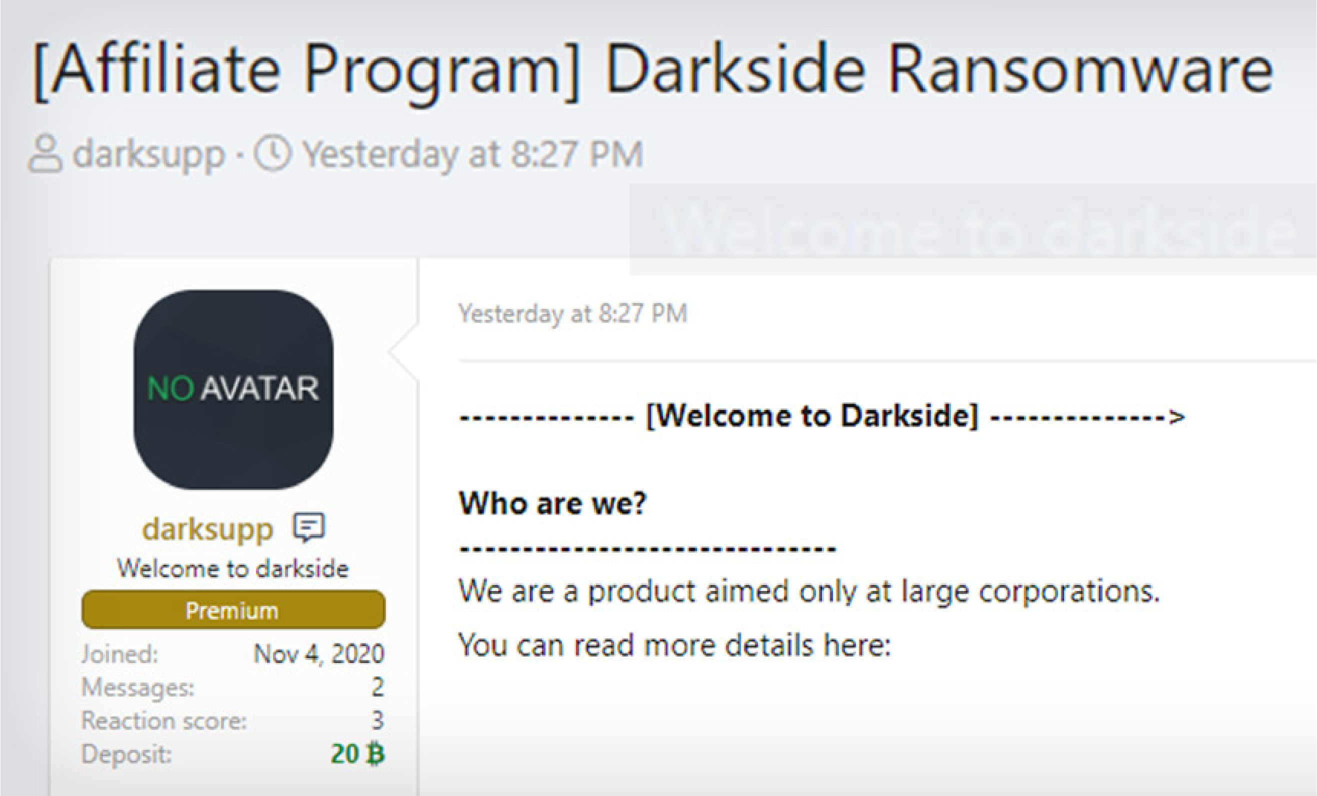
Darkside Ransomware Gang Launches Affiliate Program

databreachtoday.com/blogs/darkside-ransomware-gang-launches-affiliate-program-p-2968

Cybercrime , Cybercrime as-a-service , Endpoint Security

Using Affiliates Enables Crowdsourced Profits But Leaves Operators More Exposed Mathew J. Schwartz (euroinfosec) • November 12, 2020



[Affiliate Program] Darkside Ransomware

darksupp · Yesterday at 8:27 PM

Welcome to darkside

NO AVATAR

darksupp

Welcome to darkside

Premium

Joined:	Nov 4, 2020
Messages:	2
Reaction score:	3
Deposit:	20 ₿

Yesterday at 8:27 PM

-------------- [Welcome to Darkside] -------------->

Who are we?

