# The Karakurt Web: Threat Intel and Blockchain Analysis Reveals Extension of Conti Business Model

arcticwolf.com/resources/blog/karakurt-web

April 15, 2022

April 15, 2022

## Key Insights on Karakurt

- **We assess with a high degree of confidence that the Karakurt extortion group is operationally linked to both the Conti and Diavol ransomware groups.**
- **Since its first attacks in August 2021, Karakurt has victimized organizations in a number of industries and in at least eight countries.**
- **These connections debunk Conti ransomware's standard pledge to victims that paying the demanded ransom will keep them safe from future attacks. Paying a ransom also does not result in Karakurt deleting data.**

## Summary

Tetra Defense, an Arctic Wolf® company, partnered with Chainalysis to analyze the link between the Karakurt cyber extortion group to both Conti and Diavol ransomware through Tetra's digital forensics and Chainalysis' blockchain analytics. As recent leaks have revealed, Conti and Trickbot are complicated operations with sophisticated structures. But, our findings indicate that web is even wider than originally thought, to include additional exfiltration-only operations. The web is stickier too as we have confirmed on numerous occasions that the Karakurt group does not delete victim data and maintains a copy even after an extortion payment.

## Background

In 2021 Tetra Defense was approached by a client who claimed to have been hit with ransomware re-extortion. They were previously a victim of Conti ransomware and had paid the demand only to later discover another extortion attempt from an unknown group. Except, in the second attempt, no encryption occurred. After successfully recovering from the first intrusion, this client logged in to their systems to find yet another ransom note stating sensitive data had been stolen and exacting an additional ransom.

The timing was interesting. As Tetra Defense took the case and started examining the client’s systems, it was clear that the second extortionist had utilized the exact same backdoor left by the Conti group to access the victim’s network. This was a Cobalt Strike back door indicating that the second intruder would have needed access to the Conti Cobalt Strike server in order to use the persistence mechanism. Such access could only be obtained through some sort of purchase, relationship, or surreptitiously gaining access to Conti group infrastructure.

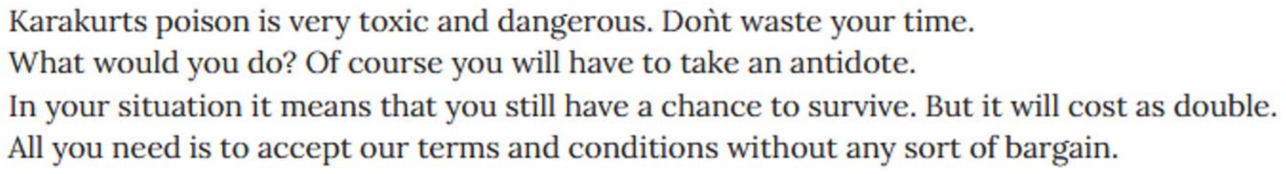
This all occurred during a turbulent period in which Conti was struggling with disgruntled affiliates angry over low pay and leaking sensitive information such as Conti’s playbooks and training materials. Tetra noted the possibility that this second actor could have been a Conti operative or affiliate, particularly given their access to the backdoor. Perhaps it was a disgruntled employee trying to “cut out the middleman” and walk away with more profit by quietly returning to steal data. Or, alternatively, perhaps this was the trial run of a strategic diversification authorized by the main group.

Thus began a more regular emergent pattern of data theft extortions. Just a few days later Tetra Defense encountered the first victim of what was called “Karakurt” employing similar tradecraft to what was observed in the previous re-extortion attempt just days before. Again, the victim reported no encryption, only a ransom note indicating that large amounts of sensitive data had been stolen. This was not unheard of. Other groups such as Marketo began using the tactic earlier and a few others such as Bl@ckt0r and Bonaci Group were largely contemporaneous. But Karakurt seemed to outlive each of its competitors in this nascent exfiltration-only space as Tetra Defense responded to numerous incidents over the next few months. Our analysis might shed light on Karakurt’s relative longevity.

