims to pay.

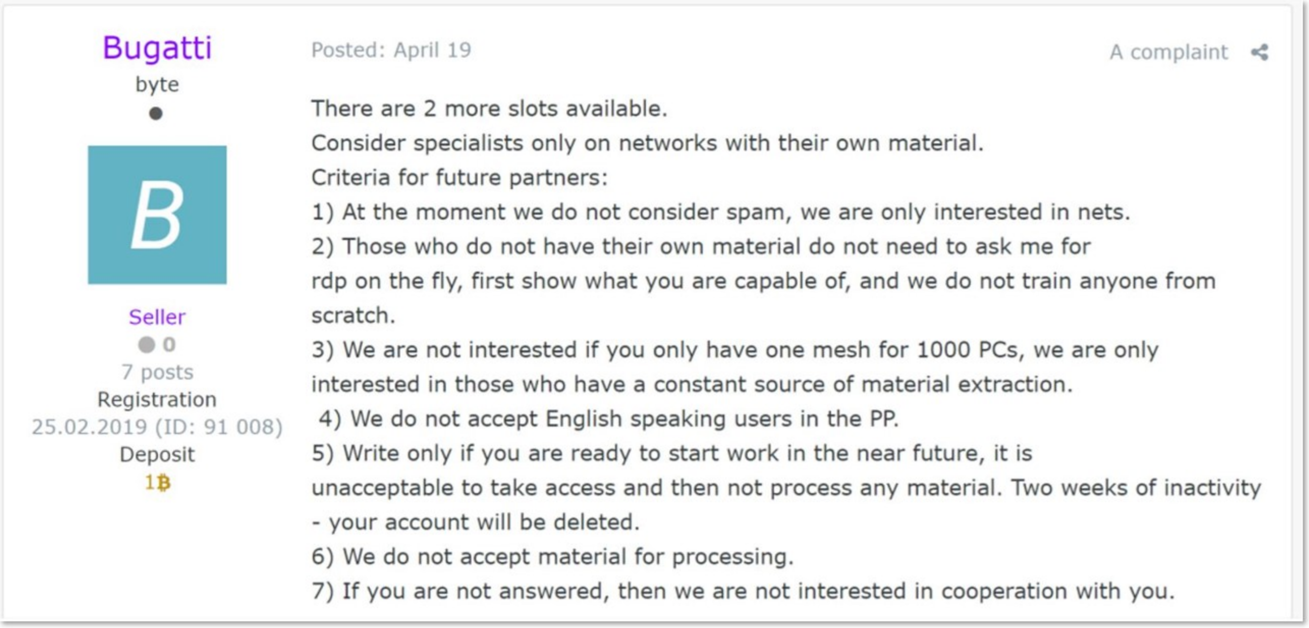
Another aspect is the **cooperation between actors facilitated by the rise of targeted ransomware**: in order to support work in scale, ransomware operators turn to partners and affiliates to fulfill their remote access needs. This cooperation results in two distinct stakeholders in the targeted ransomware-as-a-service supply chain: the ransomware developers who supply the infrastructure, and the partners who supply the network intrusion opportunities and deployment of the ransomware itself.



The affiliate model employed by GandCrab in 2019. Source: McAfee

---

Generally speaking, the affiliates working directly with ransomware operators are highly vetted, professional actors. At any given moment, most ransomware developers are recruiting only a handful of affiliates – essentially creating a pyramid-like hierarchy; some RaaS developers are very keen on their affiliates' KPIs, with underperforming affiliates being removed from the program.



Bugatti
byte

Seller
● 0
7 posts
Registration
25.02.2019 (ID: 91 008)
Deposit
1฿

Posted: April 19

A complaint

There are 2 more slots available.
Consider specialists only on networks with their own material.
Criteria for future partners:
1) At the moment we do not consider spam, we are only interested in nets.
2) Those who do not have their own material do not need to ask me for rdp on the fly, first show what you are capable of, and we do not train anyone from scratch.
3) We are not interested if you only have one mesh for 1000 PCs, we are only interested in those who have a constant source of material extraction.
4) We do not accept English speaking users in the PP.
5) Write only if you are ready to start work in the near future, it is unacceptable to take access and then not process any material. Two weeks of inactivity - your account will be deleted.
6) We do not accept material for processing.
7) If you are not answered, then we are not interested in cooperation with you.

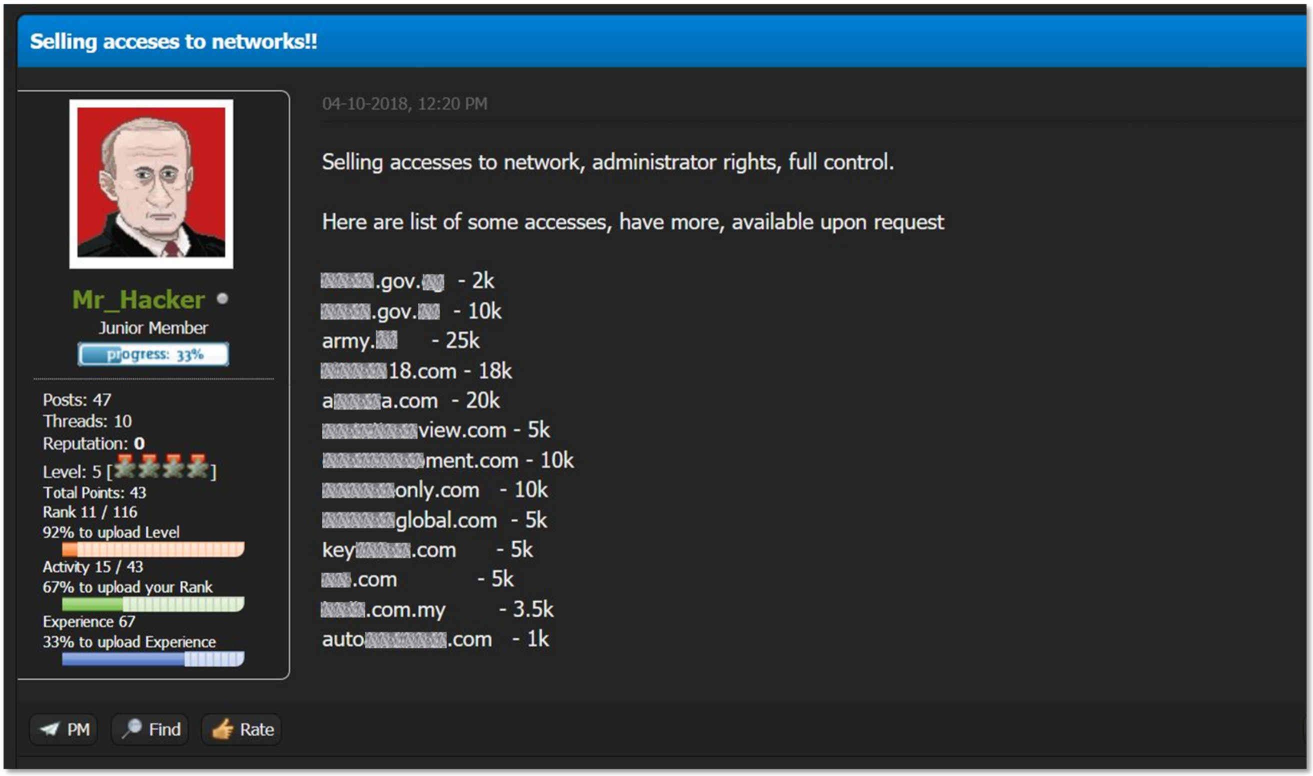
Post from a cybercrime forum (accessible and translatable through DARKBEAST) where a NetWalker ransomware recruitment ad shows a very specific criteria for affiliates

Essentially, affiliates may be perceived as mid-level management. Facing constant scrutiny from the developers and commission-based salary that’s dependent on successful network intrusions, the affiliates’ needs to constantly gain more network access gave rise to another actor type: the **initial access broker.**

Initial Access Brokers

Initial access brokers are generally lower-tier, opportunistic actors supplying the affiliates with access-as-a-service: they obtain initial access to organizations and then offer it for sale on the same underground forums occupied by RaaS affiliates. **Affiliates then buy these initial accesses**, pivot and move laterally until enough control is obtained so the ransomware can be spread and computers be locked.

