Ransomware world in 2021: who, how and why

securelist.com/ransomware-world-in-2021/102169/

Authors

- Dmitry Galov
- Expert Leonid Bezvershenko
- Ivan Kwiatkowski

As the world marks the second Anti-Ransomware Day, there's no way to deny it: ransomware has become *the* buzzword in the security community. And not without good reason. The threat may have been around a long time, but it's changed. Year after year, the attackers have grown bolder, methodologies have been refined and, of course, systems have been breached. Yet, much of the media attention ransomware gets is focused on chronicling which companies fall prey to it. In this report, we take a step back from the day-to-day ransomware news cycle and follow the ripples back into the heart of the ecosystem to understand how it is organized.

First, we will debunk three preconceived ideas that obstruct proper thinking on the ransomware threat. Next, we dive deep into the darknet to demonstrate how cybercriminals interact with each other and the types of services they provide. And finally, we conclude with a look at two high-profile ransomware brands: REvil and Babuk.

No matter how much work we put into writing this report, before you start reading, make sure your data is backed up safely!

Part I: Three preconceived ideas about ransomware

Idea #1: Ransomware gangs are gangs

Along with the rise of big-game hunting in 2020, we saw the emergence of a number of high-profile groups in the ransomware world. Criminals discovered victims would be more likely to pay ransoms if they could establish some form of reputability beforehand. To ensure that their ability to restore encrypted files would never be questioned, they cultivated an online presence, wrote press releases and generally made sure their name would be known to all potential victims.

But by placing themselves under the spotlight, such groups hide the actual complexity of the ransomware ecosystem. From the outside, they may appear to be single entities; but they are in fact only the tip of the spear. In most attacks there are a significant number of actors involved, and a key takeaway is that they supply services to each other through dark web marketplaces.

Botmasters and *account resellers* are tasked with providing initial access inside the victim's network. Other members of this ecosystem, which we'll name the *red team* for the purpose of this discussion, use this initial access to obtain full control over the target network. During this process, they will gather information about the victim and steal internal documents.

These documents may be forwarded to an outsourced team of *analysts* who will try to figure out the actual financial health of the target, in order to set the highest ransom price that they are likely to pay. Analysts will also keep a lookout for any sensitive or incriminating information which may be used to support their blackmail tactics – the goal being to put maximum pressure on decision-makers.

When the red team is ready to launch the attack, it will purchase a ransomware product from dark web *developers*, usually in exchange for a cut of the ransom. An optional role here is the *packer* developer, who may add protection layers to the ransomware program and make it harder for security products to detect for the few hours it needs to encrypt the whole network.

Finally, negotiations with the victims may be handled by yet another team and when the ransom is paid out, a whole new set of skills is needed to *launder* the cryptocurrency obtained.

An interesting aspect of all this is that the various actors in the "ransomware value chain" do not need to personally know each other, and in fact they don't. They interact with each other through internet handles, paying for services with cryptocurrency. It follows that arresting any of these entities (while useful for deterrence purposes) does little to slow down the ecosystem, as the identity of co-perpetrators cannot be obtained, and other suppliers will immediately fill the void that was created.

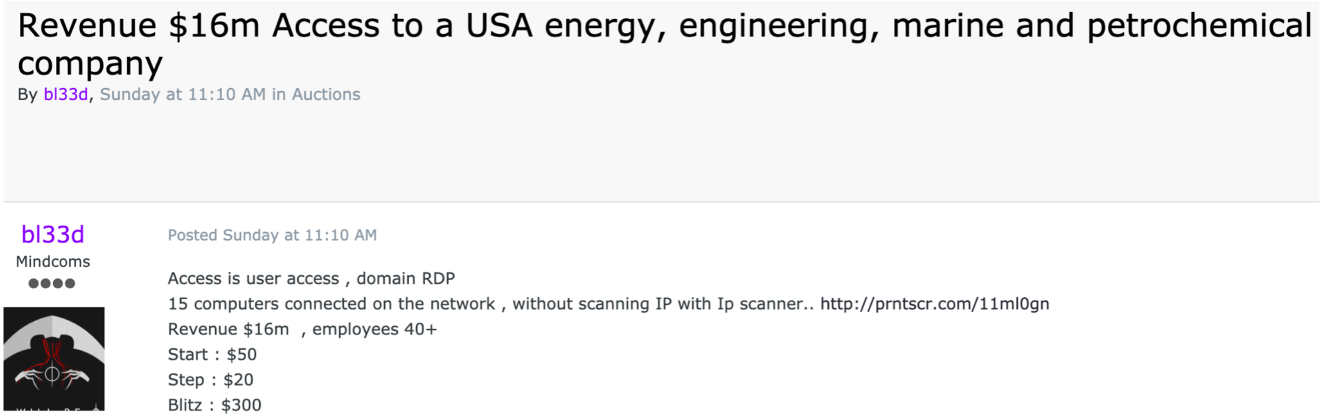
The ransomware world must be understood as an ecosystem, and treated as such: it is a problem that can only be addressed systematically, for instance by preventing the money from circulating inside of it – which involves not paying ransoms in the first place.

Idea #2: Targeted ransomware is targeted

The previous description of the ransomware ecosystem has noteworthy implications when it comes to the way victims are selected. Yes, criminal groups are getting bolder and ask for ever-increasing ransoms. But ransomware attacks have an opportunistic aspect to them. As far as we know, these groups do not peruse the Financial Times to decide who they are going after next.

Counter-intuitively, the people who obtain the initial access to the victim’s network are not the ones who deploy the ransomware later on; and it is helpful to think of access collection as an entirely separate business. For it to be viable, sellers need a steady stream of “product”. It might not make financial sense to spend weeks trying to breach a predetermined hard target like a Fortune 500 company because there’s no guarantee of success. Instead, access sellers go after the low-hanging fruit. There are two main sources for such access:

- **Botnet owners.** Well-known malware families are involved in the biggest and most wide-reaching campaigns. Their main objective is to create networks of infected computers, though the infection is only dormant at this point. Botnet owners (botmasters) sell access to the victim machines in bulk as a resource that can be monetized in many ways, such as organizing DDoS attacks, distributing spam or, in the case of ransomware, by piggybacking on this initial infection to get a foothold in a potential target.
- **Access sellers.** Hackers who are on the lookout for publicly disclosed vulnerabilities (1-days) in internet facing software, such as VPN appliances or email gateways. As soon as such a vulnerability is disclosed, they compromise as many affected servers as possible before the defenders have applied the corresponding updates.



Revenue $16m Access to a USA energy, engineering, marine and petrochemical company

By bl33d, Sunday at 11:10 AM in Auctions

bl33d

Mindcoms

Posted Sunday at 11:10 AM

Access is user access , domain RDP

15 computers connected on the network , without scanning IP with Ip scanner.. http://prntscr.com/11ml0gn

Revenue $16m , employees 40+

Start : $50

Step : $20

Blitz : $300

An example of an offer to sell access to an organization’s RDP

In both cases, it is only after the fact that the attackers take a step back and figure out who they have breached, and if this infection is likely to lead to the payment of a ransom. Actors in the ransomware ecosystem don’t do targeting in that they almost never choose to go after specific entities. Understanding this fact underlines the importance for companies to update internet-facing services in a timely fashion, and to have the ability to detect dormant infections before they can be leveraged for wrongdoing.

Idea #3: Cybercriminals are criminals

Alright, technically, they are. But this is also an area where there is more than meets the eye, because of the diversity of the ransomware ecosystem. There is, of course, a documented porosity between the ransomware ecosystem and other cybercrime domains such as carding or point-of-sale (PoS) hacking. But it is worth pointing out that not all members of this ecosystem originate from the cybercrime underworld. In the past, high-profile ransomware attacks have been used as a destructive means. It is not unreasonable to think that some APT actors are still resorting to similar tactics to destabilize rival economies while maintaining strong plausible deniability.

On the same note, we released a report last year about Lazarus group trying its hand at big-game hunting. ClearSky identified similar activity that they attributed to the Fox Kitten APT. Observers have noted that the obvious profitability of ransomware attacks has attracted a few state-sponsored threat actors to this ecosystem as a way of circumventing international sanctions.

Our data indicates that such ransomware attacks represent only a tiny fraction of the total. While they do not represent a rift in what companies need to be able to defend against, their very existence creates an additional risk for victims. On October 1, 2020, the US Department of the Treasury’s OFAC released a memo clarifying that companies wiring money to attackers need to ensure that the recipients are not subject to international sanctions. This announcement appeared to be effective as it already impacted the ransomware market. It goes without saying that performing due diligence on ransomware operators is a challenge on its own.

