

# DisCONTInued: The End of Conti's Brand Marks New Chapter For Cybercrime Landscape

[advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape](https://advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape)

May 20, 2022

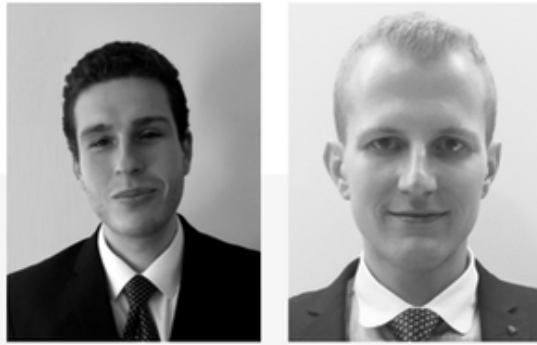
*By Yelisey Bogusalvskiy & Vitali Kremez (with special thanks to AdvIntel Intel Production Analyst Marley Smith)*



”

From the negotiations site, chatrooms, messengers to servers and proxy hosts - The Conti brand, not the organization itself, is shutting down. However, this does not mean that the threat actors themselves are retiring.

ADV:INTEL



From the negotiations site, chatrooms, messengers to servers and proxy hosts - The Conti brand, not the organization itself, is shutting down. However, this does not mean that the threat actors themselves are retiring.



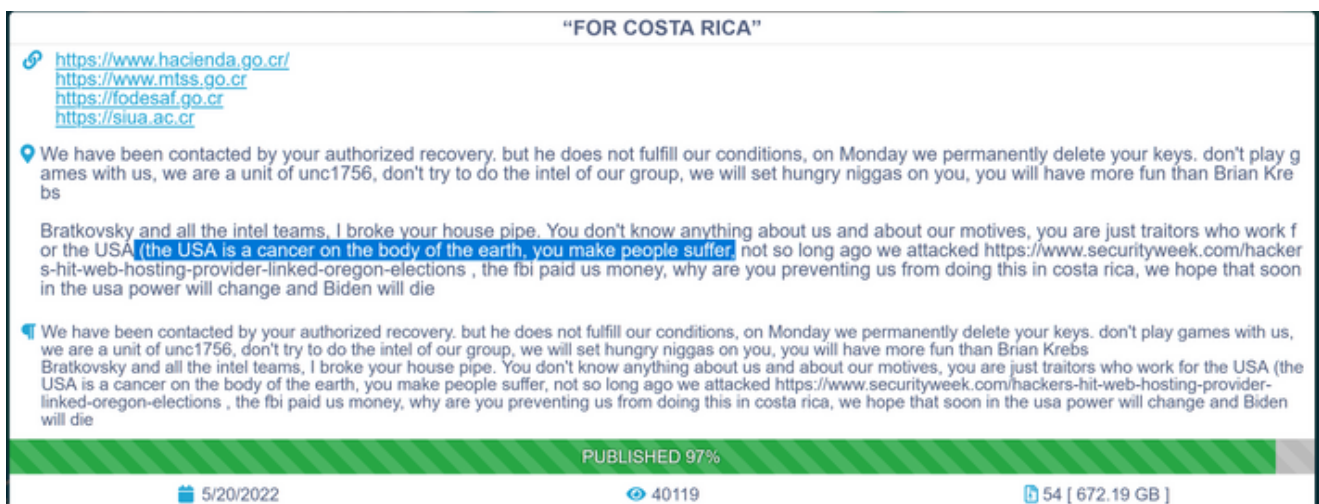
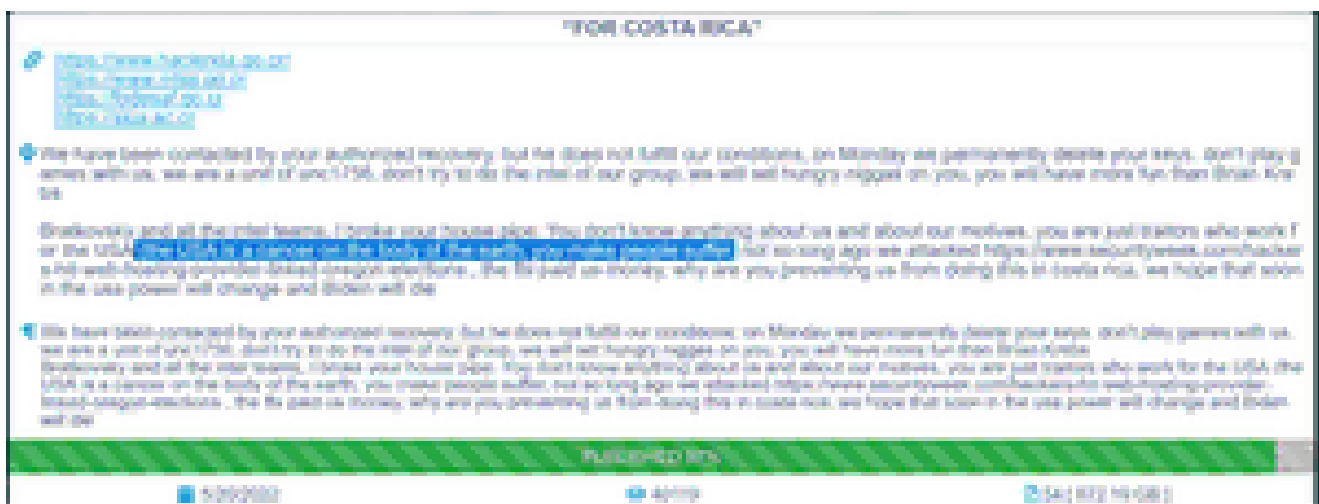
*This is a redacted report that is based on our internal investigations. The full version of the report includes additional information, evidence, IOCs, and commentary for AdvIntel customers and Law Enforcement.*

