



## Victoria Kivilevich, Threat Intelligence Analyst

28.07.2021

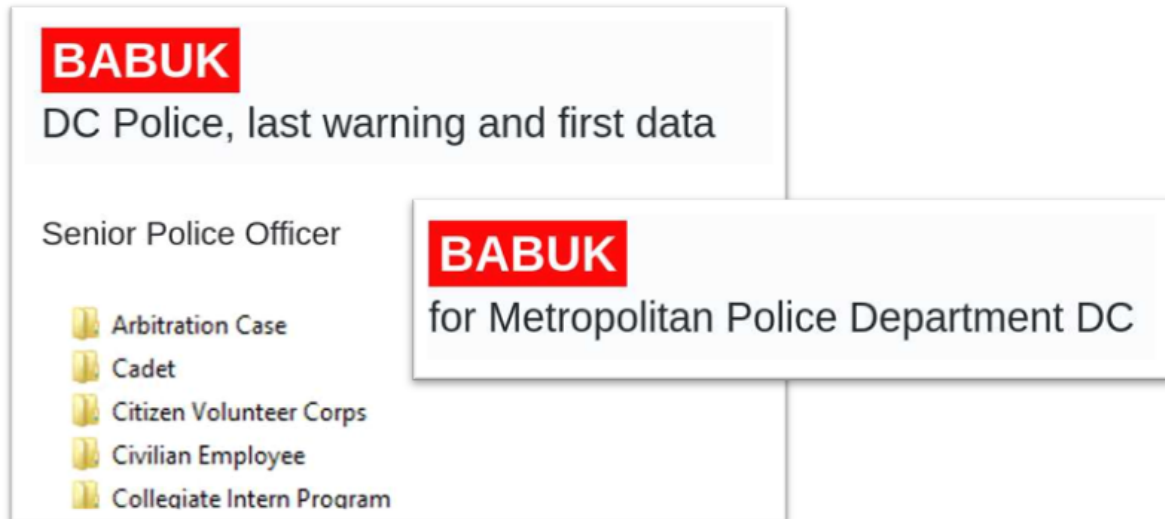
A new Russian-speaking forum called RAMP was launched in July 2021 and received much attention from researchers and cybercrime actors. The forum emerged at the domain that previously hosted the Babuk ransomware data leak site and later the Payload.bin leak site. KELA researched the contents of the new site and assessed its chances to succeed.

\*All the forum contents are described based on what KELA observed on RAMP until July 27, 2021, when the access became was restricted.

### Background

The Babuk ransomware group came into the spotlight at the beginning of the year 2021 but the gang [said that their attacks have started in October 2020](#). The group operated as ransomware-as-a-service (RaaS), and was publicly hiring affiliates on two major Russian-speaking forums, XSS and Exploit, since March 2021.

One of the gang's most notable attacks was carried out against Washington DC's Metropolitan Police Department that took place in April 2021. The gang said they had compromised the DC Police's networks and stolen 250 GB of unencrypted files. Some of them were published on their site.



*Babuk posts claiming to have compromised Washington DC's Metropolitan Police Department*

Shortly after the attack, the chaos surrounding the Babuk RaaS closure started. First, the gang stated it is closing the operation and promised to publish the source code of its malware to enable other threat actors to create their own ransomware. Then, the Babuk ransomware developers deleted the post and published a new announcement claiming they plan to continue breaching companies but instead of stealing sensitive files and encrypting local data, the group plans only to steal it. However, that second announcement was also deleted. On May 15, 2021, the Babuk representative stated on one of the forums that their RaaS affiliate program was closed.

### Hello World 3

I not so long ago wrote about the closure of babuk, yes, you all correctly understood babuk as a RaaS will be closed, but it will live in its new understanding, we are a promoted brand with the best pentesters of dark net

We are a young project and everyone already knows about us, during this time we have gone ahead of other groups, we respect other groups but not all

Babuk changes direction, we no longer encrypt information on networks, we will get to you and take your data, we will notify you about it if you do not get in touch we make an announcement.