*Karakurt's logo*

## Who is Karakurt?

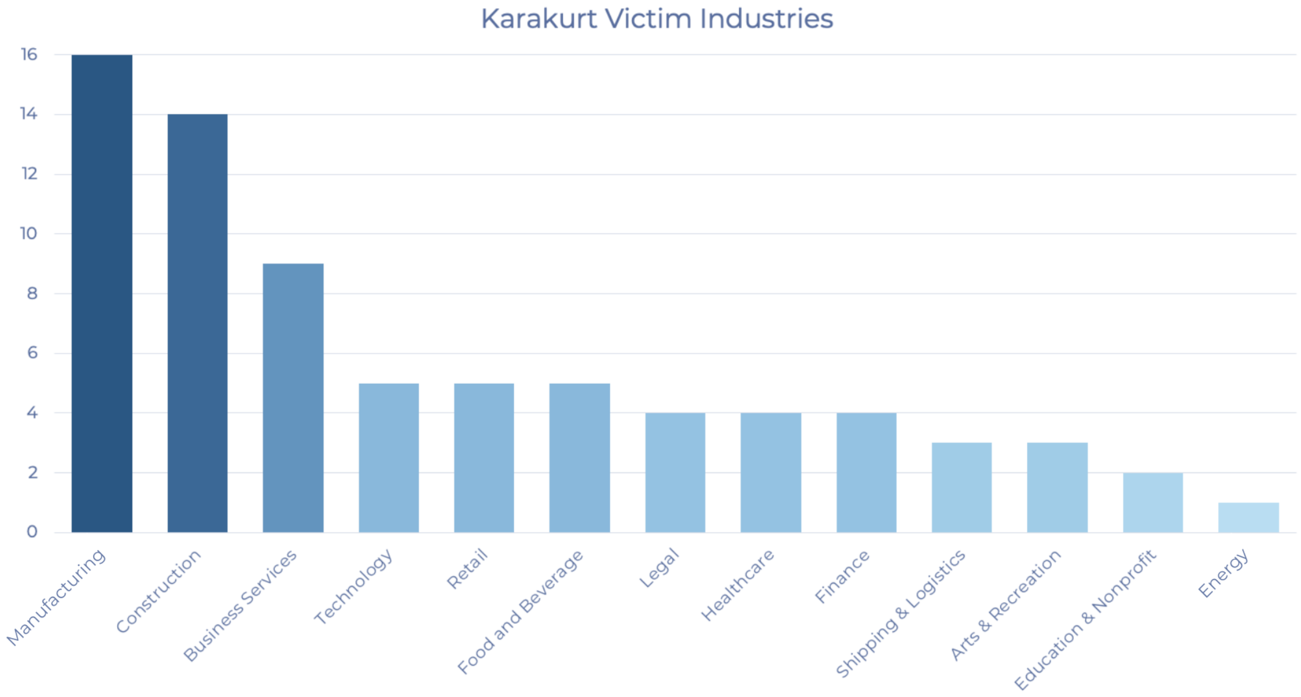
Karakurt is branded after the common name of a venomous widow spider, an image the group does not hesitate to allegorize in describing who they are. As evinced by the excerpt taken from the group's dark web leak site, a data theft extortion is compared to a toxic bite. The antidote? Cooperation, of course.