### **Conti's Death Notice**

**On May 19, 2022, the admin panel of the Conti ransomware gang's official website, *Conti News*, was *shut down*.** The negotiations service site was also down, while the rest of the infrastructure: from chatrooms to messengers, and from servers to proxy hosts was going through a massive reset.

**Conti News** - a shame blog is the last beacon of the group's public operation where *victim data was published*. It also served as a *media tool* that Conti used for their endless public statements (*one of which led to the gang's downfall*).

This publicity function of the blog is still technically active (and this activity, as shown below, is highly strategized). At the time of this publication - May 20, 2022, Conti was even uploading anti-Americanist hate speech claiming the USA to be “*a cancer on the body of the earth*”. This, however, only manifests that the website became an empty shell. At the same time, **the crucial operational function of Conti News which was to upload new data in order to intimidate victims to pay is defunct**, as all the infrastructure related to negotiations, data uploads, and hosting of stolen data was shut down.



*The message published today is strikingly different from previous Conti's political statements written in properly edited English. The extremely low quality of writing also suggests that even the public side of the Conti blog is not treated seriously by the leadership*

And this shutdown highlights a simple truth that has been evident for the Conti leadership since early Spring 2022 - the group can no longer sufficiently support and obtain extortion. The blog's key and only valid purpose are to leak new datasets, and this operation is now gone.

This was not a spontaneous decision, instead, it was a calculated move, signs of which were evident since late April. Two weeks ago, on May 6, [AdvIntel](#) explained that the Conti brand, and not the organization itself, was in the process of the final shutdown. As of May 19, 2022, our exclusive source intelligence confirms that **today is Conti's official date of death.**

In this retrospective analysis, we will not only take an **in-depth look into the reasons behind the Conti shutdown** but perhaps most importantly, **assess and project the future of a new threat landscape that is already on the horizon.** But first, we need to review how Conti prepared for its own demise, and how this group, notable for its sophistry, continued to utilize **information warfare techniques** to orchestrate the shutdown until its final days, in order to ensure the legacy of its surviving members.

### **Mr. "R" & Conti's Final Performance**

*Shutting down ransomware's iconic criminal brand is a long and complicated venture. A notorious and prolific threat group cannot simply turn off its servers, only to pop back up the following week with a new name and logo design. Even a whisper of novel threat group activity following the announcement of Conti's demise would likely spark immediate accusations of poorly executed identity theft. At best, immediate comparisons between the two would permanently leave the new group in Conti's ghostly shadow: *the collective that fell and the one which emerged.**

**REvil, DarkSide**, and countless other collectives attempted the disappearing act; the simple approach failed, and miserably. As what was one of the dominant ransomware group active at the time, Conti realized that an element of *performativity* would need to be involved. Where other groups had been attempting a grand stunt with smoke and mirrors, Conti would try a *sleight of hand*.

Conti would not be itself without its project frontman - an individual operating under the alias “**reshaev**” aka “**cybergangster**”. Besides being a talented coder (they were behind the original Ryuk payload), this person was an outstanding organizer. It was “reshaev” who set the foundation for Conti’s dominance in the cybercrime business, by creating an organizational system based on skill, teamwork, clear business processes, hierarchy, and clear foresight.

It is not surprising that “reshaev” was the first who saw Conti’s structural challenges - **due to the group’s public allegiance to Russia in the first days of the Russian invasion into Ukraine, Conti was not able to be paid**. Since February 2022 almost no payments were given to the group, while Conti’s locker became highly detectable and was rarely deployed. The only possible decision was to rebrand.

For over **two months, Conti collective had been silently creating *subdivisions*** that began operations before the start of the shutdown process. These subgroups either **utilized existing Conti alter egos and locker malware**, or took the opportunity to **create new ones**.

