SECURELIST by Kaspersky

How much does access to corporate infrastructure cost?

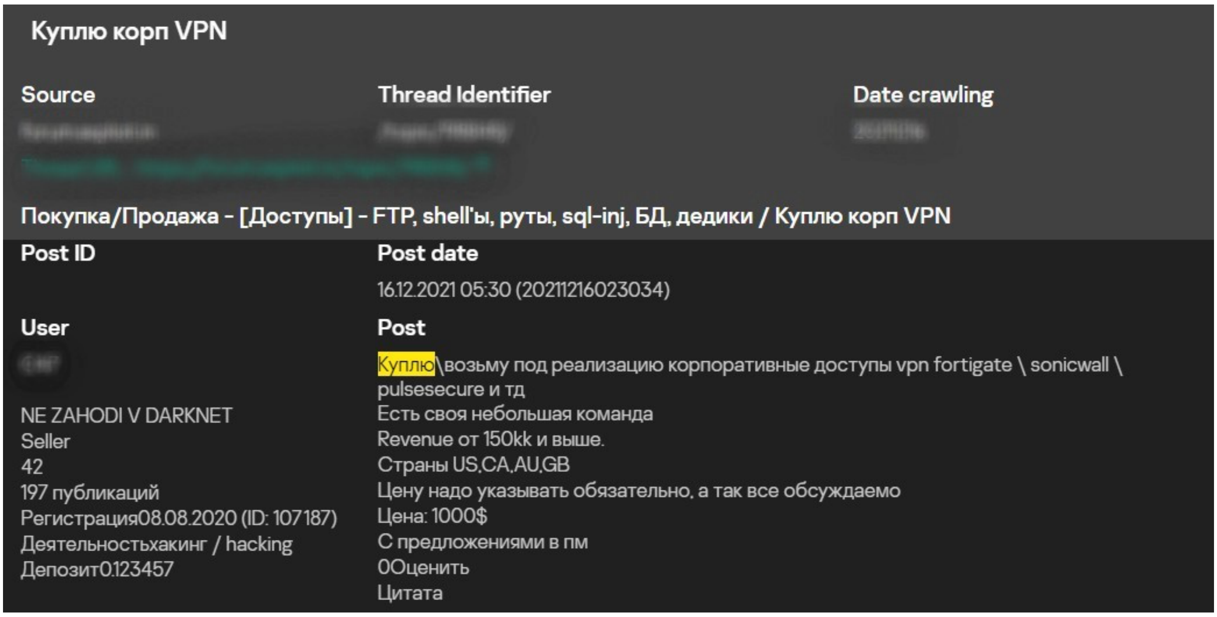
RESEARCH

15 JUN 2022

Division of labor

Money has been and remains the main motivator for cybercriminals. The most widespread techniques of monetizing cyberattacks include selling stolen databases, extortion (using ransomware) and carding. However, there is demand on the dark web not only for data obtained through an attack, but also for the data and services necessary to organize one (e.g., to perform specific steps of a multiphase attack). Complex attacks almost invariably feature several phases, such as reconnaissance, initial access to the infrastructure, gaining access to target systems and/or privileges, and the actual malicious acts (data theft, destruction or encryption, etc.). This is just one example of a phased attack where each step can be accomplished by a new contractor – if only because the different steps require different expertise.

Experienced cybercriminals seek to ensure the continuity of their business and constantly need new data for initial access to corporate systems. It's advantageous for them to pay for prearranged access rather than spend time digging for primary vulnerabilities and penetrating the perimeter.



Куплю корп VPN

Source
[redacted]

Thread Identifier
[redacted]

Date crawling
[redacted]

Покупка/Продажа - [Доступы] - FTP, shell'ы, руты, sql-inj, БД, дедики / Куплю корп VPN

Post ID

Post date
16.12.2021 05:30 (20211216023034)

User
[redacted]

NE ZAHODI V DARKNET
Seller
42
197 публикаций
Регистрация08.08.2020 (ID: 107187)
Деятельностьхакинг / hacking
Депозит0.123457

Post
Куплю\возьму под реализацию корпоративные доступы vpn fortigate \ sonicwall \ pulsesecure и тд
Есть своя небольшая команда
Revenue от 150kk и выше.
Страны US,CA,AU,GB
Цену надо указывать обязательно, а так все обсуждаемо
Цена: 1000$
С предложениями в пм
0Оценить
Цитата

Screenshot translation

Request for access to corporate VPN. Source: Kaspersky Digital Footprint Intelligence service portal

In contrast, less experienced cybercriminals are not always able to see an attack through to the end (malware execution, data theft, etc.), but are proficient enough to make money by selling initial access. This article deals specifically with this initial access market.

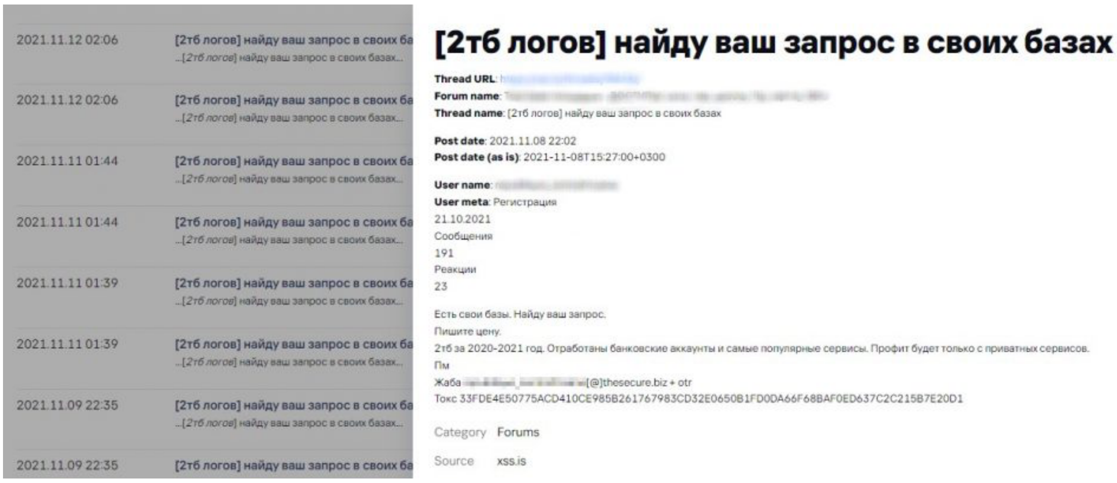
Types of initial access

These are the most common actions used by cybercriminals to obtain initial access to corporate infrastructure in order to develop an attack:

- Exploitation of software vulnerabilities. For example, attacks on a corporate web resource (exploitation of first-day vulnerabilities across website components, SQL injections, gaining access to vulnerable web app control panels, etc.).
- Obtaining legitimate corporate credentials. For example, use of data from stealer logs or password mining.
- Phishing attacks on employees. For example, an email with a malicious payload.

You can learn more about these types of attacks and the specifics of gaining initial access from our analysis report based on data from hundreds of incident investigations.

A special mention should be made of the method for capturing legitimate accounts based on stealers. These malicious programs residing in infected devices collect various account and payment data, cookie files, authorization tokens, etc. that they save to their logs. Cybercriminals scan these logs in search of data they can exploit and monetize: some are looking for credit card data, others for domain accounts, social network accounts, etc. They refer to this stage as processing. After sorting the logs, they either exchange their finds on forums by making them public or sell them to individual buyers.



2021.11.12 02:06	[2тб логов] найду ваш запрос в своих ба ...[2тб логов] найду ваш запрос в своих базах...
2021.11.12 02:06	[2тб логов] найду ваш запрос в своих ба ...[2тб логов] найду ваш запрос в своих базах...
2021.11.11 01:44	[2тб логов] найду ваш запрос в своих ба ...[2тб логов] найду ваш запрос в своих базах...
2021.11.11 01:44	[2тб логов] найду ваш запрос в своих ба ...[2тб логов] найду ваш запрос в своих базах...
2021.11.11 01:39	[2тб логов] найду ваш запрос в своих ба ...[2тб логов] найду ваш запрос в своих базах...
2021.11.11 01:39	[2тб логов] найду ваш запрос в своих ба ...[2тб логов] найду ваш запрос в своих базах...
2021.11.09 22:35	[2тб логов] найду ваш запрос в своих ба ...[2тб логов] найду ваш запрос в своих базах...
2021.11.09 22:35	[2тб логов] найду ваш запрос в своих ба

[2тб логов] найду ваш запрос в своих базах

Thread URL: [redacted]
Forum name: [redacted]
Thread name: [2тб логов] найду ваш запрос в своих базах

Post date: 2021.11.08 22:02
Post date (as is): 2021-11-08T15:27:00+0300

User name: [redacted]
User meta: Регистрация
21.10.2021
Сообщения
191
Реакции
23

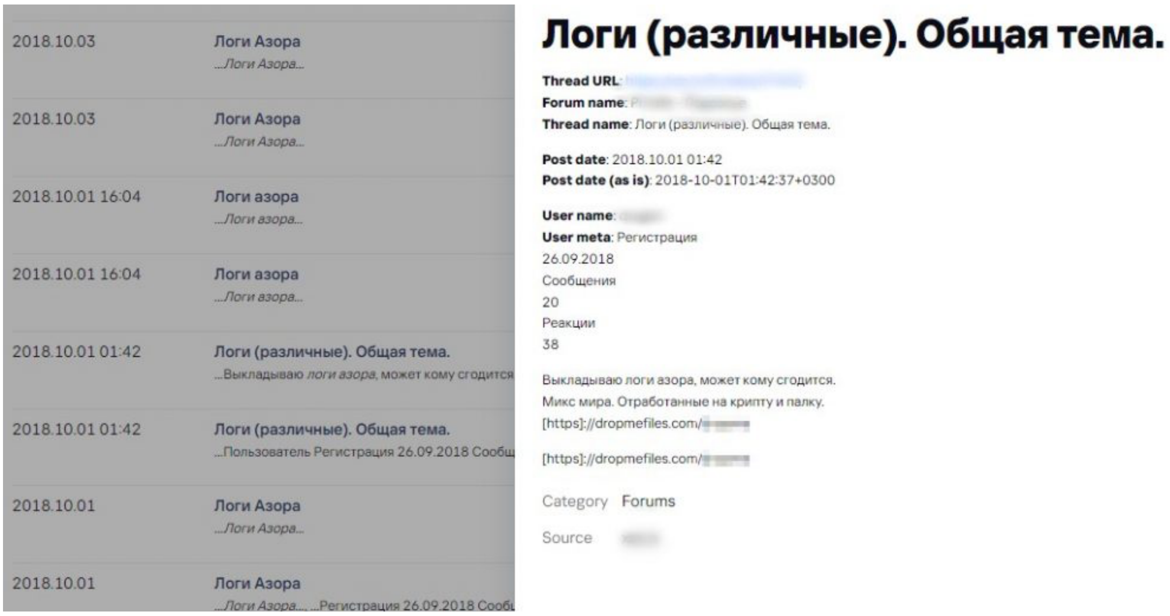
Есть свои базы. Найду ваш запрос.
Пишите цену.
2тб за 2020-2021 год. Отработаны банковские аккаунты и самые популярные сервисы. Профит будет только с приватных сервисов.
Пм
Жаба [redacted][@]thesecure.biz + otr
Токс 33FDE4E50775ACD410CE985B261767983CD32E0650B1FD0DA66F68BAF0ED637C2C215B7E20D1

Category Forums

Source xss.is

Screenshot translation

Malware log offers on a dark web forum. Source: Digital Footprint Intelligence service



2018.10.03	Логи Азора ...Логи Азора...
2018.10.03	Логи Азора ...Логи Азора...
2018.10.01 16:04	Логи азора ...Логи азора...
2018.10.01 16:04	Логи азора ...Логи азора...
2018.10.01 01:42	Логи (различные). Общая тема. ...Выкладываю *логи азора*, может кому сгодится
2018.10.01 01:42	Логи (различные). Общая тема. ...Пользователь Регистрация 26.09.2018 Сообщ
2018.10.01	Логи Азора ...Логи Азора...
2018.10.01	Логи Азора ...Логи Азора..., ...Регистрация 26.09.2018 Сообщ

Логи (различные). Общая тема.

Thread URL: [redacted]
Forum name: [redacted]
Thread name: Логи (различные). Общая тема.

