Groove VS Babuk; Groove Ransom Manifesto & RAMP Underground Platform Secret Inner Workings

By Yelisey Boguslavskiy & Anastasia Sentsova

Key Takeaways:

- On September 7, 2021, a representative of the Groove ransomware syndicate shared their experience-based perspective on inner aspects of ransomware business, including the "truth" about the association of Babuk, DarkSide, and BlackMatter, and other insights on the inner relationships within the ransomware community.
- Groove representative is likely a threat actor operating under the alias "SongBird" (obfuscated) that is known to be a former Babuk operator and creator of an underground ransomware-centered digital platform RAMP

which is entirely dedicated to providing coordination, communication, and organizational support for the top cyber extortionists.

- The actor's decision to share their insights was triggered by the reported disclosure of what was claimed to be "Babuk's source code" released on September 3, 2021, by the actor operating under the alias "DY-2" (obfuscated). The incident caused a massive backlash from the underground community which once again provoked the release of the blog by SongBird.
- The actor claims that they wish to address the issue of constant misinformation and misreporting originating from the Twitter community covering the ransomware subject. "SongBird" also denies any associations between DarkSide and BlackMatter except that two ransomware share the same source code that *"most likely has been purchased from one of the DarkSide affiliates."*

Background

On September 7, 2021, a representative of the newly-formed Groove ransomware syndicate decided to share their insights and their perspective on the inner aspects of the ransomware business.

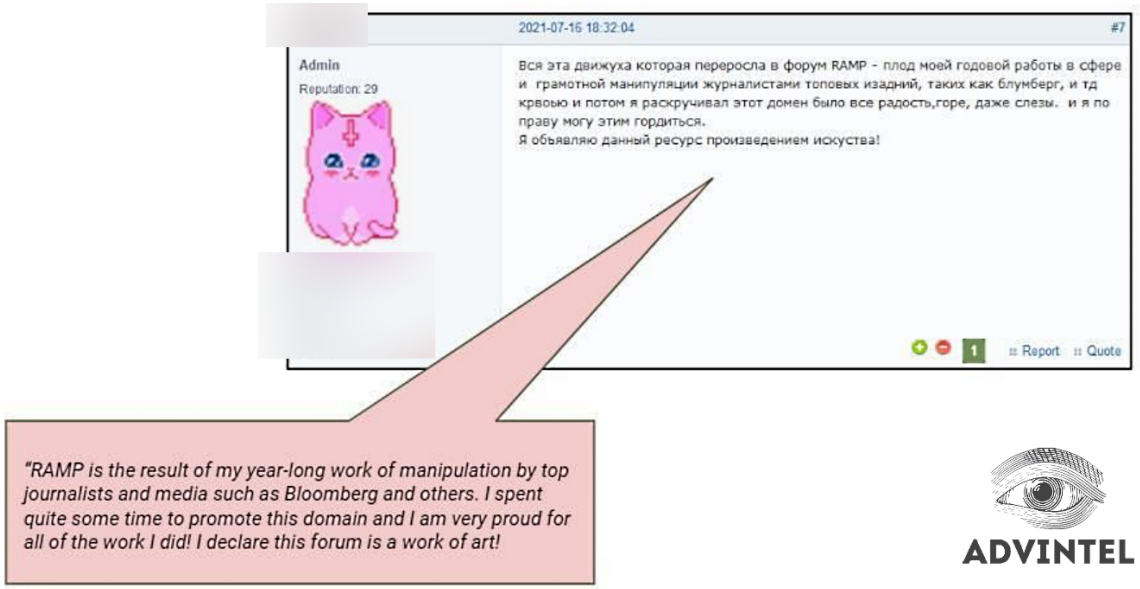
Groove ransomware was announced by a former Babuk operator and a founder of an underground forum **RAMP**. Groove data leak website currently has one victim, a manufacturing company based in Germany, whose exfiltrated data was published on August 27, 2021.

The Groove representative primarily focused on discussing the inner relationships within the ransomware community.