Brokers and affiliates are not necessarily differentiated by their level of skill or expertise, but rather by the **monetization channels** they choose to employ. While affiliates or ransomware actors monetize networks by locking them and demanding ransom, initial access brokers are use-case agnostic: they sell network access to any actor – financially-motivated APTs (such as FINx groups), ransomware actors, data brokers, nation state actors trawling the cybercrime underground for leads or essentially any threat actor that has a way to monetize said access.


Selling acceses to networks!!

Mr_Hacker
Junior Member
Progress: 33%

Posts: 47
Threads: 10
Reputation: 0
Level: 5
Total Points: 43
Rank 11 / 116
92% to upload Level
Activity 15 / 43
67% to upload your Rank
Experience 67
33% to upload Experience

04-10-2018, 12:20 PM

Selling accesses to network, administrator rights, full control.

Here are list of some accesses, have more, available upon request

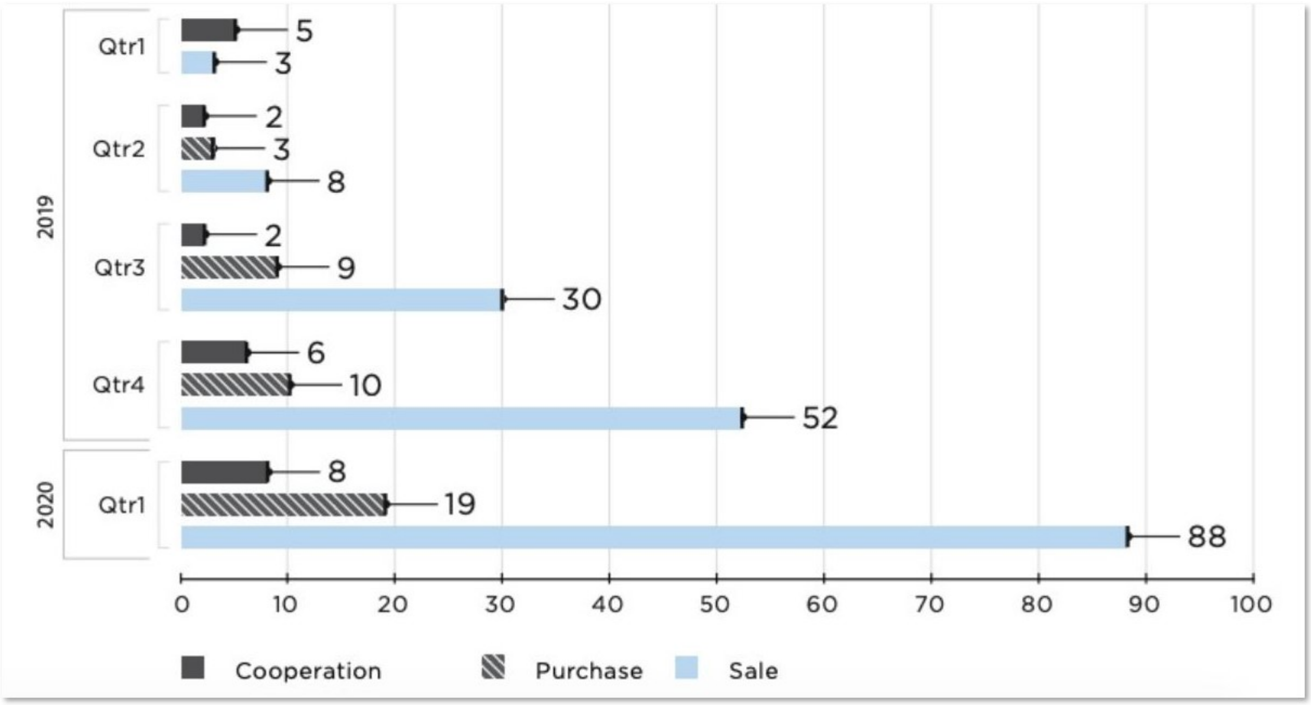
[redacted].gov.[redacted] - 2k
[redacted].gov.[redacted] - 10k
army.[redacted] - 25k
[redacted]18.com - 18k
a[redacted]a.com - 20k
[redacted]view.com - 5k
[redacted]ment.com - 10k
[redacted]only.com - 10k
[redacted]global.com - 5k
key[redacted].com - 5k
[redacted].com - 5k
[redacted].com.my - 3.5k
auto[redacted].com - 1k

A handle used by an actor associated with the access broker collective known as FXMSP, offering network access to multiple organizations on the now-defunct KickAss Forum

---

Monetizing network access in the cybercrime financial ecosystem is nothing new, and initial access brokers existed long before the rise of targeted ransomware. However, they tended to have less clients. Monetizing network access can be hard, since fraud actors – who make up the lion's share of active actors on most communities – are more interested in credentials that can be easily converted to cash in hand, whereas sophisticated actors who can monetize access to an obscure network were not, up until lately, in abundance. The recently-established **RaaS programs have simplified the process and provided easy monetization channels for network access**. These programs have enabled the entire chain of actors to increase profits, as high demand for network access (by affiliates) creates a higher supply of brokers dedicated to gaining network access.

In 2019, due the rising tide of RaaS operators, threat intelligence research efforts started shifting towards access brokers as well. One of the notable actors to attract major attention was the loose collective known as FXMSP, which operated across multiple handles and communities. Others, such as "bc.monster" or "sheriff", are currently becoming increasingly active across Russian-speaking communities. Initial access brokers are, in fact, becoming exponentially more prevalent in cybercrime communities; the amount of posts and offers dedicated to monetizing network access has risen drastically in 2020.



