How Groove Gang is Shaking up the Ransomware-as-a-Service Market to Empower Affiliates

By Max Kersten, John Fokker and Thibault Seret on Sep 08, 2021
Co-authored with Intel471 and McAfee Enterprise Advanced Threat Research (ATR) would also like to thank Coveware for its contribution.

Executive Summary

McAfee Enterprise ATR believes, with high confidence, that the Groove gang is associated with the Babuk gang, either as a former affiliate or subgroup. These cybercriminals are happy to put aside previous Ransomware-as-a-Service hierarchies to focus on the ill-gotten gains to be made from controlling victim's networks, rather than the previous approach which prioritized control of the ransomware itself.

Introduction

For many years the world of Ransomware-as-a-Service (RaaS) was perceived as a somewhat hierarchical and structured organization. Ransomware developers would advertise their RaaS program on forums and gracefully open up slots for affiliates to join their team to commit crime. The RaaS admins would conduct interviews with potential affiliates to make sure they were skilled enough to participate. Historically, i.e., with CTB locker, the emphasis was on affiliates generating enough installs via a botnet, exploit kits or stolen credentials, but it has shifted in recent years to being able to penetrate and compromise a complete network using a variety of malicious and non-malicious tools. This essentially changed the typical affiliate profile towards a highly-skilled pen-tester/sysadmin.
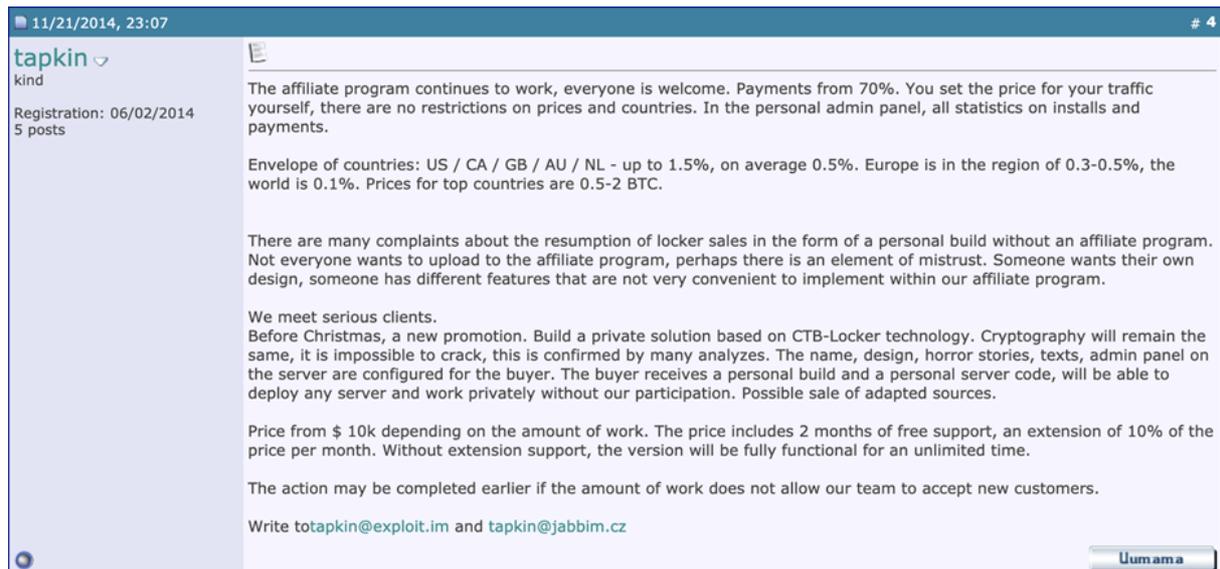
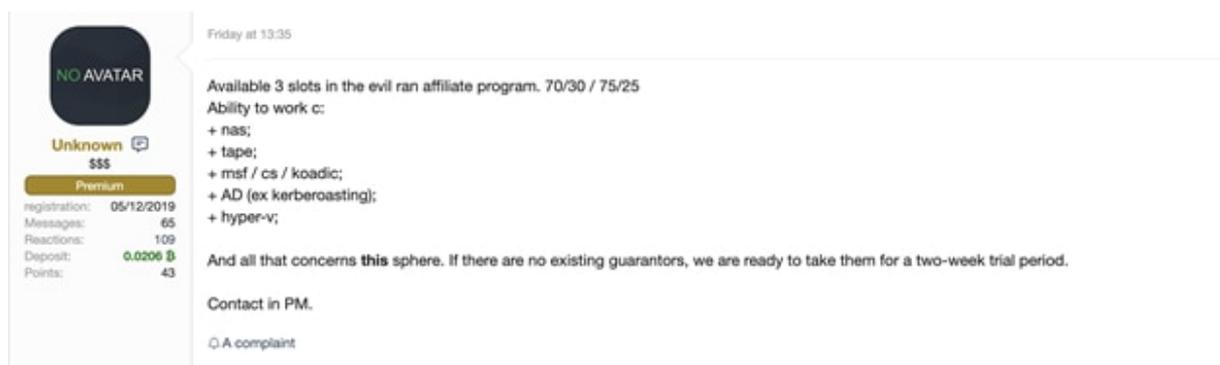*Figure 1. Recruitment posting for CTB locker from 2014*