Also for other groups that do not have their own blog or have but they want to exert additional pressure you can not be placed with us

### Hello world 4

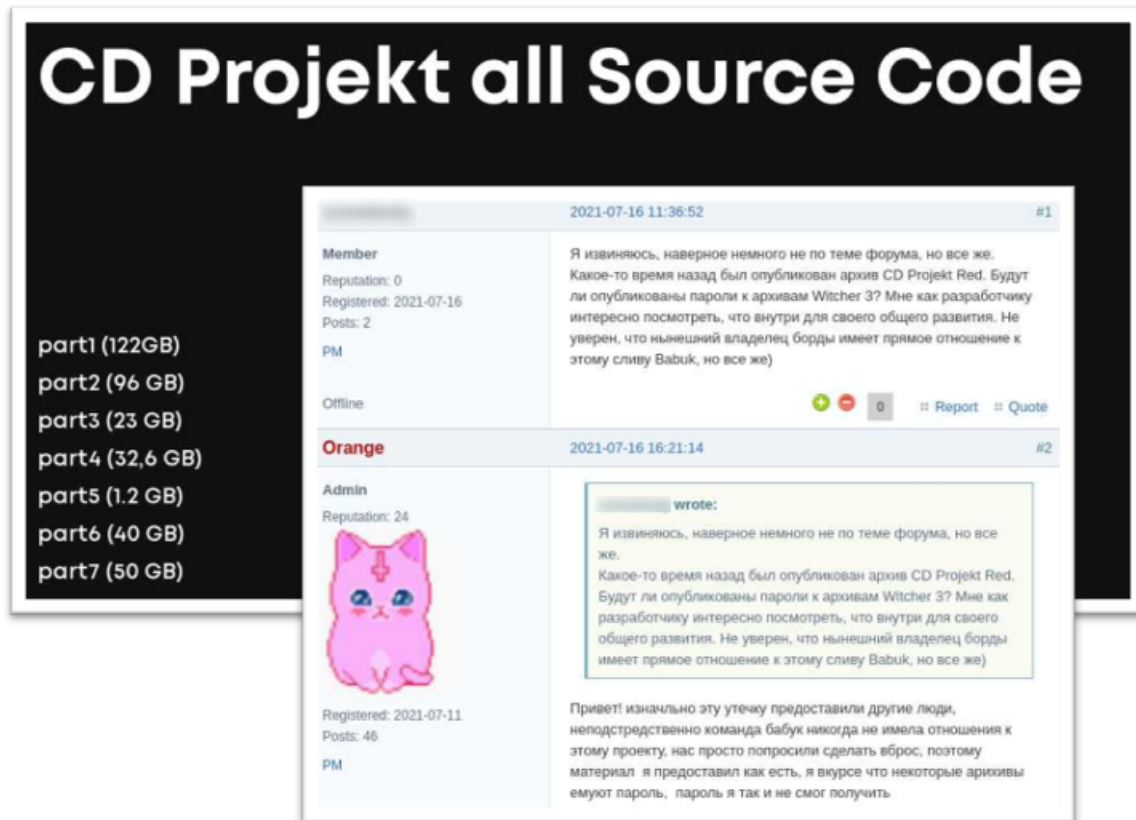
Hello! We announce the development of something really cool, a huge platform for independent leaks, we have no rules and bosses, we will publish private products in a single information platform where we will post leaks of successful no-name teams that do not have their own blogs and names, these are not girls who run with ship like rats and change the policy of their resources. these are really strong guys.

Another loud leak awaits you within a week.

*Babuk announcements of coming changes of their leak site and RaaS*

On June 1, 2021, KELA observed several changes in the content and appearance of the Babuk site. The domain used by Babuk showed a page titled "Payload.bin" with the following message on the front page: "Welcome to Leaks site created by Payload.bin." It appeared that this Payload.bin site was the promised site for leaking the stolen data.