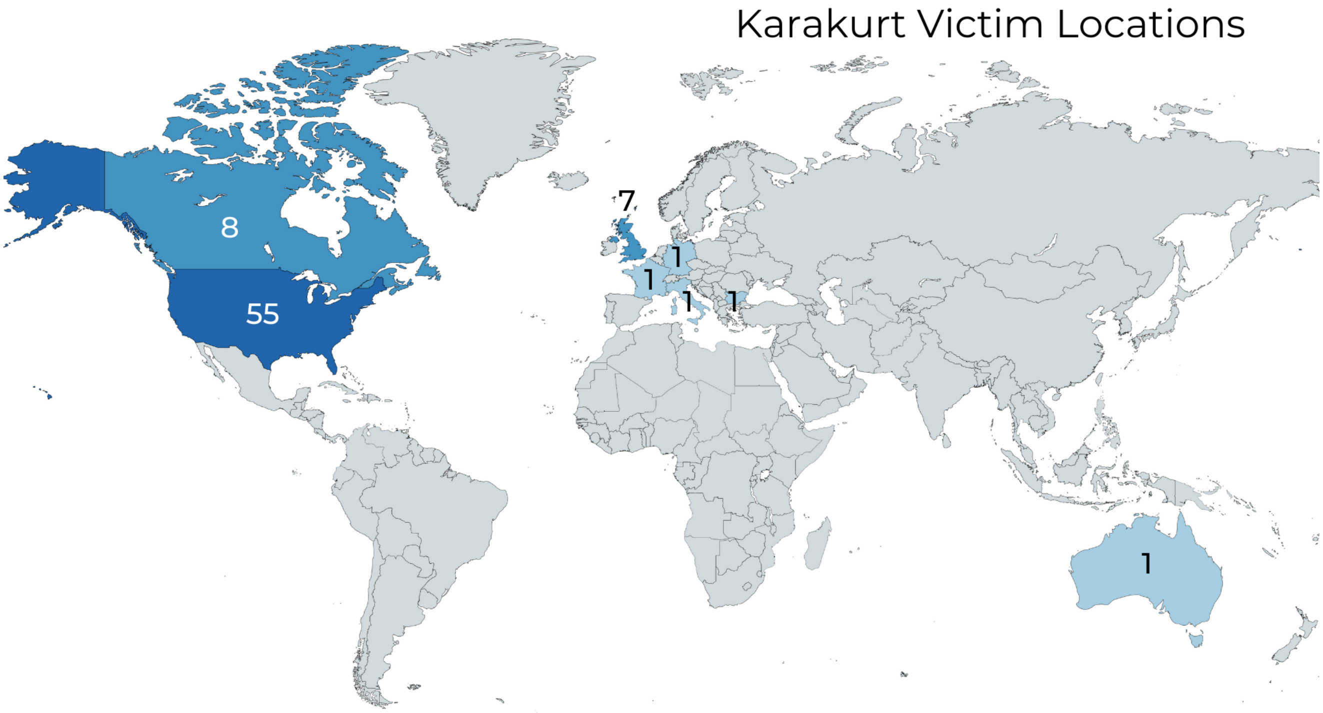


Karakurts poison is very toxic and dangerous. Doǹt waste your time.
What would you do? Of course you will have to take an antidote.
In your situation it means that you still have a chance to survive. But it will cost as double.
All you need is to accept our terms and conditions without any sort of bargain.

*Screenshot from Karakurt dark web leak site.*

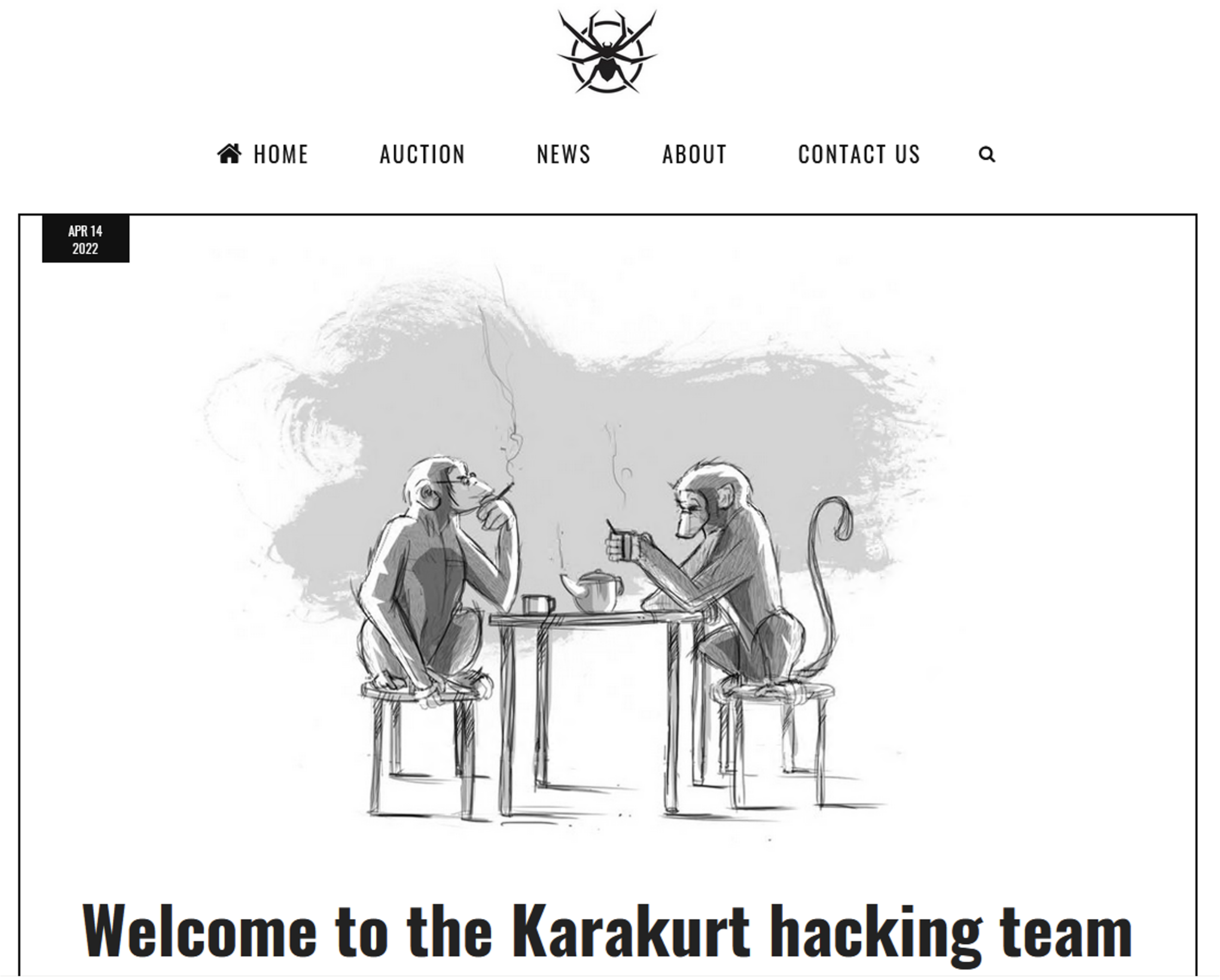
As opposed to typical ransomware in which the adversary will deny a victim access to data through encryption, Karakurt is a cybercrime group which infiltrates networks and engages in extortion by stealing and threatening to release data without any attempt to encrypt. Since its first observed attacks in August 2021, Karakurt has victimized organizations across a number of industries and in at least eight countries.[1]