This decision was convenient for Conti, as they already had a couple of subsidiaries operating under different names: ***KaraKurt, BlackByte, BlackBasta***. The rebranded version of Conti—the monster splitting into pieces still very much alive—ensured that whatever form Conti’s ex-affiliates chose to take, **they would emerge into the public eye before news of Conti’s obsolescence could spread**, controlling the narrative around the dissolution as well as significantly *complicating any future threat attributions*.

### **Weekend at Conti’s**

***“All warfare is based on deception. Hence, when we are able to attack, we must seem unable; when using our forces, we must appear inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near.”***

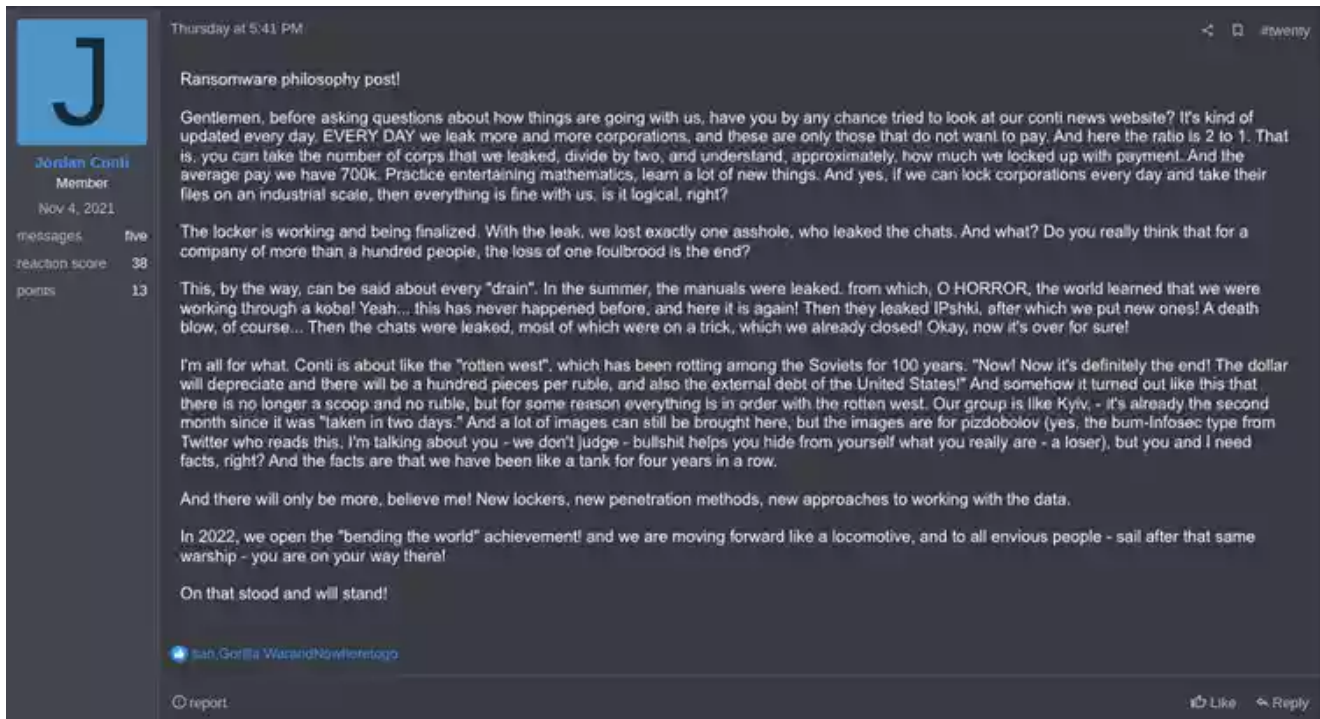
**-Sun Tzu, The Art of War**

*This is where the plans for what was left of Conti became increasingly complex.*

In order to hide the fact that Conti was now dispersed and operating via smaller, more novel brands, the former affiliates of the gang had to now convincingly simulate the actions of a dead brand.

Conti's remaining infrastructure operated like an army preparing for an ambush. Lingering actors were left to keep their fires lit, visible from behind enemy lines. Meanwhile, hidden from view, Conti's most skilled agents were instead laid low in a nearby encampment, biding their time while watching their great and empty camp send out smoke signals, meticulously emulating the movements of an active group.

Conti continued to publish documents stolen from victims (most likely targets hit earlier with attacks and lined up in a sort of "queue" for public release) and "campaigned" hard for themselves on criminal forums. Their public persona boasted a strong and enduring foundation, even one that was willing to further expand the group's operations. From the perspective of Conti's post history, the group was stronger than ever.



Thursday at 5:41 PM

**Jordan Conti**  
Member  
Nov 4, 2021  
messages five  
reaction score 38  
points 13

Ransomware philosophy post!