Part II: The darknet shenanigans

Through the market lanes

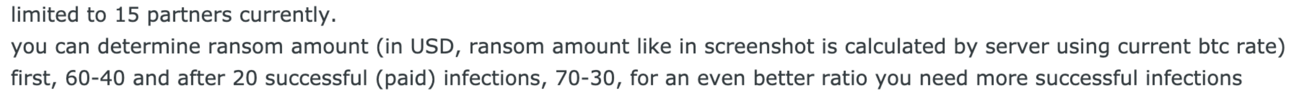
When it comes to the sale of digital goods or services related to cybercrime on the darknet, most information is aggregated on just a few large platforms, though there are multiple smaller thematic ones focusing on a single topic or product. We analyzed three main forums on which ransomware-related offers are aggregated. These forums are the main platforms where cybercriminals that work with ransomware actively communicate and trade. While the forums host hundreds of various advertisements and offers, for analysis we selected just a few dozen offers that had been verified by forum administrations and placed by groups with an established reputation. These ads included a variety of offers from the sale of source code to regularly updated recruitment advertisements, available in English and Russian.

Different types of offers

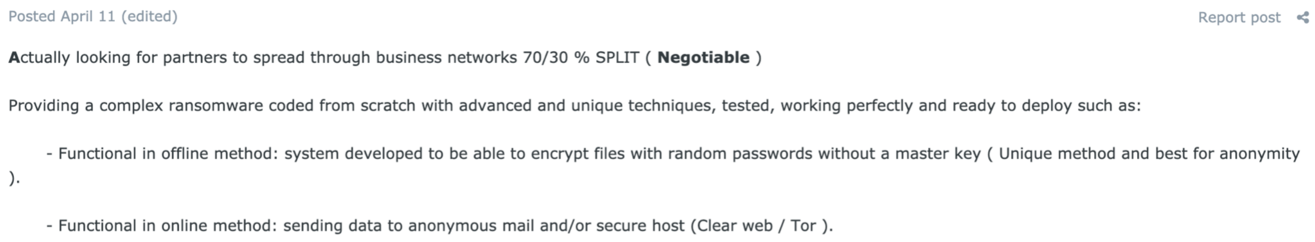
As we noted before, the ransomware ecosystem consists of players that take on different roles. Darknet forums partially reflect this state of affairs, albeit the offers on these markets are aimed primarily at selling or recruiting. Just as with any marketplace, when operators need something, they actively update their ad placements on forums and take them off as soon as that need is fulfilled. Ransomware developers and operators of affiliate ransomware programs (better known as Ransomware as a Service) offer the following:

- Invitations to join partner networks, affiliate programs for ransomware operators
- Ads for ransomware source code or ransomware builders

The first type of involvement presumes a lengthy partnership between the ransomware group operator and the affiliate. Usually, the ransomware operator takes a profit share ranging from 20% to 40%, while the remaining 60-80% stays with the affiliate.



limited to 15 partners currently.
you can determine ransom amount (in USD, ransom amount like in screenshot is calculated by server using current btc rate)
first, 60-40 and after 20 successful (paid) infections, 70-30, for an even better ratio you need more successful infections



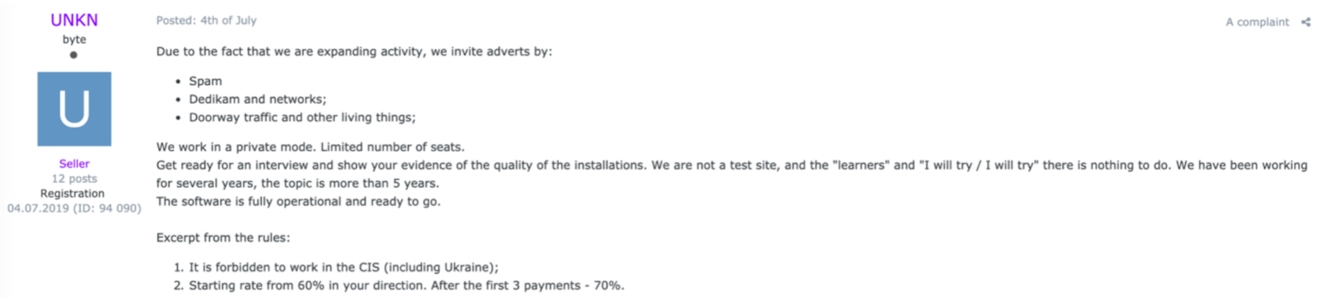
Posted April 11 (edited)

Actually looking for partners to spread through business networks 70/30 % SPLIT (**Negotiable**)

Providing a complex ransomware coded from scratch with advanced and unique techniques, tested, working perfectly and ready to deploy such as:

- Functional in offline method: system developed to be able to encrypt files with random passwords without a master key (Unique method and best for anonymity).

- Functional in online method: sending data to anonymous mail and/or secure host (Clear web / Tor).



UNKN
byte

Seller
12 posts
Registration
04.07.2019 (ID: 94 090)

Posted: 4th of July

A complaint

Due to the fact that we are expanding activity, we invite adverts by:

- Spam
- Dedikam and networks;
- Doorway traffic and other living things;

We work in a private mode. Limited number of seats.
Get ready for an interview and show your evidence of the quality of the installations. We are not a test site, and the "learners" and "I will try / I will try" there is nothing to do. We have been working for several years, the topic is more than 5 years.
The software is fully operational and ready to go.

Excerpt from the rules:

1. It is forbidden to work in the CIS (including Ukraine);
2. Starting rate from 60% in your direction. After the first 3 payments - 70%.

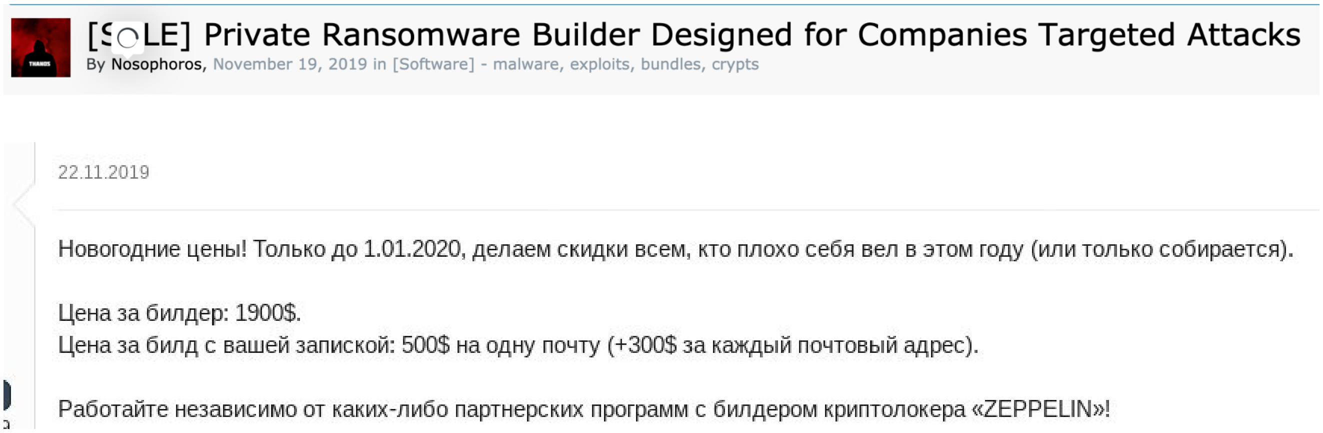
Examples of offers listing payment conditions in partner programs

While many ransomware operators look for partners, some sell ransomware source code or do-it-yourself (DIY) ransomware packages. Such offers vary from US$300 to US$5000.

Sale of ransomware source code or the sale of leaked samples is the easiest way of making money off ransomware in terms of technical proficiency and effort invested by the seller. However, such offers also make the least money, as source code and samples quickly lose their value. There are two different types of offers – with and without support. If ransomware is purchased without support, once it is detected by cybersecurity solutions, the buyer would need to figure out on their own how to repackage it, or find a service that does sample repackaging – something that it still easily detected by security solutions.

Offers with support (admittedly, more widespread in the financial malware market), usually offer regular updates and make decisions about malware updates.

In this regard, darknet forum offers have not changed much compared to 2017.