Typically, Karakurt threatens to release victims' data on a branded dark web site, noted for its bizarre aesthetic. Until recently, Karakurt posted lists of victim names who chose not to accede to the group's demands but is now beginning to make good on threats to release stolen data.

## Karakurt Dark Web Home Page



Welcome to the Karakurt hacking team

## Conti Hypothesis

In responding to well over a dozen Karakurt incidents to date, Tetra Defense has built a dataset of intrusions, leading to additional insight. The most ubiquitous point of initial intrusion for Karakurt attacks are Fortinet SSL VPNs as was also the point of compromise for the earlier seemingly Conti-related re-extortion.

While Karakurt attacks can vary with respect to tools, some notable overlaps began to emerge between some Karakurt intrusions and the earlier suspected Conti-related re-extortion, including the use of the same tools for exfiltration, a unique adversary choice to create and leave behind a file listing of exfiltrated data named “file-tree.txt” in the victim’s environment, as well as the repeated use of the same attacker hostname when remotely accessing victims’ networks (see table below).

Any single data point is far from a smoking gun but taken together as a series of choices made by an attacker to accomplish the unique goal of data theft extortion, there is evidence to make an inference-based assertion that these intrusions could be linked. If the mystery re-extortion gang were indeed connected to Conti and likewise related to Karakurt then by transitive inference this might indicate a connection between Conti and Karakurt.

In addition, Tetra was engaged by another client victimized by a Karakurt attack, only upon performing forensics analysis did we learn that they had been the prior victim of Ryuk ransomware in the past. This was the second indication of a potential Conti link, as Ryuk and Conti are both deployed by the Trickbot Group and exhibit significant technical as well as financial overlap.[2] Armed with a hypothesis that something more systemic was occurring, Tetra Defense collaborated with our intel partners at Chainalysis.