Gentlemen, before asking questions about how things are going with us, have you by any chance tried to look at our conti news website? It's kind of updated every day. EVERY DAY we leak more and more corporations, and these are only those that do not want to pay. And here the ratio is 2 to 1. That is, you can take the number of corps that we leaked, divide by two, and understand, approximately, how much we locked up with payment. And the average pay we have 700k. Practice entertaining mathematics, learn a lot of new things. And yes, if we can lock corporations every day and take their files on an industrial scale, then everything is fine with us. is it logical, right?

The locker is working and being finalized. With the leak, we lost exactly one asshole, who leaked the chats. And what? Do you really think that for a company of more than a hundred people, the loss of one foulbrood is the end?

This, by the way, can be said about every "drain". In the summer, the manuals were leaked, from which, O HORROR, the world learned that we were working through a koba! Yeah... this has never happened before, and here it is again! Then they leaked IPshki, after which we put new ones! A death blow, of course... Then the chats were leaked, most of which were on a trick, which we already closed! Okay, now it's over for sure!

I'm all for what. Conti is about like the "rotten west", which has been rotting among the Soviets for 100 years. "Now! Now it's definitely the end! The dollar will depreciate and there will be a hundred pieces per ruble, and also the external debt of the United States!" And somehow it turned out like this that there is no longer a scoop and no ruble, but for some reason everything is in order with the rotten west. Our group is like Kyiv, - it's already the second month since it was "taken in two days." And a lot of images can still be brought here, but the images are for pizdabolov (yes, the bum-Infosec type from Twitter who reads this. I'm talking about you - we don't judge - bullshit helps you hide from yourself what you really are - a loser), but you and I need facts, right? And the facts are that we have been like a tank for four years in a row.

And there will only be more, believe me! New lockers, new penetration methods, new approaches to working with the data.

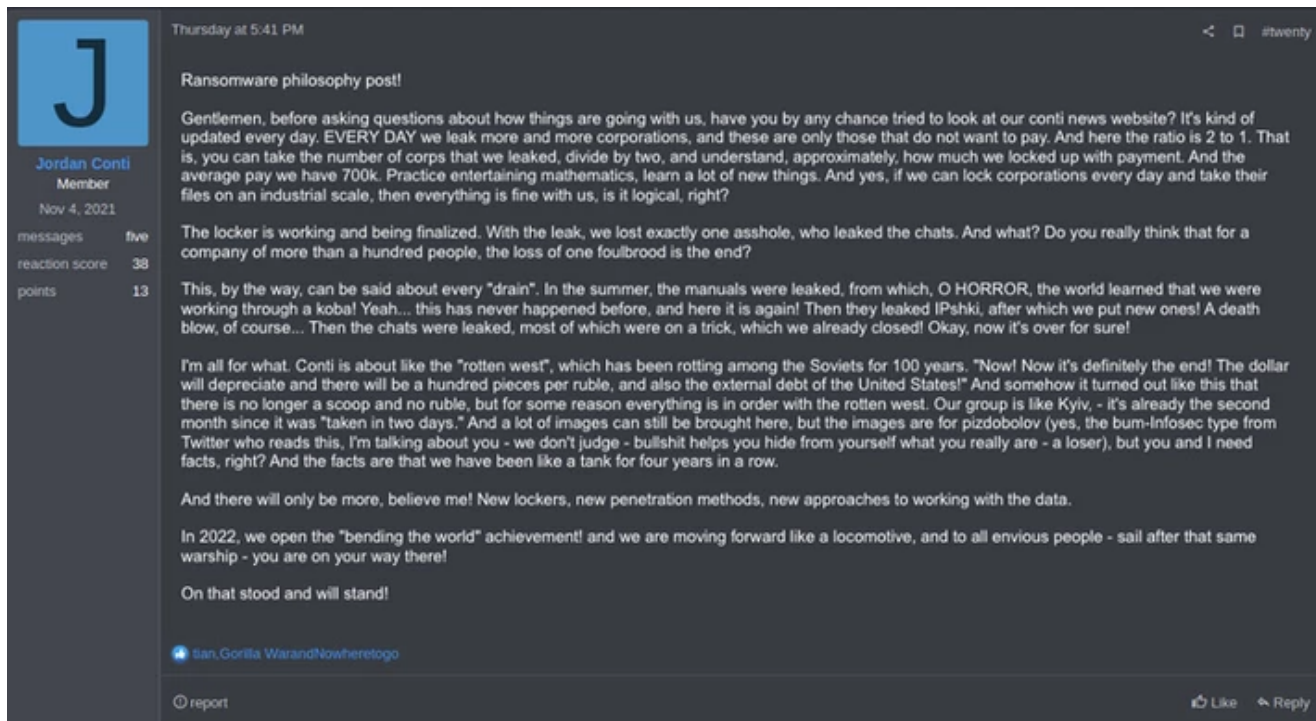
In 2022, we open the "bending the world" achievement! and we are moving forward like a locomotive, and to all envious people - sail after that same warship - you are on your way there!