We are a product aimed only at large corporations.

You can read more details here:

Advertisement by Darkside operators on a cybercrime forum (Source: Kela)

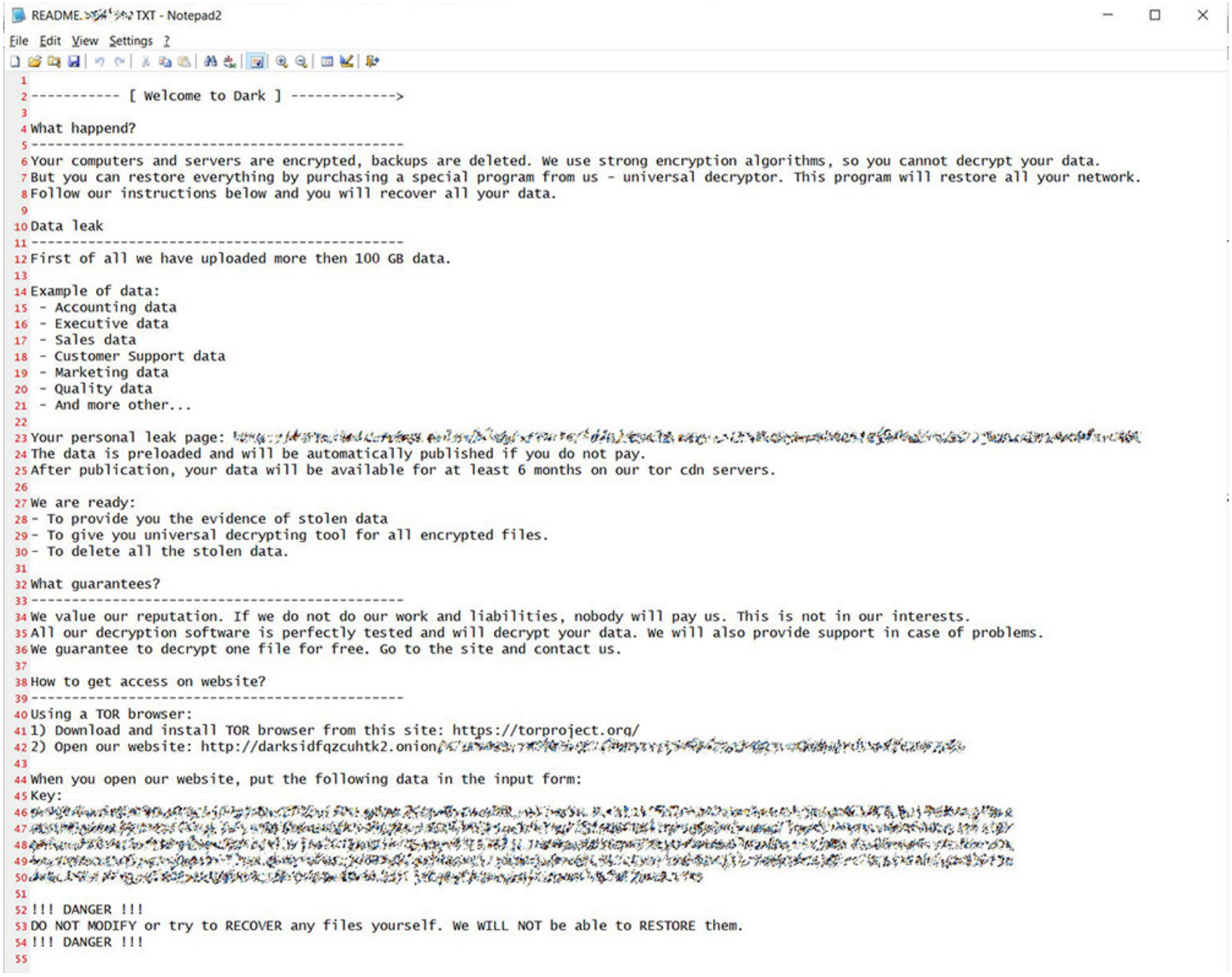
Darkside is the latest ransomware gang to announce that it's launched an affiliate program as part of its bid to maximize revenue.