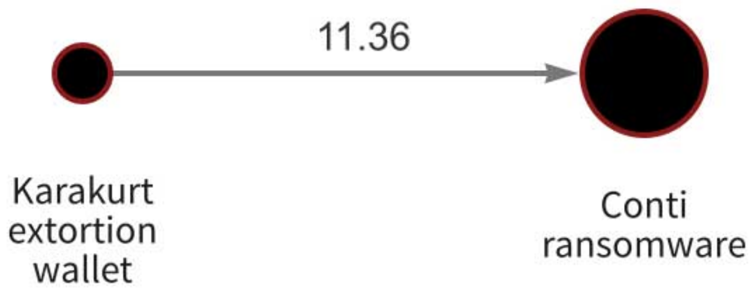
| | **Conti-Related Re-Extortion** | **Karakurt** |
|---|---|---|
| **Root Point of Compromise** | Fortinet SSL VPN | Fortinet SSL VPN |
| **Exfiltration Tool** | WinSCP | WinSCP |
| **File Listing** | “file-tree.txt” left on victim system | “file-tree.txt” left on victim system |
| **Attacker Hostname** | Identical | Identical |
| **Actions on Objective** | Data Exfiltration | Data Exfiltration |

*Comparison of earlier non-attributed re-extortion and a cluster of Karakurt intrusions*

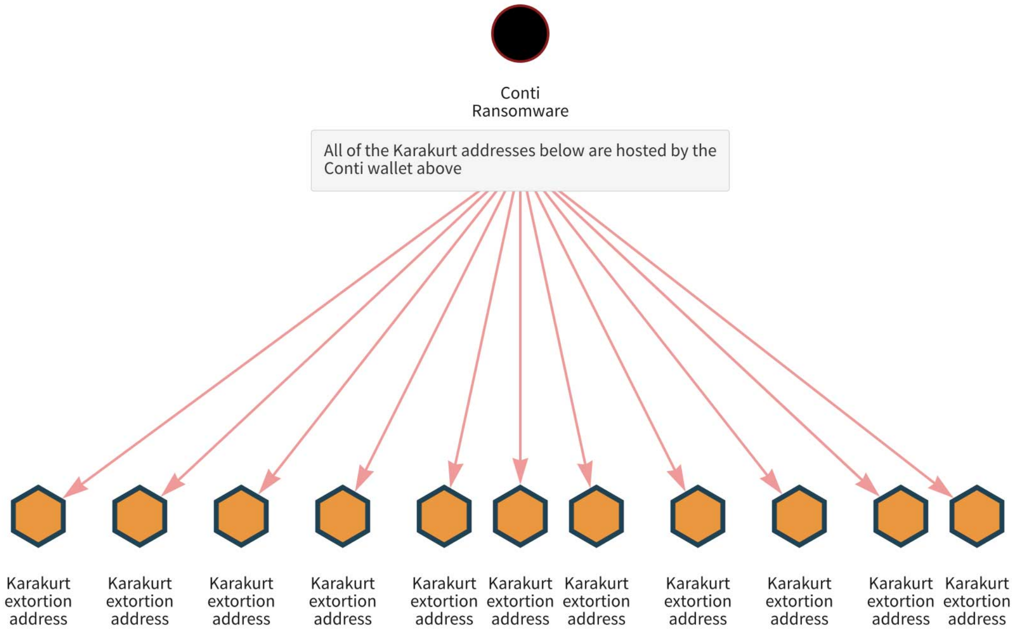
## Conti and Karakurt’s Financial Connections

In partnership with Chainalysis and its world-class blockchain analysis team, we can analyze cryptocurrency transactions carried out by Conti and Karakurt to reveal financial connections between the two. Blockchain analysis provided some of the earliest indication of Karakurt’s ties to Conti ransomware, as the relevant transactions pre-date the discovery of the similarities in Karakurt and Conti’s software and attack strategy.

Chainalysis has identified dozens of cryptocurrency addresses belonging to Karakurt, scattered across multiple wallets. Victim payments to those addresses range from $45,000 to $1 million worth of cryptocurrency. Right off the bat, we can see examples of Karakurt wallets sending substantial sums of cryptocurrency to Conti wallets.



For example, in the Chainalysis Reactor screenshot above, we see a Karakurt extortion wallet moving 11.36 Bitcoin — worth approximately $472,000 at the time of transfer — to a Conti wallet. But the connections run even deeper. Chainalysis has also found that several Karakurt victim payment addresses are hosted by wallets that also house Conti victim payment addresses.