On that stood and will stand!

San.GorillaWardN0rth0r0g0

report Like Reply





*In a March 30 post to the RAMP underground forum, a Conti representative talks up the group's success, even seeking to recruit new affiliates. [Source - ISMG]*

However, in order to pull off their ultimate tactical maneuver, the agents left behind to operate from within Conti's massive, empty shell had to ensure that their antics would successfully lure attention away from their escaping comrades. To do this, they had to be certain that they left bait big enough to satisfy all of their opposing forces. **Conti would have to perform a grand finale—one big enough to live up to the group's name.**

### **'Out With A Bang': Conti's Grand Finale**

And finally, on May 8, 2021, Costa Rican President Rodrigo Chaves **declared a national emergency as the result of a major cyber attack executed by the Conti ransomware gang.** The massive attack, which took place against multiple Costa Rican government agencies, seems almost like a last-ditch effort by the group to squeeze a few more drops of riches from foreign government funds.

However, AdvIntel's unique adversarial visibility and intelligence findings led to, what was in fact, *the opposite conclusion*: **The only goal Conti had wanted to meet with this final attack was to use the platform as a tool of publicity, performing their own death**

and subsequent rebirth in the most plausible way it could have been conceived.



*The president of Costa Rica Rodrigo Chaves declared that the country is "at war", as Conti caused major disruption to IT systems of numerous government ministries. (Source: BBC)*



**AdvIntel has been tracking the preparations for this attack since April 14, 2022** — days before even the initial compromise. **Our prevention alert was sent on April 15, 2022**, three days before the first incident compromising Costa Rica's Ministry of Finance occurred.

[BREACH PULSE] THREAT LEVEL: HIGH— 2022-04-15:

SHOW ALL TAGS

daily ...

sigint

ranso...

loader

### SPOT SUMMARY

Today's Breach Pulse includes a small number of confirmed entities. These include targets in [Ministerio de Hacienda - República de Costa Rica](#). AdvIntel is currently confirming the target identity linked to the [Affected Companies /](#)

### Breach Pulse

For more information regarding particular exposures, please reach out to [support@advintel.tech](mailto:support@advintel.tech).

### Affected Companies

- [Ministerio de Hacienda - República de Costa Rica](#)



## ¡ALERTA PARA SU SEGURIDAD!

### EVITE SER VÍCTIMA DE ESTAFAS

En sus planes de control tributario, nuestros funcionarios nunca le solicitarán contraseñas, claves de acceso, instalación de programas de cómpulo o acceso a sus cuentas bancarias.

SI RECIBE ESTE TIPO MENSAJES O LLAMADAS  
COMUNÍQUELO AL OIJ

*On the main page of el Ministerio de Hacienda - República de Costa Rica (The Ministry of Finance - Costa Rica), visitors are currently confronted by the following pop-up: Roughly translated, the text reads:*

**ALERT FOR YOUR SECURITY!**

**AVOID BEING A VICTIM OF SCAMS**

*In their tax control plans, our officials never solicit passwords, usernames, or install computer programs or access their bank accounts.*

**IF YOU RECEIVE THESE TYPES OF TEXT MESSAGES OR CALLS**

**COMMUNICATE TO THE OIJ** (the Costa Rican Judicial Investigation Department)

Although this may appear suspicious to non Costa Rican users, the pop-up is indeed confirmed to be legitimate and the phone numbers listed can be attributed to the OIJ.

Domain	Company	Industry	Revenue



hacienda.go.cr

Ministerio de Hacienda -  
República de Costa  
Rica

Government

\$169.4 million USD

**Affected Domains**

For database and customer search purposes, the domains associated with today's Breach Pulse can be found below. Each line indicates a separate domain.

- 
- 
- domain: hacienda.go.cr

[BREACH PULSE] THREAT LEVEL: HIGH— 2022-04-15:

SHOW ALL TAGS





daily ...

sigint

ranso...

loader

### SPOT SUMMARY

Today's Breach Pulse includes a small number of confirmed entities. These include targets in  AdvIntel is currently confirming the target identity linked to the  Affected Companies /  Ministerio de Hacienda - República de Costa Rica 

### Breach Pulse

For more information regarding particular exposures, please reach out to [support@advintel.tech](mailto:support@advintel.tech).

### Affected Companies

- 
- 
- 
-  Ministerio de Hacienda - República de Costa Rica
- 



## ¡ALERTA PARA SU SEGURIDAD!

### EVITE SER VÍCTIMA DE ESTAFAS

En sus planes de control tributario, nuestros funcionarios nunca le solicitarán contraseñas, claves de acceso, instalación de programas de cómputo o acceso a sus cuentas bancarias.