However, only one victim was listed on the site – Polish game developer CD Projekt Red. Interestingly enough, the company fell victim to HelloKitty ransomware in February 2021. Then, the data allegedly stolen during the attack was traded on an auction on the cybercrime forum Exploit. The sellers claimed the data was sold outside of the forum. Interestingly, one of the RAMP users asked about the origins of this leak being posted on Payload.bin. The admin claimed the Babuk gang did not attack the company and they just provided a place for the leak: "The Babuk team never had anything to do with this project, we were just asked to post it, so I provided the material as it is."



*The leak of CD Projekt's data on Payload.bin and an explanation of this leak on RAMP*

On June 27, 2021, a builder (source code) for the Babuk ransomware was [uploaded to VirusTotal](#). This builder could be used to create custom versions of the Babuk ransomware and generate decrypters. Researchers speculated the code could be leaked by former members of the groups or rivals.

On July 1, 2021, it became known that Babuk launched a new leak site stating the operation continues under the name Babuk 2.0. The gang claimed the old version of Babuk ransomware was leaked, while the new version is being used in ongoing attacks.

On July 12, 2021, KELA noticed that the former Babuk ransomware gang's leak site had changed again and was now hosting a forum named RAMP. A new admin initially named TetyaSluha (now Orange) announced it is now a place where ransomware affiliates can be protected from unscrupulous RaaS programs. The admin claimed that following the ransomware ban on other forums, he wanted to create a new community. The name of the new forum is a reference to the now-defunct Russian Anonymous Marketplace

(a drug market that closed in 2017). So the big question comes down to: *What's in this "marketplace"?*

## The Admin's Connections to Babuk

The fact that the RAMP site is hosted on the same domain that once was Babuk's leak site and then Payload.bin hints that the administrator is somehow related to Babuk. On May 13, 2021, in the post promising to leak the data of Washington DC's Metropolitan Police Department, the author stated: "I handed over the source code to another team, which will continue to develop the product under a different brand, I remain the only owner of the domain and blog, my service will continue to develop." It seems that the post author is the future admin of Payload.bin and RAMP.

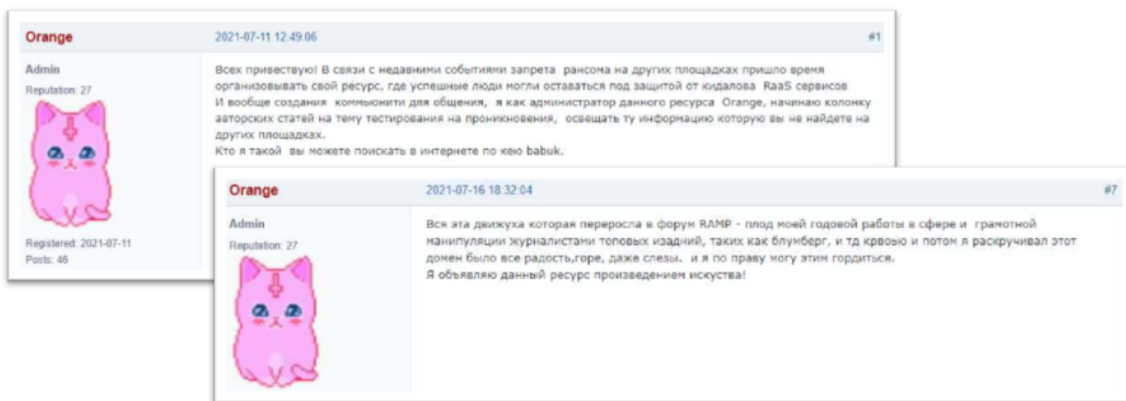
## More DC Metro Police Data



We publish the full data of the police department, including HR, Gang Database, you will find a full range of all data in the amount of 250GB in all parts, this is an indicator of why we should pay, the police also wanted to pay us, but the amount turned out to be too small. look at this wall of shame, you have every chance of not getting there, just pay us! Regarding our old promises regarding the source code of the babuk. I handed over the source code to another team, which will continue to develop the product under a different brand, I remain the only owner of the domain and blog, my service will continue to develop, we are not going to close and change the policy of our work, we advise our colleagues to leave public RaaS.