Post date: 2018.10.01 01:42
Post date (as is): 2018-10-01T01:42:37+0300

User name: [redacted]
User meta: Регистрация
26.09.2018
Сообщения
20
Реакции
38

Выкладываю логи азора, может кому сгодится.
Микс мира. Отработанные на крипту и палку.
[https]://dropmefiles.com/[redacted]

[https]://dropmefiles.com/[redacted]

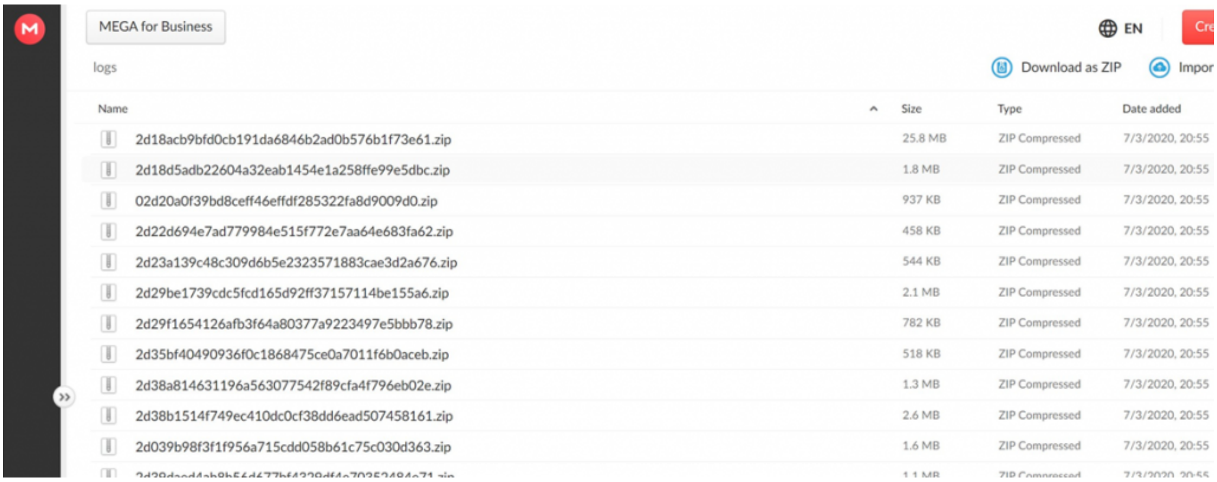
Category Forums

Source [redacted]

Screenshot translation

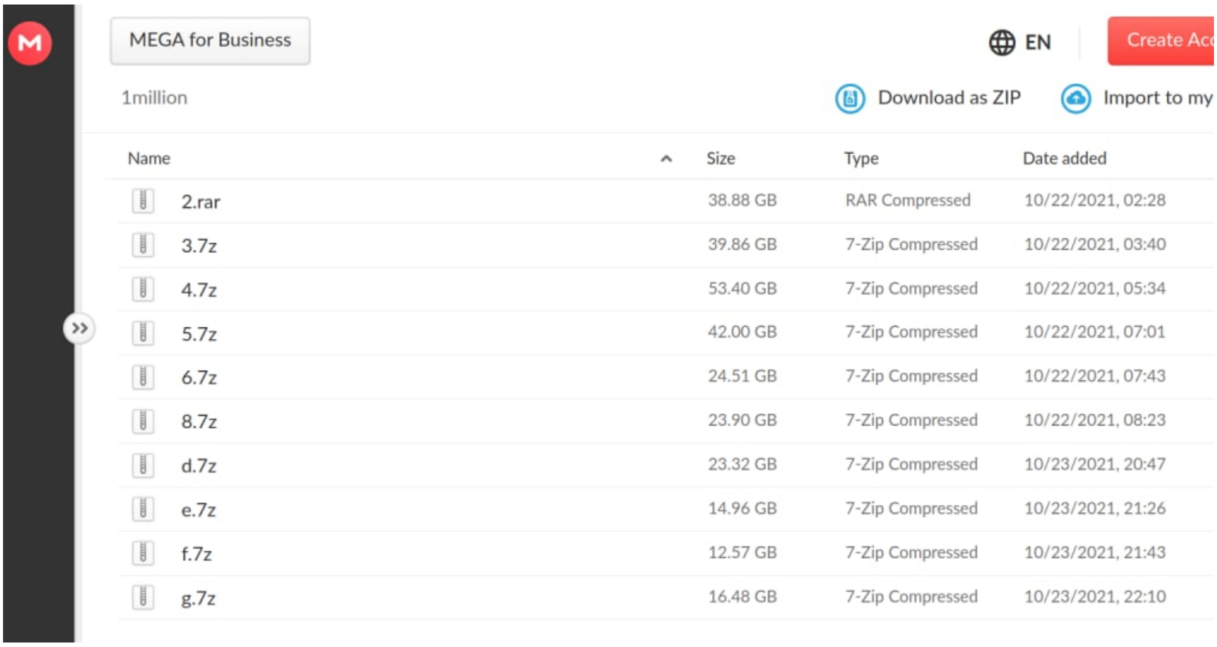
Free malware log offers on a dark web forum. Source: Digital Footprint Intelligence service

The cybercriminals are literally dealing in gigabytes of logs generated by stealers.



logs

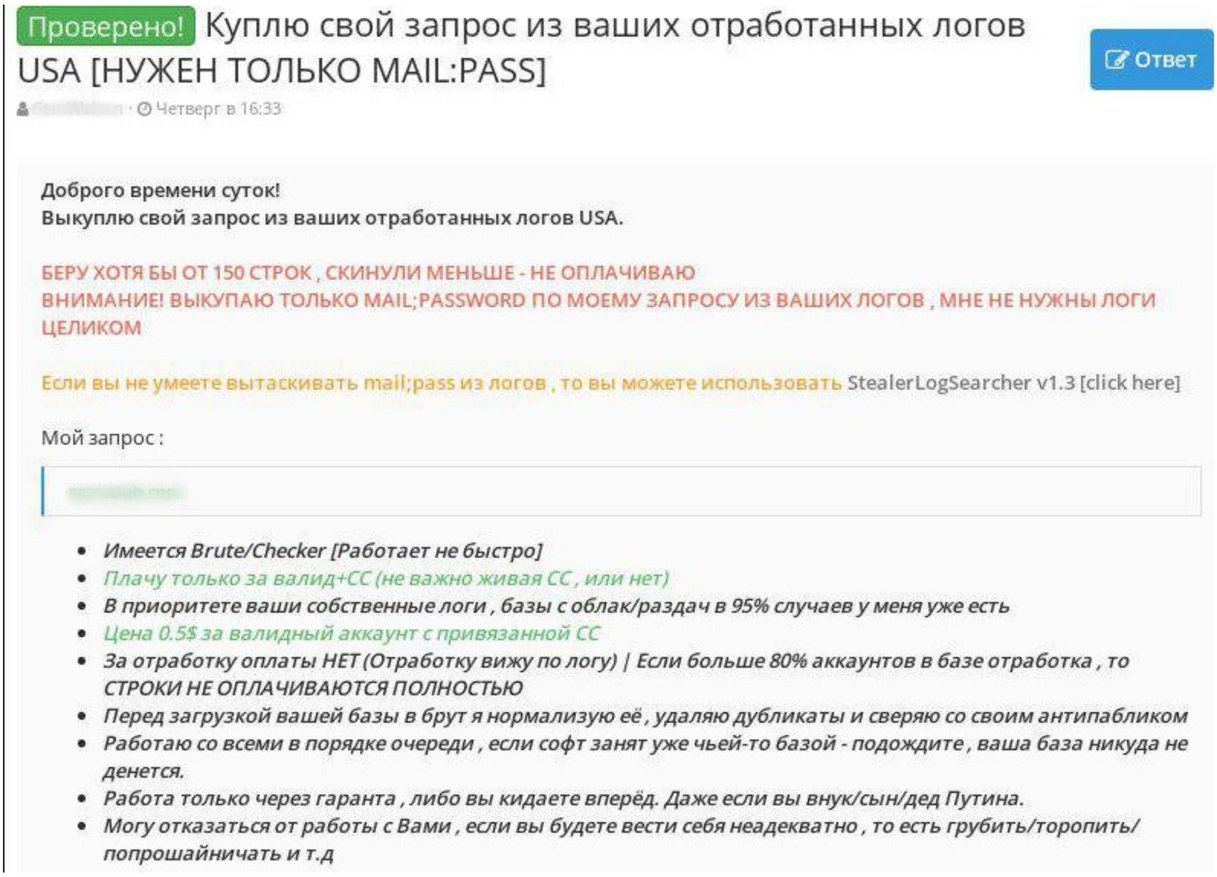
Name	Size	Type	Date added
2d18acb9bfd0cb191da6846b2ad0b576b1f73e61.zip	25.8 MB	ZIP Compressed	7/3/2020, 20:55
2d18d5adb22604a32eab1454e1a258ffe99e5dbc.zip	1.8 MB	ZIP Compressed	7/3/2020, 20:55
02d20a0f39bd8ceff46effdf285322fa8d9009d0.zip	937 KB	ZIP Compressed	7/3/2020, 20:55
2d22d694e7ad779984e515f772e7aa64e683fa62.zip	458 KB	ZIP Compressed	7/3/2020, 20:55
2d23a139c48c309d6b5e2323571883cae3d2a676.zip	544 KB	ZIP Compressed	7/3/2020, 20:55
2d29be1739cdc5fcd165d92ff37157114be155a6.zip	2.1 MB	ZIP Compressed	7/3/2020, 20:55
2d29f1654126afb3f64a80377a9223497e5bbb78.zip	782 KB	ZIP Compressed	7/3/2020, 20:55
2d35bf40490936f0c1868475ce0a7011f6b0aceb.zip	518 KB	ZIP Compressed	7/3/2020, 20:55
2d38a814631196a563077542f89cfa4f796eb02e.zip	1.3 MB	ZIP Compressed	7/3/2020, 20:55
2d38b1514f749ec410dc0cf38dd6ead507458161.zip	2.6 MB	ZIP Compressed	7/3/2020, 20:55
2d039b98f3f1f956a715cdd058b61c75c030d363.zip	1.6 MB	ZIP Compressed	7/3/2020, 20:55
2d39daed4ab8b56d677bf4329df4e70352484e71.zip	1.1 MB	ZIP Compressed	7/3/2020, 20:55



1million

Name	Size	Type	Date added
2.rar	38.88 GB	RAR Compressed	10/22/2021, 02:28
3.7z	39.86 GB	7-Zip Compressed	10/22/2021, 03:40
4.7z	53.40 GB	7-Zip Compressed	10/22/2021, 05:34
5.7z	42.00 GB	7-Zip Compressed	10/22/2021, 07:01
6.7z	24.51 GB	7-Zip Compressed	10/22/2021, 07:43
8.7z	23.90 GB	7-Zip Compressed	10/22/2021, 08:23
d.7z	23.32 GB	7-Zip Compressed	10/23/2021, 20:47
e.7z	14.96 GB	7-Zip Compressed	10/23/2021, 21:26
f.7z	12.57 GB	7-Zip Compressed	10/23/2021, 21:43
g.7z	16.48 GB	7-Zip Compressed	10/23/2021, 22:10

Large volume of logs uploaded to a file exchange service



Проверено! Куплю свой запрос из ваших отработанных логов USA [НУЖЕН ТОЛЬКО MAIL:PASS]

Ответ

[redacted] · Четверг в 16:33

Доброго времени суток!
Выкуплю свой запрос из ваших отработанных логов USA.

БЕРУ ХОТЯ БЫ ОТ 150 СТРОК , СКИНУЛИ МЕНЬШЕ - НЕ ОПЛАЧИВАЮ
ВНИМАНИЕ! ВЫКУПАЮ ТОЛЬКО MAIL;PASSWORD ПО МОЕМУ ЗАПРОСУ ИЗ ВАШИХ ЛОГОВ , МНЕ НЕ НУЖНЫ ЛОГИ ЦЕЛИКОМ

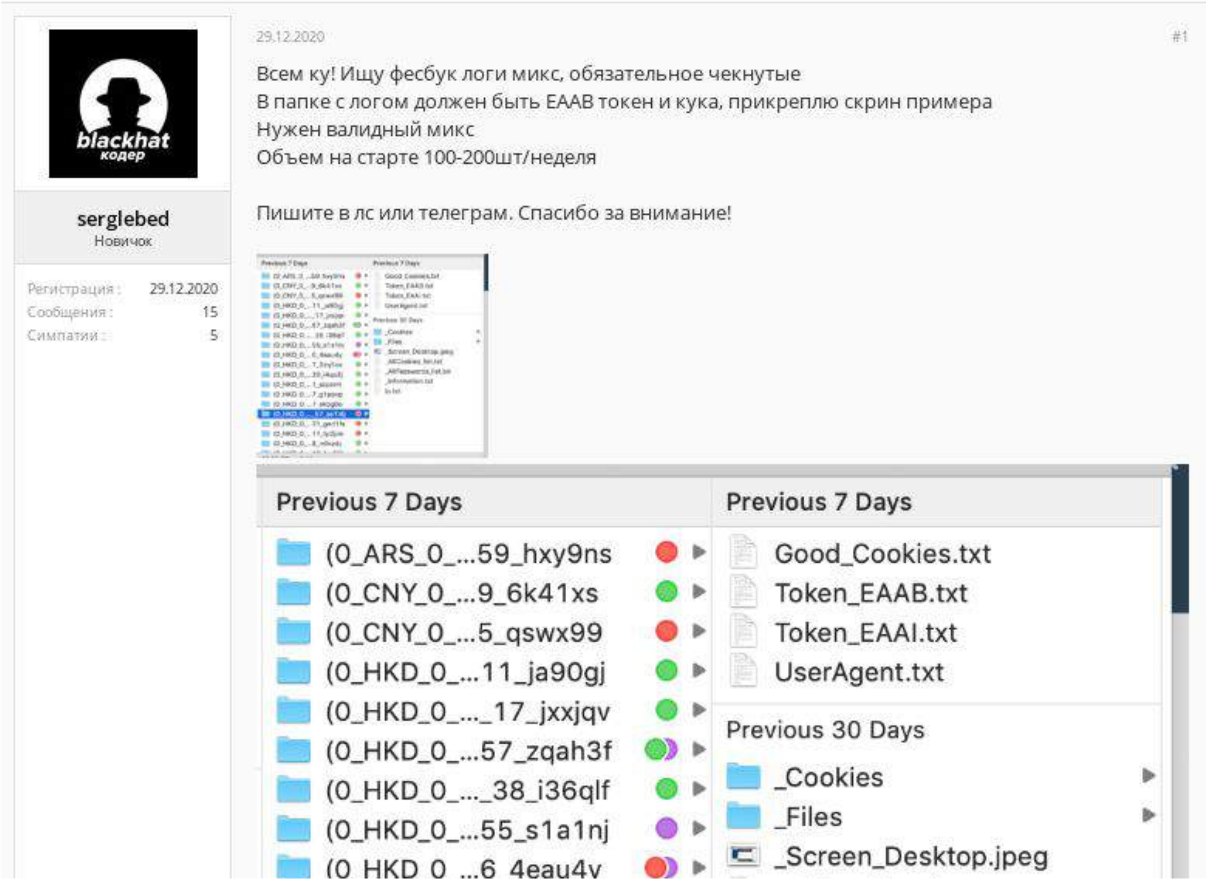
Если вы не умеете вытаскивать mail;pass из логов , то вы можете использовать StealerLogSearcher v1.3 [click here]