SI RECIBE ESTE TIPO MENSAJES O LLAMADAS  
COMUNÍQUELO AL OIJ

*On the main page of el Ministerio de Hacienda - República de Costa Rica (The Ministry of Finance - Costa Rica), visitors are currently confronted by the following pop-up: Roughly translated, the text reads:*

**ALERT FOR YOUR SECURITY!**

**AVOID BEING A VICTIM OF SCAMS**

*In their tax control plans, our officials never solicit passwords, usernames, or install computer programs or access their bank accounts.*

**IF YOU RECEIVE THESE TYPES OF TEXT MESSAGES OR CALLS**

**COMMUNICATE TO THE OIJ** (the Costa Rican Judicial Investigation Department)

Although this may appear suspicious to non Costa Rican users, the pop-up is indeed confirmed to be legitimate and the phone numbers listed can be attributed to the OIJ.

Domain	Company	Industry	Revenue
			



*Screenshot of AdvIntel's 2022-04-15 Breach Pulse, detailing one of the Costa Rican attacks.*

*In our pre-and-post attack investigation, we have found:*

- The **agenda to conduct the attack on Costa Rica** for the purpose of publicity instead of ransom **was declared internally by the Conti leadership.**
- Internal communications between group members suggested that the **requested ransom payment was far below \$1 million USD** (despite unverified claims of the ransom being \$10 million USD, followed by Conti's own claims that the sum was \$20 million USD). A low demand such as this, made to a state entity no less, was only made with the **knowledge that the group would never see payment for the ransom.**
- Conti was very vocal about the attack, **constantly adding new political statements, any and all political statements being banned within Conti** as of March 2022, resulting from private chat leaks.

***The attack on Costa Rica indeed brought Conti into the spotlight*** and helped them to maintain the illusion of life for just a bit longer, **while the real restructuring was taking place.**

### **Disposing of a Toxic Brand: Conti's Afterlife**

While Conti had been busy with its diversion tactics, other brands such as **KaraKurt**, **BlackByte**, and numerous other groups which existed as *extensions of Conti* but *without taking the group's name* were extremely operationally active, although they worked in silence. Working concurrently with them, talented infiltration specialists, who were



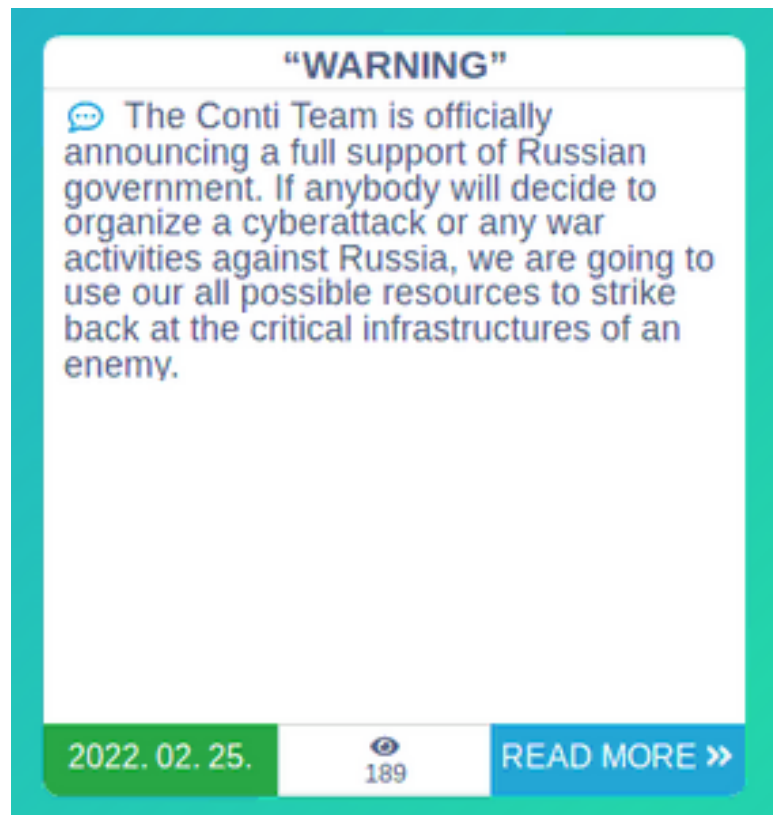
ultimately the backbone of Conti's gang, were also more active than ever, forming alliances with **BlackCat**, **AvosLocker**, **HIVE**, **HelloKitty/FiveHands**, and a whole other cadre of ransomware groups. **These pen-testers maintain personal loyalty to the people who created Conti** but ultimately continued their work with other gangs in order to finally shed Conti's name and image.

