

Hydra with Three Heads: BlackByte & The Future of Ransomware Subsidiary Groups

advintel.io/post/hydra-with-three-heads-blackbyte-the-future-of-ransomware-subsidiary-groups

AdvIntel

May 17, 2022

- o May 17
- o
- o 9 min read

By Vitali Kremez & Yelisey Boguslavskiy



As it stands, BlackByte is already coming into their own as an independent group, spurred on by Conti's sudden fall from power. Only time will tell if they can someday grow into the space left by the cybercriminal giant.



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."

Prologue: BlackByte's True Face

On February 13, 2022, a novel, lesser-known ransomware collective posted the alleged financial documents of the **San Francisco 49ers** football team on their underground site. The threat group, known as **BlackByte**, was widely credited with the orchestration of the attack—However, AdvIntel's **sensitive primary-source intelligence** and **factual data evidence** (including IOCs) point to a different conclusion: **that BlackByte was instead being used as a shell group to process the breach.**

AdvIntel instead attributes the 49ers' February security compromise to the **now-dying Conti ransomware group**. This story hints at the answers to two *now pressing questions*:

- ***How can established ransomware collectives utilize subsidiary groups for operations involving data exfiltration without also utilizing extortion tactics?***
- ***What will happen to ransomware groups after Conti's final shutdown?***

AdvIntel already published primary research regarding these trends, centered around the case study of **KaraKurt**, (***Enter KaraKurt: Data Extortion Arm of Prolific Ransomware Group***, published April 18). Since these findings became public, AdvIntel's intelligence team has assembled its newest findings into another case: an in-depth analysis of **BlackByte**, the **Conti affiliate which was created for the sole purpose of maximizing Conti's monetary data extortion.**



The 49ers Security Incident

Posted on the group’s “shame blog” in a file labeled “2020 Invoices”, *BlackByte*’s operatives advertised 292 megabytes of what was allegedly stolen financial data belonging to the NFL team for download, available free of charge. That same day, a statement issued by the 49ers team alluded to a “network security incident”—one which had apparently disrupted corporate IT systems, but had not affected stadium operations or ticketholders (meaning that there may not have been a network lock). The data being offered was not vital to the 49ers’ operations, but rather a sample, perhaps representing an early step in what could become exponentially higher stakes for the team later on.

BlackByte BLOG

San Francisco 49ers



The San Francisco 49ers are a professional American football team based in the San Francisco Bay Area. The 49ers compete in the National Football League (NFL) as a member of the league's National Football Conference (NFC) West division, and play their home games at Levi's Stadium in Santa Clara, California, located 38 miles (61 km) southeast of San Francisco. The team is named after the prospectors who arrived in Northern California in the 1849 Gold Rush. The team was founded in 1946 as a charter member of the All-America Football Conference (AAFC), and joined the NFL in 1949 when the leagues merged. The 49ers were the first major league professional sports franchise based in San Francisco, and are the 10th oldest franchise in the NFL. The team began play at Kezar Stadium in San Francisco before moving to Candlestick Park in 1971, and then to Levi's Stadium in 2014. Since 1988, the 49ers have been headquartered in Santa Clara.



846



Web Site



\$ 530 Million



(408) 562-4949



20 days 6:8:57



DOWNLOAD FREE

DOWNLOAD 292.72MB

Screenshot of the BlackByte page advertising the stolen data. [Source: BleepingComputer](#)

Attack Anatomy: BlackByte, or Something More?

Media outlets were quick to speculate on the nature of the attack, noting that *BlackByte*, although positioned with a number of successful ransomware attacks under their belt, was still relatively inactive and decentralized as a group. The breach was notable more so for widespread name recognition in regards to its victim, and how it contributed to public anxieties for increasingly common large-scale and high-profile ransomware attacks. After all,

the incident raised reasonable questions both in and out of the cybersecurity world—How had this smaller, newer, less-organized group of cybercriminals managed to orchestrate a major data theft from one of the most valuable franchises of a multi-billion dollar association?

The answer is that BlackByte, as a collective, does not exist, at least not autonomously. Instead, it's a working part of something *larger*, and not only in the organizational sense.

Almost exactly two months prior to this breach on December 14, 2021, *AdvIntel* published its daily *Breach Pulse* report via our private security platform, **Andariel**. *Breach Pulse* is an ever-updating early alert deliverable sent by AdvIntel to customers and Law Enforcement, *intended to notify them when related companies and organizations have experienced a security breach*. The digital newsletter contains both the names and small amounts of background information about entities that have experienced a detected security exposure, as well as a full list of domains included in the detected compromise. The bulletin is intended for clients so they can take preemptive action before a breach worsens, *tightening their defenses* as needed and *notifying relevant parties*.