Figure 2. Recruitment posting for REvil from 2020

Experts often describe the hierarchy of a conventional organized crime group as a pyramid structure. Historically, La Cosa Nostra, drug cartels and outlaw motor gangs were organized in such a fashion. However, due to further professionalization and specialization of the logistics involved with committing crime, groups have evolved into more opportunistic network-based groups that will work together more fluidly, according to their current needs.

While criminals collaborating in the world of cybercrime isn't a novel concept, a RaaS group's hierarchy is more rigid compared to other forms of cybercrime, due to the power imbalance between the group's developers/admins and affiliates.

For a long time, RaaS admins and developers were prioritized as the top targets, often neglecting the affiliates since they were perceived as less-skilled. This, combined with the lack of disruptions in the RaaS ecosystem, created an atmosphere where those lesser-skilled affiliates could thrive and grow into very competent cybercriminals.

However, this growth isn't without consequences. Recently we have observed certain events that might be the beginning of a new chapter in the RaaS ecosystem.

Cracks in the RaaS model

Trust in the cybercriminal underground is based on a few things, such as keeping your word and paying people what they deserve. Just like with legitimate jobs, when employees feel their contributions aren't adequately rewarded, those people start causing friction within the organization. Ransomware has been generating billions of dollars in recent years and with revenue like that, it's only a matter of time before some individuals who believe they aren't getting their fair share become unhappy.

Recently, a former Conti affiliate was unhappy with their financial portion and decided to disclose the complete Conti attack playbook and their Cobalt Strike infrastructure online, as shown in the screenshot below.
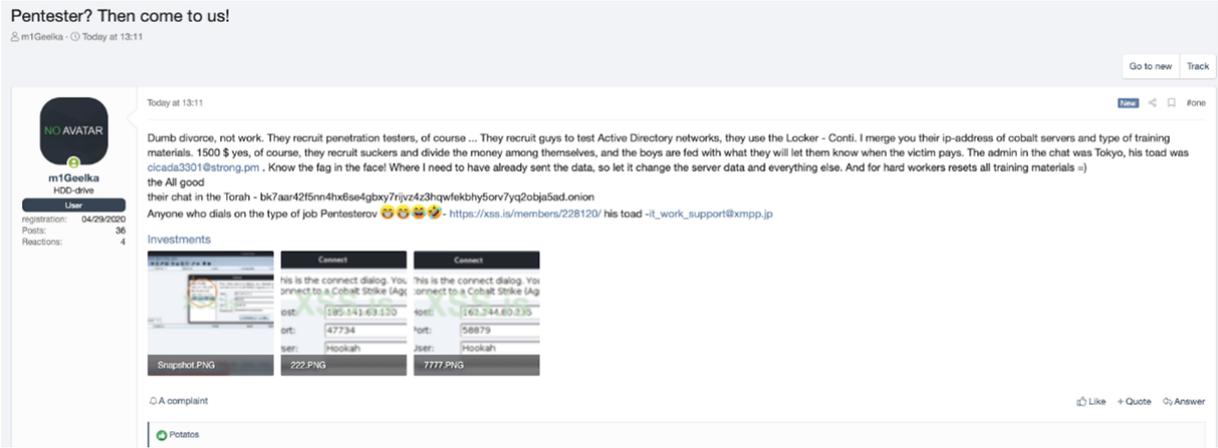

Figure 3. Disgruntled Conti affiliate

In the past, ATR has been approached by individuals affiliated with certain RaaS groups expressing grudges with other RaaS members and admins, claiming they haven't been paid in time or that their share wasn't proportionate to the amount of work they put in.