Мой запрос :

[redacted]

- *Имеется Brute/Checker [Работает не быстро]*
- *Плачу только за валид+CC (не важно живая CC , или нет)*
- *В приоритете ваши собственные логи , базы с облак/раздач в 95% случаев у меня уже есть*
- *Цена 0.5$ за валидный аккаунт с привязанной CC*
- *За отработку оплаты НЕТ (Отработку вижу по логу) | Если больше 80% аккаунтов в базе отработка , то СТРОКИ НЕ ОПЛАЧИВАЮТСЯ ПОЛНОСТЬЮ*
- *Перед загрузкой вашей базы в брут я нормализую её , удаляю дубликаты и сверяю со своим антипабликом*
- *Работаю со всеми в порядке очереди , если софт занят уже чьей-то базой - подождите , ваша база никуда не денется.*
- *Работа только через гаранта , либо вы кидаете вперёд. Даже если вы внук/сын/дед Путина.*
- *Могу отказаться от работы с Вами , если вы будете вести себя неадекватно , то есть грубить/торопить/попрошайничать и т.д*

Screenshot translation



blackhat кодер

serglebed
Новичок

Регистрация :	29.12.2020
Сообщения :	15
Симпатии :	5

29.12.2020 #1

Всем ку! Ищу фесбук логи микс, обязательное чекнутые
В папке с логом должен быть EAAB токен и кука, прикреплю скрин примера
Нужен валидный микс
Объем на старте 100-200шт/неделя

Пишите в лс или телеграм. Спасибо за внимание!

Previous 7 Days
(0_ARS_0_...59_hxy9ns
(0_CNY_0_...9_6k41xs
(0_CNY_0_...5_qswx99
(0_HKD_0_...11_ja90gj
(0_HKD_0_..._17_jxxjqv
(0_HKD_0_...57_zqah3f
(0_HKD_0_..._38_i36qlf
(0_HKD_0_...55_s1a1nj
(0 HKD 0 ...6 4eau4v

Previous 7 Days
Good_Cookies.txt
Token_EAAB.txt
Token_EAAI.txt
UserAgent.txt

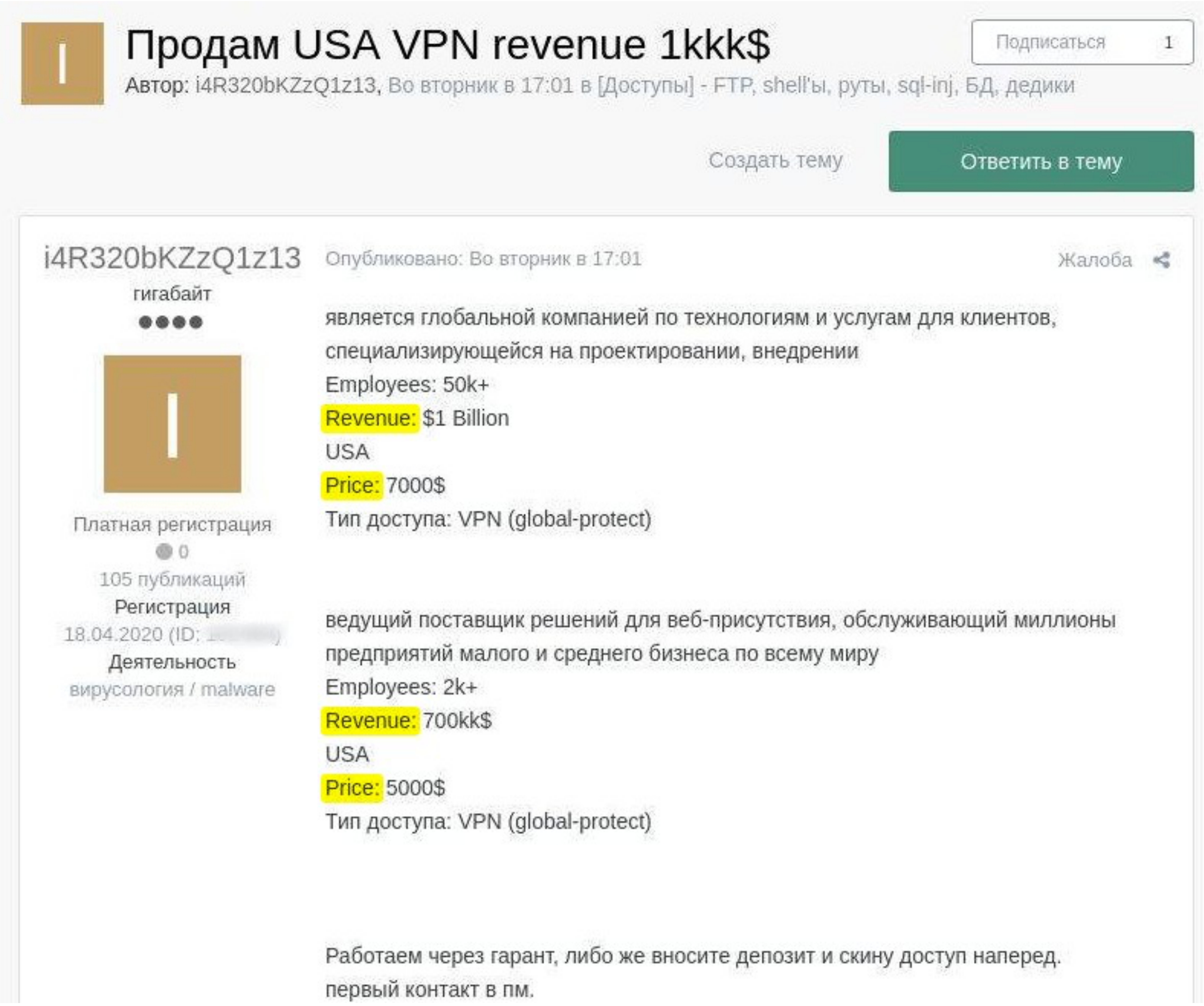
Previous 30 Days
_Cookies
_Files
_Screen_Desktop.jpeg

Screenshot translation

Topic on dark web forum with a request for specific malware logs

Main criteria for initial access valuation

Cybercriminals use a set of criteria when describing which company they sell access to on dark web forums: company size, revenue, business area, region and so forth. Yet, from analyzing a lot of posts you could conclude that corporate revenue is the main criterion: almost all posts mention revenue, whereas the region and business area of the target company are advertised much less. Some posts also refer to the level of complexity as a reason for high prices, i.e., how much time and effort the seller spent to gain access. But this is quite a subjective criterion that depends, among other things, on the cybercriminal's expertise.



Продам USA VPN revenue 1kkk$

Автор: i4R320bKZzQ1z13, Во вторник в 17:01 в [Доступы] - FTP, shell'ы, руты, sql-inj, БД, дедики

i4R320bKZzQ1z13
гигабайт

Платная регистрация
0
105 публикаций
Регистрация
18.04.2020 (ID: [redacted])
Деятельность
вирусология / malware

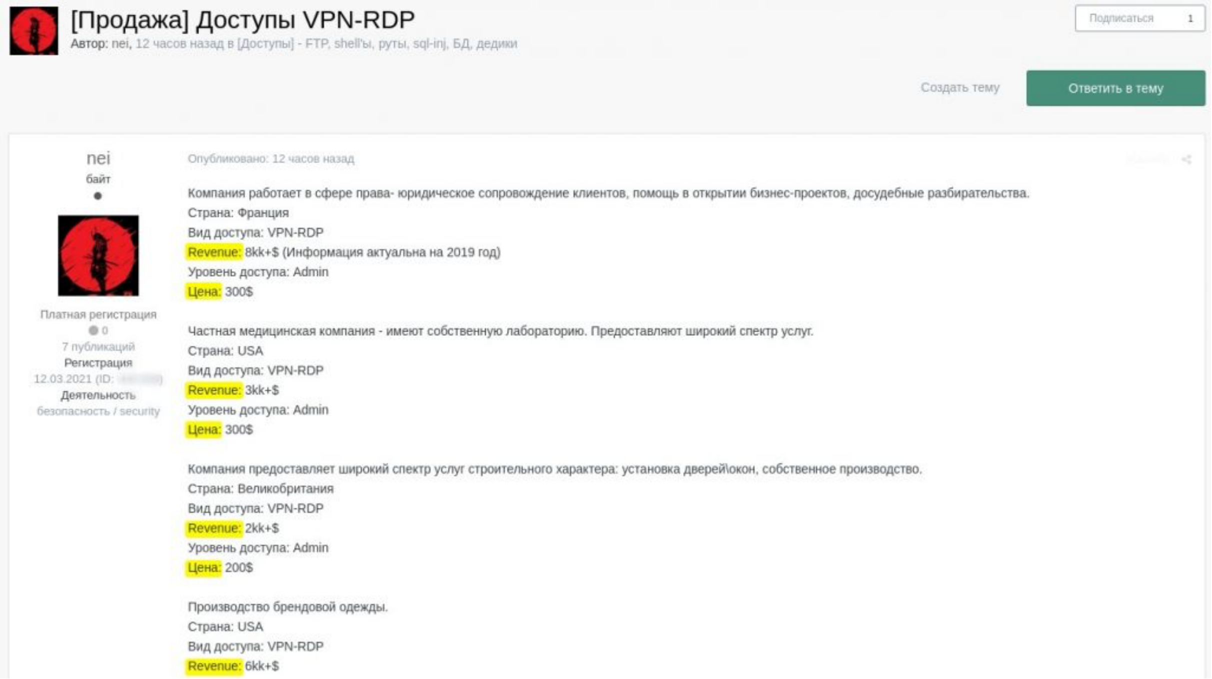
Опубликовано: Во вторник в 17:01

является глобальной компанией по технологиям и услугам для клиентов, специализирующейся на проектировании, внедрении
Employees: 50k+
Revenue: $1 Billion
USA
Price: 7000$
Тип доступа: VPN (global-protect)

ведущий поставщик решений для веб-присутствия, обслуживающий миллионы предприятий малого и среднего бизнеса по всему миру
Employees: 2k+
Revenue: 700kk$
USA
Price: 5000$
Тип доступа: VPN (global-protect)

Работаем через гарант, либо же вносите депозит и скину доступ наперед.
первый контакт в пм.

Screenshot translation



[Продажа] Доступы VPN-RDP

Автор: nei, 12 часов назад в [Доступы] - FTP, shell'ы, руты, sql-inj, БД, дедики

nei
байт
Платная регистрация
0
7 публикаций
Регистрация
12.03.2021 (ID: [redacted])
Деятельность
безопасность / security

Опубликовано: 12 часов назад

Компания работает в сфере права- юридическое сопровождение клиентов, помощь в открытии бизнес-проектов, досудебные разбирательства.
Страна: Франция
Вид доступа: VPN-RDP
Revenue: 8kk+$ (Информация актуальна на 2019 год)
Уровень доступа: Admin
Цена: 300$

Частная медицинская компания - имеют собственную лабораторию. Предоставляют широкий спектр услуг.
Страна: USA
Вид доступа: VPN-RDP
Revenue: 3kk+$
Уровень доступа: Admin
Цена: 300$

Компания предоставляет широкий спектр услуг строительного характера: установка дверей\окон, собственное производство.
Страна: Великобритания
Вид доступа: VPN-RDP
Revenue: 2kk+$
Уровень доступа: Admin
Цена: 200$

Производство брендовой одежды.
Страна: USA
Вид доступа: VPN-RDP
Revenue: 6kk+$

Screenshot translation

Announcements on a dark web forum offering VPN/RDP network access to different organizations

In addition to the target company's features, the price can also depend on the type of access offered. Information about a vulnerability (e.g., SQL injection) and legitimate credentials (e.g., RDP/SSH) will be priced very differently for companies with comparable revenues, because they offer a different probability of a successful attack. Selling an account to access remote management interfaces (RDP, SSH) means that access to a system in the corporate network infrastructure has already been gained, whereas a vulnerability merely offers the chance to achieve a similar level of access. Even when it comes to the same issue, such as an SQL injection, there are many factors affecting the potential development of the attack (vulnerable host location (e.g., corporate network or cloud server), what DBMS is used, the intended vulnerability exploitation technique, database volume, etc.) and, therefore, its cost.

Cost of initial access

To find out how these criteria influence the cost of access, we analyzed about 200 posts published on two popular dark web forums. We identified a set of relevant parameters for each one:

- Corporate revenue
- Type of access
- Price of data
- Company info (region, business area, etc.)

That done, we screened out from our selection the irrelevant posts – those not stating revenue or the price of network access data. This reduced the total number to 117 posts.