On December 14, 2021, AdvIntel's Breach Pulse reported a direct network security breach (via Cobalt Strike) of the San Francisco 49ers football team.

San Francisco 49ers

Domain: 49ers[.]com
Group Accounts for \\REDACTED49ers-HQ.lan

Examples (network shares):

Accounting
Admins
Alumni
Coaching
Compensation Plans
Domain Admins
Facilities
Finance
Group Policy Creator Owners

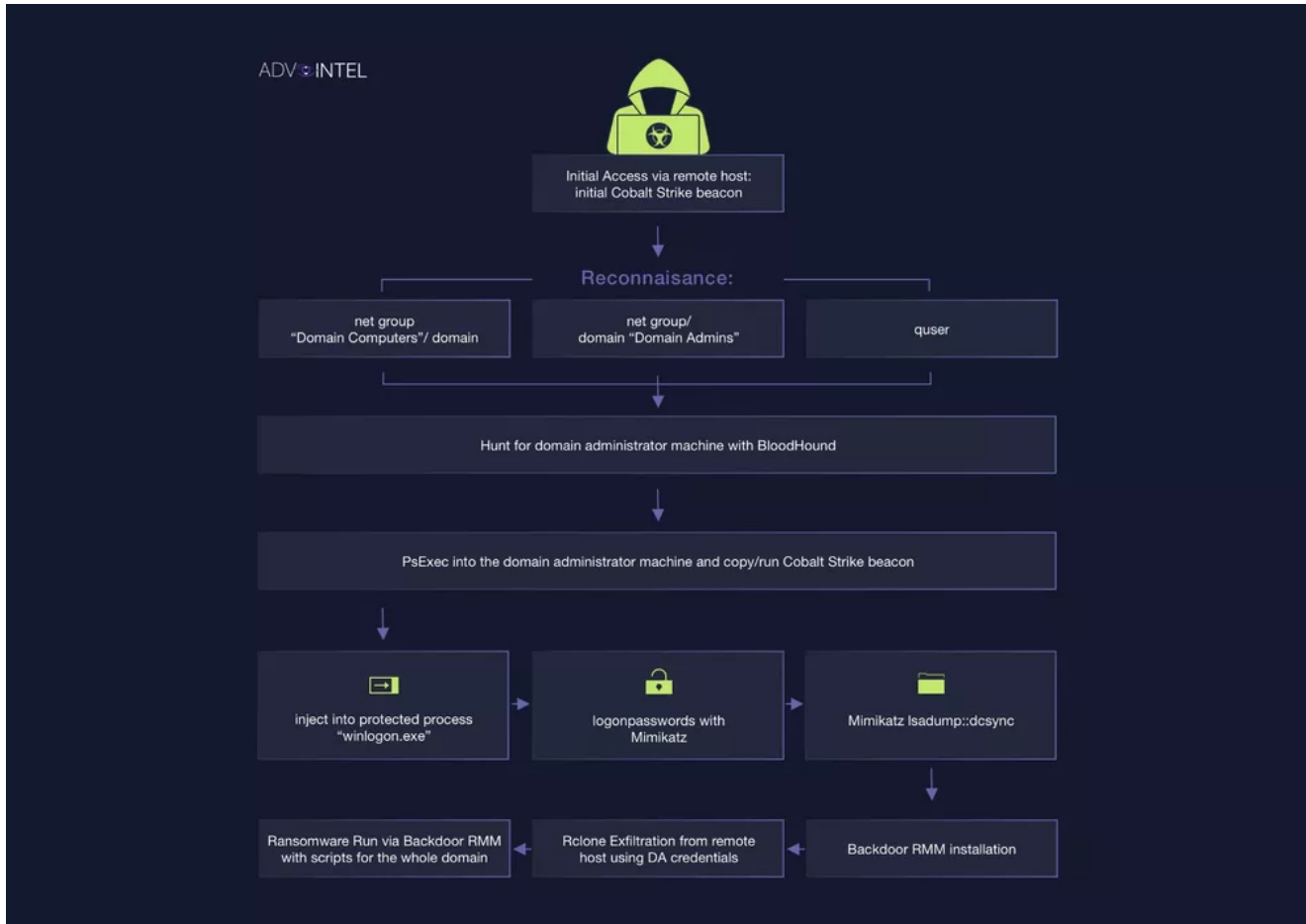
For more information on Ransomware victimology and initial accesses please reach out directly via the request to support@advintel.tech.