Recently, security researcher Fabian Wosar opened a dedicated Jabber account for disgruntled cybercriminals to reach out anonymously and he stated that there was a high level of response.

Figure 4. Jabber group for unhappy threat actors

Moreover, the popular cybercrime forums have banned ransomware actors from advertising since the Colonial Pipeline attack. Now, the groups no longer have a platform on which to actively recruit, show their seniority, offer escrow, have their binaries tested by moderators, or settle disputes. The lack of visibility has made it harder for RaaS groups to establish or maintain credibility and will make it harder for RaaS developers to maintain their current top tier position in the underground.

Paying respects…. RAMP Forum and Orange

After a turbulent shutdown of Babuk and the fallout from the Colonial Pipeline and Kaseya attacks, it seems that some of the ransomware-affiliated cybercriminals have found a home in a forum known as RAMP.

🔒 Публикация закрыта

Рынок → Работа

[Конкурс] WEB разработчиков 1000 USD

👤 **Orange** Администратор

AYESHA PRAKASH VP Global   💬 1   👁 85

Опубликован: 23 Августа 2021 в 00:02

Здравствуйте.Друзья! Я торжественно объявляю первый конкурс на рампе.

Сразу хочу сказать: мы ничего не делаем просто так, даже этот конкурс нужен впервую очередь нам:)

Суть: помимо новых и старых проектов у меня всегда было подразделение которое называлось

GROOVE, я никогда не афишировал его название и напрямую не упоминали в СМИ, но оно существует, мы как МОСАД (нас мало и в груп мы больше никого не берем) результат работы groove это весь пиар **babuk локера**.

Groove сила, babuk могила :)

Задача конкурсатнов: Используя стек PHP+MYSQL+бутстрап   написать стандартный рансом блог на **РУССКОМ ЯЗЫКЕ** со следующими страницами:

1)О нас

Это описание группы, должно редактироваться из админки и использоваться такой же визуальный редактор как у нас на форуме.

2)Утечки.

Тут не будет хидден блогов только утечки.

Исопльзовать стандартный вывод как у других рансом блогов.

3)Новости

Страничка новостей все должно редактироваться и добавляться из админки.

Прием работ до **30** августа включительно.

Кто и как будет оценивать?

Победитель только 1 я Orange оцениваю юзабилити и дизайн. MRT исходный код и его безопасность. Помимо 1к usd победитель скорей всего получит работу в команде **RAMP!**

Для тех кому нужно совсем другое:

1)Нет мы не спецслужбы казахстана.

https://www.fr.sogeti.com/globalassets/france/avis-dexperts--livres-blancs/cybersecchronicles_-_babuk.pdf

2)У groove никогда небыло и не будет Ransomware продукта

3)Команды бабук не существует мы его брали в аренду у кодера который не повез взятую на себя ответственность испугался и нарошно сделал ошибку в esx билдере, ественно для того что бы мы его отправили куда подальше (его мотивация? а вот хуй его знает)

babuk 2.0 о чем писали журналисты считать высером каких то клоунов

4)GROOVE это впервую очередь агрессивно настроеная финансово мотивированная преступная групировка занимающаяся промышленым шпионажем около 2х лет RANSOMWARE как дополнительный источник денег не более, нам нет разницы с кем работать и как работать. у вас есть деньги? Мы работаем с вами

Figure 5. RAMP posting by Orange, introducing Groove and explaining relationships

Translated Posting

When analyzing RAMP and looking at the posting above from the main admin Orange, it's hard to ignore numerous references that are made: From the names chosen, to the avatar of Orange's profile, which happens to be a picture of a legitimate cyber threat intelligence professional.

Orange

Hello, friends! I am happy to announce the first contest on Ramp.

Let's make it clear that we don't do anything without a reason, so at the end of the day, it's us who will benefit most from this contest 🙂

Here's the thing: besides my new projects and old, I have always had this unit called

GROOVE — I've never revealed its name before and it's never been mentioned directly in the media, but it does exist — we're like Mossad (we are few and aren't hiring). It's Groove whom the babuk ransomware needs to thank for its fame.

Groove rocks, and babuk stinks 🙂

Challenge: Using a PHP stack+MYSQL+Bootstrap, code a standard ransomware operators' blog in THE RUSSIAN LANGUAGE with the following pages:

1) About us

The description of a group, which must be editable from the admin panel and use the same visual editor as our forum.