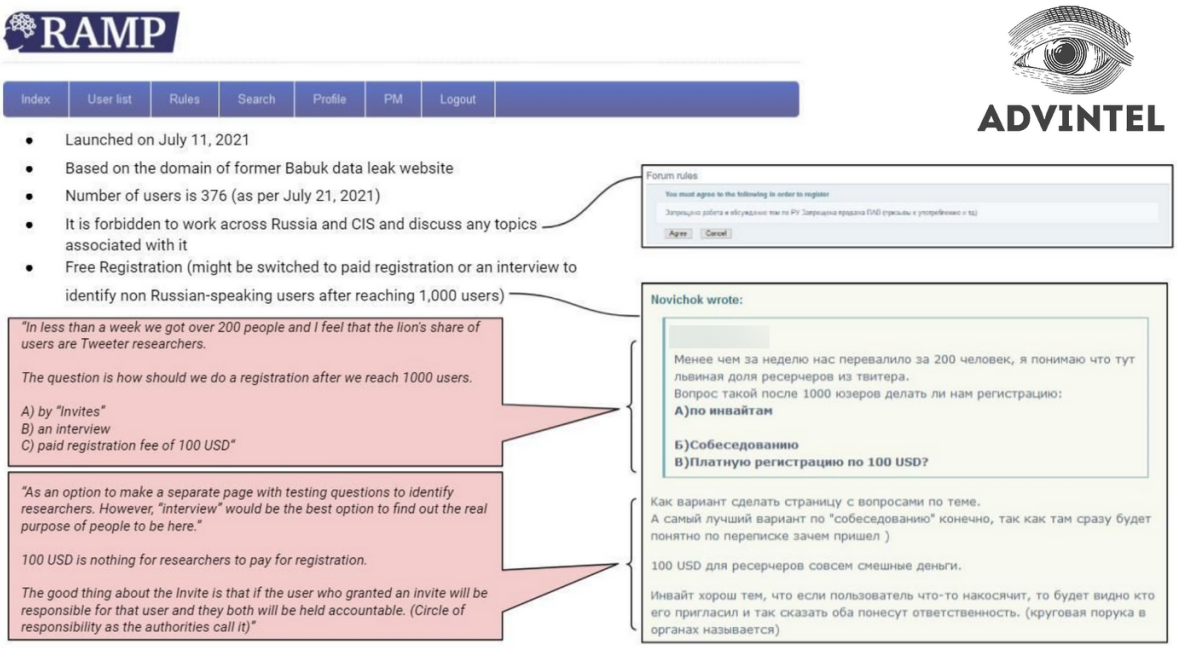
"Hello! Lately, some of the researchers on "Twitter" began dumping tons of flawed information (about ransomware). As a direct participant of recent events, I want to bring clarity as some to make sure that the truth is presented to future generations"

Actor "SongBird"

Groove representative is likely a threat actor operating under the alias "SongBird" (obfuscated) that is known to be a former Babuk operator and creator of an underground ransomware-centered digital platform RAMP.



RAMP forum was launched on July 11, 2021, and was initially based on the former Babuk's data leak website domain. Soon after the forum was relocated to the new domain where it successfully operates to this date. The forum is entirely dedicated to providing coordination, communication, and organizational support for the top cyber extortionists.