The following diagram shows the correlation between lot price and revenue without considering the technical factors:

The correlation between the price of network access data and a company's revenue (download)

As you can see:

- Most offers fall within the $0–$5,000 price range
- Most offers refer to moderately sized companies
- Average price of access data (depicted as a trend line) is between several hundred and five thousand dollars, and grows as revenue increases

Some of the major deviations from the price range can be explained by lot characteristics, such as business area specifics. For instance, network access data for a company specializing in POS terminals and providing internet acquiring services is valued much higher ($20,000) than other similar offers. The price may also be increased by "bonuses" attached to the lot, such as an already compromised database containing email addresses or other sensitive or confidential data sold in the same package along with the access. The buyer can either process these later or use and resell them separately.

If we take a closer look at the price distribution across the whole body of offers, almost half of them (42.74%) are under $1,000.

Offers grouped by price category (download)

If analyzed in terms of access type, most posts offer RDP access or a VPN + RDP bundle (75.21% of lots). In the diagram below both of these options belong to the categories "RDP access (without details)", "RDP access (local admin)", "RDP access (domain admin)" and "RDP access (user)".

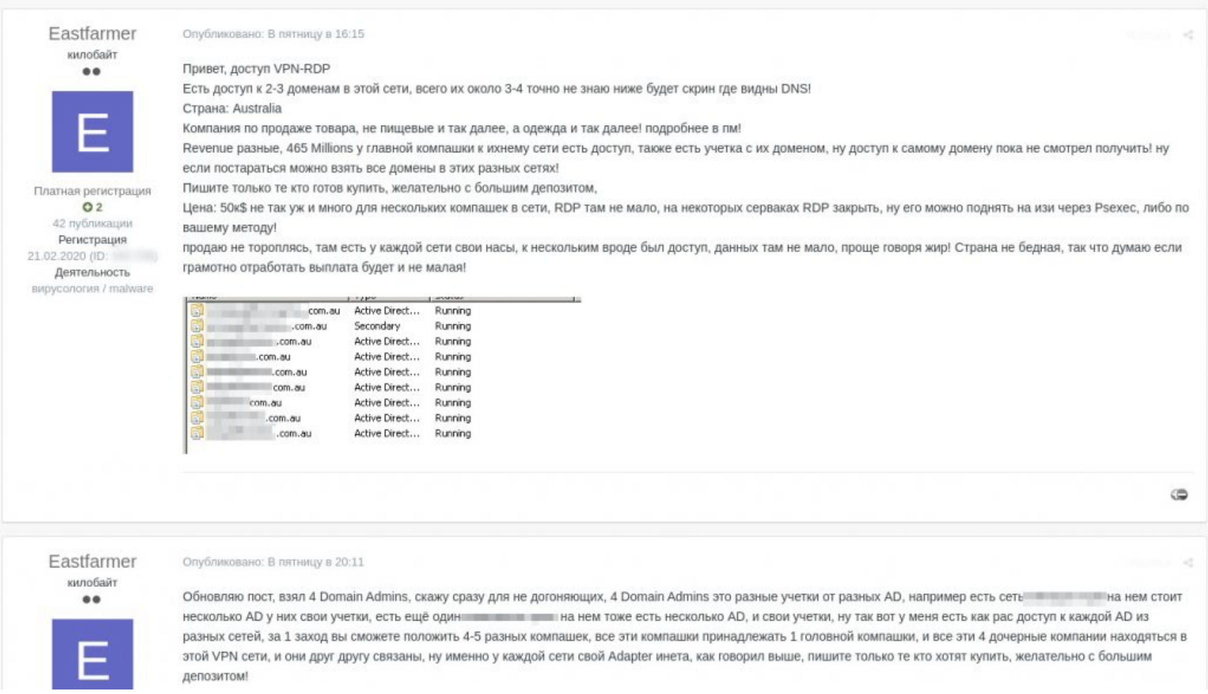
Offers grouped by access type (download)

To get a clearer picture of the connection between lot price and corporate revenue, we analyzed the posts offering data for RDP access – the most common access category and most uniform pricewise – for large businesses with revenue of over $500 million. The following diagram shows how revenue affects the cost of data for RDP access.

The correlation between RDP access cost and large company revenue (download)

This diagram doesn't demonstrate a direct correlation between access cost and corporate income. However, the selection is quite small, meaning the disproportionate influence of variable access properties (user privileges, a company's country/region/industry) could skew any remotely objective conclusions based on quantitative analysis.

One way or another, access to large business infrastructure usually costs between $2,000 and $4,000, which are relatively modest prices. But there is no upper limit to the cost either. For example, in the topic below the original lot price was $50,000 (the lot also covered a number of sub-companies). And even though the price was later halved by the seller, one of the thread members called the offer overpriced.



Eastfarmer
килобайт
●●
Платная регистрация
2
42 публикации
Регистрация
21.02.2020 (ID: [redacted])
Деятельность
вирусология / malware

Опубликовано: В пятницу в 16:15

Привет, доступ VPN-RDP
Есть доступ к 2-3 доменам в этой сети, всего их около 3-4 точно не знаю ниже будет скрин где видны DNS!
Страна: Australia
Компания по продаже товара, не пищевые и так далее, а одежда и так далее! подробнее в пм!
Revenue разные, 465 Millions у главной компашки к ихнему сети есть доступ, также есть учетка с их доменом, ну доступ к самому домену пока не смотрел получить! ну если постараться можно взять все домены в этих разных сетях!
Пишите только те кто готов купить, желательно с большим депозитом,
Цена: 50к$ не так уж и много для нескольких компашек в сети, RDP там не мало, на некоторых серваках RDP закрыть, ну его можно поднять на изи через Psexec, либо по вашему методу!
продаю не тороплясь, там есть у каждой сети свои насы, к нескольким вроде был доступ, данных там не мало, проще говоря жир! Страна не бедная, так что думаю если грамотно отработать выплата будет и не малая!

[redacted] com.au	Active Direct...	Running
[redacted].com.au	Secondary	Running
[redacted].com.au	Active Direct...	Running
[redacted].com.au	Active Direct...	Running
[redacted].com.au	Active Direct...	Running
[redacted] com.au	Active Direct...	Running
[redacted] com.au	Active Direct...	Running
[redacted].com.au	Active Direct...	Running
[redacted].com.au	Active Direct...	Running

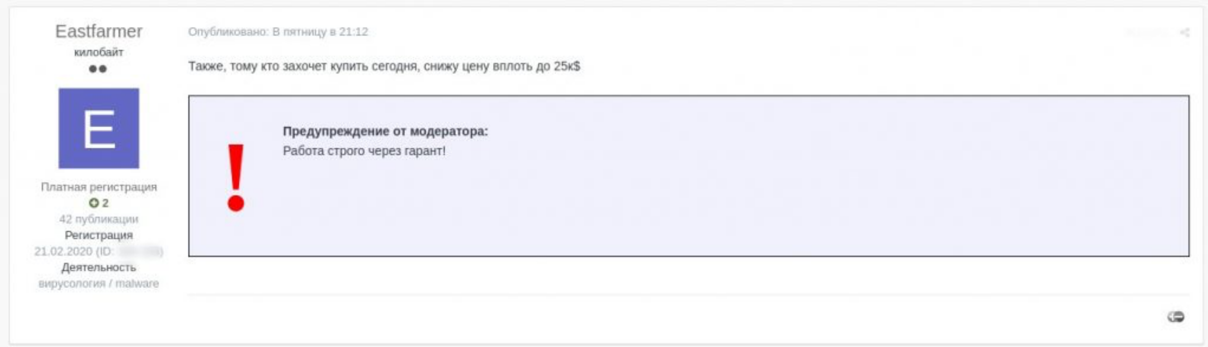
Eastfarmer
килобайт
●●

Опубликовано: В пятницу в 20:11

Обновляю пост, взял 4 Domain Admins, скажу сразу для не догоняющих, 4 Domain Admins это разные учетки от разных AD, например есть сеть [redacted] на нем стоит несколько AD у них свои учетки, есть ещё один [redacted] на нем тоже есть несколько AD, и свои учетки, ну так вот у меня есть как рас доступ к каждой AD из разных сетей, за 1 заход вы сможете положить 4-5 разных компашек, все эти компашки принадлежать 1 головной компашки, и все эти 4 дочерные компании находяться в этой VPN сети, и они друг другу связаны, ну именно у каждой сети свой Adapter инета, как говорил выше, пишите только те кто хотят купить, желательно с большим депозитом!

Screenshot translation

Sale of data for remote access to five companies in one network for $50,000



Eastfarmer
килобайт
●●
Платная регистрация
2
42 публикации
Регистрация
21.02.2020 (ID: [redacted])
Деятельность
вирусология / malware

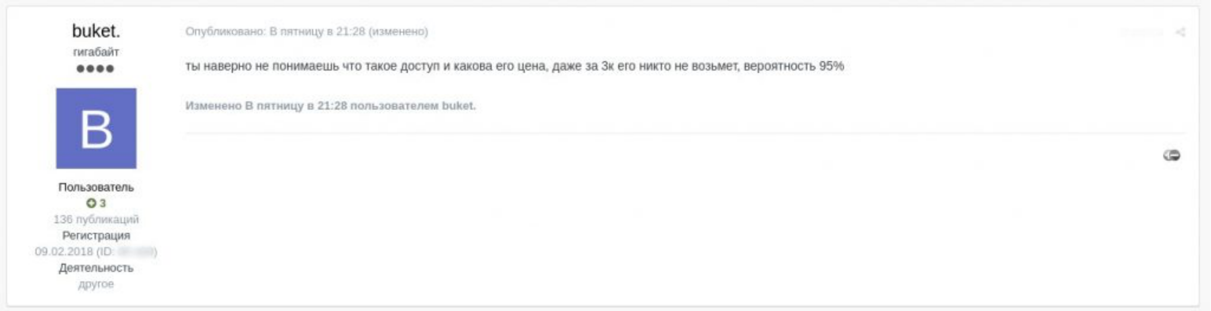
Опубликовано: В пятницу в 21:12

Также, тому кто захочет купить сегодня, снижу цену вплоть до 25к$

Предупреждение от модератора:
Работа строго через гарант!

Screenshot translation

Price reduced from $50,000 to $25,000



buket.
гигабайт
●●●●
B
Пользователь
3
136 публикаций
Регистрация
09.02.2018 (ID: [redacted])
Деятельность
другое

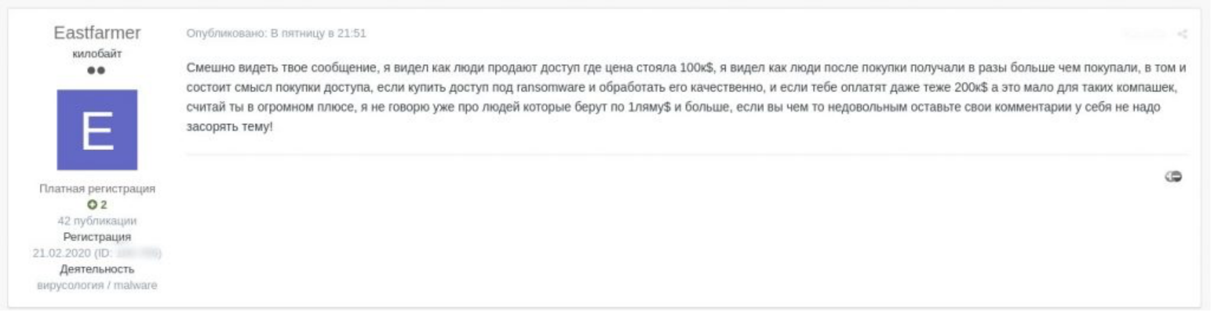
Опубликовано: В пятницу в 21:28 (изменено)

ты наверно не понимаешь что такое доступ и какова его цена, даже за 3к его никто не возьмет, вероятность 95%

Изменено В пятницу в 21:28 пользователем buket.

Screenshot translation

Comment about the offer being overpriced



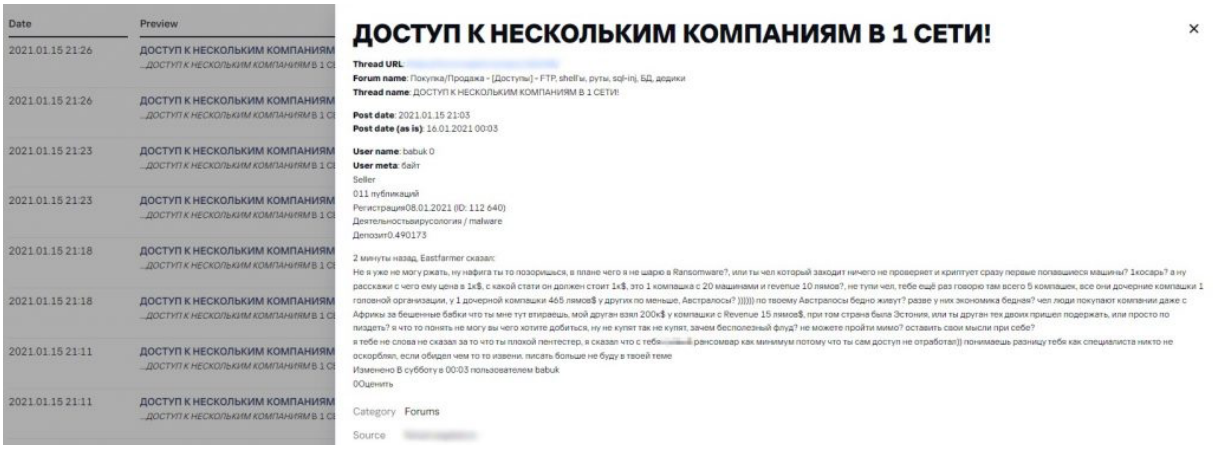
Eastfarmer
килобайт
●●
E
Платная регистрация
2
42 публикации
Регистрация
21.02.2020 (ID: [redacted])
Деятельность
вирусология / malware

Опубликовано: В пятницу в 21:51

Смешно видеть твое сообщение, я видел как люди продают доступ где цена стояла 100к$, я видел как люди после покупки получали в разы больше чем покупали, в том и состоит смысл покупки доступа, если купить доступ под ransomware и обработать его качественно, и если тебе оплатят даже теже 200к$ а это мало для таких компашек, считай ты в огромном плюсе, я не говорю уже про людей которые берут по 1ляму$ и больше, если вы чем то недовольным оставьте свои комментарии у себя не надо засорять тему!