*Redacted screenshots from the 2021-12-14 Breach Pulse sent to AdvIntel clients, from the **Andariel Database**. Identifying information of adjacent compromises has been redacted. A full report, containing specific IOCs and details about the scale of compromise is available per request via support@advintel.tech.*

The attack developed through the following set of *Cobalt Strike commands* on the targeted 49ers host (the following actual executed commands are listed in chronological order of execution during this incident).

With the use of Cobalt Strike, the Conti team who began the operation against the 49ers on December 14 were able to compromise the victim's *primary domain* and get access to the *local shares* and core *network segments* for several departments, including the team's

finance and accounting sectors. Using its unique adversarial insight, AdvIntel was not only able to spot the initial compromise by finding the Cobalt Strike intrusion but also identified the actor behind the attack (the likely Patient Zero), as well as the scale of the initial intrusion.



It should be noted that Conti's presence in the network shares enabled them to map internal folders and identify critical information which could be then handled by other groups for exfiltration and data encryption. In this case, Conti used a *Cobalt Strike* beacon to *move laterally through a network silently* in order to investigate it and map it to full capacity, rather than hit it directly.

AdvIntel identified at least **14 domain admins** that were targeted. Several of the network shares accessed are shown in the above image, such as **Accounting, Finance, and Compensation Plans**, along with numerous others, including:

- Compliance Management

- Corporate Partnerships
- EngineeringOps
- Equipment
- Human Resources
- IT
- Legal
- Payroll-grp
- Records Management
- Sales

This reconnaissance and initial mapping operation is the most fundamental stage in any ransomware attack. If Conti's presence had been addressed when it was reported in December, the recent incident involving the 49ers would most likely never have taken place.

Cut Off the Head & the Body Survives

AdvIntel's credible primary source confirmed that Conti was the true architect of the 49ers breach. So how did BlackByte get their hands on the data?

The *BlackByte-Conti* liaison is more than just an organizational nuance—it is a *use case* for a much bigger trend sweeping the threat landscape: that of ransomware groups creating *sub-divisions* that are aimed exclusively at data exfiltration, without any encryption involved.

Suspicious files were also discovered at:

%AppData%\BB.ico

This file is the icon given to files with a .blackbyte file extension.

%AppData%\BlackByteRestore.txt

This file is the ransom note that is left in every folder where files are encrypted.

%AppData%\dummy

This file is a text file containing a list of machine names that can be reached on the network.

%HOMEPATH%\complex.exe

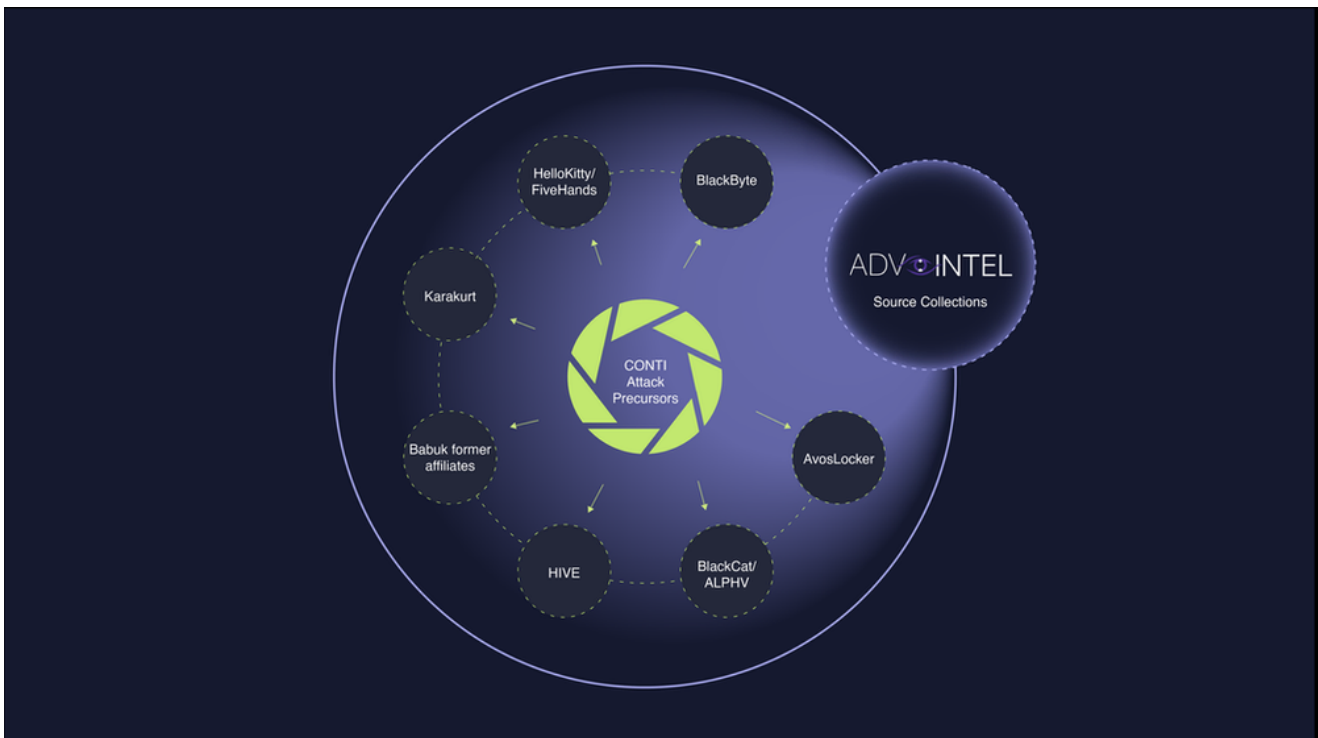
This file is the ransomware executable.