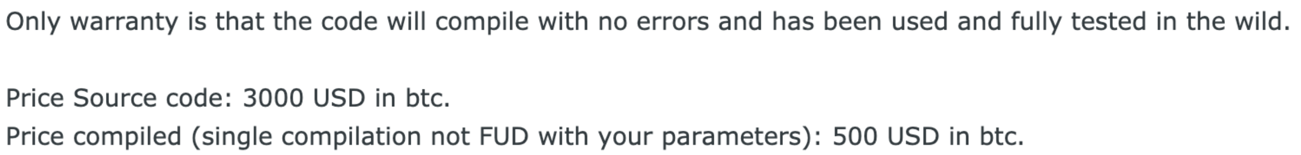
[S○LE] Private Ransomware Builder Designed for Companies Targeted Attacks
By Nosophoros, November 19, 2019 in [Software] - malware, exploits, bundles, crypts

22.11.2019

Новогодние цены! Только до 1.01.2020, делаем скидки всем, кто плохо себя вел в этом году (или только собирается).

Цена за билдер: 1900$.
Цена за билд с вашей запиской: 500$ на одну почту (+300$ за каждый почтовый адрес).

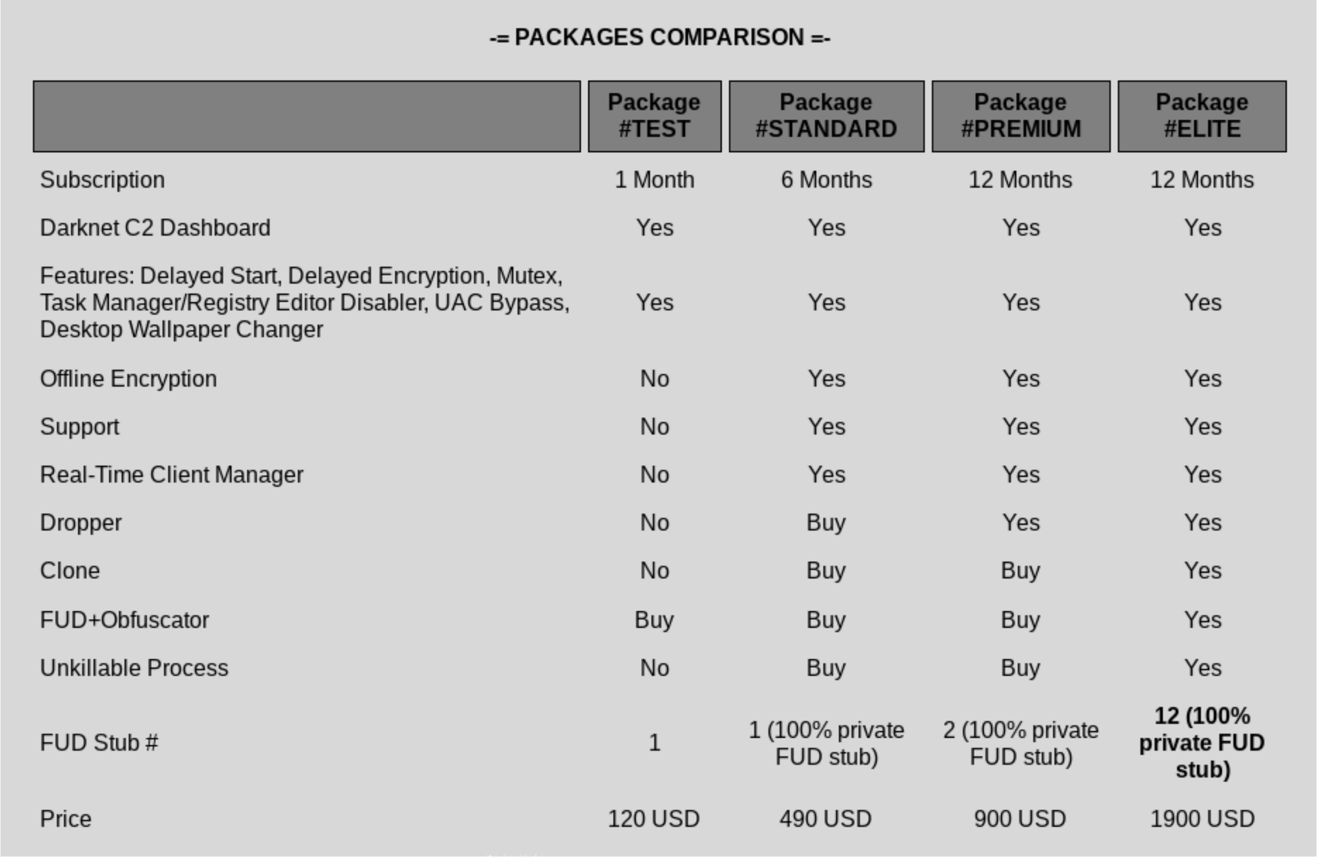
Работайте независимо от каких-либо партнерских программ с билдером криптолокера «ZEPPELIN»!



Only warranty is that the code will compile with no errors and has been used and fully tested in the wild.

Price Source code: 3000 USD in btc.
Price compiled (single compilation not FUD with your parameters): 500 USD in btc.

Ransomware developers sometimes advertise builders and source code as a one-off purchase with no customer support



-= PACKAGES COMPARISON =-

	Package #TEST	Package #STANDARD	Package #PREMIUM	Package #ELITE
Subscription	1 Month	6 Months	12 Months	12 Months
Darknet C2 Dashboard	Yes	Yes	Yes	Yes
Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer	Yes	Yes	Yes	Yes
Offline Encryption	No	Yes	Yes	Yes
Support	No	Yes	Yes	Yes
Real-Time Client Manager	No	Yes	Yes	Yes
Dropper	No	Buy	Yes	Yes
Clone	No	Buy	Buy	Yes
FUD+Obfuscator	Buy	Buy	Buy	Yes
Unkillable Process	No	Buy	Buy	Yes
FUD Stub #	1	1 (100% private FUD stub)	2 (100% private FUD stub)	**12 (100% private FUD stub)**
Price	120 USD	490 USD	900 USD	1900 USD

An offer of a subscription for ransomware and additional services looks very similar to any other ad for a legitimate product, with varying benefits and price range

Some of the big players aren’t seen on the darknet

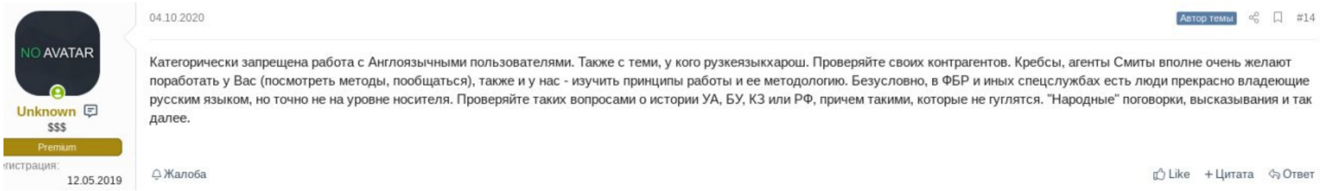
Even though the number and the range of offers available on the darknet certainly is not small, the markets do not reflect the whole ransomware ecosystem. Some large ransomware groups either work independently or find partners directly (for instance, as far as we know, Ryuk was able to access some of its victims’ systems after a Trickbot infection, which suggests a potential partnership between two groups). Therefore, the forums generally host smaller players – either medium-sized RaaS operators, smaller actors that sell source code and newbies.

Ground rules for affiliates on the darknet

The ransomware market is a closed one, and the operators behind it are careful about who they choose to work with. This caution is reflected in the ads the operators place and criteria they impose when selecting partners.

The first general rule is that of geographical restrictions placed on the operators. When malware operators work with partners, they avoid using the malware in the jurisdiction where they are based. This rule is strictly adhered to and partners that don’t abide by it quickly lose access to the programs they have been working with.

Additionally, operators screen potential partners to reduce the chances of hiring an undercover official, for instance, by checking their knowledge of the country they claim to be from, as illustrated in the example below. They may also impose restrictions on certain nationalities based on their political views. These are just some of the ways operators try to ensure their security.