Conti Ransomware
All of the Karakurt addresses below are hosted by the Conti wallet above
Karakurt extortion address
Karakurt extortion address
Karakurt extortion address
Karakurt extortion address
Karakurt extortion address
Karakurt extortion address
Karakurt extortion address
Karakurt extortion address
Karakurt extortion address
Karakurt extortion address
Karakurt extortion address

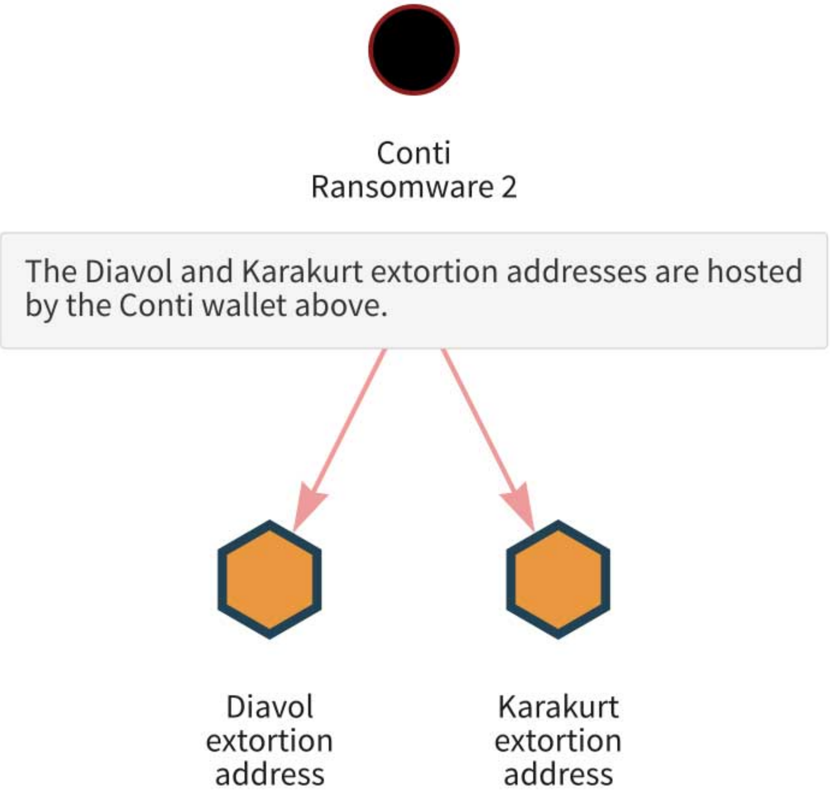
Shared wallet hosting leaves virtually no doubt that Conti and Karakurt are deployed by the same individual or group.

### How Diavol Fits

Tetra has discovered some oversights by Karakurt operatives which reveal a connection to Diavol ransomware, another group which emerged around the same time (July 2021) and has been associated with Trickbot.[3] Tetra responders observed adversary actions across multiple cases which proved shared use of tools and infrastructure, though, like Conti, Diavol employs encryption whereas Karakurt does not.

Diavol, Conti, and Ryuk had been reported using the same malware loader[4] and the Conti Jabber chat leaks in Feb – March 2022 further revealed the nature of the connection with Diavol.[5] In the chats, Stern (the Trickbot Group administrator and Conti manager) wrote to Mango (the people manager) in early July 2021 to inform that Baget, another operative, had completed the Diavol locker and that it had come back clean on antivirus detection tests. Both Karakurt and Diavol sprang from within the heart of Conti and Tetra Defense was able to confirm that Karakurt and Diavol operators were sharing attacker infrastructure during the same period of time.

Once again though, blockchain analysis confirms Diavol's connection to Karakurt and Conti. Similar to Karakurt, the Reactor graph below shows a Diavol extortion address hosted by a wallet containing addresses used in Conti ransomware attacks.


Conti
Ransomware 2
The Diavol and Karakurt extortion addresses are hosted by the Conti wallet above.
Diavol extortion address
Karakurt extortion address

Again, this common address ownership confirms with near total certainty that Diavol is deployed by the same actors behind Conti and Karakurt.