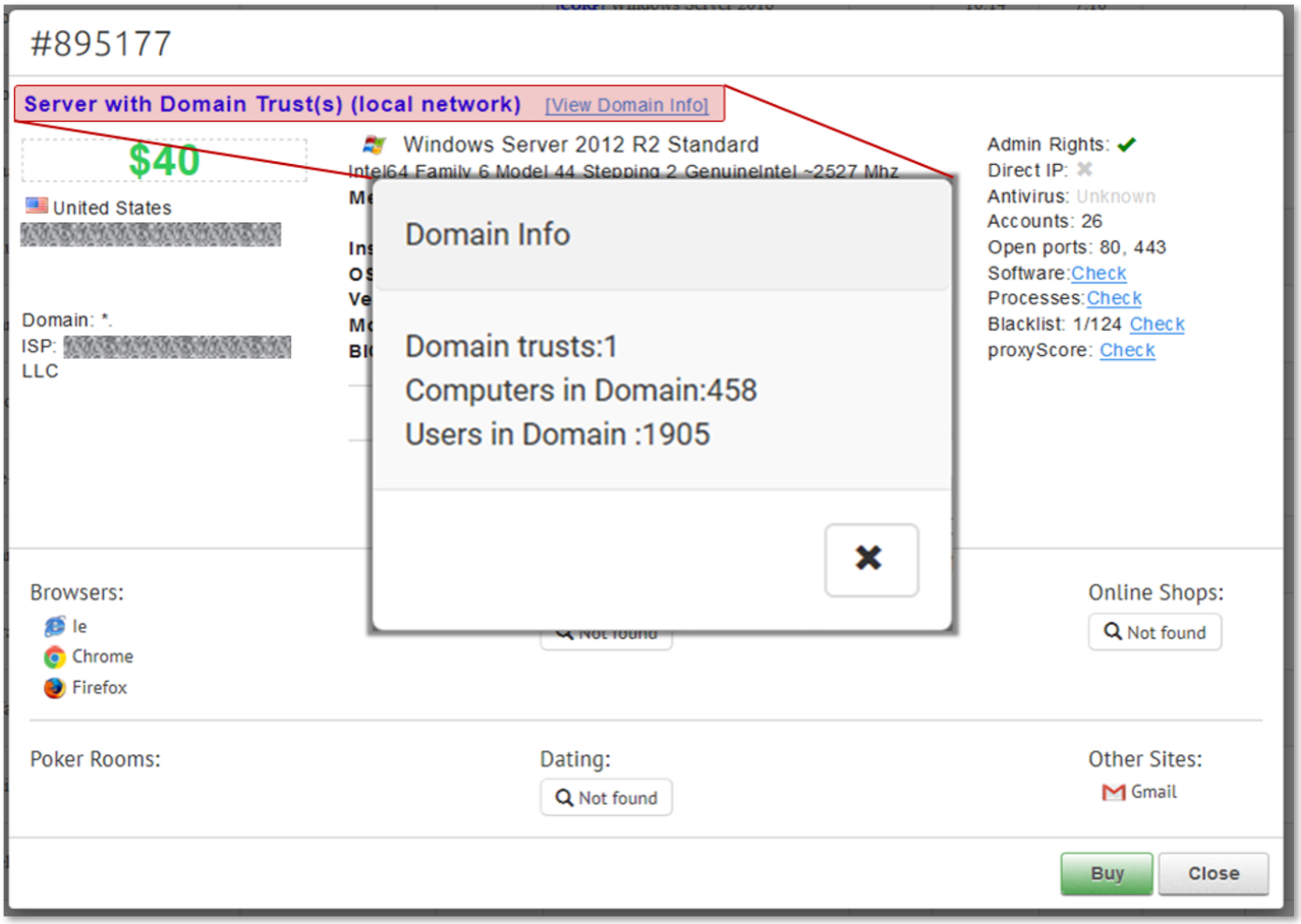
Remote access offering on cybercrime forums over time. Source: Positive Technologies

The Value Proposition of Access Brokers

Key enabling factors for the prevalence of access brokers (and, indirectly, to the rapid rise in targeted ransomware) **are the automation and servitization of cybercrime**.

Let’s take Remote Desktop Protocol – a key vector in targeted ransomware. A few years ago, threat actors needed to employ a wide variety of tools to get access to a valuable, functioning RDP server belonging to a corporation – including much time spent on reconnaissance, brute forcing and nitpicking victims.

Today, one only needs to obtain an invite to one of the many Remote Access Markets and browse the continuously-updated selection of compromised machines offered for sale. One of the major RDP markets has lately also added a “CORP” flag – servers that are part of a corporate network are marked (and priced) differently, so actors can easily spot them and get the most bang for their RDP buck.



#895177

Server with Domain Trust(s) (local network) [View Domain Info]

$40

United States

[redacted]

Domain: *.

ISP: [redacted]

LLC

Windows Server 2012 R2 Standard

Intel64 Family 6 Model 44 Stepping 2 GenuineIntel ~2527 Mhz

Me

Ins

OS

Ve

Mo

BI

Admin Rights: ✓

Direct IP: ✗

Antivirus: Unknown

Accounts: 26

Open ports: 80, 443

Software:Check

Processes:Check

Blacklist: 1/124 Check

proxyScore: Check

Domain Info

Domain trusts:1

Computers in Domain:458

Users in Domain :1905

✖

Browsers:

Ie

Chrome

Firefox

Online Shops:

Not found

Poker Rooms:

Dating:

Not found

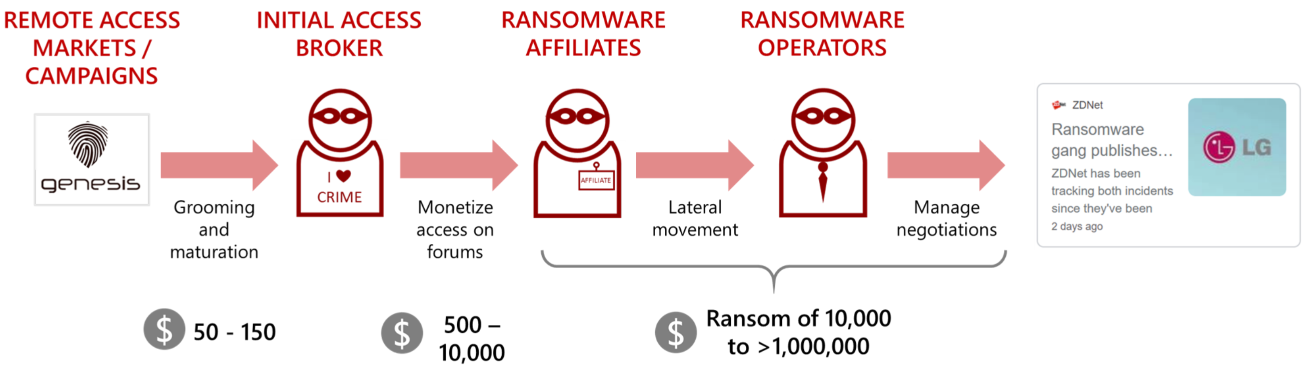
Other Sites:

Gmail

Buy Close

An RDP server belonging to an organization offered for sale on an automated market for USD 40

This wide selection of goods allows actors a higher volume of work. For a few hundred dollars, initial access brokers can acquire multiple RDP corporate servers; from that selection they can “groom” the ones that look interesting – perform some reconnaissance, escalate privileges or install further tooling. Once a target is ripe and ready, it can be offered for thousands of dollars on cybercrime markets where ransomware affiliates can acquire it and move forward with the final attack.



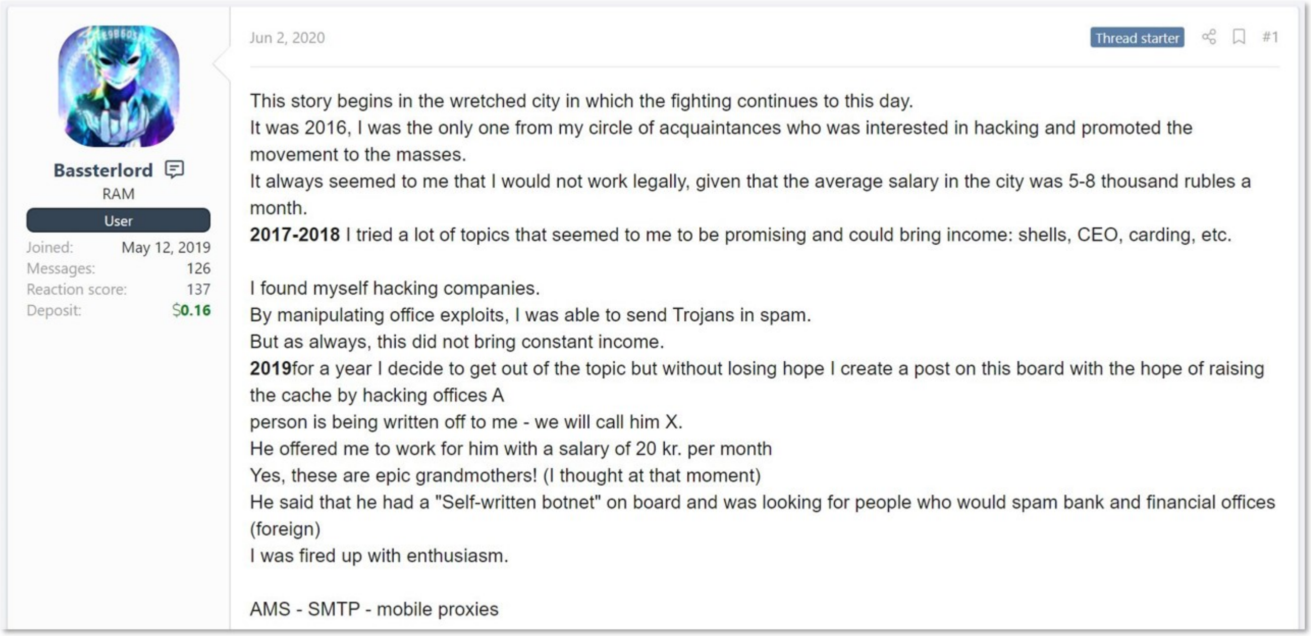
This model creates different stakeholders in the supply chain – each with their own expertise, scale of operations and profit margins. During each step of the process both the scope and price of the access get bigger – yielding profits to each stakeholder, and creating small, self-contained ecosystems that can support large-scale cybercrime efforts.