This situation presents the first, and foremost reason for Conti's timely end—**toxic branding**. Indeed, the first two months of 2022 left a major mark on the Conti name. While there is no tangible evidence to suggest that the well-known *Conti leaks* had any impact on the group's operations, the event which *provoked* the leak— **Conti's claim to support the Russian government**, seems to have been the fatal blow for the group, despite being *revoked almost immediately*.

The statement had several key consequences, all of which completely reshaped the environment Conti was operating within.

*First, by **engaging in political discourse**, Conti broke the first unspoken rule of the Russian-speaking cybercrime community—**not to intervene in state matters**.*

In AdvIntel's **public blog** regarding **REvil's** ultimate takedown by the Russian government, AdvIntel provided an in-depth analysis of this unspoken agreement, making case studies of the two most notable groups to break it—**Avaddon** and **REvil**. With the ongoing Russian invasion of Ukraine, it may be very plausible that **Russia's state security apparatus is attempting to exert governmental control over its cyberspace**, even taking down groups that appear to have been allies, but who exhibited undue independence with their actions.





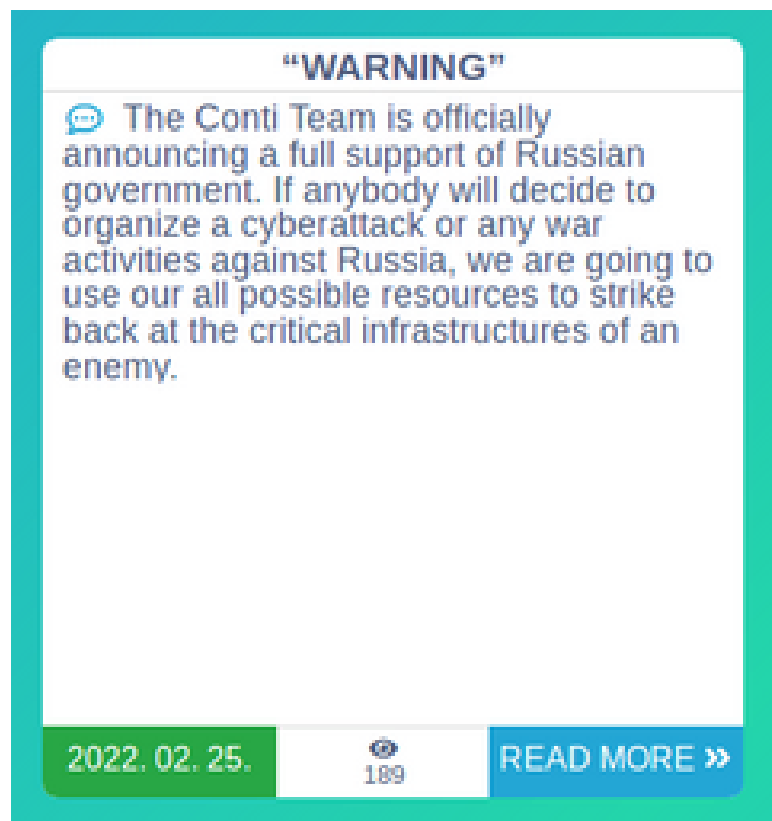
AdvIntel had seen internal communication of the Conti leadership suggesting that the Russian FSB had been pressuring the group, and even though non-factual evidence was involved, **the REvil scenario may have simply repeated itself with Conti, the group’s brand becoming a target for Russian authorities despite their pledged loyalties.**

*Second, Conti’s allegiance to the Russian invasion of Ukraine provoked internal conflict, and brought shame on the Conti name from members who were either ethnically Ukrainian, or were Russian but supported Ukraine, or simply wanted to maintain an anti-war ethic.*

Considering that one of these members decided to betray the gang and leak private Conti chat logs not long after, this conflict illustrated the final nail in Conti’s self-made coffin:

The *third*, and most important factor—by pledging their allegiance to the Russian government, **Conti as a brand became associated with the Russian state—a state that is currently undergoing extreme sanctions.**

In the eyes of the state, each ransom payment going to Conti may have potentially gone to an individual under sanction, turning simple data extortion into a violation of OFAC regulation and sanction policies against Russia. This liability came to a head on May 6, 2022, when **the US State Department offered rewards up to \$10 million USD for information that led to the takedown of the Conti group.**



## “WARNING”

As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

2/25/2022

391

0 [ 0.00 B ]

## “WARNING”

As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

2/25/2022

391

0 [ 0.00 B ]

*Conti decided to revoke their support of the Russian government immediately, turning it into an anti-war statement backed by anti-western sentiments, but this did not repair the damage that had been done to their reputation. [Source].*

As a result of these limitations, Conti had essentially cut itself from the main source of income. Our sensitive source intelligence shows that many victims were prohibited to pay ransom to Conti. **Other victims and companies who would have negotiated ransomware payments were more ready to risk the financial damage of not paying the ransom than they were to make payments to a state-sanctioned entity.**

### *The Villian With a Thousand Faces*



### Semi Autonomous Groups

For those who prefer to use a locker, a former Conti team joins a group, works there semi-independently as a "collective affiliate" (loyal to Conti) and uses the group's locker instead of Conti's locker.