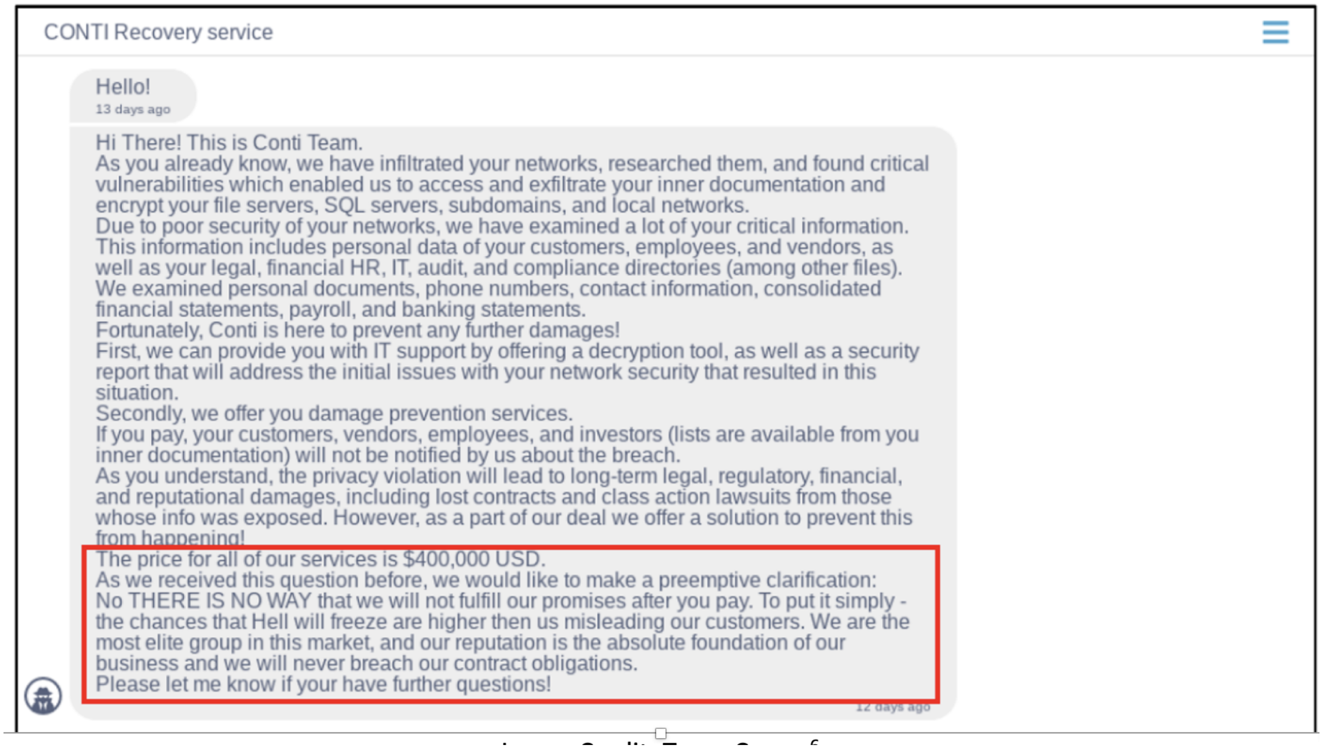
### Karakurt may be Conti's diversification strategy, but not a wise one

We have been able to demonstrate relatively high-confidence connections between Conti, Karakurt, and Diavol. However Karakurt is being run, it no doubt gains some advantage with access to Conti resources such as access to victims or the tools and infrastructure used by the rest of the group. Knowing who you are dealing with in the fight against ransomware is a rare opportunity, which helps defenders know how to respond. Through collaborative efforts in Tetra’s forensic investigations with Chainalysis’ blockchain analytics and IR partners, there is a strong case to be made that Karakurt and Diavol are part of the evolving Conti web.

Why might Conti deploy a quasi-ransomware strain like Karakurt? The Conti Leaks may hold the answer. Chats between Trickbot Group managers show that they’ve thought long and hard about how to diversify their business model, with some proposing ideas like selling exfiltrated data or access to victims. Operating multiple ransomware strains could also be a way to enhance resiliency and enable business continuity amid any possible government actions. Amid unprecedented Law Enforcement action on ransomware in 2021 when Karakurt emerged, Conti managers may have perceived that launching a strain that does not encrypt can bypass scrutiny incurred by “ransomware” while still achieving financial objectives.

Whether Karakurt is an elaborate side hustle by Conti and Diavol operatives or whether this is an enterprise sanctioned by the overall organization remains to be seen. What we can say is this connection perhaps explains why Karakurt is surviving and thriving despite some of its exfiltration-only competitors dying out.