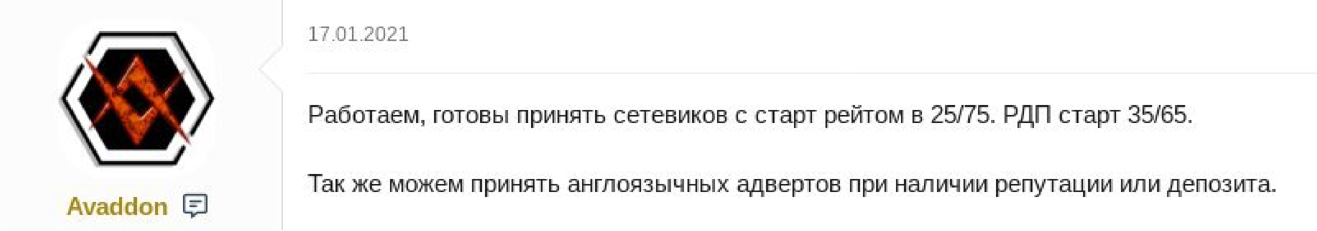


ıгистрация: 12.05.2019

04.10.2020

Категорически запрещена работа с Англоязычными пользователями. Также с теми, у кого рузкеязыкхарош. Проверяйте своих контрагентов. Кребсы, агенты Смиты вполне очень желают поработать у Вас (посмотреть методы, пообщаться), также и у нас - изучить принципы работы и ее методологию. Безусловно, в ФБР и иных спецслужбах есть люди прекрасно владеющие русским языком, но точно не на уровне носителя. Проверяйте таких вопросами о истории УА, БУ, КЗ или РФ, причем такими, которые не гуглятся. "Народные" поговорки, высказывания и так далее.

In this example the gang recommends vetting new affiliates by asking obscure questions about the history of former Soviet republics and expressions that typically only native Russian speakers could answer



17.01.2021

Работаем, готовы принять сетевиков с старт рейтом в 25/75. РДП старт 35/65.

Так же можем принять англоязычных адвертов при наличии репутации или депозита.

Avaddon may consider English-speaking affiliates if they have an established reputation or can provide a deposit, according to this ad

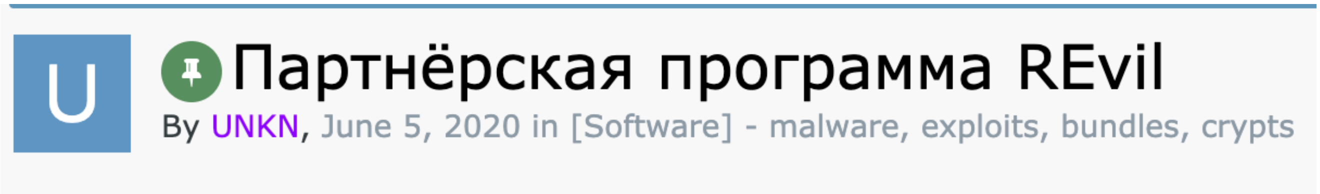
The merchants

For a more detailed overview we chose two of the most noteworthy Big Game Hunting ransomware in 2021.

The first one is the REvil (aka Sodinokibi) gang. Since 2019, this ransomware has been advertised on underground forums and has a strong reputation as a RaaS operator. The gang’s name REvil often appears in news headlines in the infosecurity community. REvil operators have demanded the highest ransoms in 2021.

The other is the Babuk locker. Babuk is the first new RaaS threat discovered in 2021, demonstrating a high level of activity.

REvil



Партнёрская программа REvil

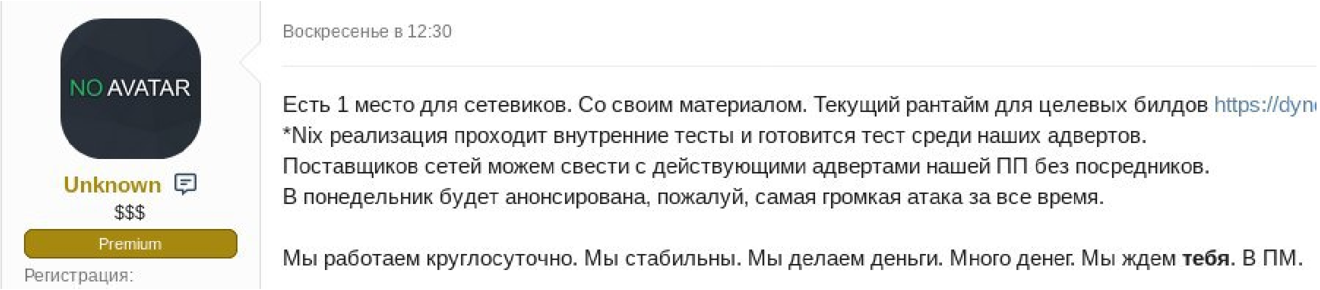
By UNKN, June 5, 2020 in [Software] - malware, exploits, bundles, crypts

An example of an ad placed by the REvil affiliate program

REvil is one of the most prolific RaaS operations. The group’s first activity was observed in April 2019 after the shutdown of GandCrab, another now-defunct ransomware gang.

To distribute ransomware, REvil cooperates with affiliates hired on cybercriminal forums. The ransom demand is based on the annual revenue of the victim, and distributors earn between 60% and 75% of the ransom. Monero (XMR) cryptocurrency is used for payment. According to the interview with the REvil operator, the gang earned over $100 million from its operations in 2020.

The developers regularly update the REvil ransomware to avoid detection and improve the reliability of ongoing attacks. The group announces all major updates and availability of new partner program items in their various threads on cybercriminal forums. On April 18, 2021, the developer announced that the *nix implementation of the ransomware was undergoing closed testing.



Воскресенье в 12:30

Есть 1 место для сетевиков. Со своим материалом. Текущий рантайм для целевых билдов https://dyn
*Nix реализация проходит внутренние тесты и готовится тест среди наших адвертов.
Поставщиков сетей можем свести с действующими адвертами нашей ПП без посредников.
В понедельник будет анонсирована, пожалуй, самая громкая атака за все время.

Мы работаем круглосуточно. Мы стабильны. Мы делаем деньги. Много денег. Мы ждем **тебя**. В ПМ.

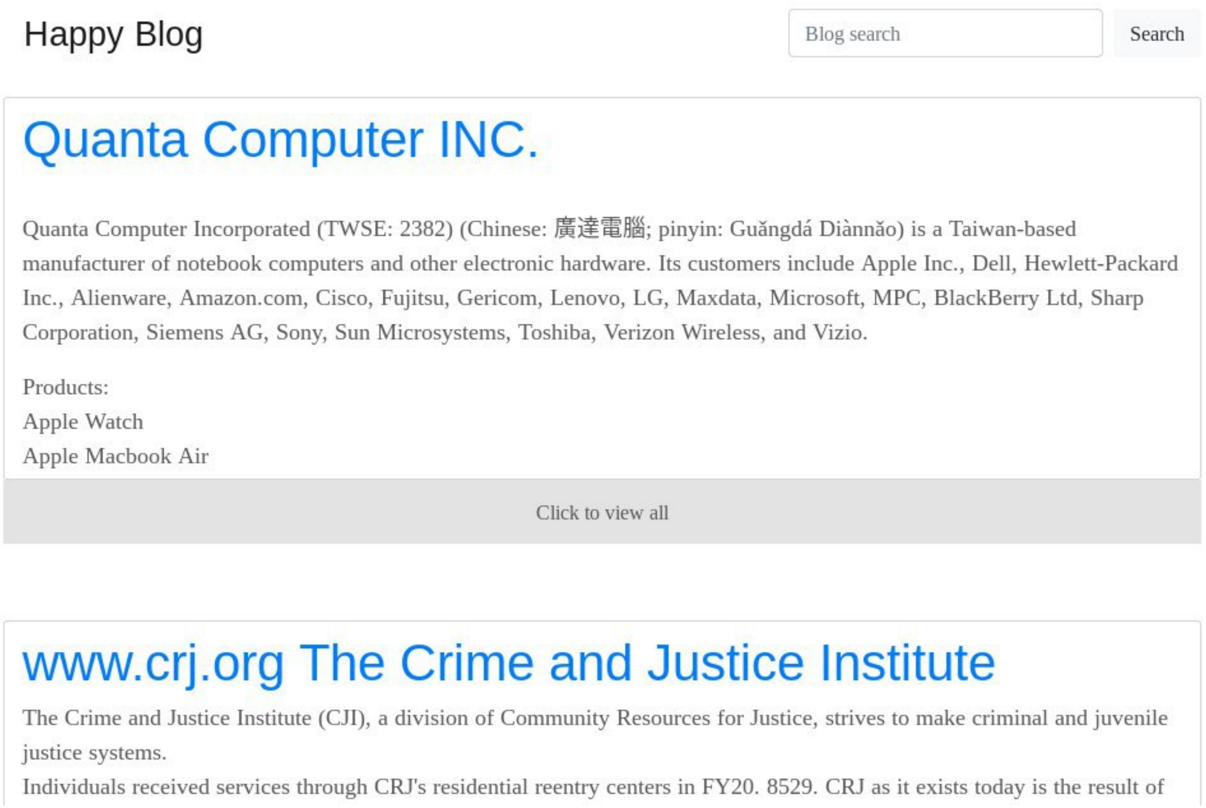
*REvil informs about the internal testing of the *nix implementation of the ransomware*

Technical details

REvil uses the Salsa20 symmetric stream algorithm for encrypting the content of files and the keys for it with an elliptic curve asymmetric algorithm. The malware sample has an encrypted configuration block with many fields, which allow attackers to fine-tune the payload. The executable can terminate blacklisted processes prior to encryption, exfiltrate basic host information, encrypt non-whitelisted files and folders on local storage devices and network shares. A more detailed account of the technical capabilities of REvil is available in our private and public reports.