2) Leaks.

No hidden blogs, just leaks.

Use standard display, just like other ransomware operators' blogs do.

3) News

A news page; it must be possible to add and edit news via the admin panel.

We'll be accepting your submissions up to and including August 30.

Who will rate the entries and how?

There will be only one winner. I, Orange, will rate the usability and design of blogs. MRT will rate each entry's source code and its security. In addition to USD 1k, the winner will most likely get a job in the RAMP team!

Now, for those of you who are interested in entirely different things:

1) No, we are not with the Kazakh intelligence agency.

https://www.fr.sogeti.com/globalassets/france/avis-dexperts–livres-blancs/cybersecchronicles_-_babuk.pdf

2) Groove has never had a ransomware product, nor will that ever change.

3) The babuk team doesn't exist. We rented the ransomware from a coder who could not shoulder the responsibility, got too scared and decided to leave an error in the ESX builder — naturally, to give us a reason to chuck him out (his motives? Fxxx if I know)

babuk 2.0, which hit the headlines, is not to be taken seriously and must be regarded as nothing but a very stupid joke

4) GROOVE is first and foremost an aggressive financially motivated criminal organization dealing in industrial espionage for about two years. RANSOMWARE is no more than an additional source of income. We don't care who we work with and how. You've got money? We're in

RAMP Ransom Anon Mark[et] Place

RAMP was created in July 2021 by a threat actor TetyaSluha, who later changed their moniker to 'Orange.' This actor claimed the forum would specifically cater to other ransomware-related threat actors after they were ousted from major cybercrime forums for being too toxic, following the high-profile ransomware attacks against the Colonial Pipeline and Washington D.C.'s Metropolitan Police Department in the spring of 2021.

At the time of the initial launch, Orange claimed the forum's name was a tribute to a now-defunct Russian-language underground drug marketplace, "Russian Anonymous Marketplace," which was taken down by Russian law enforcement agencies in 2017. The re-

launched cybercrime forum's name now supposedly stands for "Ransom Anon Mark[et] Place".

The forum was initially launched on the same TOR-based resource that previously hosted a name-and-shame blog operated by the Babuk ransomware gang and the Payload.bin marketplace of leaked corporate data. The forum was later moved to a dedicated TOR-based resource and relaunched with a new layout and a revamped administrative team, where Orange acted as the admin, with other known actors MRT, 999 and KAJIT serving as moderators.

Why the name Orange?

Why the admin changed handles from TetyaSluha to Orange isn't 100 percent clear. However, looking back, the early days of RAMP provides us some evidence on who this person has been affiliated with. We found a posting from where the names Orange and Darkside are mentioned as potential monikers. Very shortly after that, TetyaSluha changed their handle to Orange. While the initial message has been removed from the forum itself, the content was saved thanks to Intel 471.

July 12th 2021 by Mnemo

Congratulations on the successful beginning of struggle for the right to choose and not to be evicted. I hope, the community will soon fill with reasonable individuals.

*Oh yeah, you've unexpectedly reminded everyone about the wonderful RAMP forum. Are the handles **Orange** and **Darkside** still free?*

The name Darkside might sound more familiar than Orange but, as we saw with the naming of RAMP, TetyaSluha is one for cybercrime sentiment, so there is almost certainly some hidden meaning behind it.

Based on ATR's previous research, we believe the name Orange was chosen as a tribute to REvil/GandCrab. People familiar with those campaigns have likely heard of the actor 'UNKN'. However, there was a less well known REvil affiliate admin named Orange. A tribute seems fitting if Tetyasluha isn't the notorious Orange as that moniker is tied to some successful ransomware families, GandCrab and REvil, that shaped the RaaS ecosystem as we know it today.

In the past, UNKN was linked to several other monikers, however Orange was hardly mentioned since there wasn't a matching public handle used on any particular cybercrime forum. However, REvil insiders will recognize the name Orange as one of their admins.

Based on ATR's closed-source underground research, we believe with a high level of confidence, that UNKN was indeed linked to the aforementioned accounts, as well as the

infamous "Crab"handle used by GandCrab. Crab was one of the two affiliate-facing accounts that the GandCrab team had (The other being Funnycrab). We believe with a high level of confidence that after the closure of GandCrab, the individual behind the Funnycrab account changed to the account name to Orange and continued operations with REvil, with only a subset of skilled GandCrab affiliates, (as described in our Virus Bulletin 2019 whitepaper) since GandCrab grew too big and needed to shed some weight.