Screenshot translation

Response to comment about the offer being overpriced



Date	Preview
2021.01.15 21:26	ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ ...ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ В 1 С
2021.01.15 21:26	ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ ...ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ В 1 С
2021.01.15 21:23	ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ ...ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ В 1 С
2021.01.15 21:23	ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ ...ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ В 1 С
2021.01.15 21:18	ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ ...ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ В 1 С
2021.01.15 21:18	ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ ...ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ В 1 С
2021.01.15 21:11	ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ ...ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ В 1 С
2021.01.15 21:11	ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ ...ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ В 1 С

ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ В 1 СЕТИ!

×

Thread URL: [redacted]
Forum name: Покупка/Продажа - [Доступы] - FTP, shell'ы, руты, sql-inj, БД, дедики
Thread name: ДОСТУП К НЕСКОЛЬКИМ КОМПАНИЯМ В 1 СЕТИ!

Post date: 2021.01.15 21:03
Post date (as is): 16.01.2021 00:03

User name: babuk 0
User meta: байт
Seller
011 публикаций
Регистрация08.01.2021 (ID: 112 640)
Деятельностьвирусология / malware
Депозит0.490173

2 минуты назад, Eastfarmer сказал:
Не я уже не могу ржать, ну нафига ты то позоришься, в плане чего я не шарю в Ransomware?, или ты чел который заходит ничего не проверяет и криптует сразу первые попавшиеся машины? 1косарь? а ну расскажи с чего ему цена в 1к$, с какой стати он должен стоит 1к$, это 1 компашка с 20 машинами и revenue 10 лямов?, не тупи чел, тебе ещё раз говорю там всего 5 компашек, все они дочерние компашки 1 головной организации, у 1 дочерной компашки 465 лямов$ у других по меньше, Австралосы?)))))) по твоему Австралосы бедно живут? разве у них экономика бедная? чел люди покупают компании даже с Африки за бешенные бабки что ты мне тут втираешь, мой друган взял 200к$ у компашки с Revenue 15 лямов$, при том страна была Эстония, или ты друган тех двоих пришел подержать, или просто по пиздеть? я что то понять не могу вы чего хотите добиться, ну не купят так не купят, зачем бесполезный флуд? не можете пройти мимо? оставить свои мысли при себе?
я тебе не слова не сказал за то что ты плохой пентестер, я сказал что с тебя[redacted] рансомвар как минимум потому что ты сам доступ не отработал)) понимаешь разницу тебя как специалиста никто не оскорблял, если обидел чем то то извени. писать больше не буду в твоей теме
Изменено В субботу в 00:03 пользователем babuk
0Оценить

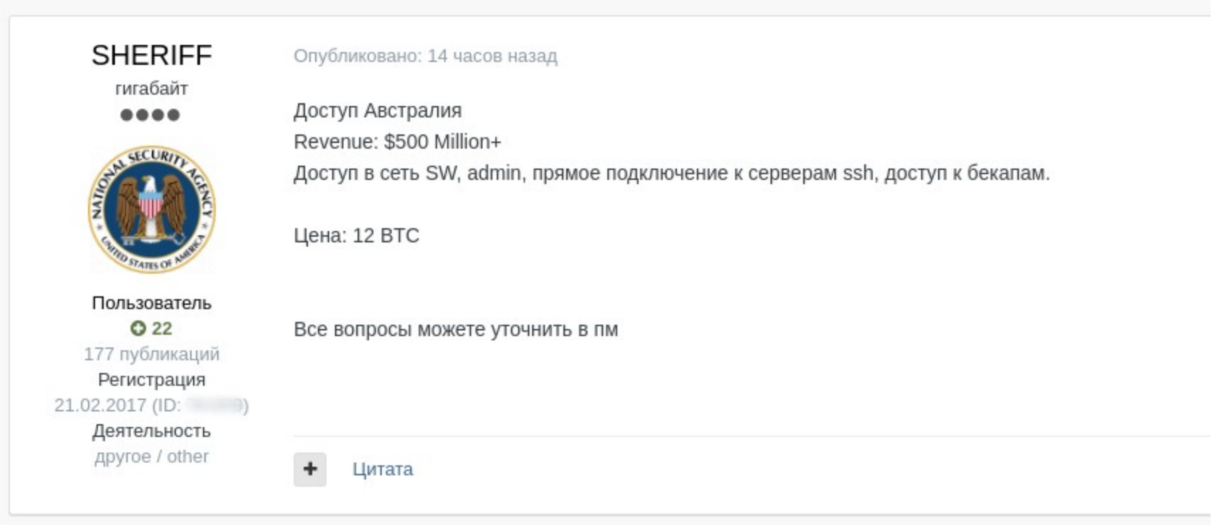
Category Forums

Source [redacted]

Screenshot translation

Discussion continuation. Source: Digital Footprint Intelligence service

Here is another example of a high price being asked for data belonging to a company with a revenue of $500 million. The asking price is 12 BTC.



SHERIFF
гигабайт
●●●●

Пользователь
22
177 публикаций
Регистрация
21.02.2017 (ID: [redacted])
Деятельность
другое / other

Опубликовано: 14 часов назад

Доступ Австралия
Revenue: $500 Million+
Доступ в сеть SW, admin, прямое подключение к серверам ssh, доступ к бекапам.

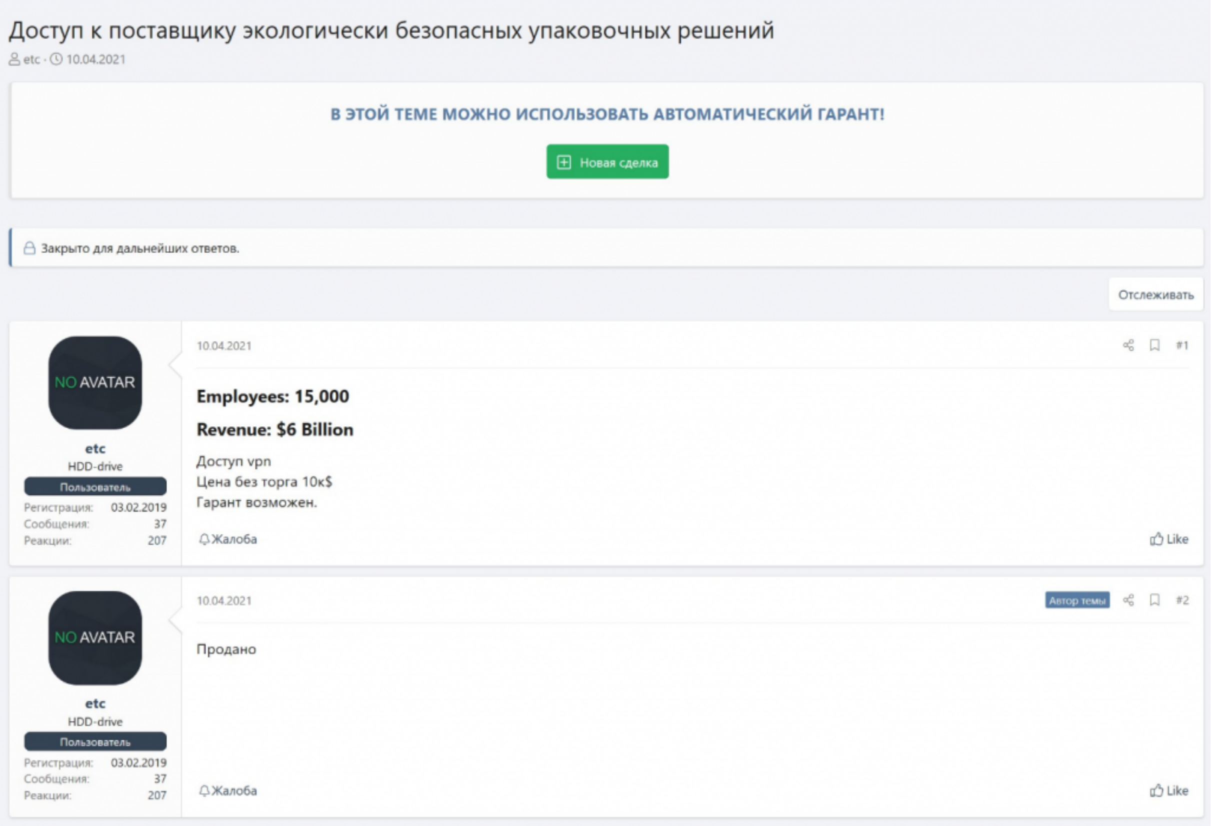
Цена: 12 BTC

Все вопросы можете уточнить в пм

Screenshot translation

Lot price 12 BTC

Interestingly, gaining access to corporate networks is in high demand, with some lots selling the same day they are published.



Доступ к поставщику экологически безопасных упаковочных решений
etc · 10.04.2021

В ЭТОЙ ТЕМЕ МОЖНО ИСПОЛЬЗОВАТЬ АВТОМАТИЧЕСКИЙ ГАРАНТ!

Закрыто для дальнейших ответов.

etc
HDD-drive
Пользователь
Регистрация: 03.02.2019
Сообщения: 37
Реакции: 207

10.04.2021 #1

Employees: 15,000

Revenue: $6 Billion

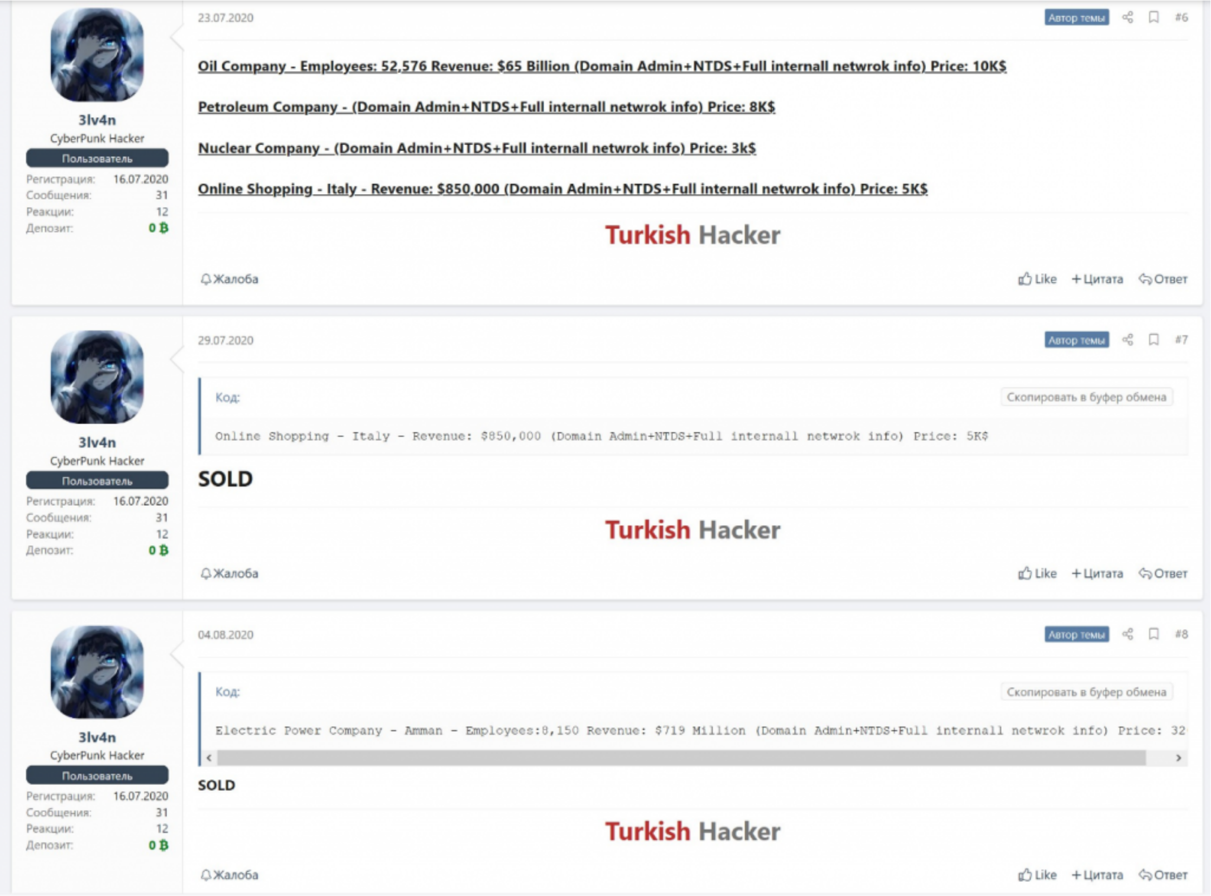
Доступ vpn
Цена без торга 10к$
Гарант возможен.

etc
HDD-drive
Пользователь
Регистрация: 03.02.2019
Сообщения: 37
Реакции: 207

10.04.2021 Автор темы #2

Продано

Access data sold on the day of publication



3lv4n
CyberPunk Hacker
Пользователь
Регистрация: 16.07.2020
Сообщения: 31
Реакции: 12
Депозит: 0 ฿