**Announcement about handing over source code and remaining an owner of the domain, most likely written by the current RAMP admin**

When announcing the forum's opening, the admin stated: “[If you want to know – KELA] who I am you can search online for the Babuk key.” The mention of “Babuk key” probably meant the builder leak mentioned above. In addition, the admin said: “All this activity that grew into the RAMP forum is the result of my year'-long work in the field and the competent manipulation of journalists from top outlets, such as Bloomberg, and so on. I promoted this domain through blood and sweat.” This again implies that the admin was involved in the Babuk operation from the beginning.




**The RAMP admin's announcement about the RAMP launch and his affiliation with the Babuk team and the domain**

Moreover, when sharing the Babuk builder on RAMP, the admin claimed: “A guy who made Babuk for me just took the Darkside ESX locker and reversed it. I can't tell if there is a problem with the ESX [version] because I've used it only for three companies.” From this and other posts sharing insights on how to attack the company's network, we can suggest that the admin was conducting ransomware attacks by himself.

The admin said that now he is not affiliated with the gang and even stated: “I recommend to blacklist this product to all security firms and data security [specialists].”

Orange 2021-07-18 14:31:07 #5

**Admin**  
Reputation: 24



Registered: 2021-07-11  
Posts: 46

**wrote:**  
Хуево, хотел накрыть всферу из соседней темы  
Кто-то смотрел есхи локеры от ревил?там ключи  
захардкожены или в параметрах указываются?

Дам наводку, поц что делал мне бабука просто взял локер esx дарк сайда и разревелсил его.  
я не могу точно тебе сказать есть ли проблема с esx, так как ставил я им 3 конторы  
1 из 2х расшировалась, да если бы не было бы проблемы с esx, думаешь я бы его сбрасывал в паблик?

*The RAMP admin's post about the Babuk ESXi version being based on the DarkSide ESXi version*

## RAMP Forum's Contents

The new forum is Russian-speaking and named RAMP in honor of the now-defunct Russian drug marketplace, but its purpose is far away from selling drugs. The admin who renamed himself to Orange (the old RAMP's admin's handle) claimed the forum will be a community for various cybercriminals, including ransomware developers and affiliates [recently banned on XSS and Exploit](#). He stated the forum's full name is "Ransom Anon Mark Place." Rules of the forum stated that members are prohibited from attacking Russia and CIS countries (which is [common for such forums](#)), using multiple accounts, spamming, and performing some other actions. Curiously, the moderators claimed it is prohibited to propagate "different actions going against Criminal Code of RF [Russian Federation]."

2021-07-15 20:17:32 #1

Moderator  
Reputation: 10  
From: the middle of nowhere  
Registered: 2021-07-14  
Posts: 21  
PM

*не знание не освобождает от ответственности*

*запрещено!*

*работа в сфере по гео РФ и СНГ*

*мультиакаунт*  
*спам*  
*попрошайничество*  
*шантаж*

*избыток цитат*  
*оскорбление на все почвах*  
*жульничество с репутацией*  
*угрозы*

*выяснение отношений не относящихся к тематике площадки*

*пропаганда ПАВ*  
*пропаганда суицида*

*пропаганда терроризма*  
*пропаганда насилия*  
*пропаганда любого порна*  
*пропаганда нарушения закона*  
*пропаганда метяжа*

*пропаганда всяческого рода деятельности перечисленной УК РФ*  
*деанон(исключение: доказанное недопропорядочное действие)*

*P.S. под словом "пропаганда" подразумевается любое упоминание и любые материалы связанные с вышеперечисленными вещами*

*правила будут дополняться*  
**RAMP rules**

The forum has multiple sections typical for such cybercrime forums, with a general notice “welcoming” both RaaS and other services. Two sections that attract a particular interest are called “Vendor” and “Affiliate Programs” – they are intended for “people and services in which we [administration – KELA] and our community trust.” As such, KELA observed a thread dedicated to the LockBit 2.0 affiliate program thread. In the thread, a user named LockBit (most likely the gang’s representative) claimed he will launch the LockBit 2.0 ransomware ESXi version soon.