The posting in figure 5 is also shedding some light on the start of the Groove Gang, their relationship to Babuk and, subsequently, BlackMatter.

Groove Gang

In the post from Figure 5, "Orange" also claims to have always had a small group of people that the group collaborates with. Additionally, the actor claims that the name has not been mentioned in the media before, comparing the group to the Israeli secret service group Mossad. The group's comparison to Mossad is extremely doubtful at best, given the drama that has publicly played out. Groove claims several of Babuk's victims, including the Metropolitan Police Department, brought them a lot of attention. The several mentions to Babuk isn't by mistake: we have evidence the two groups also have connections, which we've pieced together from examining the behavior of — and particularly the fallout between — the two groups.

Babuk's Fallout

Originally, the Babuk gang paid affiliates by each victim they attacked. Yet on April 30, it was reported that the gang suddenly had stopped working with affiliates, including the act of encrypting a victim's system. Instead, their focus shifted to data exfiltration and extortion of targeted organizations. That was followed by the group releasing the builder for the old versions of its ransomware as it pivoted to a new one for themselves.

The attention that Babuk drew by hacking and extorting the Metropolitan Police Department meant their brand name became widely known. It also meant that more firms and agencies were interested in finding out who was behind it. This kind of heat is unwanted by most gangs, as any loose ends that are out there can come back to bite them.

Then, on September 3, the threat actor with the handle 'dyadka0220' stated that they were the principal developer of Babuk ransomware and posted what they claimed was the Babuk ransomware source code. They claimed the reason they were sharing everything was due to being terminally ill with lung cancer.
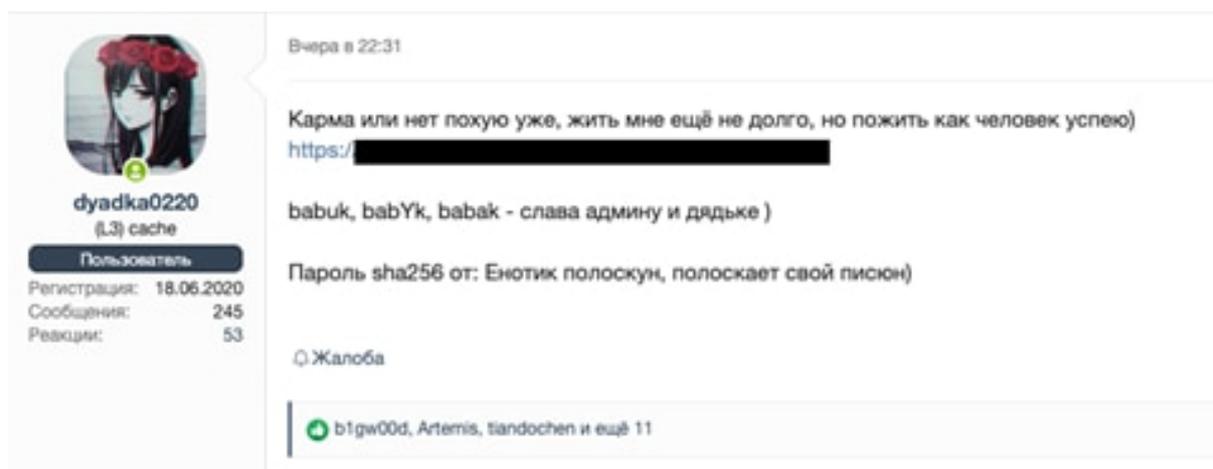
On September 7, the Groove gang responded with a blog on their own website, titled "Thoughts about the meaning", which rhymes in Russian. In this blog, the gang (allegedly) provides information on several recent happenings. Per their statement, the illness of 'dyadka0220' is a lie. Additionally, their response alleges that the Groove gang never created the Babuk ransomware themselves, but worked with someone else to produce it.

The validity of the claims in Groove's latest blog is hard to determine, although this does not matter too much: the Babuk group, including affiliates, had a fallout that caused the group to break up, causing the retaliation of several (ex-)members.