Users\tree.dll

This file contains the message "Your HACKED by BlackByte team. Connect us to restore your system." (SIC)

From the FBI's recent report on BlackByte. [Source]

The Conti syndicate is not what it was at the beginning of this year. The group, which has until recently been the largest and most enduring ransomware organization to continue well into 2022 (with REvil being dissolved at the top of the new year), is quickly shattering.







Since 2021, AdvIntel has observed Conti creating multiple alliances with other ransomware groups. These dynamics accelerated Conti's increasing disintegration, but at the same time enabled innovations to develop. One of the main innovations was the data exfiltration without encryption - tactics used by BlackByte in the 49ers case.

In November 2021, AdvIntel reported on Andariel that Conti had formed an alliance with fellow ransomware group HIVE while simultaneously attempting to negotiate similar agreements with both *BlackCat* and *HelloKitty*. Like a true criminal syndicate, Conti was folding into smaller gangs for peripheral operations to outsource some of its “dirty work”, and by December, Conti and HIVE had infiltrated the networks of an area of over 500,000 in Southern Italy.

At first glance, this may appear to cast a shadow of doubt on the notion of future ransomware subsidiaries (*AdvIntel has assessed that the reasoning behind the succession of splits was due to the sanctions involved in belonging to a powerful and well-established syndicate*) however, it is possible that this turn of events is instead illuminating the path to ransomware’s next *evolution*—one where fledgling subsidiary groups are poised to become cybercrime’s next major syndicates.

By handing over external commands on some of their smaller projects, Conti has, until recently, been able to harness a far greater breadth of control while still ensuring financial gain from all of their targets, in addition to protecting themselves from business interruptions in the case of unforeseen circumstances, such as server failure.

Title	Activity	RevShare	Offer	Expires at	Status
 <small>No disclosure links</small>	0	80%		—	created
 <small>No disclosure links</small>	0	80%		—	created
 <small>No disclosure links</small>	0	80%		—	created

AdvIntel has identified networks initially accessed by Conti on HIVE’s admin panel, listed as active targets.

By the beginning of 2022, the group's reliance on external brands for operations had begun to *internalize*: Instead of "networking", trying to build solid business connections within the chaotic and perpetually shifting ecosystem of ransomware groups, Conti began to delegate from *within*, spawning *in-house* subgroups specifically designed for data exfiltration. This method was what eventually led to the creation of BlackByte, as well as a second case study for Conti's expansion, **Karakurt**.

Karakurt emerged in December 2021 and quickly amassed records of over forty victims, becoming known for the rapacity with which it moved from target to target. In 2022, AdvIntel published a customer deliverable revealing that *Karakurt had been supplied with both network access and intelligence information prior to their credited compromises* by none other than Conti themselves. This was done in order to delegate Karakurt with cases in which data *theft* had to be performed, but not data *encryption*. The reasons for this decision are embedded in the inherent challenges of the *locker-centric model*, which have been explored by AdvIntel in its public blog post, which details the *Karakurt-Conti symbiosis* as well as gives further context into the history and psychology of Conti's various business ventures.