On August 4, 2020, ZDNet, in collaboration with KELA's tools, exclusively reported on a threat actor exposing a list of over 900 compromised Secure Pulse VPN servers – including credentials, session keys and other sensitive information being exposed. This was an interesting event for several reasons. First and foremost, the actual leakage provided visibility into targeted servers being used as potential ransomware targets – which has great intelligence monitoring value. Second, the leak – and the story behind it – provides an interesting behind-the-scenes look into the activity on an initial access broker.

First, in order to understand the story behind the recent leak, one needs to get familiar with the threat actors involved. The first – a man from Ukraine who, according to his posts, started his hacking activities in 2016 – goes by the handle "**Bassterlord"**. According to the actor's own accounts, after launching spam campaigns designed to deliver trojans and infostealers, he switched to targeting organizations under the mentorship of an unknown threat actor who hired him in 2019 and provided counselling.

In a competition of hacking-related articles held on a Russian-speaking underground forum, Bassterlord shared a writeup of his original story, of how his mentor offered him around $300 a month to send spam emails containing malicious attachments to banking and financial organizations. The actors have targeted 12,000 companies over almost one year, though they managed to infect only two of them. "Nothing worked for me, I was desperate," shared Bassterlord in this write-up. This was when his mentor taught him how to compromise organizations via RDP. At the same time, Bassterlord claims that his mentor "got access to Sodinokibi" – probably referring to the mentor becoming a Sodinokibi affiliate, showcasing the typical relationship between an affiliate and a soon-to-be initial access broker. Eager to get more money, Bassterlord switched to another TTP.

Bassterlord's current primary TTP involves the use of an automated script weaponizing CVE-2019-11510, an arbitrary file read vulnerability affecting Pulse Connect Secure SSL VPN, which has lately become popular with ransomware actors. Moreover, he states that he continues to work with his mentor and former employer, which is apparently still involved in Sodinokibi operations.

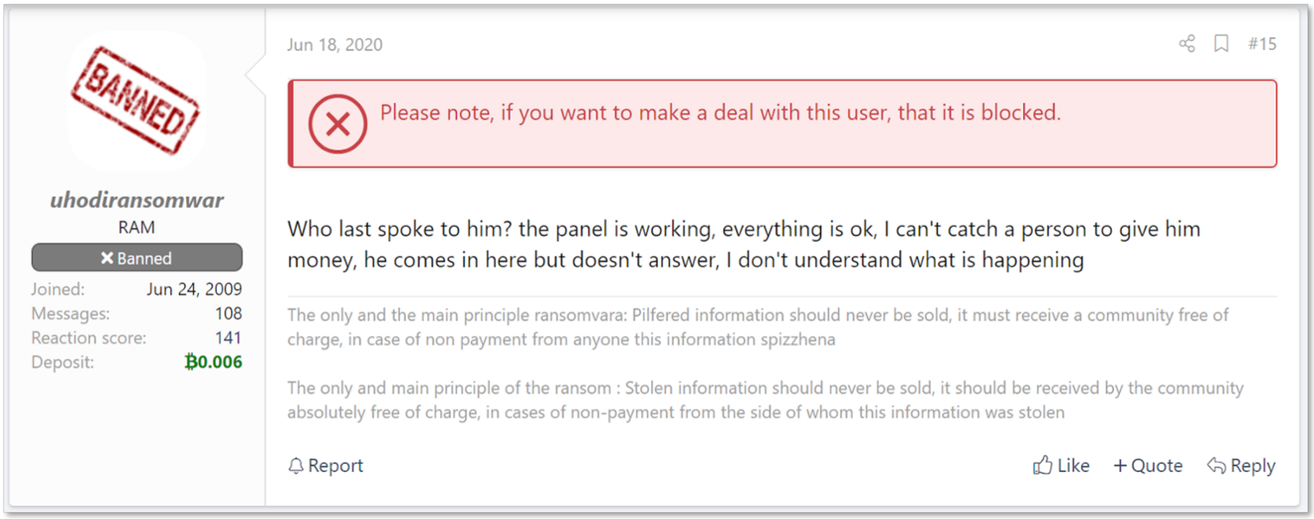


This story begins in the wretched city in which the fighting continues to this day.
It was 2016, I was the only one from my circle of acquaintances who was interested in hacking and promoted the movement to the masses.
It always seemed to me that I would not work legally, given that the average salary in the city was 5-8 thousand rubles a month.
2017-2018 I tried a lot of topics that seemed to me to be promising and could bring income: shells, CEO, carding, etc.

I found myself hacking companies.
By manipulating office exploits, I was able to send Trojans in spam.
But as always, this did not bring constant income.
2019for a year I decide to get out of the topic but without losing hope I create a post on this board with the hope of raising the cache by hacking offices A
person is being written off to me - we will call him X.
He offered me to work for him with a salary of 20 kr. per month
Yes, these are epic grandmothers! (I thought at that moment)
He said that he had a "Self-written botnet" on board and was looking for people who would spam bank and financial offices (foreign)
I was fired up with enthusiasm.

AMS - SMTP - mobile proxies

Another threat actor involved in the story is named “**uhodiransomwar**” (from Russian – “Go away, ransomware”), previously known as “m1x”. He is a veteran actor, active since 2009 (though freshly banned) on the same underground forum as Bassterlord. A major part of uhodiransomwar’s latest activity is small-scale ransomware: he mostly shares data from organizations he claimed to breach once no payment is received. It seems that he sometimes acts independently, and is also self-associated with known RaaS actors – such as LockBit.



Please note, if you want to make a deal with this user, that it is blocked.