The ransomware is now distributed mainly through compromised RDP accesses, phishing, and software vulnerabilities. The affiliates are responsible for gaining initial access to corporate networks and deploying the locker – a standard practice for the RaaS model. It should be noted that the gang has very strict recruitment rules for new affiliates: REvil recruits only Russian-speaking highly skilled partners with experience in gaining access to networks.

Privilege elevation, reconnaissance and lateral movement follow a successful breach. The operators then evaluate, exfiltrate and encrypt sensitive files. The next stage is negotiations with the attacked company. If the victim decides not to pay their ransom, the REvil operators will start publishing the sensitive data of the attacked company on the .onion Happy Blog site. The tactic of publishing exfiltrated confidential data on leak sites has recently gone mainstream among Big Game Hunting players.



Quanta Computer INC.

Quanta Computer Incorporated (TWSE: 2382) (Chinese: 廣達電腦; pinyin: Guǎngdá Diànnǎo) is a Taiwan-based manufacturer of notebook computers and other electronic hardware. Its customers include Apple Inc., Dell, Hewlett-Packard Inc., Alienware, Amazon.com, Cisco, Fujitsu, Gericom, Lenovo, LG, Maxdata, Microsoft, MPC, BlackBerry Ltd, Sharp Corporation, Siemens AG, Sony, Sun Microsystems, Toshiba, Verizon Wireless, and Vizio.

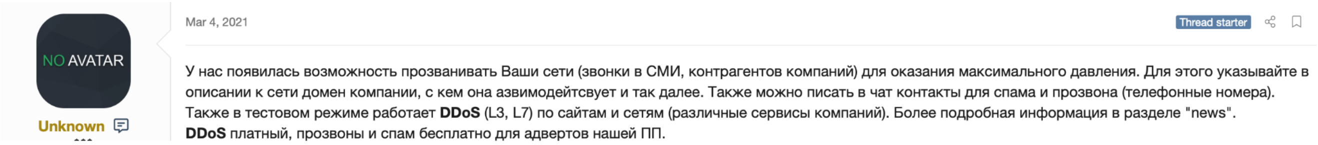
Products:
Apple Watch
Apple Macbook Air

www.crj.org The Crime and Justice Institute

The Crime and Justice Institute (CJI), a division of Community Resources for Justice, strives to make criminal and juvenile justice systems.
Individuals received services through CRJ's residential reentry centers in FY20. 8529. CRJ as it exists today is the result of

An example of a post on REvil's blog that includes data stolen from the victim

It's worth noting that ransomware operators have started using voice calls to business partners and journalists, as well as DDoS attacks, to force their victims to pay a ransom. In March 2021, according to the operator, the gang launched a service at no extra cost for affiliates that contacts the victim's partners and the media to exert maximum pressure, plus DDoS (L3, L7) as a paid service.



Mar 4, 2021

У нас появилась возможность прозванивать Ваши сети (звонки в СМИ, контрагентов компаний) для оказания максимального давления. Для этого указывайте в описании к сети домен компании, с кем она азвимодейтсвует и так далее. Также можно писать в чат контакты для спама и прозвона (телефонные номера). Также в тестовом режиме работает **DDoS** (L3, L7) по сайтам и сетям (различные сервисы компаний). Более подробная информация в разделе "news".
DDoS платный, прозвоны и спам бесплатно для адвертов нашей ПП.

REvil announces a new feature to arrange calls to the media and the target's partners to exert additional pressure when demanding a ransom

According to our research, this malware affected almost 20 business sectors. The largest share of victims fell into the category Engineering & Manufacturing (30%), followed by Finance (14%), Professional & Consumer Services (9%), Legal (7%), and IT & Telecommunications (7%).

The victims of this campaign include companies such as Travelex, Brown-Forman Corp., the pharmaceutical group Pierre Fabre, and the celebrity law firm Grubman Shire Meiselas & Sacks. In March 2021, the gang breached Acer and demanded the highest recorded ransom of $50 million.

On April 18, 2021, a member of the REvil group announced that the gang was on the cusp of declaring its "most high-profile attack ever" in a post on forums where cybercriminals recruit new affiliates. On April 20, the group published a number of alleged blueprints for Apple devices on the Happy Blog site. According to the attackers, the data was stolen from Quanta's network. Quanta Computer is a Taiwan-based manufacturer and one of Apple's partners. Quanta's initial ransom demand was $50 million.

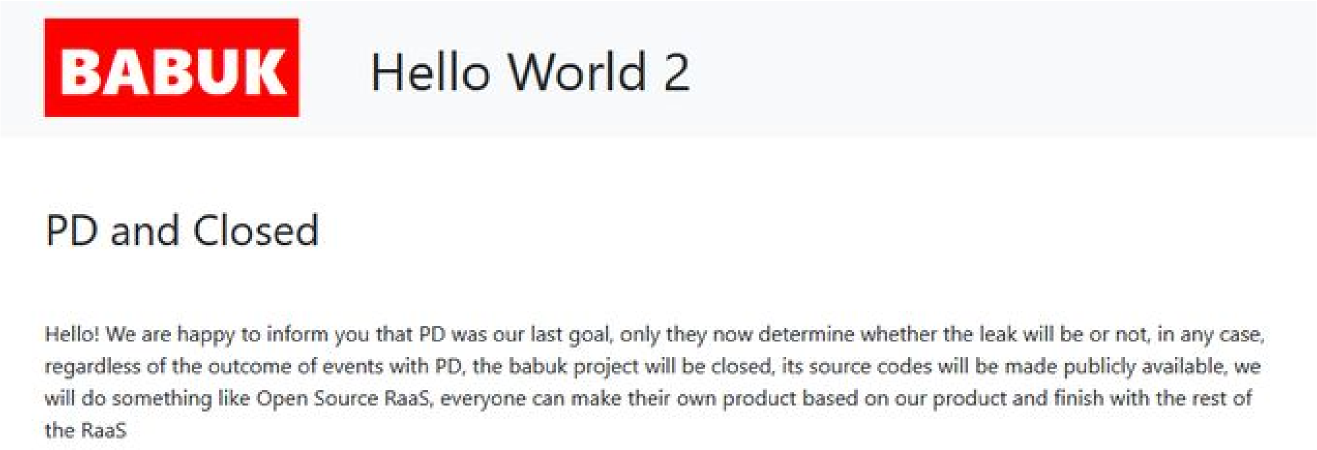
In the past few quarters there has been a sharp spike in REvil's targeted activity (download)

The REvil gang is a prime example of a Big Game Hunting player. In 2021, we are seeing a trend towards bigger ransoms for sensitive company data. The use of new tactics to pressure the victim, the active development of non-Windows versions and the regular recruitment of new affiliates all suggest that the number and scale of attacks will only grow in 2021.

Babuk

Another player in the Big Game Hunting scene in 2021 is the Babuk locker. At the beginning of 2021 we observed several incidents involving this ransomware.

At the end of April 2021, the threat actors behind Babuk announced the end of their activity, stating that they will make their source code publicly available in order to "do something like Open Source RaaS". This means that we'll probably see a new wave of ransomware activity as soon as various smaller threat actors adopt the leaked source code for their operations. We've seen this sort of situation happen before with other RaaS and MaaS projects – the Cerberus banking Trojan for Android is a good example from last year.