23.07.2020 #6

Oil Company - Employees: 52,576 Revenue: $65 Billion (Domain Admin+NTDS+Full internall netwrok info) Price: 10K$

Petroleum Company - (Domain Admin+NTDS+Full internall netwrok info) Price: 8K$

Nuclear Company - (Domain Admin+NTDS+Full internall netwrok info) Price: 3k$

Online Shopping - Italy - Revenue: $850,000 (Domain Admin+NTDS+Full internall netwrok info) Price: 5K$

Turkish Hacker

3lv4n
CyberPunk Hacker
Пользователь
Регистрация: 16.07.2020
Сообщения: 31
Реакции: 12
Депозит: 0 ฿

29.07.2020 #7

Код:

```
Online Shopping - Italy - Revenue: $850,000 (Domain Admin+NTDS+Full internall netwrok info) Price: 5K$
```

SOLD

Turkish Hacker

3lv4n
CyberPunk Hacker
Пользователь
Регистрация: 16.07.2020
Сообщения: 31
Реакции: 12
Депозит: 0 ฿

04.08.2020 #8

Код:

```
Electric Power Company - Amman - Employees:8,150 Revenue: $719 Million (Domain Admin+NTDS+Full internall netwrok info) Price: 32
```

SOLD

Turkish Hacker

Access data sold a few days after publication

Ransomware auctions: stolen data pricing

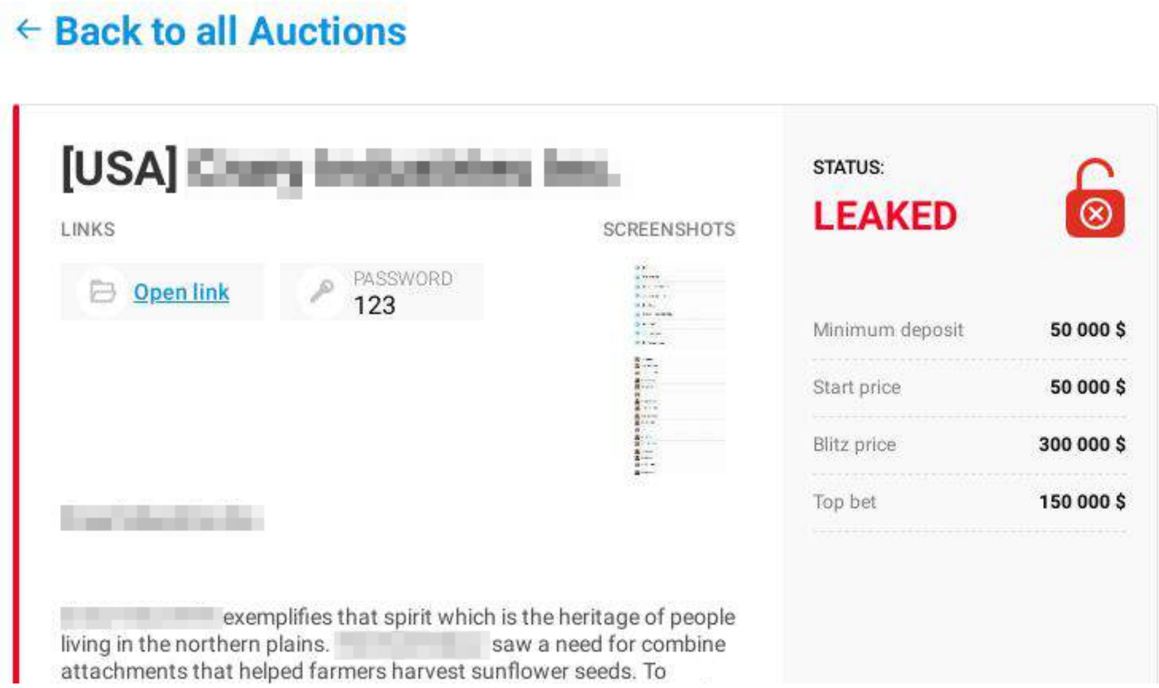
Undoubtedly, one of the most important components of the initial access price is the amount of money the buyer can potentially earn from an attack conducted using that access. Cybercriminals are ready to pay thousands or even tens of thousands of dollars for the opportunity to infiltrate a corporate network for a reason. Successful attacks pay off very nicely. Ransomware attacks are a prime example. In attacks like that malware usually encrypts a significant amount of data on workstations or servers, virtually paralyzing the company's operations or causing material risks to its business processes. Once encryption is accomplished, the attackers contact the victim with an offer to buy decryption keys. These often cost millions of dollars. For example, according to media reports, a European travel agency dished out $4.5 million, and a large American insurer a whopping $40 million in ransom money.

Of late, cybercriminals have tended not only to encrypt but also steal corporate data. They may later post some of the stolen data in their blogs – primarily as proof but also as extra leverage –threatening to publish more unless the company pays them the money they demand within the stipulated timeframe.

Different ransomware groups follow different approaches to publishing stolen data.

- Some of them publish information about the incident (along with the data) only if no agreement is reached with the victim.
- Some publicize the incident immediately after the attack and state exactly when they plan to begin disclosing critical data.
- Some set up an auction in which the stolen data will go to whoever is willing to pay the highest price (presumably a single buyer). In this latter case, the auction price of a lot – though smaller than the ransom charged for data decryption – can still be several times more than the price of access to the corporate system.

If we take a look at posts offering stolen data to a single buyer, the lot price normally starts in the tens of thousands of dollars, often reaching sums of around a million.



← Back to all Auctions

[USA] [redacted]

LINKS

SCREENSHOTS

Open link

PASSWORD
123

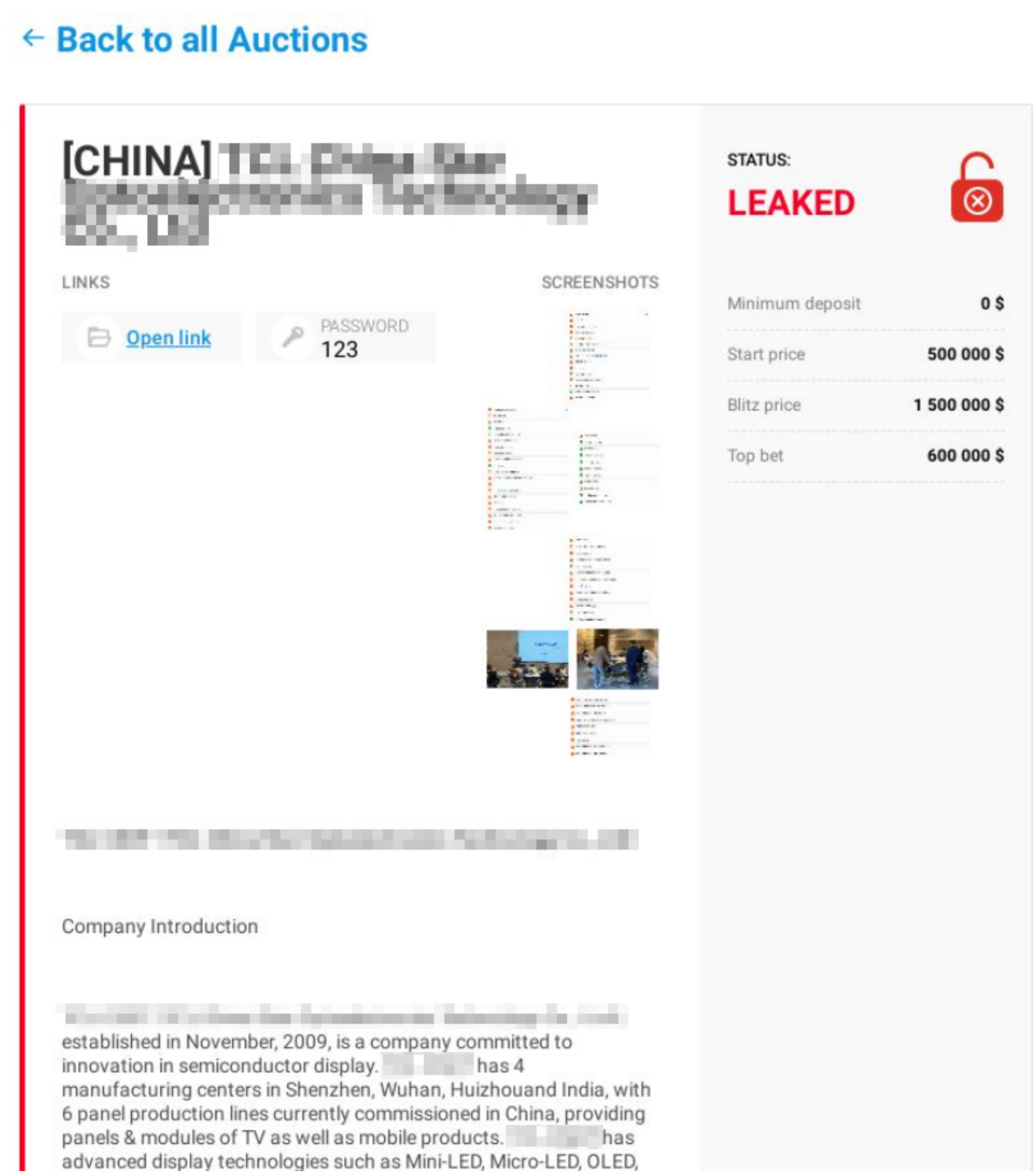
[redacted]

[redacted] exemplifies that spirit which is the heritage of people living in the northern plains. [redacted] saw a need for combine attachments that helped farmers harvest sunflower seeds. To

STATUS:
LEAKED

Minimum deposit	50 000 $
Start price	50 000 $
Blitz price	300 000 $
Top bet	150 000 $

Blackmailer blog: auction price of stolen data



[CHINA] [redacted]

LINKS

SCREENSHOTS

PASSWORD
123

STATUS:
LEAKED

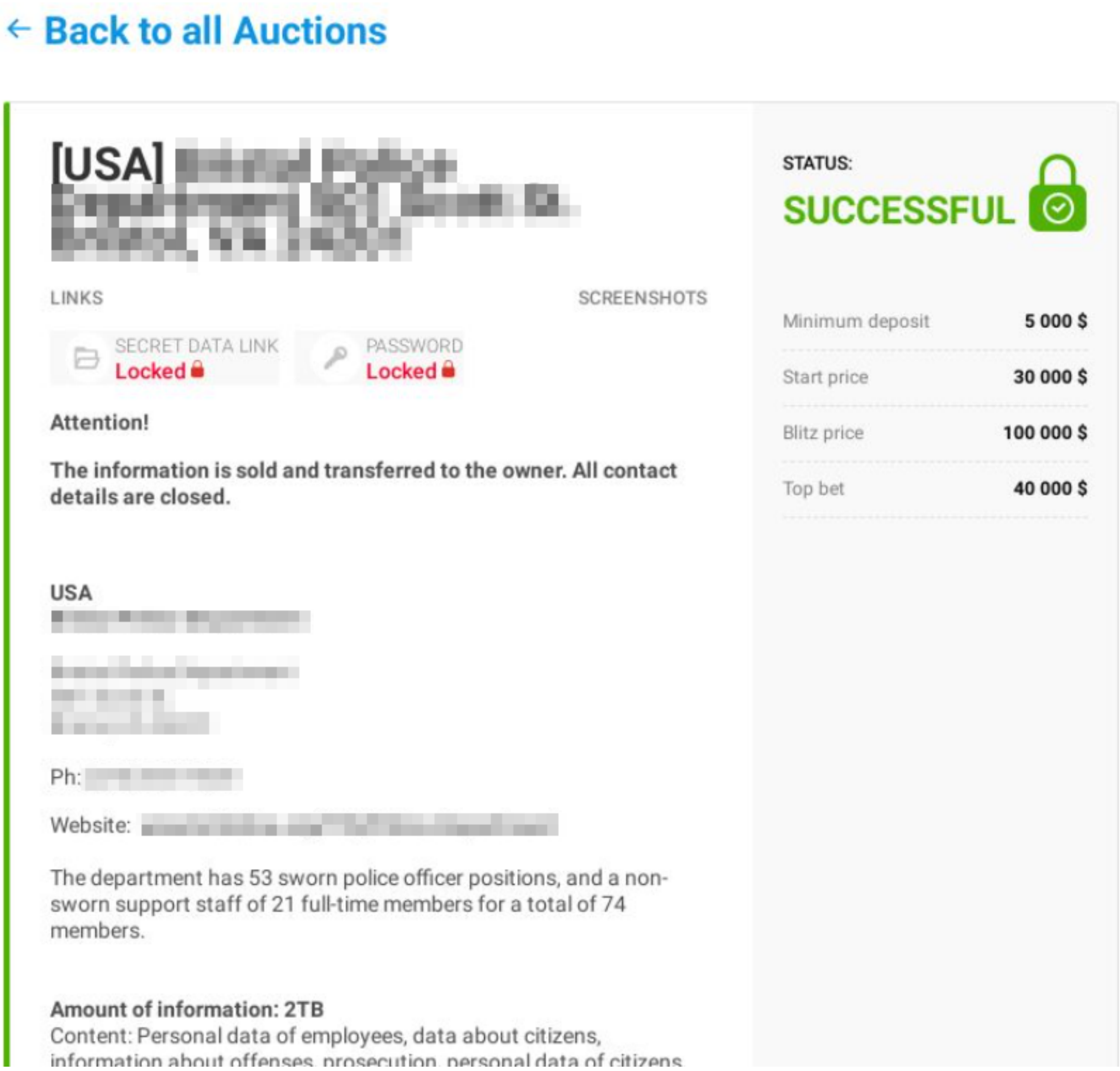
Minimum deposit	0 $
Start price	500 000 $
Blitz price	1 500 000 $
Top bet	600 000 $

[redacted]

Company Introduction

[redacted] established in November, 2009, is a company committed to innovation in semiconductor display. [redacted] has 4 manufacturing centers in Shenzhen, Wuhan, Huizhouand India, with 6 panel production lines currently commissioned in China, providing panels & modules of TV as well as mobile products. [redacted] has advanced display technologies such as Mini-LED, Micro-LED, OLED,

Blackmailer blog: auction price of stolen data along with published data



← Back to all Auctions

[USA] [redacted]

LINKS

SCREENSHOTS

SECRET DATA LINK
Locked 🔒

PASSWORD
Locked 🔒

Attention!