See Also: Ransomware Demystified: What Security Analysts Need to Know

In recent days, the operators behind Darkside have taken to XSS and Exploit - two major, Russian-language cybercrime forums - to announce the details of the gang's new affiliate program, Israeli cyberthreat intelligence monitoring firm Kela reports.

> "The share paid to affiliates is 75% to 90%, depending on the size of the ransom." — Kela

Here's how such affiliate programs work: Ransomware operators provide crypto-locking malware code to third parties. Each affiliate receives a version of code with their unique ID embedded. For every victim that pays a ransom, the affiliate shares the take with the ransomware operator.

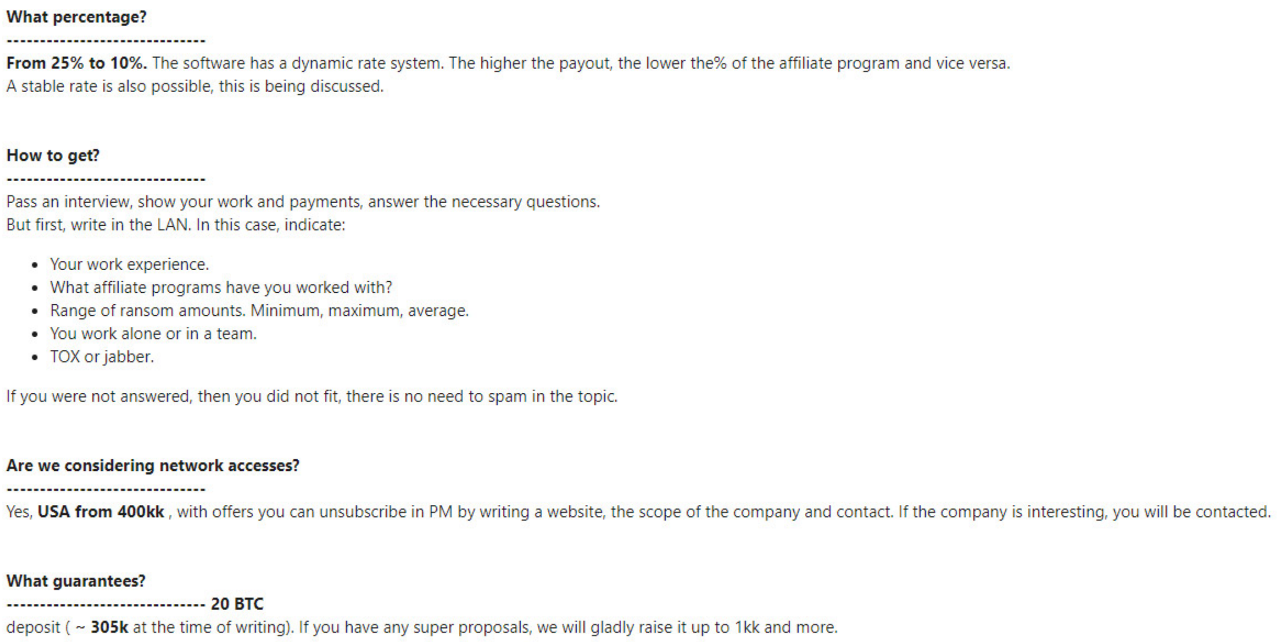


```

----------- [ Welcome to Dark ] ------------->

What happend?
----------------------------------------------
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
Follow our instructions below and you will recover all your data.

Data leak
----------------------------------------------
First of all we have uploaded more then 100 GB data.

Example of data:
 - Accounting data
 - Executive data
 - Sales data
 - Customer Support data
 - Marketing data
 - Quality data
 - And more other...

Your personal leak page: [redacted]
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.

We are ready:
- To provide you the evidence of stolen data
- To give you universal decrypting tool for all encrypted files.
- To delete all the stolen data.

What guarantees?
----------------------------------------------
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.

How to get access on website?
----------------------------------------------
Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://darksidfqzcuhtk2.onion[redacted]

When you open our website, put the following data in the input form:
Key:
[redacted]

!!! DANGER !!!
DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.
!!! DANGER !!!