Who last spoke to him? the panel is working, everything is ok, I can't catch a person to give him money, he comes in here but doesn't answer, I don't understand what is happening

The only and the main principle ransomvara: Pilfered information should never be sold, it must receive a community free of charge, in case of non payment from anyone this information spizzhena

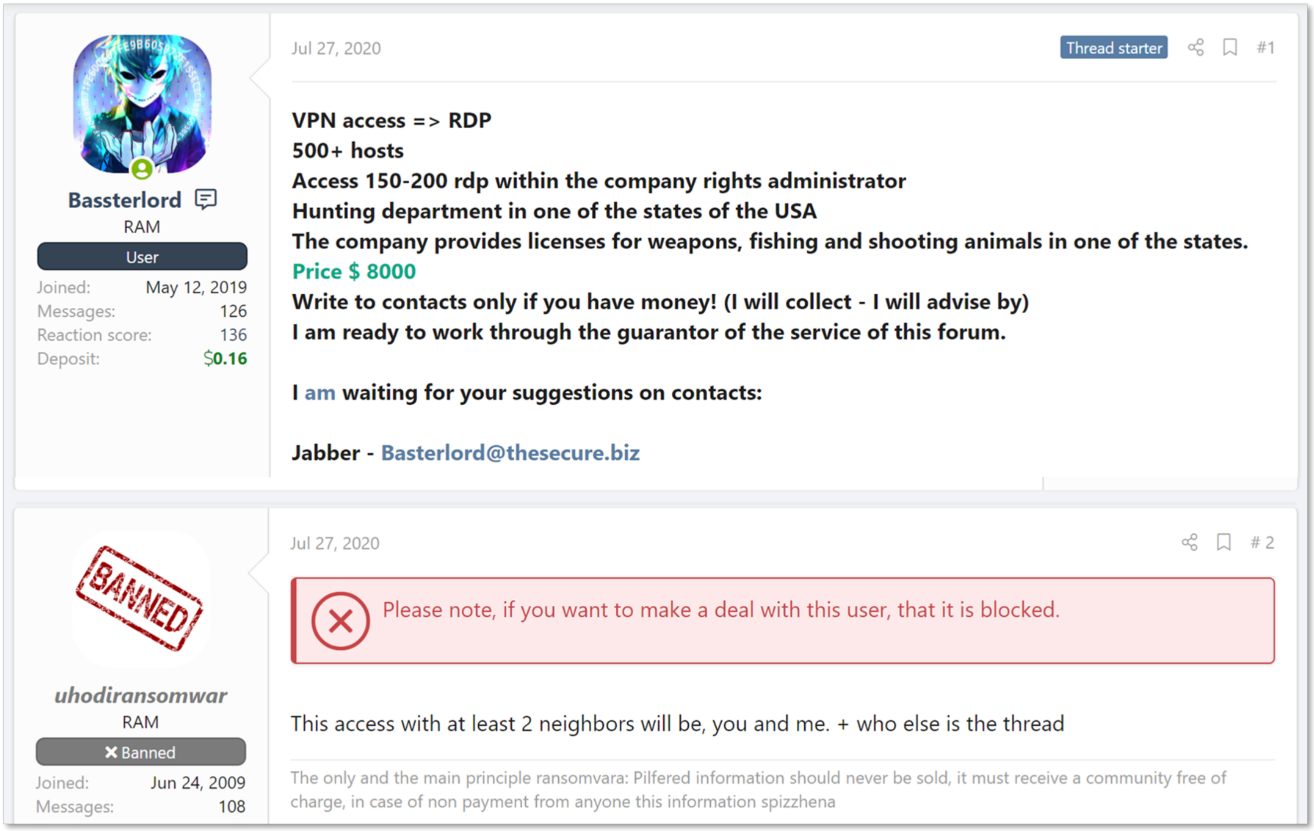
The only and main principle of the ransom : Stolen information should never be sold, it should be received by the community absolutely free of charge, in cases of non-payment from the side of whom this information was stolen

A comment in the official LockBit affiliate recruitment thread by uhodiransomwar, claiming to have access to the affiliates panel

In the last few weeks, Bassterlord and uhodiransomwar have been publicly clashing in the forum – showing the contrasting views of a novice initial access broker and a ransomware affiliate, respectively. These ongoing clashes have led to the credentials leak mentioned above.

Setting the Stage: a Not-So-Great Initial Access Broker

On July 27, 2020, Bassterlord offered network access to a US-based, state-level government organization for USD 8,000. The post claimed that the initial vector was VPN access which then was leveraged into RDP. First responder to the thread was uhodiransomwar, who claimed that the infiltrated network was shared between a few different actors – implying that the backdoor Bassterlord was offering wasn't exclusive and that he himself has access to the server already, and therefore may be worth less than the price asked.



Bassterlord
RAM
User
Joined: May 12, 2019
Messages: 126
Reaction score: 136
Deposit: $0.16

Jul 27, 2020 Thread starter #1

VPN access => RDP
500+ hosts
Access 150-200 rdp within the company rights administrator
Hunting department in one of the states of the USA
The company provides licenses for weapons, fishing and shooting animals in one of the states.
Price $ 8000
Write to contacts only if you have money! (I will collect - I will advise by)
I am ready to work through the guarantor of the service of this forum.

I am waiting for your suggestions on contacts:

Jabber - Basterlord@thesecure.biz

uhodiransomwar
RAM
✕ Banned
Joined: Jun 24, 2009
Messages: 108

Jul 27, 2020 # 2

Please note, if you want to make a deal with this user, that it is blocked.

This access with at least 2 neighbors will be, you and me. + who else is the thread

The only and the main principle ransomvara: Pilfered information should never be sold, it must receive a community free of charge, in case of non payment from anyone this information spizzhena

Google-translated post where Bassterlord recently posted access to a government entity in the US for sale.

The actors continued their public discussion, with Bassterlord admitting that the initial VPN access was indeed public knowledge – implying that multiple actors knew about it to begin with. He later made the case that even though multiple actors may be aware of the access itself, he's not aware of the inner workings on the network – only to his own access, leveraged into RDP. He also claims that in his eyes, network access – even if shared –

should be “first come, first serve”: the first actor to leverage it into a full-blown attack gets the spoils. **This exemplifies the role of an initial access broker in the ransomware supply chain**: they are the function that can take an initial lead to a vulnerability, and work it into a full blown network access. Thus, several actors working on the same initial access may come up with different results – creating an arms race between brokers and the affiliates who drive them.

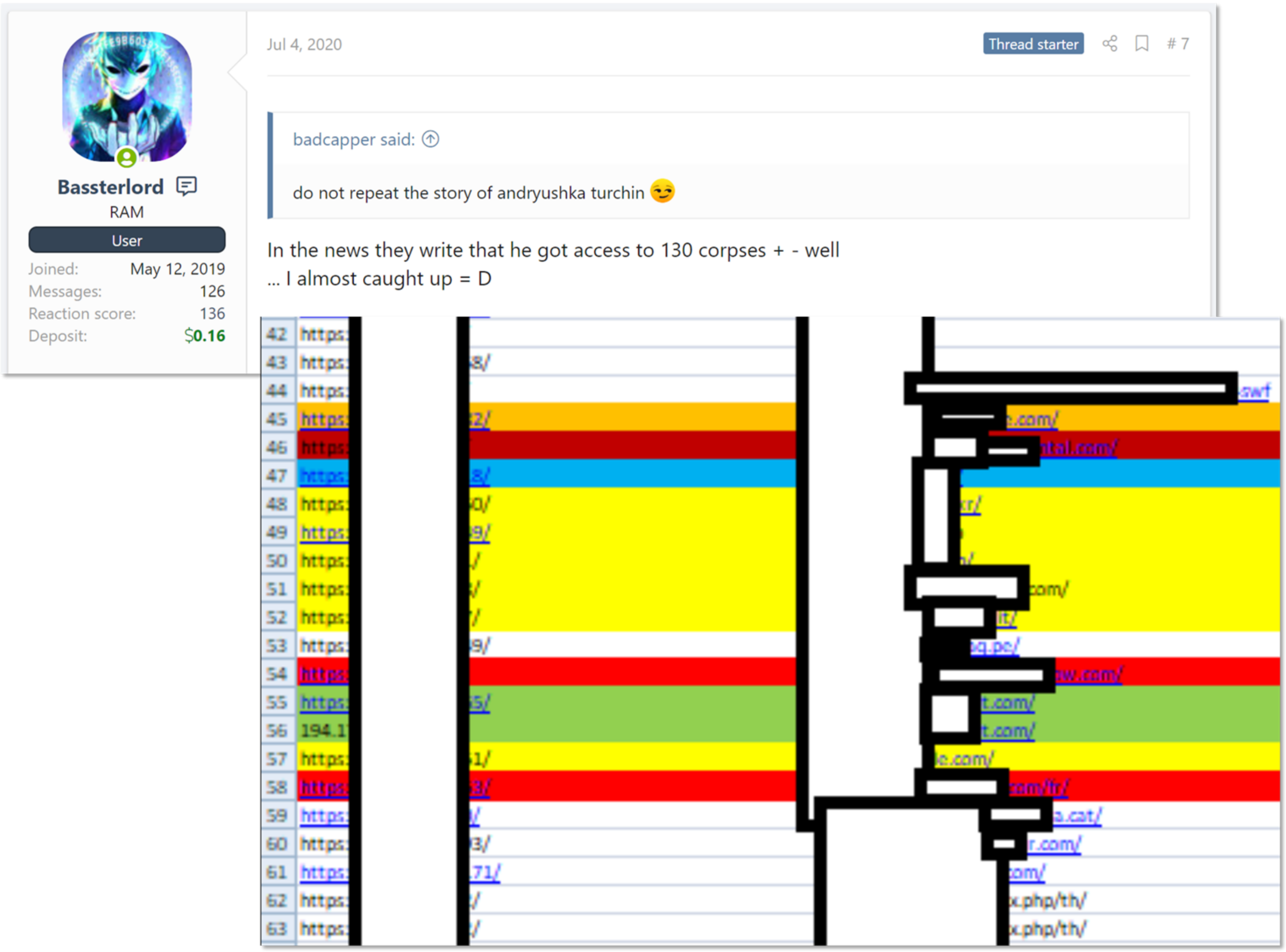
This dialogue, though appears to be superficial, showcases that uhodiransomwar was able to identify the victim only through Bassterlord’s description of it – meaning he had actual access to it as well. This fact implies that, somewhere, **initial access brokers and affiliates may have access to some shared database of breached entities.**