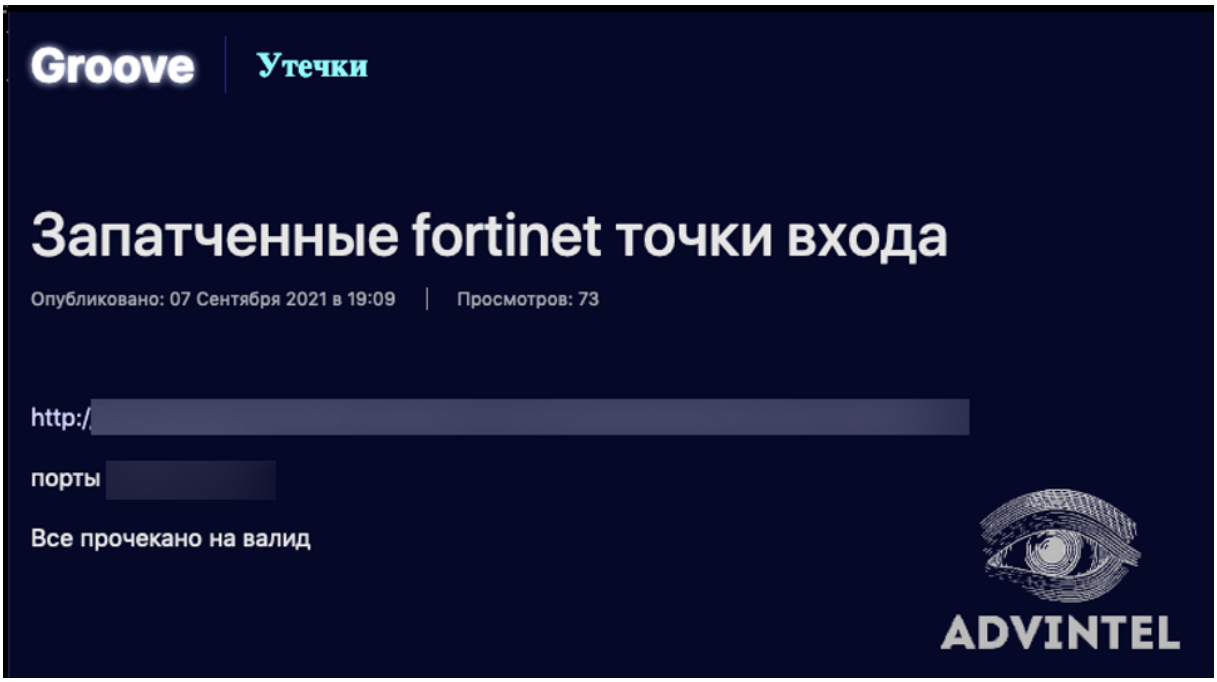


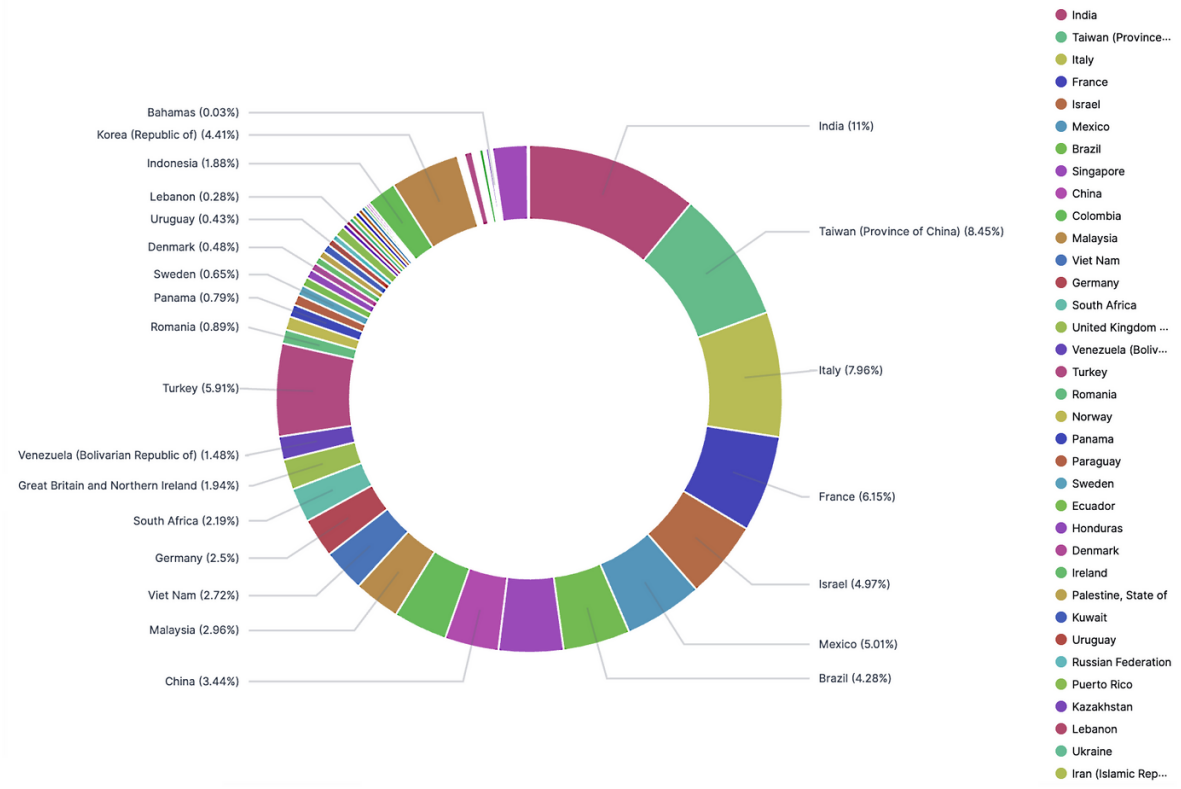
RAMP forum, 10 days in. Threat actor "SongBird" discusses the Registration Policy. Soon after the forum administrators implemented a new rule requiring new members to be screened and accepted by the forum moderator.