```

Darkside ransom note (Source: Bleeping Computer)

For example, the affiliate program run by Sodinokibi - aka REvil - as of last year was giving 30% of every ransom payment to an affiliate, rising to 40% after three successful ransom payments (see: *Sodinokibi Ransomware Gang Appears to Be Making a Killing*).

Darkside's terms and conditions differ. "They stated that their average payments to their affiliates are about $400,000 and the share paid to affiliates is about 75-90% of every haul, depending on the size of the ransom, with the ransomware operators keeping the remainder," Kela says, noting that Darkside claims the average ransom it receives is between $1.6 million and $4 million.



What percentage?

From 25% to 10%. The software has a dynamic rate system. The higher the payout, the lower the% of the affiliate program and vice versa.
A stable rate is also possible, this is being discussed.

How to get?

Pass an interview, show your work and payments, answer the necessary questions.
But first, write in the LAN. In this case, indicate:

- Your work experience.
- What affiliate programs have you worked with?
- Range of ransom amounts. Minimum, maximum, average.
- You work alone or in a team.
- TOX or jabber.

If you were not answered, then you did not fit, there is no need to spam in the topic.

Are we considering network accesses?

Yes, **USA from 400kk** , with offers you can unsubscribe in PM by writing a website, the scope of the company and contact. If the company is interesting, you will be contacted.

What guarantees?

----------------------------- **20 BTC**
deposit (~ **305k** at the time of writing). If you have any super proposals, we will gladly raise it up to 1kk and more.

Post by Darkside operators to a Russian-language cybercrime forum (Source and translation: Kela)

Ransomware affiliate programs abound. Victoria Kivilevich, a threat intelligence analyst at Kela, says some of the more famous "big game" ransomware operators running affiliate programs - as well as blogs for leaking stolen data - include:

- Avaddon;
- Darkside;
- LockBit;
- Netwalker;
- Ranzy;
- Sodinokibi, aka REvil;
- Suncrypt - now apparently retired.

Other ransomware operations - some active, some now defunct - that have run affiliate programs include Chimera, CryLock, Exorcist, Gretta, Makop, Thanos and Zeppelin, she says.

Affiliate Program Upsides

Running an affiliate program offers numerous upsides. For starters, the ransomware operator handles the technical side, including "product updates." Once the operator has built all required infrastructure - typically including a self-service portal for victims to pay - they can, in theory, scale to handle as many affiliates as they want. This crowdsourcing model can give them the ability to realize much greater profits, especially compared to trying to hit victims themselves. Affiliates, meanwhile, don't need to build and maintain their own malware and infrastructure.

Other upsides include the ability of the operation to attract specialists - in network penetration, for example - who can focus on amassing victims while leaving tech support and customer service, so to speak, to the operator.

Two Main Downsides

So, what are the downsides to running an affiliate program? Kivilevich highlights two main problems: reputation and infiltration.