*LockBit 2.0 thread on RAMP*

Since Initial Access Brokers' services are on the rise, the forum offers a section for access listings. Moreover, in honor of the forum's launch, some accesses through Fortinet VPN were offered for free. The access listings seem to be unique; the forum moderators promised to change them periodically to avoid multiple targeting.


The forum also has a section "Tools" for selling/sharing exploits and malware, though its contents so far do not seem to be unique. Interestingly, the Babuk builder was shared again in this section by the admin who specified that the builder works fine for encrypting/decrypting files on Windows computers. He mentioned that the VMware ESXi version does not enable users to decrypt files.

Other sections are intended for sharing articles about hacking, chatting, and discussing the forum.

## The Spam Incident and the Building of the Forum

The site, built on the FluxBB engine, experienced a spam attack. On July 23, 2021, a threat actor created a thread where he demanded a 5,000 USD ransom to avoid spamming. Apparently, the admin didn't pay the ransom

and over a few coming days, multiple users were posting porn GIFs in all sections and threads in the forum. Following the incident, many users were deleted from the forum. The admin (who previously looked for someone capable of auditing the forum's security for 2,000 USD) stated the forum will be relaunched using a new engine built from scratch. First, the admin "cleaned" the forum and deleted most of the users. On July 27, 2021, he restricted access to the forum.

|  |   |    |
|--|---|----|
| <b>Orange</b>  | 2021-07-11 13:44:52   | #1 |
| <b>Admin</b><br>Reputation: 24<br> | Требуется специалист для аудита безопасности форума, без доступа к его ядру, аудит методом blackbox.<br>От вас отчет с меня оплата в 2000 usd.<br><br>Критерии для кандидатов:<br>1) У вас есть профили на площадках xss, exploit<br>2) У вас есть отзывы<br>3) Когда либо сталкивались с форумом FluxBB<br><br>Писать в лс |    |

*The RAMP admin's announcement of looking for a specialist to make a security audit of the forum*

## Forum's Perspectives

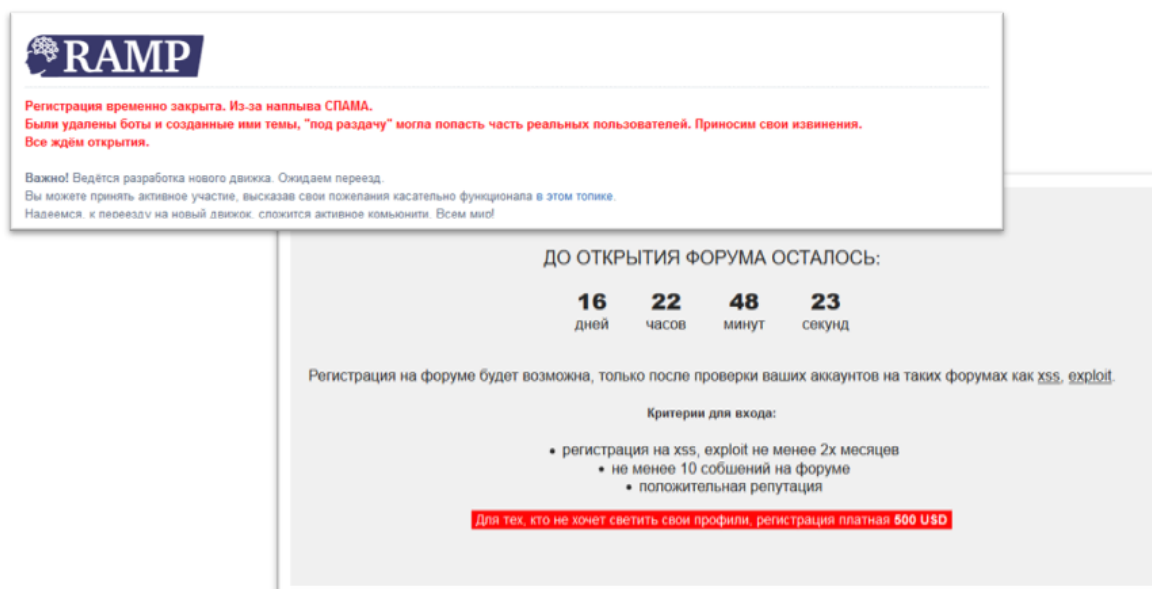
The forum seemed to attract some interest from members of other cybercrime forums: KELA observed several users registered with the same handles as on two major Russian-speaking forums. Due to the "cleaning" of the forum, on July 26, 2021, the number of users was 59 who seem to be the users that somehow participated in the forum discussion. During the first ten days of its existence and before the wave of spammers the number of registered users was around 350. The number of published posts was above 100.