But in the long run, the strategy may backfire, as these discoveries discredit Conti ransomware’s standard pledge to victims that paying the demanded ransom will keep them safe from future attacks and result in the criminal enterprise keeping its word. We have been able to confirm on numerous occasions that the Karakurt group does not delete victim data after payment and maintains a copy. However, the motivation behind this is unclear. While we have not as yet observed re-extortion after a Karakurt payment, the victim’s deal is only partially honored. In addition, there is plausible evidence to assert that Conti has used Karakurt against former victims.



CONTI Recovery service

Hello!
13 days ago

Hi There! This is Conti Team.
As you already know, we have infiltrated your networks, researched them, and found critical vulnerabilities which enabled us to access and exfiltrate your inner documentation and encrypt your file servers, SQL servers, subdomains, and local networks.
Due to poor security of your networks, we have examined a lot of your critical information.
This information includes personal data of your customers, employees, and vendors, as well as your legal, financial HR, IT, audit, and compliance directories (among other files).
We examined personal documents, phone numbers, contact information, consolidated financial statements, payroll, and banking statements.
Fortunately, Conti is here to prevent any further damages!
First, we can provide you with IT support by offering a decryption tool, as well as a security report that will address the initial issues with your network security that resulted in this situation.
Secondly, we offer you damage prevention services.
If you pay, your customers, vendors, employees, and investors (lists are available from you inner documentation) will not be notified by us about the breach.
As you understand, the privacy violation will lead to long-term legal, regulatory, financial, and reputational damages, including lost contracts and class action lawsuits from those whose info was exposed. However, as a part of our deal we offer a solution to prevent this from happening!
The price for all of our services is $400,000 USD.
As we received this question before, we would like to make a preemptive clarification:
No THERE IS NO WAY that we will not fulfill our promises after you pay. To put it simply - the chances that Hell will freeze are higher then us misleading our customers. We are the most elite group in this market, and our reputation is the absolute foundation of our business and we will never breach our contract obligations.
Please let me know if your have further questions!
12 days ago

*Image Credit: Team Cymru[6]*

Check out the highlighted portion of the Conti ransom note above. Ransomware attacks are premised on the victim's trust that their payment will end the attack and return to them control of their data. If victims and their incident response firms know Conti may have re-extorted prior victims using Karakurt and that data won't actually be deleted, there's much less incentive to pay. Don't get caught in the web.

### Credits

**Arctic Wolf** is a leader in security operations, delivering a premier cloud-native security operations platform designed to end cyber risk. For more information, visit www.arcticwolf.com.

**Chainalysis** is the blockchain data platform. We provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 70 countries. Our data powers investigation, compliance, and market intelligence software used to solve some of the world's most high-profile criminal cases. For more information, visit www.chainalysis.com.

**Tetra Defense, an Arctic Wolf Company,** is a leading incident response, cyber risk management and digital forensics firm. For more information, visit www.tetradefense.com.

*Arctic Wolf's Threat Research & Detection teams continually work to leverage intelligence from Tetra Defense responders on how threat groups like Conti, Karakurt, and Diavol operate to bolster detections in the Arctic Wolf platform. The threat landscape is constantly evolving,* *especially with ransomware groups and how they conduct their attacks. The visibility that Tetra Defense responders have into the tactics, techniques, and procedures (TTPs) of these groups allows Arctic Wolf to push forward new intel-driven detections on a daily basis.*

This article was based on research performed by Tetra Defense, an Arctic Wolf® company, with contributions from Chainalysis and Northwave.

---

[1] This data and the graphic representations of Karakurt victim industries and geographic locations are based on dark web intelligence data collected by Tetra Defense. This represents victims who elected not to pay the ransom

[2] Unfortunately, forensic data had not been preserved from the distant Ryuk intrusion from which the client recovered for Tetra to be able to do analysis by which to correlate the intrusions.

[3] https://www.bleepingcomputer.com/news/security/fbi-links-diavol-ransomware-to-the-trickbot-cybercrime-group/

[4]

https://thedfirreport.com/2021/12/13/diavol-ransomware/
[5]

https://arcticwolf.com/resources/blog/conti-ransomware-leak-analyzed
[6]

https://team-cymru.com/wp-content/uploads/2021/10/Conti_Paper_1.pdf

Error - something went wrong!

Get cybersecurity updates delivered to your inbox.

Thanks for subscribing!