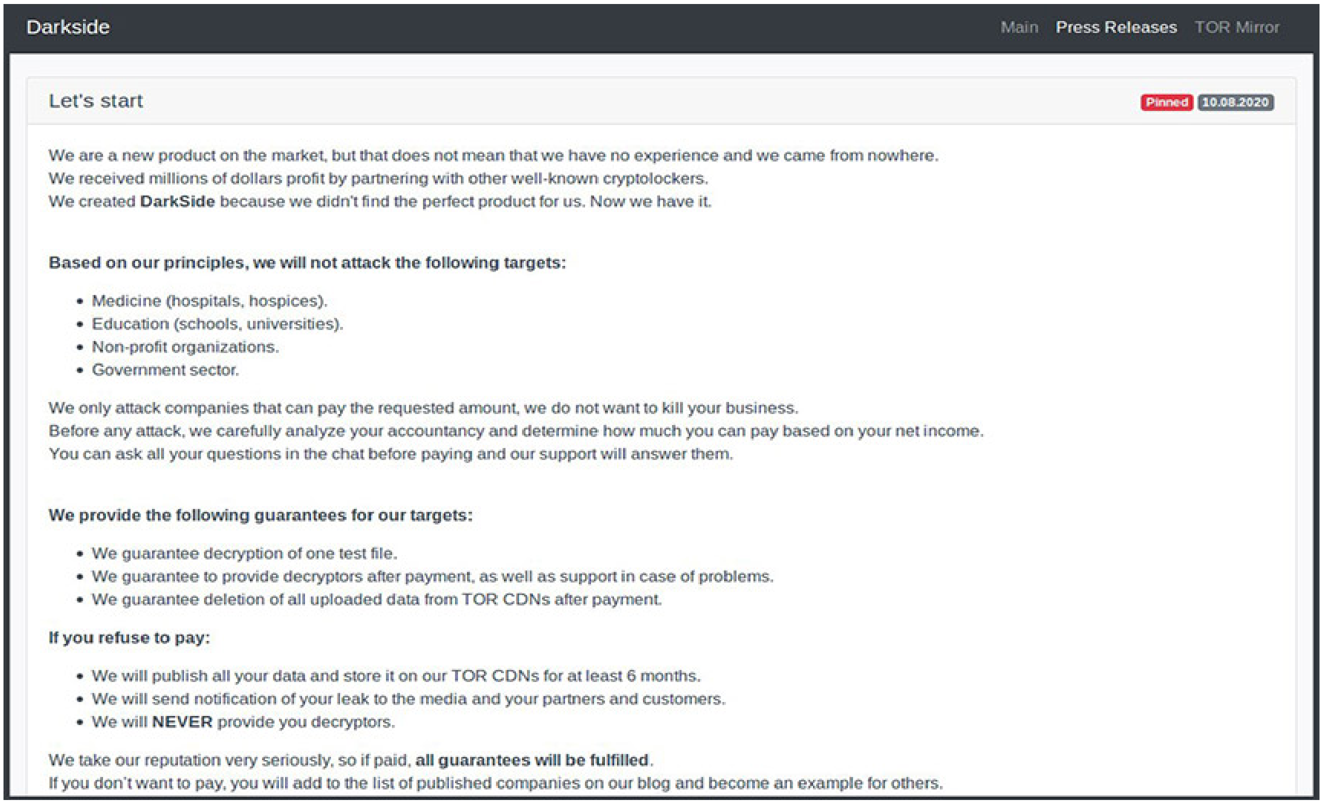
If an affiliate does something bad, that reflects on the operator, as Darkside has noted in one of its posts. "For example, when an affiliate of Suncrypt attacked hospitals, you see Suncrypt writing: 'A new affiliate locked it unknowingly, and for this he was punished! Hospitals, government, airports, etc., we do not attack,'" she says.

Relying on affiliates also means that the ransomware operation may be inadvertently recruiting undercover security researchers or law enforcement agents who might potentially "gather more intelligence about their activities," Kivilevich says.