Observed Behavior

The ATR team has covered Babuk multiple times. The first blog, published last February, covers the initial observations of the group's malware. The second blog, published last July, dives into the ESXi version of the ransomware and its issues. The group's tactics, techniques, and procedures (TTPs) are in-line with commonly observed techniques from ransomware actors. The deployment of dual-use tools, which can be used for both benign and malicious purposes, is difficult to defend against, as intent is an unknown term for a machine. Together with other vendors we have narrowed down some of the TTPs observed by the Groove gang.

Initial Access

The actor needs to get a foothold within the targeted environment. The access can be bought, in terms of stolen (yet valid) credentials, or direct access in the form of a live backdoor on one or more of the victim's systems. Alternatively, the actor can exploit publicly facing infrastructure using a known or unknown exploit. To ATR's understanding, the latter has been used several times by exploiting vulnerable VPN servers.

Lateral Movement, Discovery and Privilege Escalation

Moving around within the network is an important step for the actor, for two reasons. Firstly, it allows the attacker to find as much data as possible, which is then exfiltrated. Secondly, access to all machines is required in order to deploy the ransomware at a later stage. By encrypting numerous devices at once, it becomes even harder to control the damage from a defender's point of view. The actor uses commonly known tools, such as Ad-Find and NetScan, to gather information on the network. Based on the gathered information, the actor will move laterally through the network. One of the most frequently observed methods by this actor to do so, is by using RDP.

To work with more than user-level privileges, the actor has a variety of options to escalate their privilege to a domain administrator. Brute forcing RDP accounts, the dumping of credentials, and the use of *legacy* exploits such as EternalBlue (CVE-2017-0144), are ways to quickly obtain access to one or more privileged accounts. Once access to these systems is established, the next phase of the attack begins.

Data Exfiltration and Ransomware Deployment

The actor navigates through the machines on the network using the earlier obtained access. To exfiltrate the collected data, the attacker uses WinSCP. Note that other, similar, tools can also be used. Once all relevant data has been stolen, the attacker will execute the ransomware in bulk. This can be done in a variety of ways, ranging from manually starting the ransomware on the targeted machines, scheduling a task per machine, or using PsExec to launch the ransomware.

Linking Groove to Babuk and BlackMatter

As discussed above, there was a fallout within Babuk. From that fallout, a part of the group stayed together to form Groove. The server that Babuk used, which we will refer to as the "wyyad" server due to the ending of the onion URL, rebranded in late August 2021. The similarities can be seen in the two screenshots below.

Figure 7. The changes to the landing page from Babuk to Groove

Aside from this, data from old Babuk victims is still hosted on this server. The ATR team found, among others, leaks that belong to:

- a major US sports team,
- a British IT service provider,
- an Italian pharmaceutical company,
- a major US police department,
- a US based interior shop.

All these victims have previously been claimed by (and attributed to) Babuk.

Another gang, known as BlackMatter, uses a variety of locations to host their extorted files, which can be done out of convenience or to avoid a single notice and takedown to remove all offending files. Additionally, the ATR team assumes, with medium confidence, that different affiliates use different hosting locations.

The data of one of the BlackMatter gang's victims, a Thai IT service provider, is stored on the "wyyad" server. As such, it can mean that the Groove gang worked as an affiliate for the BlackMatter gang. This is in line with their claim to work with anybody, as long as they profit from it. The image below shows the BlackMatter leak website linking to the "wyyad" server.
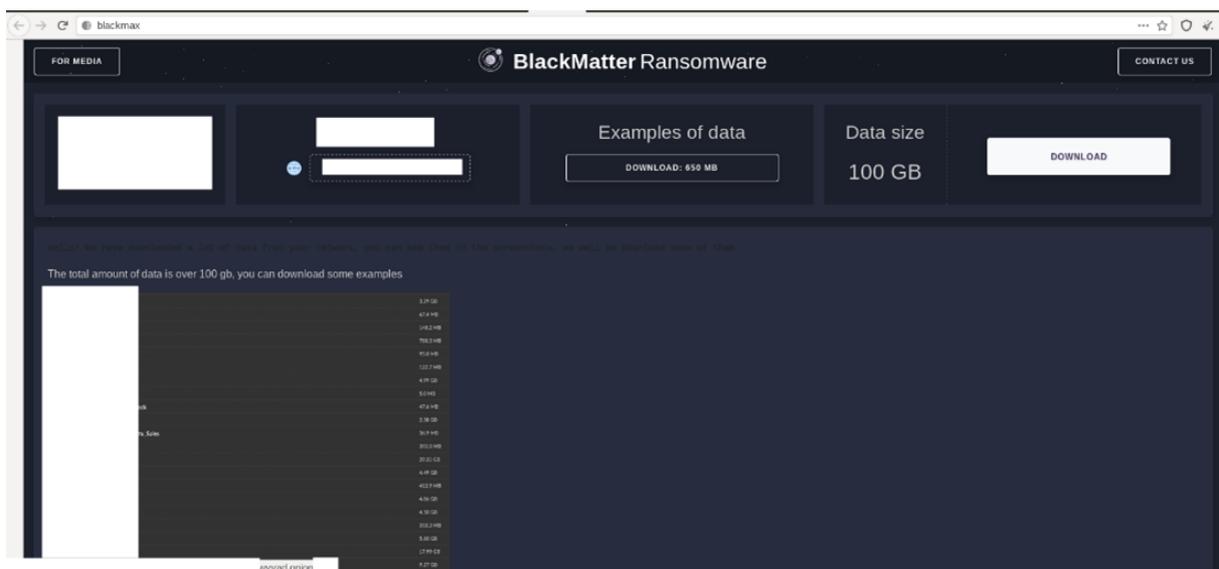
Figure 8. screenshot of BlackMatter, where the data is stored on the Groove server