Groove is a novel ransomware group that became especially active in August and September 2021. Groove allegedly employs former Babuk developers and possesses advanced tactics and tools. For instance, on September 7, 2021, the same day as the publication of the "Ransomware Thoughts" Groove released leaks of Fortinet VPN SSL

credentials via their leak website. The list contains 799 directories and 86,941 purportedly compromised VPN connections. The reason behind the leak is unclear.

The breach list contains raw access to the top companies.





The geographical distribution of the Fortinet VPN SSL list includes 74 countries. 2,959 out of 22,500 victims are US entities.

Babuk VS Groove. Ransomware Drama

1. Babuk Beginning - the Development of Ransomware

According to the actor, at the end of summer (the year is unclear), they were approached by another member of the underground with an offer to work on the development of ransomware which later was presented as Babuk. The source code was successfully modified and soon after tested against two manufacturing companies based in Europe, as well as other businesses whose names the author did not disclose as these victims "*paid the ransom and fulfilled their contract, while we fulfilled ours"* meaning that they can not share any information regarding the attacks. They conclude *"everything worked for me, the product was satisfying."*

2. "The Netherlands Cheese Crisis" Causing The Rift Within the Syndicate

Soon after, in early April 2020, Babuk attacked a Dutch transport company, possibly using a Microsoft Exchange server CVE (which has been particularly trending as an attack vector for ransomware groups in April and May 2020). The attack has led to the supply chain disruption and the limited availability of prepackaged cheese in the Netherlands.

"SongBird" shares that due to the poor development of the source code, operators weren't able to successfully decrypt the files and return the data even though the victim was reportedly willing to pay the ransom. This turned Babuk's for-profit operation into a simple damaging and destructive attack with no benefit and compromised the group's reputation. According to the Groove representative, the code was poorly written on purpose and they are still struggling to identify the motives behind it.

3. Washington, D.C.'s Metropolitan Police Department Attack that Led to the Split of Babuk Team

According to the blog, one of the ransomware affiliates contacted Babuk offering access to the police department. The ransomware attack occurred in May of 2021 when Babuk operators demanded $4 million USD in exchange for the decryption key. After a short period of negotiation and refusal of their victim to pay a ransom, the syndicate started to release what it claimed to be internal law enforcement data. The negotiation process ended in failure.

SongBird claims that the negotiation failed due to the lack of pressure and “unprofessionalism” by their affiliate. The actor then decided to end the business relationship with their former “colleagues”. It was agreed that SongBird would keep the domain (where the threat actor later built RAMP forum) where the shame blog was based, while their affiliate would keep the source code.

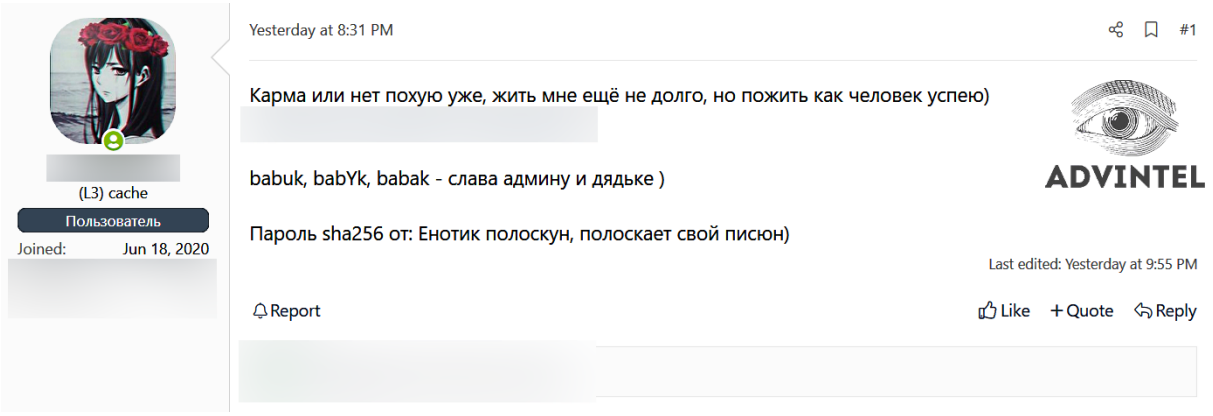
The attack on the police department became the turning point that led the initial team of the Babuk syndicate to disintegration. According to SongBird, they lost half of their team and were struggling to keep the domain, which was attacked by their former syndicate members. Soon after SongBird was forced to relocate RAMP. 15 days prior to the official opening of the forum, the actor added:

“The old team causes trouble. We agreed that they would take their source code and I would take the domain. Don't try to hurt me, I know your skills and what you are capable of as well as my skills too. If you keep interfering in my business I will start working against you (I have insiders).”