Ransomware Features

How big a threat does Darkside pose? The operators say that the crypto-locking malware that Darkside provides to affiliates can encrypt both Windows and Linux files. Researchers at Russian security firm Kaspersky recently determined that RansomEXX ransomware also can crypto-lock Linux files (see: *RansomEXX Ransomware Can Now Target Linux Systems*).

Like many types of malware, Darkside is designed so it cannot infect PCs that are in one of the member states of the post-Soviet Commonwealth of Independent States, which includes Russia and 11 other nations (see: *Russia's Cybercrime Rule Reminder: Never Hack Russians*).



Let's start

We are a new product on the market, but that does not mean that we have no experience and we came from nowhere.
We received millions of dollars profit by partnering with other well-known cryptolockers.
We created **DarkSide** because we didn't find the perfect product for us. Now we have it.

Based on our principles, we will not attack the following targets:

- Medicine (hospitals, hospices).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business.
Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income.
You can ask all your questions in the chat before paying and our support will answer them.

We provide the following guarantees for our targets:

- We guarantee decryption of one test file.
- We guarantee to provide decryptors after payment, as well as support in case of problems.
- We guarantee deletion of all uploaded data from TOR CDNs after payment.

If you refuse to pay:

- We will publish all your data and store it on our TOR CDNs for at least 6 months.
- We will send notification of your leak to the media and your partners and customers.
- We will **NEVER** provide you decryptors.

We take our reputation very seriously, so if paid, **all guarantees will be fulfilled**.
If you don't want to pay, you will add to the list of published companies on our blog and become an example for others.

"Press release" from Darkside in August announcing its debut (Source: MalwareHunterTeam)

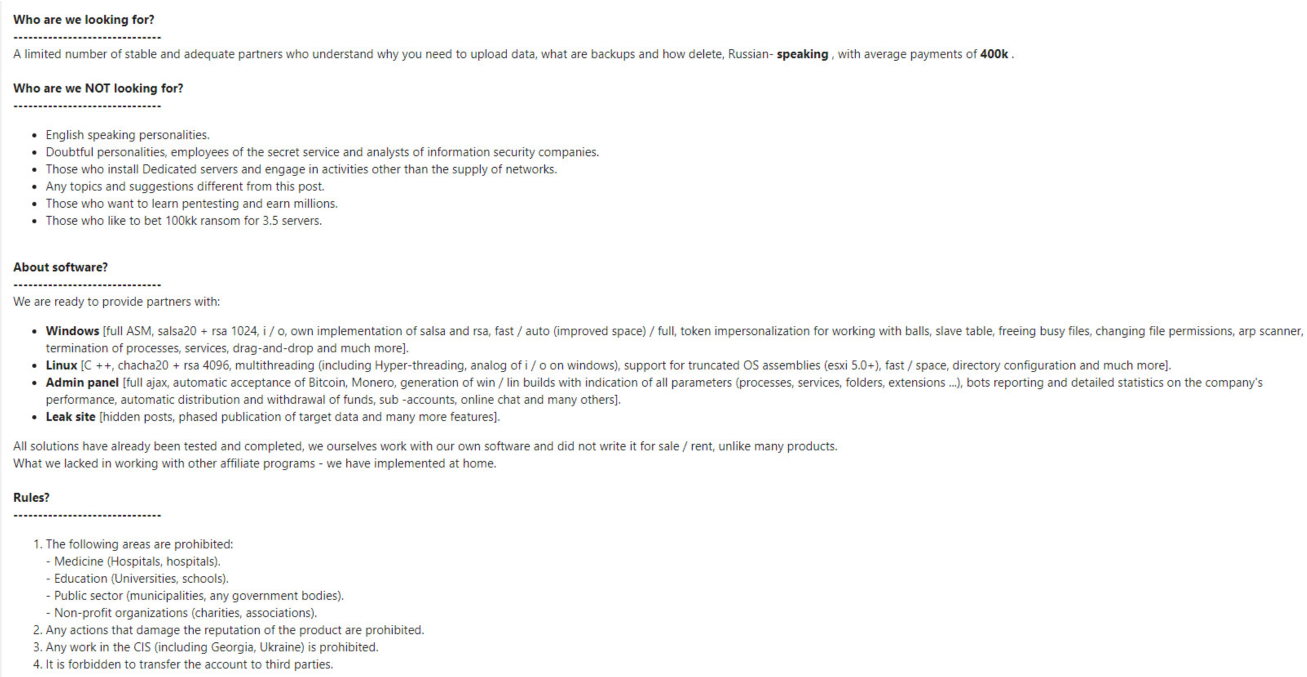
As proof of its success to date, Darkside has deposited 20 bitcoins - worth about $315,000 - with the XSS forum. Kivilevich says this is "a common method ransomware gangs will use to show that their operation generates plenty of profit."