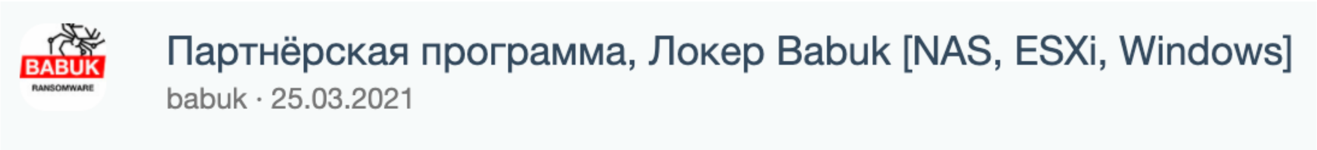
BABUK Hello World 2

PD and Closed

Hello! We are happy to inform you that PD was our last goal, only they now determine whether the leak will be or not, in any case, regardless of the outcome of events with PD, the babuk project will be closed, its source codes will be made publicly available, we will do something like Open Source RaaS, everyone can make their own product based on our product and finish with the rest of the RaaS

Babuk announcement about the end of operations

The group obviously customizes each sample for each victim because it includes a hardcoded name of the organization, personal ransomware note and extensions of the encrypted files. Babuk’s operators also use the RaaS model. Prior to infection, affiliates or the operators compromise the target network, so they can identify how to deploy the ransomware effectively and evaluate the sensitive data in order to set the highest realistic ransom price for the victim. The team behind Babuk defines their group as CyberPunks that “randomly test corporate networks security,” using RDP as an infection vector. The gang offers 80% of the ransom to their affiliates.

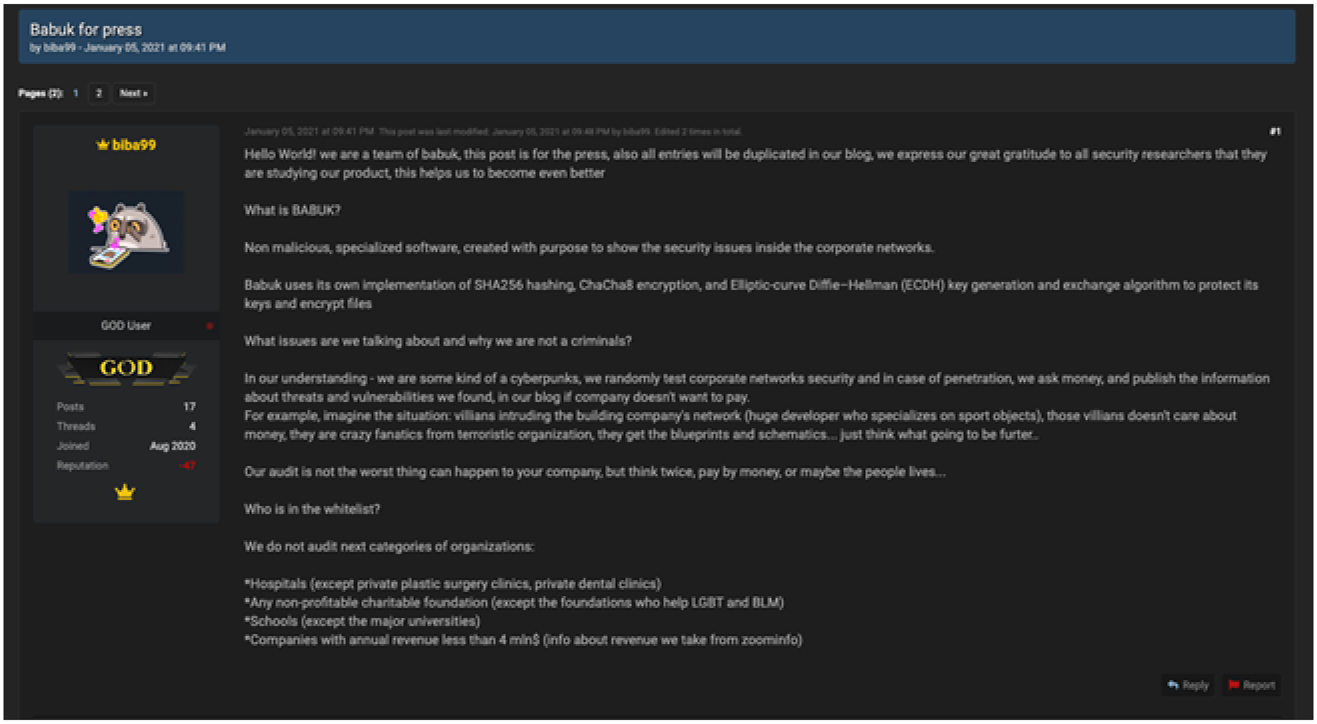


Партнёрская программа, Локер Babuk [NAS, ESXi, Windows]

babuk · 25.03.2021

An example of an ad placed by the Babuk affiliate program

Babuk advertises on both Russian-speaking and English-speaking underground forums. At the beginning of January 2021, an announcement appeared on one forum about the new ransomware Babuk, with subsequent posts focusing on updates and affiliate recruitment.



Babuk for press
by biba99 - January 05, 2021 at 09:41 PM

biba99

GOD User

Posts 17
Threads 4
Joined Aug 2020
Reputation -47

January 05, 2021 at 09:41 PM This post was last modified: January 05, 2021 at 09:48 PM by biba99. Edited 2 times in total. #1

Hello World! we are a team of babuk, this post is for the press, also all entries will be duplicated in our blog, we express our great gratitude to all security researchers that they are studying our product, this helps us to become even better

What is BABUK?

Non malicious, specialized software, created with purpose to show the security issues inside the corporate networks.

Babuk uses its own implementation of SHA256 hashing, ChaCha8 encryption, and Elliptic-curve Diffie–Hellman (ECDH) key generation and exchange algorithm to protect its keys and encrypt files

What issues are we talking about and why we are not a criminals?

In our understanding - we are some kind of a cyberpunks, we randomly test corporate networks security and in case of penetration, we ask money, and publish the information about threats and vulnerabilities we found, in our blog if company doesn't want to pay.
For example, imagine the situation: villians intruding the building company's network (huge developer who specializes on sport objects), those villians doesn't care about money, they are crazy fanatics from terroristic organization, they get the blueprints and schematics... just think what going to be furter..

Our audit is not the worst thing can happen to your company, but think twice, pay by money, or maybe the people lives...

Who is in the whitelist?

We do not audit next categories of organizations:

*Hospitals (except private plastic surgery clinics, private dental clinics)
*Any non-profitable charitable foundation (except the foundations who help LGBT and BLM)
*Schools (except the major universities)
*Companies with annual revenue less than 4 mln$ (info about revenue we take from zoominfo)

Babuk's announcement to the press explaining their strategy and victim selection

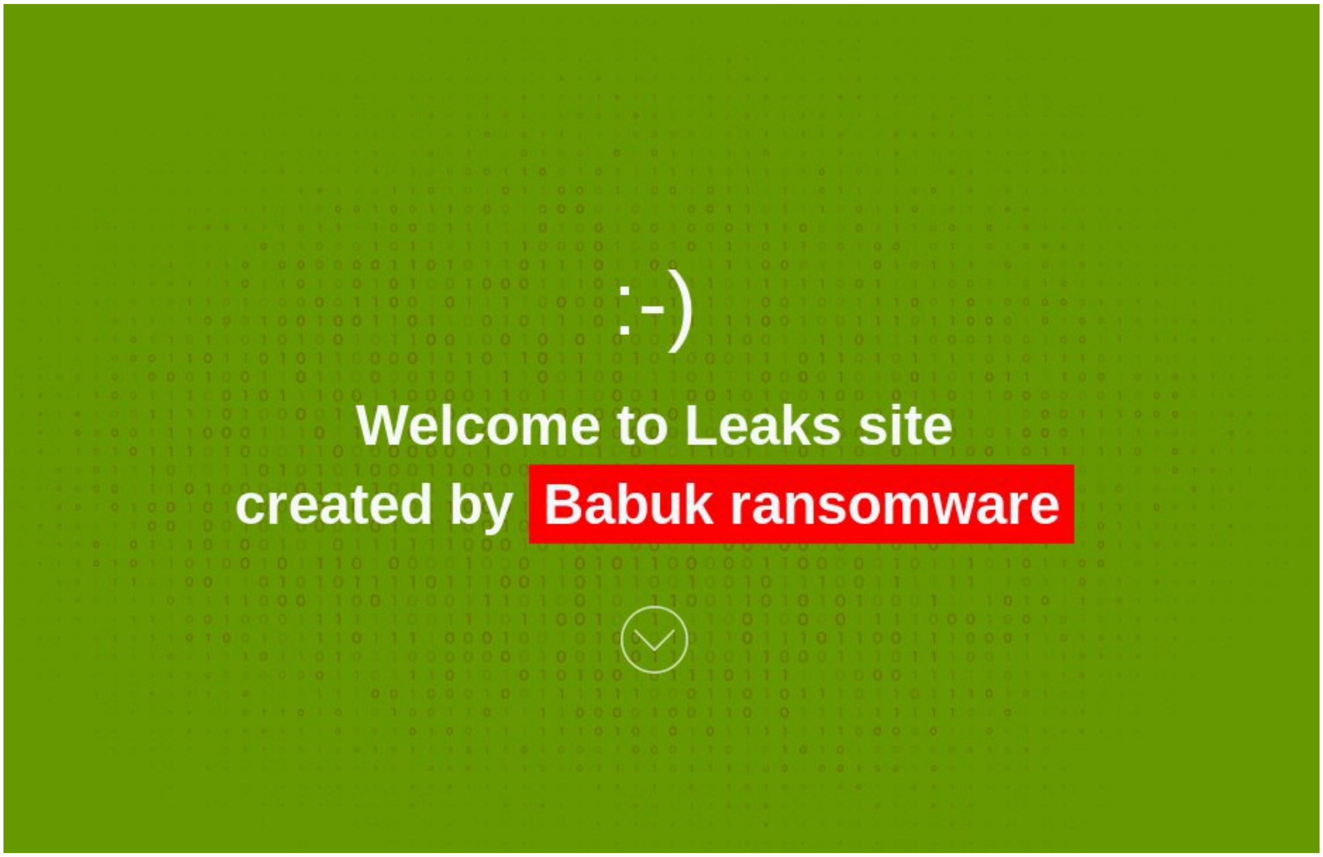
Babuk's whitelist prevents any targeting in the following countries: China, Vietnam, Cyprus, Russia and other CIS countries. The operators also prohibit the compromise of hospitals, non-profit charities, and companies with an annual revenue of less than $30 million according to ZoomInfo. To join the affiliate program, a partner must pass an interview on Hyper-V and ESXi hypervisors.