Very quickly this proved to indeed be the case, as on August 3, 2020, uhodiransomwar published the aforementioned Pulse Secure leak. In his main post, the actor claimed to be tired of other actors posing these so-called “public” compromises as private access to corporations and trying to profit off of them – hinting towards Bassterlord’s latest offers.

Bassterlord’s Little Black Book

Upon investigating the content of the leak, KELA was quickly able to match against several network accesses offered by the actor – proving that the leak indeed was the source of multiple (if not all) of Bassterlord’s offers as an initial access broker. Specifically, **we were able to trace servers back to the government entity mentioned in the paragraph above** – as well as another of Bassterlord’s victims: **a university to which he sold access for USD 12,000** on July 12.

After identifying several victims, we tried to get to the bottom of the list; where did it originate, and was it really passed between actors who were discreetly sharing compromises? Digging a bit back into previous posts by the actor, we found a reference in which **Bassterlord stated that he has potential access to at least 77 organizations** known to be vulnerable. In this thread, Bassterlord, somewhat braggingly, likened himself to Andrey Turchin – the main figure behind the notorious initial access broker FXMSP – stating that “in the news, they write that he [FXMSP – KELA] got access to more than 130 corporations. So… I’m almost caught up with him”. To this post, Bassterlord attached a heavily redacted screenshot of an Excel file that seems to contain dozens of entries, each one representing an initial entry vector (assumed to be a vulnerable Pulse Secure server) to an organization.



Bassterlord
RAM
User
Joined: May 12, 2019
Messages: 126
Reaction score: 136
Deposit: $0.16

Jul 4, 2020 Thread starter # 7

> badcapper said:
>
> do not repeat the story of andryushka turchin 😏

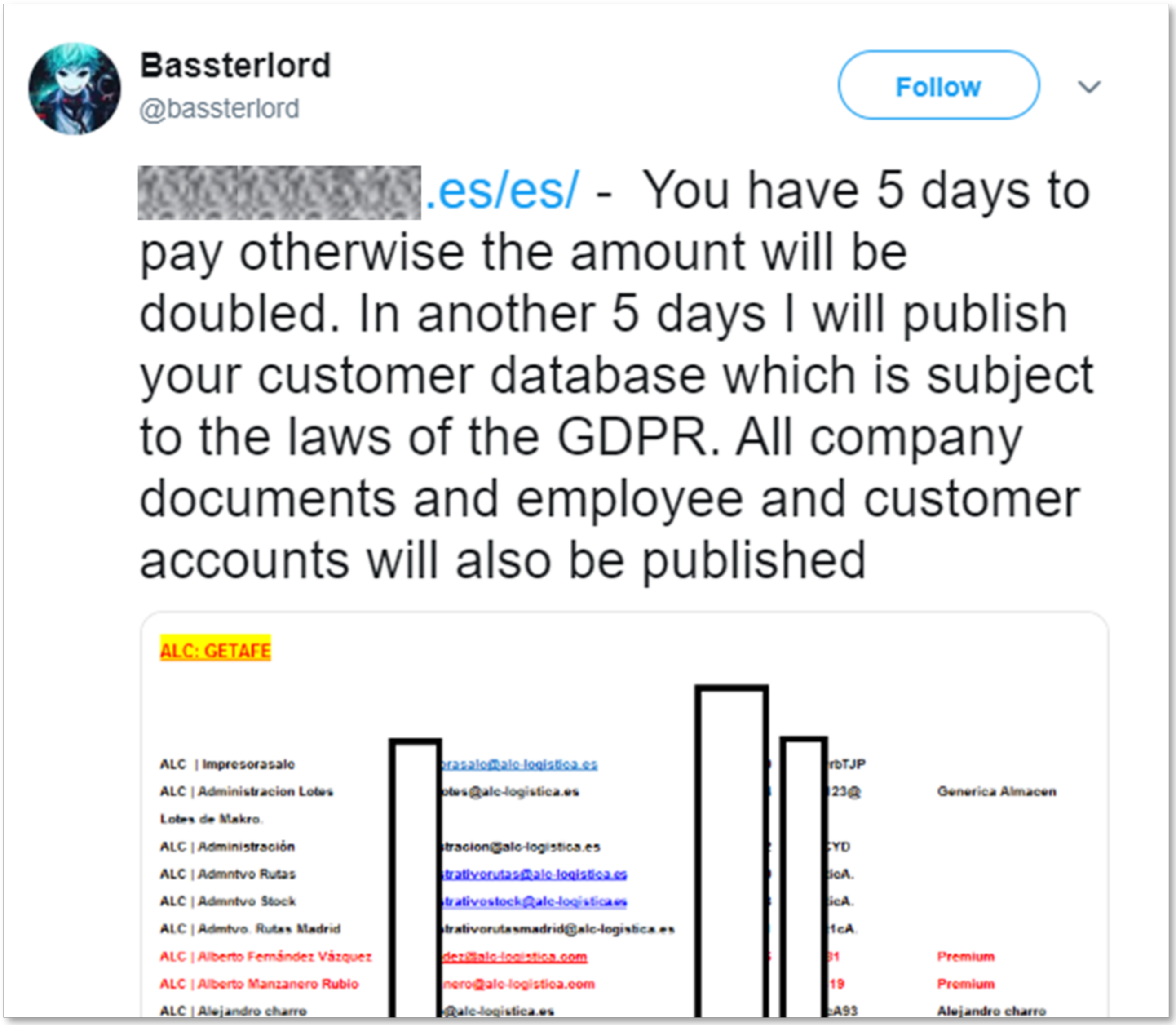
In the news they write that he got access to 130 corpses + - well
... I almost caught up = D