4. From Colleagues to Enemies - Babuk Source Code Leak

On September 3, 2021, a threat actor operating under the alias "DY-2" (obfuscated) released what they claimed to be Babuk’s source code also stating that they are doing it as they face a terminal stage of cancer. The actor "DY-2" in fact might be that initial syndicate member who approached “SongBird” with the request to improve the source code - an event that led to a Babuk ransomware development. (see point 1 - “Babuk Beginning”).

“DY-2” intentions to release the source code might have been a desire for simple revenge for their former colleague that quickly became one of the main competitors in the ransomware business. “SongBird” in turn mentioned actor "DY-2" in their debut passage and claims that in reality the actor does not have a cancer diagnosis and is deliberately misleading the underground community. They did not provide any further comments on the legitimacy of the source code itself, however.



One of the alleged developers of Babuk ransomware created a major discussion across the underground forums when they claimed that due to cancer they are willing to share Babuk’s source code. The news was quickly transferred by English-speaking social media.

5. Epilogue - DarkSide & BlackMatter

“SongBird” denies any associations between DarkSide and BlackMatter except that two ransomware share the same source code that *“most likely has been purchased from one of the DarkSide affiliates”*

They believe that BlackMatter has been initiated by some of the older affiliates of DarkSide. However, AdvIntel's visibility into BlackMatter operation suggests that the group institutionalizes the mechanisms which were practiced not by DarkSide's affiliates, but by DarkSide's core leadership. Specifically, DarkSide founders were reportedly scamming their affiliates by intercepting victim negotiations and squeezing the affiliate of the process of obtaining ransom from the victim. This enabled the DarkSide founders to receive the entire ransom payment and not provide affiliates with their percentage share.

DarkSide performed this scheme by indirectly controlling the victim's negotiations chats and creating hidden chats in which they continued negotiations, while the affiliate's chat was blacked as if the victim was not responding. BlackMatter institutionalized this scheme openly stating within their panel that they have an ultimate right to intercept any victim chat and seize the negotiations from the affiliate at any point. This initialization of affiliate scamming schemes suggests that BlackMatter is more likely founded by the DarkSide core team and not by their affiliates as suggested by "SongBird".

Conclusion

The blog released by the Groove representative is a missing piece of a puzzle that allowed us to build a better picture of the Groove and Babuk conflict and take a closer look at the ransomware ecosystem.

The personal disagreement between actors (most likely "SongBird" and "DY-2") that developed within the syndicate led to the withdrawal from the group of one of them and to the establishment of a new brand Groove. As both syndicates continue to exist, we are likely to see more drama coming our way.

This state of affairs demonstrates a complex ransomware ecosystem where new groups emerge as a result of the competition within larger gangs that fall apart and due to inner conflicts, while older groups attempt to rebrand in order to institutionalize the paradigms which they considered operationally existential.

Mitigations & Recommendations:

Groove group consists of ransomware specialists who have been extensively using the following attack vectors - RDPs, Infrastructure Vulnerabilities, Software framework vulnerabilities.

Based on these vectors, AdvIntel recommends addressing the following set of vulnerabilities.

1. Monitor externally exposed RDPs and RDP access sold on major underground marketplaces.
2. Monitor infrastructure vulnerabilities, especially Fortinet VPN SSL.
3. Apply patching and rapid security updates for ransomware-exploited CVEs, specifically ProxyLogon, latest Microsoft Exchange server CVEs, and OWA server CVEs.

Endpoint Vulnerability Exposures for monitoring

- CVE-2019-0708 Bluekeep RDP vulnerability
- CVE-2021-27065 Microsoft Exchange server RCE
- CVE-2021-26857 Microsoft Exchange server RCE
- CVE-2020-0796 - SMBGhost “Bluecorona” RCE vulnerability
- CVE-2019-11510 Pulse VPN vulnerability
- CVE-2020-0829 Citrix scan vulnerability
- CVE-2021-21972 - vmware scan vulnerability
- MS17-010 “Eternalblue” vulnerability
- CVE-2019-19781 - Citrix netscaler vulnerability

Important offensive techniques to monitor

- T1562.001: Impair defenses: disable or modify tools
- T1070.001: Indicator removal on host: clear Windows Event Logs
- T1041: Exfiltration Over C2 Channel
- T1486: Data encrypted for impact
- T1489: Service stop
- T1490: Inhibit System Recovery