Babuk made the headlines for being probably the first ransomware gang to publicly declare a negative stance towards the LGBT and Black Lives Matter (BLM) communities. It was due to this fact that the group excluded these communities from their whitelist. But in a post on the Babuk data leak site about the results of two months of work, the gang reported that they had added LGBT and BLM foundations and charity organizations to their whitelist.

Technical details

For encryption Babuk uses a symmetric algorithm combined with Elliptic curve Diffie–Hellman (ECDH). After successful encryption, the malware drops a hardcoded ransom note as "How To Restore Your Files.txt" into each processed directory. In addition to the text, the ransom note contains a list of links to screenshots of some exfiltrated data. This proves that the malware sample is crafted after the victim's data is exfiltrated. As mentioned above, each sample is customized for the specific target.

In the ransom note, the gang also suggests that the victim starts the negotiation process using their personal chat portal. These steps aren't exclusively tied to Babuk but are commonly present in Big Game Hunting campaigns. Remarkably, the text of the ransom note also contains a private link to the related post on the .onion data leak site, which is not accessible from the main page of the site. There are some screenshots, as well as a text description of the types of stolen files, and general threats addressed to the victim. If the victim decides not to negotiate with cybercriminals, the link to this post will be made public.

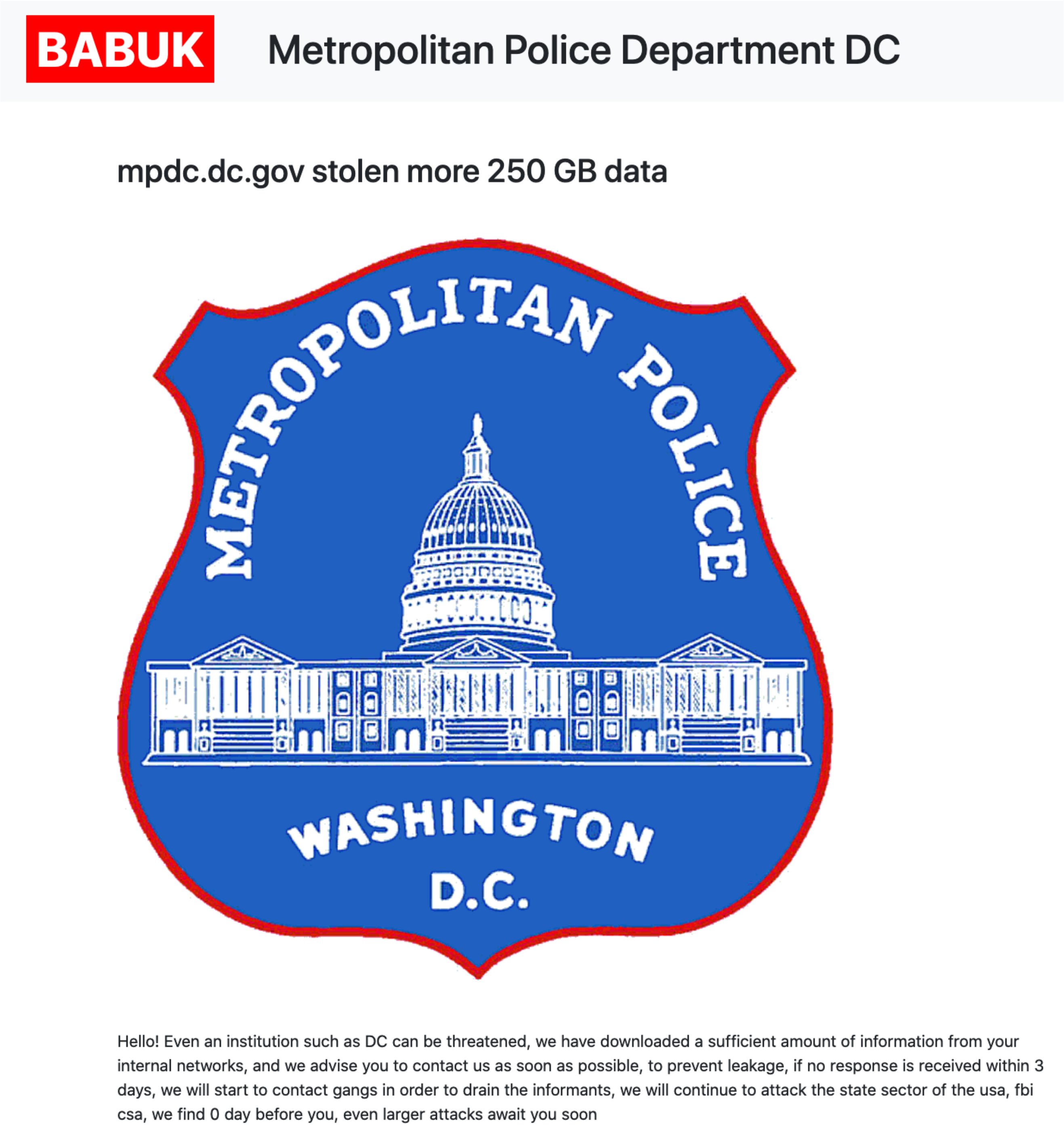


:-)

Welcome to Leaks site

created by Babuk ransomware

The group behind the Babuk locker primarily targets large industrial organizations in Europe, the US and Oceania. Targeted industries include, but are not limited to, transportation services, the healthcare sector, and various suppliers of industrial equipment. In fact, recent cases show that Babuk operators are expanding their targets. On April 26, the D.C. Police Department confirmed that its network had been breached, with the Babuk operator claiming responsibility and announcing the attack on their .onion leak site.