The Groove gang's website contains, at the time of writing, a single leak: data from a German printing company. Even though the website is accessible via a different address, the leaked data is stored on the "wyyad" server.

Figure 9. Another Groove victim but stored on their own page

The affected company does not meet BlackMatter's "requirements," the group has said it only goes after companies that make more than $US 100 million. This company's annual revenue is estimated at $US 75 million, as seen in the below screenshot.

At the end of Orange's announcement comes a call to action and collaboration: "GROOVE is first and foremost an aggressive financially motivated criminal organization dealing in industrial espionage for about two years. RANSOMWARE is no more than an additional source of income. We don't care who we work with and how. You've got money? We're in".

The group's primary goal, making money, is not limited to ransomware. Inversely, ransomware would be the cherry on top. This is yet another indication of the ransomware group's shift to a less hierarchical set-up and a more fluid and opportunistic network-based way of working.

In the Groove gang's blog on September 7, a reference is made with regards to BlackMatter, and its links to DarkSide. If true, these insights show that the Groove gang has insider knowledge of the BlackMatter gang. This makes the collaboration between Groove and BlackMatter more likely. If these claims are false, it makes one wonder as to why the Groove gang felt the need to talk about other gangs, since they seem to want to make a name for themselves.

Due to the above outlined actions ATR believes, with high confidence, that the Groove gang is a former affiliate or subgroup of the Babuk gang, who are willing to collaborate with other parties, as long as there is financial gain for them. Thus, an affiliation with the BlackMatter gang is likely.

Conclusion

Ever since Ransomware-as-a-Service became a viable, and highly profitable, business model for cybercriminals, it has operated in much the same way with affiliates being the sometimes underpaid workhorses at the bottom of a rigid pyramid shaped hierarchy.

For some affiliates there was an opportunity to become competent cybercriminals while, for many others, the lack of recompense and appreciation for their efforts led to ill-feeling. Combined with underground forums banning ransomware actors, this created the perfect opportunity for the threat actor known as Orange to emerge, with the Groove gang in tow, with the offer of new ways of working where an associate's worth was based entirely on their ability to earn money.

Time will tell if this approach enhances the reputation of the Groove gang to the level of the cybercriminals they seem to admire. One thing is clear though; with the manifestation of more self-reliant cybercrime groups the power balance within the RaaS eco-climate will change from he who controls the ransomware to he who controls the victim's networks.

MITRE TTPs

We have compiled a list of TTPs based on older Babuk cases and some recent cases linked to Groove:

- T1190: Exploit Public-Facing Application (VPN services)
- T1003: OS Credential Dumping
- 002: Valid Accounts: Domain Accounts
- T1059: Command and Scripting Interpreter
- T1021:002: SMB/Windows Admin Shares
- T1210: Exploitation of Remote Services
- T1087: Account Discovery
- T1482: Domain Trust Discovery
- T1562: Impair Defense
- T1537: Transfer Data to Cloud Account
- T1567: Exfiltration Over Web Service

If a partnership is achieved with a Ransomware family:

- T1486 Data Encrypted for Impact