The information is sold and transferred to the owner. All contact details are closed.

USA
[redacted]

[redacted]

Ph: [redacted]

Website: [redacted]

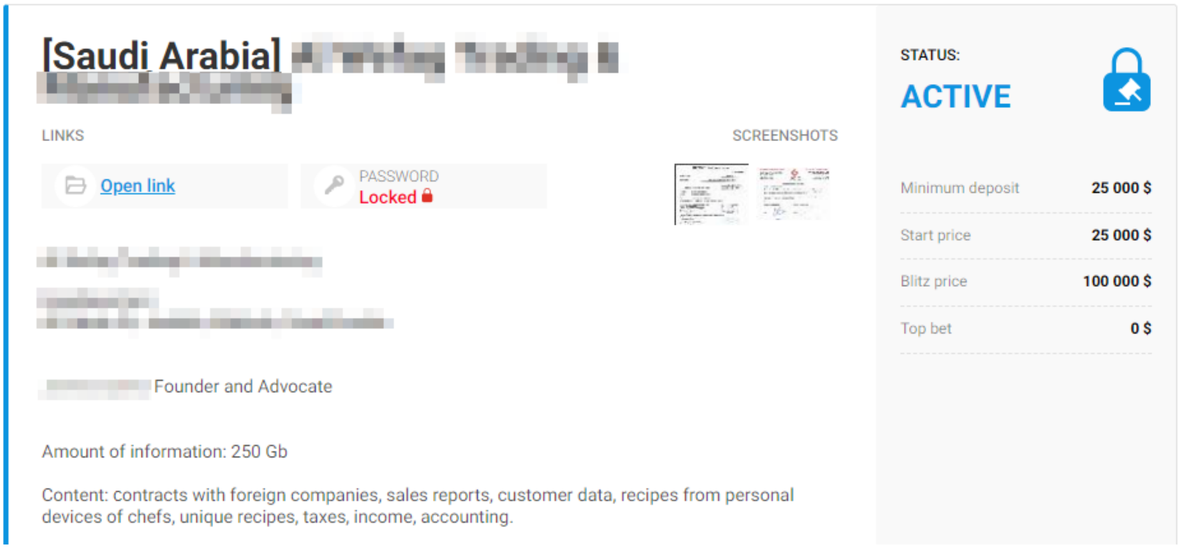
The department has 53 sworn police officer positions, and a non-sworn support staff of 21 full-time members for a total of 74 members.

Amount of information: 2TB
Content: Personal data of employees, data about citizens, information about offenses, prosecution, personal data of citizens

STATUS:
SUCCESSFUL

Minimum deposit	5 000 $
Start price	30 000 $
Blitz price	100 000 $
Top bet	40 000 $

Blackmailer blog: auction closed (stolen data sold to a single buyer)



[Saudi Arabia] [redacted]

LINKS

SCREENSHOTS

Open link

PASSWORD
Locked 🔒

[redacted]

[redacted]

[redacted] Founder and Advocate

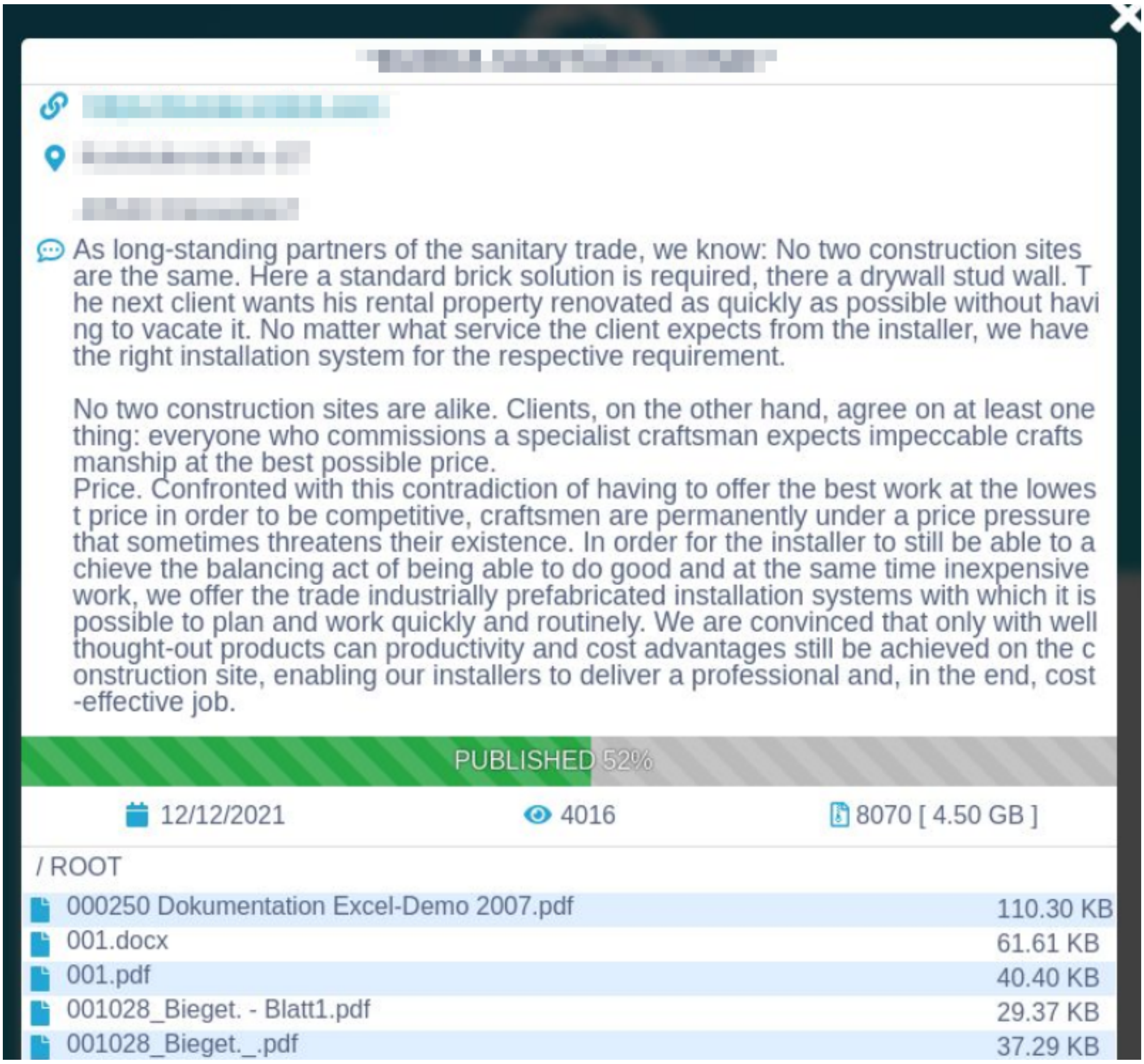
Amount of information: 250 Gb

Content: contracts with foreign companies, sales reports, customer data, recipes from personal devices of chefs, unique recipes, taxes, income, accounting.

STATUS:
ACTIVE

Minimum deposit	25 000 $
Start price	25 000 $
Blitz price	100 000 $
Top bet	0 $

Blackmailer blog: active auction



[redacted]

[redacted]

[redacted]

[redacted]

As long-standing partners of the sanitary trade, we know: No two construction sites are the same. Here a standard brick solution is required, there a drywall stud wall. The next client wants his rental property renovated as quickly as possible without having to vacate it. No matter what service the client expects from the installer, we have the right installation system for the respective requirement.

No two construction sites are alike. Clients, on the other hand, agree on at least one thing: everyone who commissions a specialist craftsman expects impeccable craftsmanship at the best possible price.
Price. Confronted with this contradiction of having to offer the best work at the lowest price in order to be competitive, craftsmen are permanently under a price pressure that sometimes threatens their existence. In order for the installer to still be able to achieve the balancing act of being able to do good and at the same time inexpensive work, we offer the trade industrially prefabricated installation systems with which it is possible to plan and work quickly and routinely. We are convinced that only with well thought-out products can productivity and cost advantages still be achieved on the construction site, enabling our installers to deliver a professional and, in the end, cost-effective job.

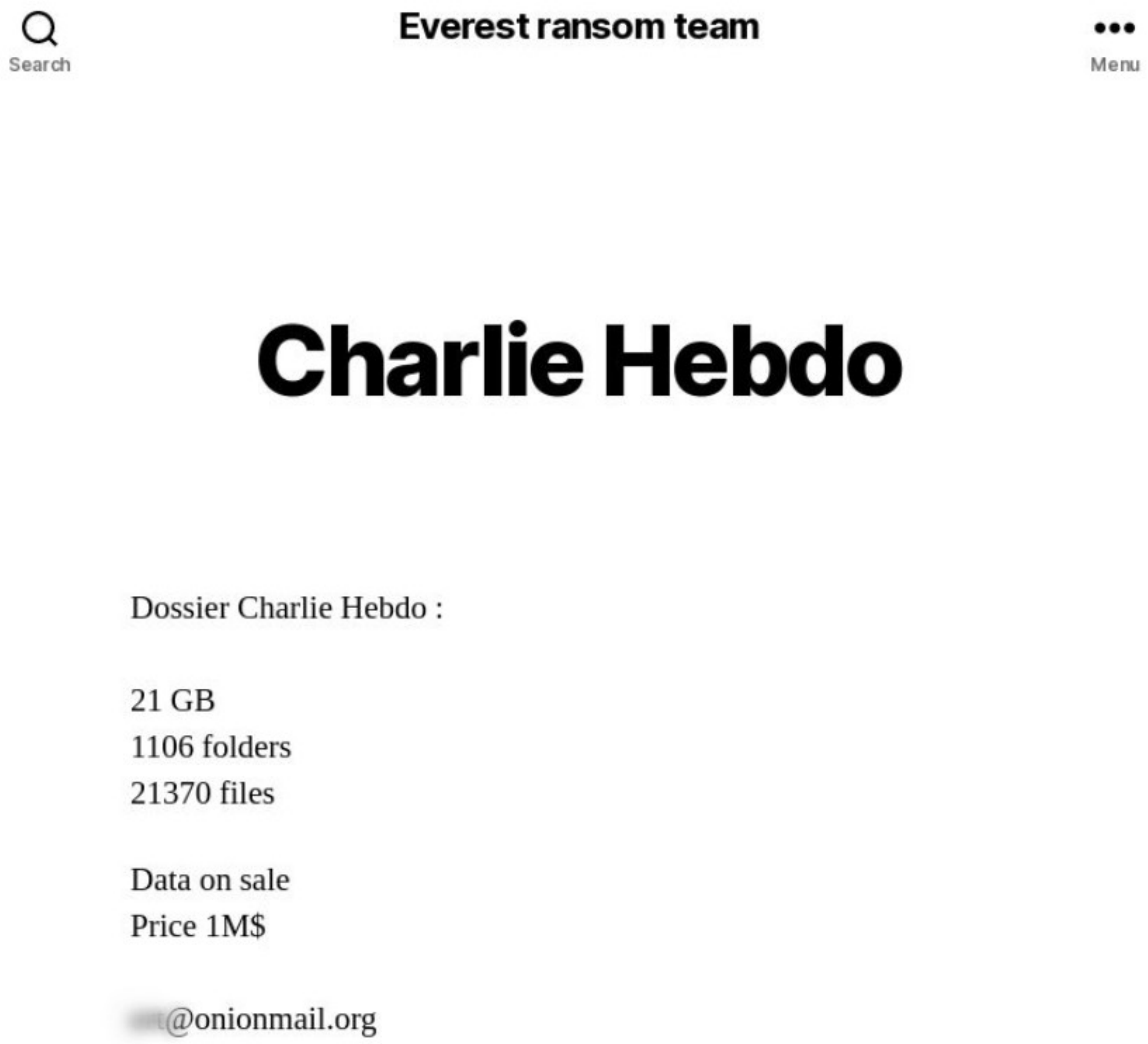
PUBLISHED 52%

12/12/2021 | 4016 | 8070 [4.50 GB]

/ ROOT

000250 Dokumentation Excel-Demo 2007.pdf	110.30 KB
001.docx	61.61 KB
001.pdf	40.40 KB
001028_Bieget. - Blatt1.pdf	29.37 KB
001028_Bieget._.pdf	37.29 KB

Blackmailer blog: stolen data published in parts (one part at a time)