42	https:	[redacted]		[redacted]	
43	https:	[redacted]	8/	[redacted]	
44	https:	[redacted]		[redacted]	swf
45	https:	[redacted]	2/	[redacted]	.com/
46	https:	[redacted]		[redacted]	ntal.com/
47	https:	[redacted]	8/	[redacted]	
48	https:	[redacted]	0/	[redacted]	r/
49	https:	[redacted]	9/	[redacted]	
50	https:	[redacted]	/	[redacted]	/
51	https:	[redacted]	/	[redacted]	com/
52	https:	[redacted]	/	[redacted]	it/
53	https:	[redacted]	9/	[redacted]	q.pe/
54	https:	[redacted]		[redacted]	w.com/
55	https:	[redacted]	5/	[redacted]	t.com/
56	194.1	[redacted]		[redacted]	t.com/
57	https:	[redacted]	1/	[redacted]	e.com/
58	https:	[redacted]	3/	[redacted]	com/fr/
59	https:	[redacted]	/	[redacted]	a.cat/
60	https:	[redacted]	3/	[redacted]	r.com/
61	https:	[redacted]	71/	[redacted]	om/
62	https:	[redacted]	/	[redacted]	x.php/th/
63	https:	[redacted]	/	[redacted]	x.php/th/

Bassterlord’s post and a snapshot of his access list

The fact that Bassterlord was maintaining an active list of VPN-based accesses, coupled with the fact that uhodiransomwar claimed to have knowledge and access to it, implies that some version of this list was being shared or circulated internally between actors.

At times it seems that Bassterlord was trying to break out of the initial access broker cage and monetize his network accesses via direct extortion demands. A now-deleted tweet from July 11 by the actor taunts a Spain-based firm to pay within 5 days, or risk GDPR fines. However, it’s unclear whether this claimed attack was carried out via actual ransomware or manual extortion. Another hint to Bassterlord’s attempts to deploy ransomware is his post from July 12, where he discontinued the sale of access to a Thailand media company because it was “locked by me [him] personally”.



Bassterlord
@bassterlord

[redacted].es/es/ - You have 5 days to pay otherwise the amount will be doubled. In another 5 days I will publish your customer database which is subject to the laws of the GDPR. All company documents and employee and customer accounts will also be published

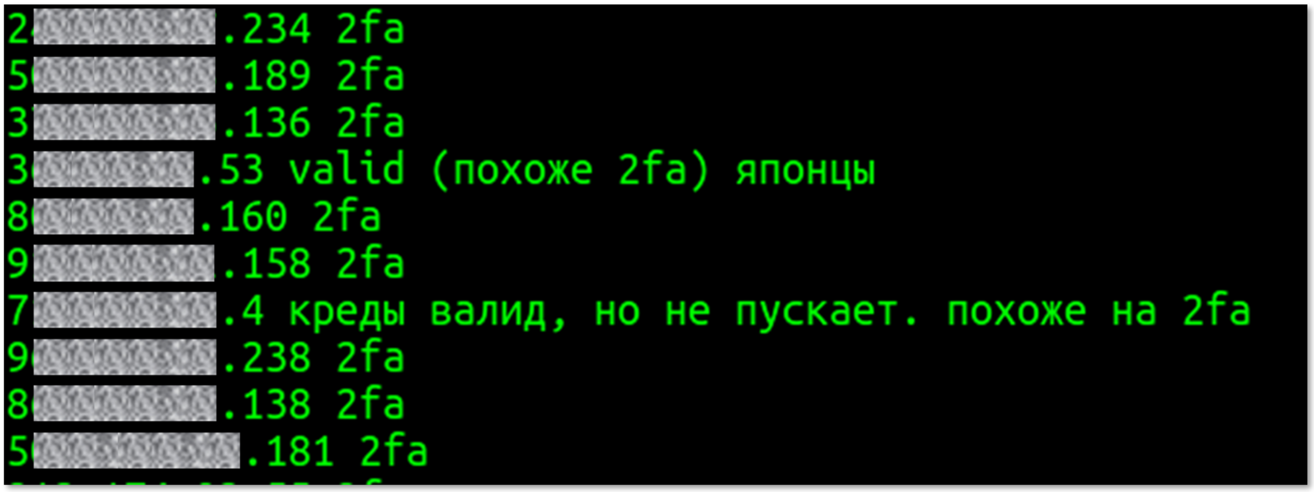
ALC: GETAFE

ALC | Impresorasalo	[redacted]	rasalo@alc-logistica.es	[redacted]	[redacted]	rbTJP	
ALC | Administracion Lotes	[redacted]	otes@alc-logistica.es	[redacted]	[redacted]	123@	Generica Almacen
Lotes de Makro.	[redacted]		[redacted]	[redacted]		
ALC | Administración	[redacted]	tracion@alc-logistica.es	[redacted]	[redacted]	YD	
ALC | Admntvo Rutas	[redacted]	trativorutas@alc-logistica.es	[redacted]	[redacted]	ioA.	
ALC | Admntvo Stock	[redacted]	trativostock@alc-logistica.es	[redacted]	[redacted]	icA.	
ALC | Admtvo. Rutas Madrid	[redacted]	trativorutasmadrid@alc-logistica.es	[redacted]	[redacted]	1cA.	
ALC | Alberto Fernández Vázquez	[redacted]	dez@alc-logistica.com	[redacted]	[redacted]	31	Premium
ALC | Alberto Manzanero Rubio	[redacted]	nero@alc-logistica.com	[redacted]	[redacted]	19	Premium
ALC | Alejandro charro	[redacted]	@alc-logistica.es	[redacted]	[redacted]	A93	Alejandro charro

What's in a List?

The full files leaked by uhodiransomwar and covered by ZDNet were in fact an archive, containing over 900 txt files – each pertaining to an exploited Secure Pulse server, and accompanied with notes taken by the actor who compiled the archive.

For example, 49 of the 900+ servers are noted to require two factor authentication in order to login to the admin panel:

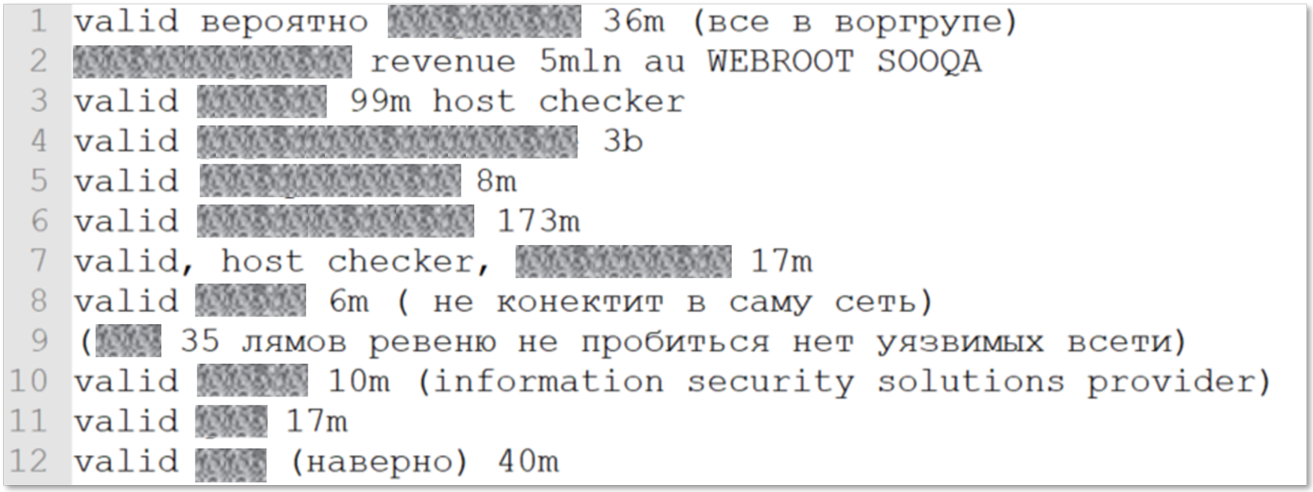


```
2[redacted].234 2fa
5[redacted].189 2fa
3[redacted].136 2fa
3[redacted].53 valid (похоже 2fa) японцы
8[redacted].160 2fa
9[redacted].158 2fa
7[redacted].4 креды валид, но не пускает. похоже на 2fa
9[redacted].238 2fa
8[redacted].138 2fa
5[redacted].181 2fa
```

Raw notes from the leaked archive, mentioning servers with 2FA

Of the remaining servers, around 250 are noted to be “bad”, “invalid” or otherwise inaccessible – and over 150 are noted as “need hash” (probably referring to a lack of a key data point – a password hash or a key – within the data obtained from the server, probably rendering it not as easily accessible).