BABUK

Metropolitan Police Department DC

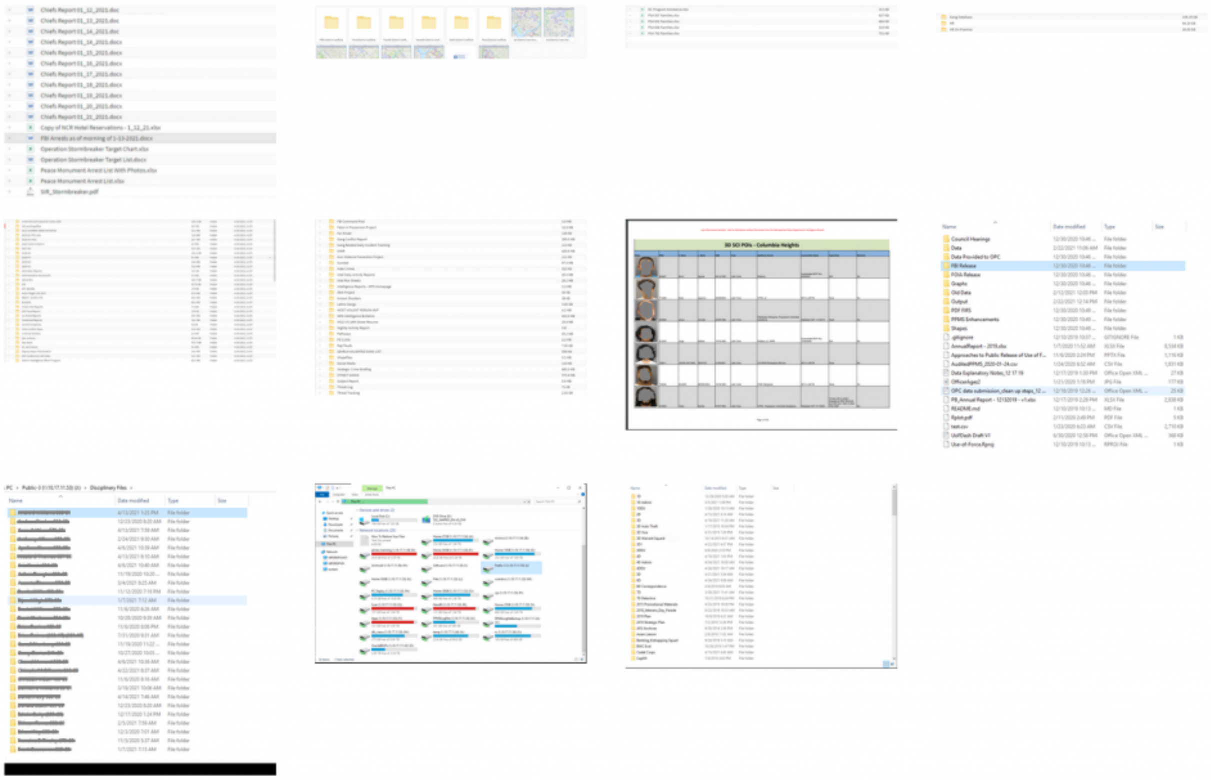
mpdc.dc.gov stolen more 250 GB data

Hello! Even an institution such as DC can be threatened, we have downloaded a sufficient amount of information from your internal networks, and we advise you to contact us as soon as possible, to prevent leakage, if no response is received within 3 days, we will start to contact gangs in order to drain the informants, we will continue to attack the state sector of the usa, fbi csa, we find 0 day before you, even larger attacks await you soon

Babuk's announcement of a successful attack on the D.C. Police Department

According to the post on this site, the gang was able to exfiltrate more than 250 GB of data from Washington's Metropolitan Police Department network. At the time of writing, the police department had three days to start the negotiation process with the attackers; otherwise, the group would start leaking data to criminal gangs. Babuk also warned that it would continue to attack the US state sector.

Image Gallery



Chiefs Report 01_12_2021.doc
Chiefs Report 01_13_2021.doc
Chiefs Report 01_14_2021.doc
Chiefs Report 01_14_2021.docx
Chiefs Report 01_15_2021.docx
Chiefs Report 01_16_2021.docx
Chiefs Report 01_17_2021.docx
Chiefs Report 01_18_2021.docx
Chiefs Report 01_19_2021.docx
Chiefs Report 01_20_2021.docx
Chiefs Report 01_21_2021.docx
Copy of NCR Hotel Reservations - 1_12_21.xlsx
FBI Arrests as of morning of 1-13-2021.docx
Operation Stormbreaker Target Chart.xlsx
Operation Stormbreaker Target List.docx
Peace Monument Arrest List With Photos.xlsx
Peace Monument Arrest List.xlsx
SIR_Stormbreaker.pdf

Name	Date modified	Type	Size
Council Hearings	12/30/2020 10:46 ...	File folder	
Data	2/22/2021 11:06 AM	File folder	
Data Provided to OPC	12/30/2020 10:46 ...	File folder	
FBI Release	12/30/2020 10:46 ...	File folder	
FOIA Release	12/30/2020 10:46 ...	File folder	
Graphs	12/30/2020 10:46 ...	File folder	
Old Data	2/12/2021 12:03 PM	File folder	
Output	2/22/2021 12:14 PM	File folder	
PDF RIRS	12/30/2020 10:49 ...	File folder	
PPMS Enhancements	12/30/2020 10:49 ...	File folder	
Shapes	12/30/2020 10:49 ...	File folder	
.gitignore	12/10/2019 10:07 ...	GITIGNORE File	1 KB
AnnualReport - 2019.xlsx	1/7/2020 11:52 AM	XLSX File	8,534 KB
Approaches to Public Release of Use of F...	11/6/2020 2:24 PM	PPTX File	1,116 KB
AuditedPPMS_2020-01-24.csv	1/24/2020 6:52 AM	CSV File	1,831 KB
Data Explanatory Notes_12 17 19	12/17/2019 1:30 PM	Office Open XML ...	27 KB
OfficerAges2	1/21/2020 1:16 PM	JPG File	177 KB
OPC data submission_clean-up steps_12 ...	12/18/2019 12:26 ...	Office Open XML ...	25 KB
PB_Annual Report - 12132019 -- v1.xlsx	12/17/2019 2:28 PM	XLSX File	2,838 KB
README.md	12/10/2019 10:13 ...	MD File	1 KB
Rplot.pdf	2/11/2020 2:49 PM	PDF File	5 KB
test.csv	1/23/2020 6:23 AM	CSV File	2,710 KB
UoFDash Draft V1	6/30/2020 12:58 PM	Office Open XML ...	368 KB
Use-of-Force.Rproj	12/10/2019 10:13 ...	RPROJ File	1 KB

Download links:

Babuk operator’s screenshots of stolen files from the D.C. Police Department’s network published on the darknet leak site

Conclusion

On April 23, 2021, we released ransomware statistics that revealed a significant decline in the number of users who had encountered this threat. These numbers should not be misinterpreted: while it is true that random individuals are less likely to encounter ransomware than they used to, the risk for companies has never been higher.

Ever eager to maximize profits, the ransomware ecosystem has evolved and can now be considered a systemic threat for corporations all around the world.

There was a time where SMBs could mostly ignore the challenges posed by information security: they were small enough to stay under the radar of APT actors, but still big enough not to be affected by random and generic attacks. Those days are over, and all companies today are now in a position where they must be prepared to fend off criminal groups.

Thankfully, such attackers will usually go after the low-hanging fruit first, and setting up appropriate security practices will make a world of difference.

On May 12, which is **Anti-Ransomware Day**, Kaspersky encourages organizations to follow these best practices to help safeguard your organization against ransomware:

- Always keep software up to date on all your devices to prevent attackers from infiltrating your network by exploiting vulnerabilities.
- Focus your defense strategy on detecting lateral movements and data exfiltration to the internet. Pay special attention to the outgoing traffic to detect cybercriminal connections. Set up offline backups that intruders cannot tamper with. Make sure you can quickly access them in an emergency.
- To protect the corporate environment, educate your employees. Dedicated training courses can help, such as the ones provided in the Kaspersky Automated Security Awareness Platform. A free lesson on how to protect against ransomware attacks is available here.
- Carry out a cybersecurity audit of your networks and remediate any weaknesses discovered in the perimeter or inside the network.
- Enable ransomware protection for all endpoints. There is the free Kaspersky Anti-Ransomware Tool for Business that shields computers and servers from ransomware and other types of malware, prevents exploits and is compatible with other installed security solutions.
- Install anti-APT and EDR solutions, enabling capabilities for advanced threat discovery and detection, investigation and timely remediation of incidents. Provide your SOC team with access to the latest threat intelligence and regularly upskill them with professional training. Ask for help from your MDR provider if you lack internal threat hunting experts. They will take responsibility for continuously finding, detecting and responding to threats targeting your business. All of the above is available within the Kaspersky Expert Security framework.
- If you become a victim, never pay the ransom. It won’t guarantee you get your data back but will encourage criminals to continue their activities. Instead, report the incident to your local law enforcement agency. Try to find a decryptor on the internet – quite a few are available at https://www.nomoreransom.org/en/index.html

- Cybercrime
- Darknet
- Malware Descriptions
- Ransomware
- Russian-speaking cybercrime
- Targeted attacks

Authors

- Dmitry Galov
-

 Leonid Bezvershenko
- Ivan Kwiatkowski

Ransomware world in 2021: who, how and why

Your email address will not be published. Required fields are marked *