Everest ransom team

Charlie Hebdo

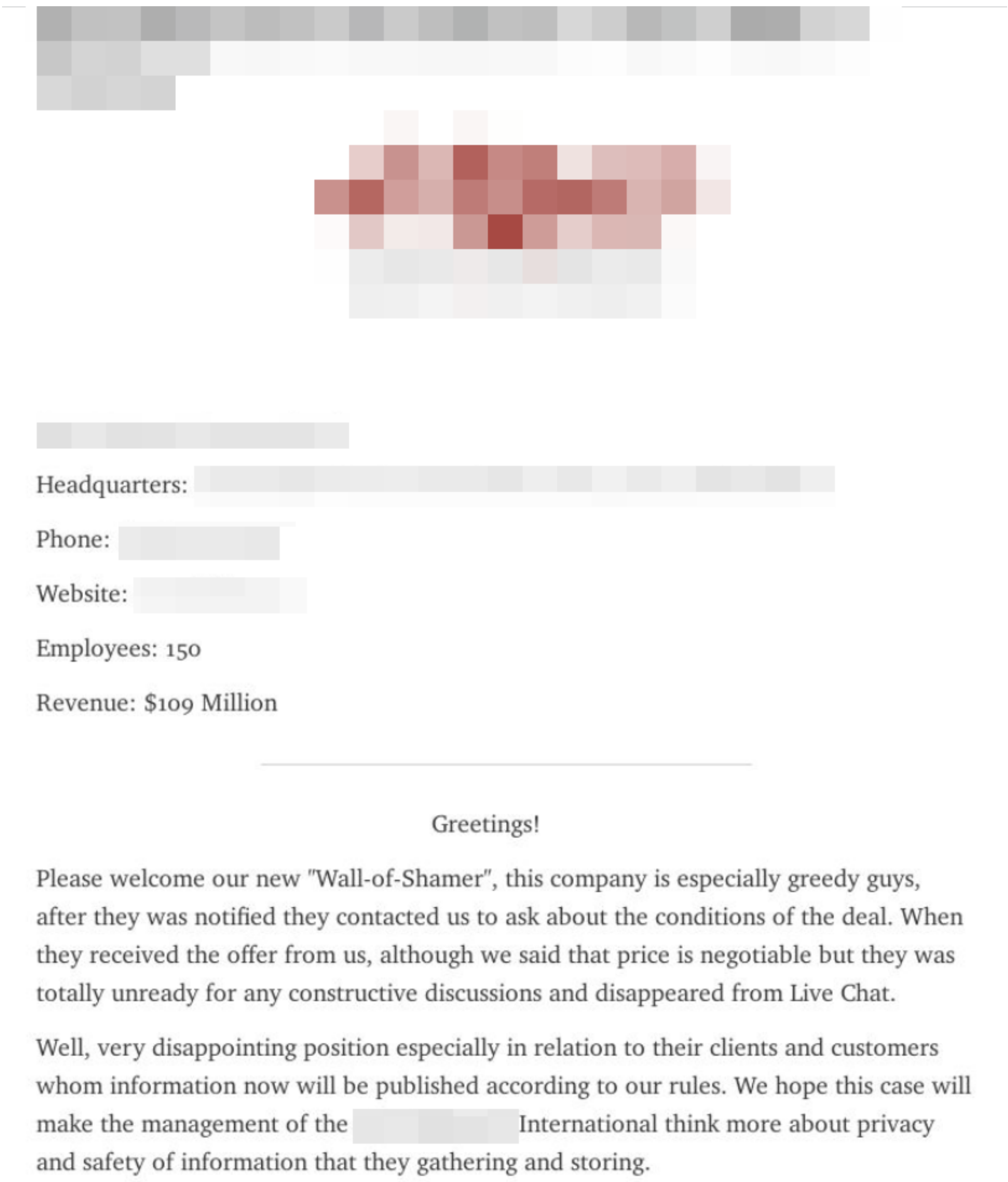
Dossier Charlie Hebdo :

21 GB
1106 folders
21370 files

Data on sale
Price 1M$

[redacted]@onionmail.org

Blackmailer blog: data on Charlie Hebdo terrorist attack stolen from a legal firm are available for $1 million



[redacted]

[redacted]

[redacted]

Headquarters: [redacted]

Phone: [redacted]

Website: [redacted]

Employees: 150

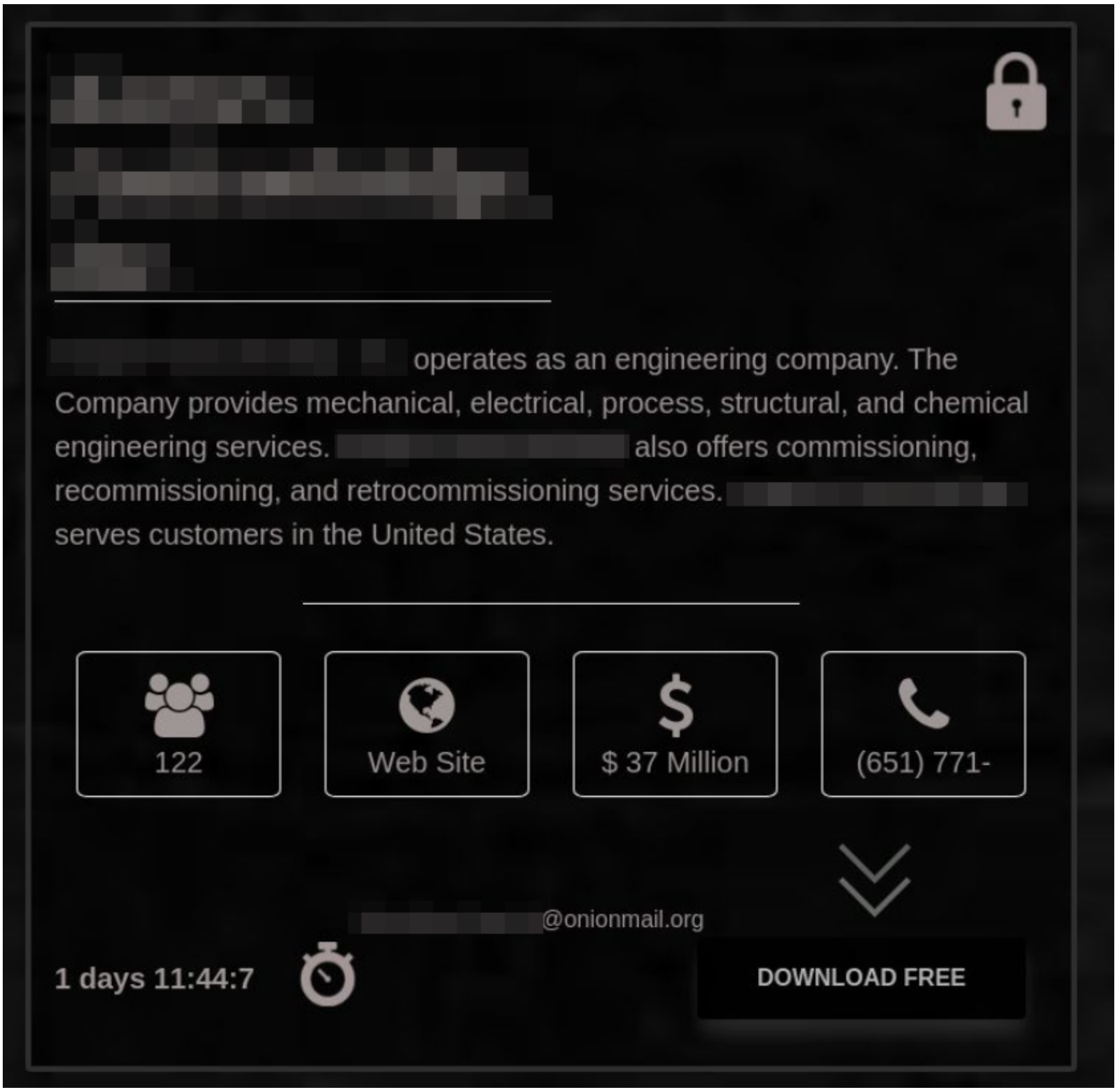
Revenue: $109 Million

Greetings!

Please welcome our new "Wall-of-Shamer", this company is especially greedy guys, after they was notified they contacted us to ask about the conditions of the deal. When they received the offer from us, although we said that price is negotiable but they was totally unready for any constructive discussions and disappeared from Live Chat.

Well, very disappointing position especially in relation to their clients and customers whom information now will be published according to our rules. We hope this case will make the management of the [redacted] International think more about privacy and safety of information that they gathering and storing.

Blackmailer blog: attackers announce the publication of stolen data after they failed to negotiate with the victim company



[redacted]

[redacted] operates as an engineering company. The Company provides mechanical, electrical, process, structural, and chemical engineering services. [redacted] also offers commissioning, recommissioning, and retrocommissioning services. [redacted] serves customers in the United States.

122

Web Site

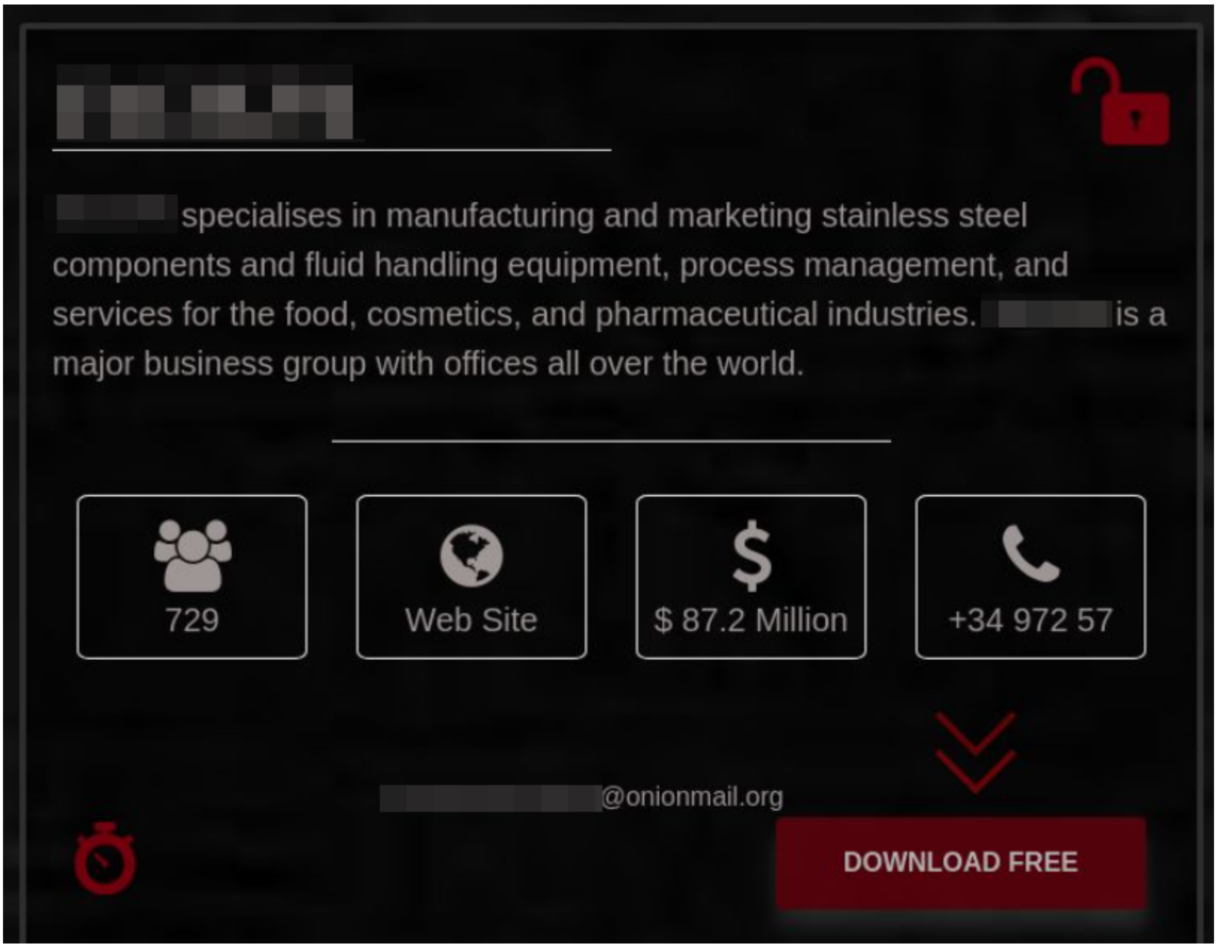
$ 37 Million

(651) 771-

[redacted]@onionmail.org

1 days 11:44:7

Blackmailer blog: attackers announce they are waiting for the ransom (1 day and 11 hours left before the publication of stolen data)



[redacted]

[redacted] specialises in manufacturing and marketing stainless steel components and fluid handling equipment, process management, and services for the food, cosmetics, and pharmaceutical industries. [redacted] is a major business group with offices all over the world.

[redacted]@onionmail.org

Blackmailer blog: the attackers published the stolen data because the ransom was not paid

Conclusion

Demand for corporate data on the black market is high, and it doesn’t always involve targeted attacks. Attackers may gain access to the infrastructure of a random company to sell it to blackmailers or other advanced cybercriminals later. An attack like that can affect a company of any size, big or small, because corporate system access is often priced moderately on underground forums, especially compared to the potential damage to a business.

Sellers on the dark web most often offer remote access via RDP. To protect corporate infrastructure from attacks through remote access and control services, make sure the connection via this protocol is secure by:

- providing access to services (for example, RDP) only through a VPN,
- using strong passwords and Network Level Authentication (NLA),
- using two-factor authentication for all services,
- monitoring for leaks of access data. Dark web monitoring is available on Kaspersky Threat Intelligence Portal[1].

[1] For details of the service and test access, please contact us at intelligence@kaspersky.com