- \*Alpha/BlackCat
- \*HIVE
- \*AvosLocker
- \*HelloKitty/FiveHands

### Autonomous Groups

For those who prefer not to use the locker and work via data exfiltration. An independent collective is created from scratch. They can avoid locker deployment and have their own brand.

- \*Karakurt
- \*Blackbasta
- \*BlackByte

### Independent Members

- Loyal to CONTI
- Working individually

### Mergers & Acquisitions

Conti leadership infiltrates an already existing small brand and consumes it entirely, keeping the small brand name. The small group's leader loses independence but receives massive influx of manpower, while Conti receives a new brand name.

\*Groups names obfuscated for security reasons.



### Semi Autonomous Groups

For those who prefer to use a locker, a former Conti team joins a group, works there semi-independently as a "collective affiliate" (loyal to Conti) and uses the group's locker instead of Conti's locker.

- \*AlphV/BlackCat
- \*HIVE
- \*AvosLocker
- \*HelloKitty/FiveHands

### Autonomous Groups

For those who prefer not to use the locker and work via data exfiltration. An independent collective is created from scratch. They can avoid locker deployment and have their own brand.

- \*Karakurt
- \*Blackbasta
- \*BlackByte

### Independent Members

- Loyal to CONTI
- Working individually

### Mergers & Acquisitions

Conti leadership infiltrates an already existing small brand and consumes it entirely, keeping the small brand name. The small group's leader loses independence but receives massive influx of manpower, while Conti receives a new brand name.

\*Groups names obfuscated for security reasons

As AdvIntel previously stated, ***the end of the Conti brand does not equal the end of Conti as an organization.*** As seen with the Costa Rica case, Conti has been planning the rebranding for several months and prepared a comprehensive strategy to execute it. This strategy is based on *two pillars*:

*First*, Conti is adopting a **network organizational structure**, more *horizontal and decentralized* than the previously rigid Conti hierarchy. This structure will be a coalition of several equal subdivisions, some of which will be independent, and some existing within another ransomware collective. However, **they will all be united by internal loyalty to both each other and the Conti leadership, especially “reshaev”.**

*At this point, this network includes the following groups:*

**TYPE1. Fully autonomous: No locker involved, pure data-stealing:**

- *Karakurt*
- *BlackBasta*
- *BlackByte*

**TYPE2. Semi-autonomous: Acting as Conti-loyal collective affiliates within other collectives in order to use their locker:**

- *AlphV/BlackCat*
- *HIVE*
- *HelloKitty/FiveHands*
- *AvosLocker*

**TYPE3. Independent affiliates: Working individually, but keeping their loyalty to the organization**

**TYPE4. Mergers & Acquisitions:** Conti leadership infiltrates an already-existing small brand and consumes it entirely, keeping the small brand name. The small group's leader loses independence, but receives a massive influx of manpower, while Conti receives a new

subsidiary group. ***(for this type, Groups' names are obfuscated for security reasons. Please contact AdvIntel with questions).***

This is different from *Ransomware-as-a-Service*, since this network, at least at the time of writing, does not seem to be accepting new members as part of its structure. Moreover, unlike RaaS, this model seems to value operations being executed in an *organized, team-led manner*. Finally, unlike RaaS, all the members know each other very well personally and are able to leverage these personal connections and the loyalty that comes with them.

***This model is more flexible and adaptive than the previous Conti hierarchy but is more secure and resilient than RaaS.***

The other major development for this new ransomware model is the **transition from data encryption to data exfiltration**, covered extensively by AdvIntel [in our analysis of Karakurt and BlackByte](#). In a nutshell, relying on pure data exfiltration maintains most major *benefits* of a data encryption operation, while avoiding the issues of a locker altogether. Most likely, *this will become the most important outcome of Conti's re-brand*.

## **Conclusion**

Within the short but tumultuous timeline of ransomware's history, May 19, 2022, *the day that Conti died*, will leave a mark that severs the threat landscape from its past and casts a shadow on its future. However, in the grand scheme of the group's existence, this day is not something new.

Looking back, a trail of similar marks lead from the group's days as the organization *Ryuk* to their first rebranding from the collective's *Overdose* division. Each mark represents a shift in the threat landscape, a series of tics that, only when viewed from a great distance, show the dramatic impact the group has made on ransomware's very existence. However, the actors that formed and worked under the Conti name have not, and will not cease to move forward with the threat landscape—*their impact will simply leave a different shape*.