Like many other ransomware operations, the gang maintains a leak site, where it names and shames victims and can post samples of stolen data to try to force victims to pay (see: *Data-Exfiltrating Ransomware Gangs Pedal False Promises*).

Even so, it's not yet clear how many organizations Darkside or its affiliates might have hit.

"Darkside has been relatively quiet since the gang emerged. They've published only four victims on their site, with one being removed," Kivilevich says. "It's possible the gang is extending their efforts, meaning that we could expect to see them performing more attacks."

In a likely bid to boost profits, the gang has posted that it's looking for initial access brokers that can give it access to U.S. businesses with annual revenue of at least $400 million.



Who are we looking for?

A limited number of stable and adequate partners who understand why you need to upload data, what are backups and how delete, Russian- **speaking** , with average payments of **400k** .

Who are we NOT looking for?

- English speaking personalities.
- Doubtful personalities, employees of the secret service and analysts of information security companies.
- Those who install Dedicated servers and engage in activities other than the supply of networks.
- Any topics and suggestions different from this post.
- Those who want to learn pentesting and earn millions.
- Those who like to bet 100kk ransom for 3.5 servers.

About software?

We are ready to provide partners with:

- **Windows** [full ASM, salsa20 + rsa 1024, i / o, own implementation of salsa and rsa, fast / auto (improved space) / full, token impersonalization for working with balls, slave table, freeing busy files, changing file permissions, arp scanner, termination of processes, services, drag-and-drop and much more].
- **Linux** [C ++, chacha20 + rsa 4096, multithreading (including Hyper-threading, analog of i / o on windows), support for truncated OS assemblies (esxi 5.0+), fast / space, directory configuration and much more].
- **Admin panel** [full ajax, automatic acceptance of Bitcoin, Monero, generation of win / lin builds with indication of all parameters (processes, services, folders, extensions ...), bots reporting and detailed statistics on the company's performance, automatic distribution and withdrawal of funds, sub -accounts, online chat and many others].
- **Leak site** [hidden posts, phased publication of target data and many more features].

All solutions have already been tested and completed, we ourselves work with our own software and did not write it for sale / rent, unlike many products.
What we lacked in working with other affiliate programs - we have implemented at home.

Rules?
----

1. The following areas are prohibited:
   - Medicine (Hospitals, hospitals).
   - Education (Universities, schools).
   - Public sector (municipalities, any government bodies).
   - Non-profit organizations (charities, associations).
2. Any actions that damage the reputation of the product are prohibited.
3. Any work in the CIS (including Georgia, Ukraine) is prohibited.
4. It is forbidden to transfer the account to third parties.

Post by Darkside operators to a Russian-language cybercrime forum (Source and translation: Kela)

"Darkside is aiming for big targets," Kivilevich says, adding that it's the first time she's seen "ransomware operators offering initial access brokers the opportunity to directly trade with them" rather than attempting to rely on "affiliates or other middlemen."

As always with ransomware, criminal innovation - in a nonstop drive by attackers to maximize profits - appears to be paying off at victims' expense.

This piece has been updated to clarify the amount DarkSide pays to affiliates.