Overall, it seems that around 400 of the servers included in the list are potentially valid and can be leveraged to deploy ransomware. Of these, some have notes mentioning the name of the company and, quite commonly, the organization’s revenue as well:



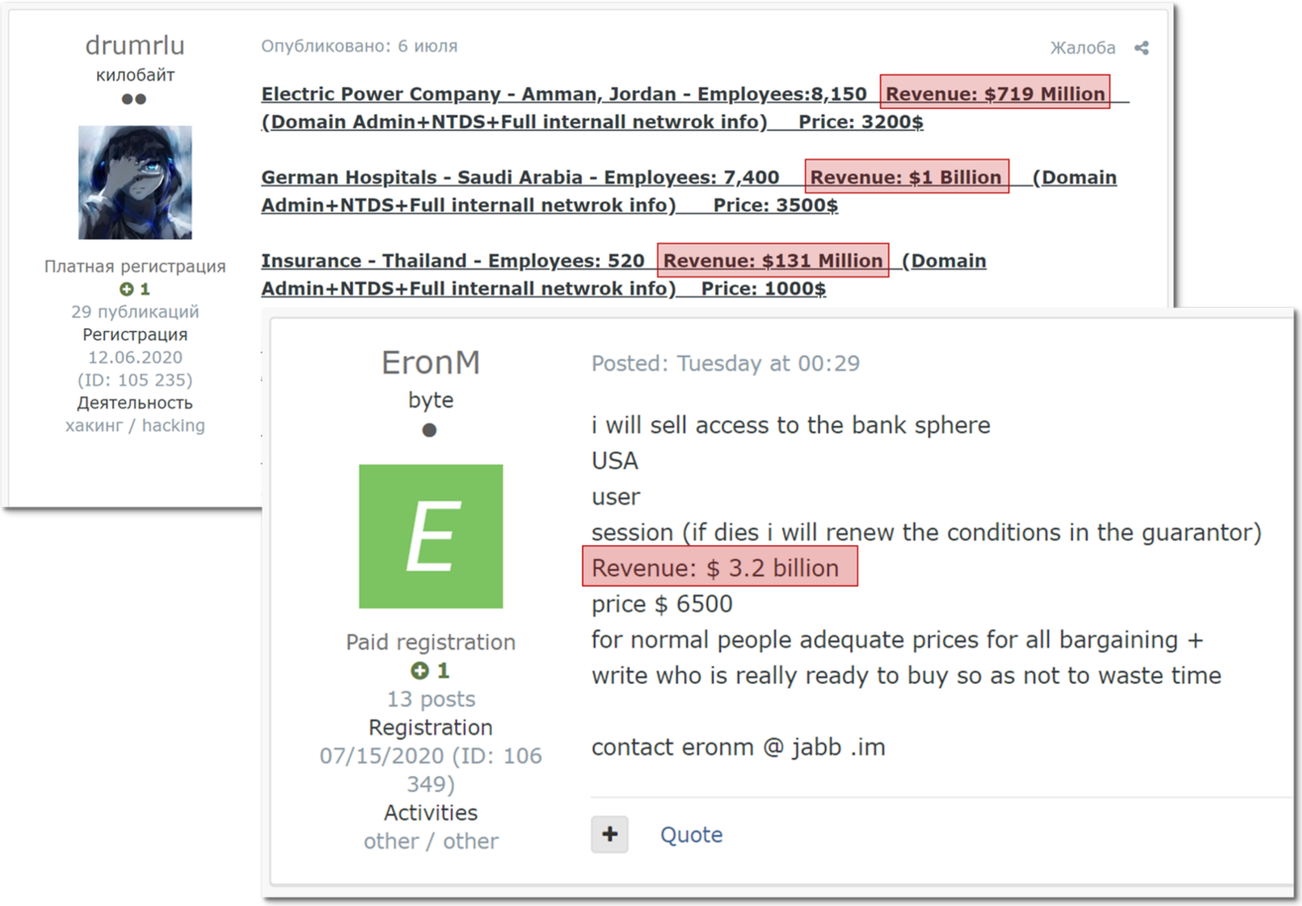
```
 1 valid вероятно [redacted] 36m (все в воргрупе)
 2 [redacted] revenue 5mln au WEBROOT SOOQA
 3 valid [redacted] 99m host checker
 4 valid [redacted] 3b
 5 valid [redacted] 8m
 6 valid [redacted] 173m
 7 valid, host checker, [redacted] 17m
 8 valid [redacted] 6m ( не конектит в саму сеть)
 9 ([redacted] 35 лямов ревеню не пробиться нет уязвимых всети)
10 valid [redacted] 10m (information security solutions provider)
11 valid [redacted] 17m
12 valid [redacted] (наверно) 40m
```

Notes mentioning potential victims’ revenue in a shortened notation. For example, “17m” (row 7) means USD 17 million, and “3b” means USD 3 billion

---

Sifting through these notes, one can easily trace several multi-million dollar companies – several of them public – as well as a few with over a billion USD in revenue. **These findings showcase the threat level that big, seemingly well-protected organizations may face from relatively novice actors acting as initial access brokers**.

Researching victims' revenue is a very common practice for initial access brokers, whose posts lately tend to mention revenue of their victims in order to entice potential buyers – based on an assumption that organizations with higher revenues would have the potential for a multi-million dollar ransom.



drumrlu
килобайт
●●

Платная регистрация
⊕ 1
29 публикаций
Регистрация
12.06.2020
(ID: 105 235)
Деятельность
хакинг / hacking

Опубликовано: 6 июля

Жалоба

Electric Power Company - Amman, Jordan - Employees:8,150 Revenue: $719 Million (Domain Admin+NTDS+Full internall netwrok info) Price: 3200$

German Hospitals - Saudi Arabia - Employees: 7,400 Revenue: $1 Billion (Domain Admin+NTDS+Full internall netwrok info) Price: 3500$

Insurance - Thailand - Employees: 520 Revenue: $131 Million (Domain Admin+NTDS+Full internall netwrok info) Price: 1000$

EronM
byte
●

Paid registration
⊕ 1
13 posts
Registration
07/15/2020 (ID: 106 349)
Activities
other / other

Posted: Tuesday at 00:29

i will sell access to the bank sphere
USA
user
session (if dies i will renew the conditions in the guarantor)
Revenue: $ 3.2 billion
price $ 6500
for normal people adequate prices for all bargaining +
write who is really ready to buy so as not to waste time

contact eronm @ jabb .im

Sales posts made by initial access brokers noting their victims' revenues

---

The real question to try and answer is: **How many of the entries in the archive made it past initial access brokers to ransomware affiliates – suffering a full-blown ransomware attack.** Here, the main obstacle in finding an answer is the sheer amount of ransomware attacks that go unreported by the victims.

Still, we were able to track leads to several companies that are publicly known to have suffered a breach that were mentioned in the files. For example, the file contains a mention of a company known to have impacted by a naming-and-shaming ransom actor; while we can’t corroborate a direct cause-and-effect relationship here, this leak still serves as a reminder that monitoring cybercrime sources can prove crucial for organizations.