This pace was impressive, however, after the spam incident and deleting of the users it will definitely slow down. The registration is now closed.

According to a message now appearing on the homepage, on August 13, 2021, the forum will be relaunched and registration will become available based on certain conditions. Those include users registered on XSS and Exploit for more than 2 months, with more than 10 messages on a forum and a positive reputation. An alternative option is to pay a registration fee of

500 USD, which seems to be exaggerated compared to other forums. For example, a premium user on XSS costs 120 USD for a year. Moreover, Russian cybercriminals are not used to paying money for registration on forums, especially such a (relatively) big sum.

Once the forum will be relaunched, it is possible that cybercrime actors tired of the ransomware ban will try it out. So far, the welcoming of the RaaS programs and their affiliates is the only competitive advantage of RAMP. It seems it is the only factor that can attract users from other well-established forums. As for the demand of ransomware groups for Initial Access Brokers, intrusion specialists, and other partners, they can still find them on existing forums.



The screenshot shows the RAMP forum homepage. At the top left is the RAMP logo. Below it, a red text box contains the following message: "Регистрация временно закрыта. Из-за наплыва СПАМА. Были удалены боты и созданные ими темы, "под раздачу" могла попасть часть реальных пользователей. Приносим свои извинения. Все ждем открытия." Below this, a blue text box says: "Важно! Ведётся разработка нового движка. Ожидаем переизд. Вы можете принять активное участие, высказав свои пожелания касательно функционала в этом топике. Надеемся к переизд на новый движок, сложится активное комьюнити. Всем мир!" In the center, a countdown timer displays: "ДО ОТКРЫТИЯ ФОРУМА ОСТАЛОСЬ:" followed by "16 дней", "22 часов", "48 минут", and "23 секунд". Below the timer, a message states: "Регистрация на форуме будет возможна, только после проверки ваших аккаунтов на таких форумах как [xss](#), [exploit](#)". Underneath, the criteria for entry are listed: "Критерии для входа: • регистрация на xss, exploit не менее 2х месяцев • не менее 10 сообщений на форуме • положительная репутация". At the bottom, a red text box reads: "Для тех, кто не хочет светить свои профили, регистрация платная 500 USD".

Frontpage of RAMP as seen on July 26 and on July 27, 2021

The success of the forum also depends on the interest of ransomware groups in publicly recruiting affiliates again. Some players (like Avaddon and REvil) closed their RaaS or disappeared from the public space. However, there are new groups that can use a new community to promote their RaaS. If the admins can leverage their competitive advantage of welcoming RaaS programs, chances to grow are fairly high.