What is essential to note in the breach of the San Francisco 49ers is that Conti had already *meticulously mapped the network environment* prior to the data theft before handing off the final processes of the operation to BlackByte.

As relatively small and decentralized collectives that have rarely participated in large-scale attacks, it makes little sense for groups such as Karakurt or BlackByte to emerge alone, seemingly fully formed, from the ether of the criminal underground as a new wave of expansionist cyber-predators. Without Conti's interventionism at the head of a widespread realm of ransomware operations, the logic of smaller, independent groups like BlackByte as lone actors begins to fall apart.

CONCLUSIONS

What does this all mean for the future of the threat landscape?

Although we can only speculate for now, the *diversification* of Conti's criminal portfolio paired with its shockingly swift dissolution does bring into question whether their business model will be repeated among other groups.

Although not a ransomware-focused threat group, the well-known adversarial collective **TrickBot** did directly lead to the creation of Conti. Specifically, it was their "Overdose" division that helped to spawn the threat group **Ryuk**, which later rebranded as Conti. Conti continued to grow on its own until, in a reversal of its original dynamic with TrickBot, the syndicate essentially absorbed it into its own operations, turning TrickBot into a Conti subsidiary itself.

This is a strong candidate for the projected future of ransomware groups: As groups grow in size and scope, they will begin to spawn business derivatives to handle some of their smaller operations in return for assistance and resources. This, in turn, will allow those subgroups to grow independently of the larger group, before extenuating circumstances, such as *sanctions, struggles for power, or impending dissolution of the parent collective* eventually lead that subgroup to *split off* and become their own threat entity. Using this methodology, affiliates will have more direct pathways to find future groups as their current affiliation begins to die—and then the cycle begins again.

As it stands, BlackByte is already coming into their own as an independent group, spurred on by Conti's sudden fall from power. *Only time will tell if they can someday grow into the space left by the cybercriminal giant.*


Recommendations & Mitigations

- BlackByte is a data-stealing venture. Most mitigations should be directed at the detection of **abnormal network presence**.
- Special emphasis should be placed on **network investigation tools** typical for Conti's sub-divisions such as BlackByte, Black Basta, and Karakurt. These tools include: **Cobalt Strike sessions opened, Metasploit, and customized PowerShell commands** since all these tools are ubiquitous for Conti attacks.
- **Rclone** is the main data exfiltration command-line interface. Rclone activity can be captured through proper logging of process execution with command-line arguments.


- [For AdvIntel Customers]: 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. BlackByte focuses on extensive lateral movement to be able to find the most important shares containing data.

Secure Systems Against Conti Ransomware


The Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and National Security Agency recommend immediate and long-term actions to protect networks from Conti ransomware-as-a-service malware. The joint advisory details access and exploitation techniques observed, top mitigations to reduce risk of ransomware compromise, and these immediate actions for net defenders to take:




Require multi-factor authentication



Implement network segmentation



Consider using a patch management system to keep software updated



Go to [StopRansomware.gov](https://www.stopransomware.gov) for this and more actionable guidance to secure systems and counter the ransomware threat.

In addition to AdvIntel mitigations, the **FBI** has also published several recommended mitigations in regards to **BlackByte**. These mitigations include the following:

- Implement **regular backups of all data** to be stored as air-gapped, password-protected copies offline. Ensure these copies are not accessible for modification or deletion from any system where the original data resides.
- Install and regularly update **antivirus software on all hosts, and enable real-time detection**.
- Install **updates/patch operating systems, software, and firmware** as soon as updates/patches are released.
- **Review domain controllers, servers, workstations, and active directories** for new or unrecognized user accounts.

- **Audit user accounts with administrative privileges** and configure access controls with least privilege in mind. Do not give all users administrative privileges.
- **Disable unused remote access/Remote Desktop Protocol (RDP)** ports and monitor remote access/RDP logs for any unusual activity.
- Consider adding an **email banner** to emails received from outside your organization.
- **Disable hyperlinks** in received emails.
- Use **double authentication** when logging into accounts or services.
- Ensure **routine auditing** is conducted for all accounts.
- **Ensure all the identified IOCs are input into the network SIEM** for continuous monitoring and alerts.

Adversarial Assessment Summary [BlackByte]

BlackByte [Threat Group]

Malware Type: Ransomware

Origin: Eastern Europe

Intelligence Source: High Confidence

Functionality:

- Data encryption
- Data exfiltration
- Backup removal
- Utilization of legitimate software agents

MITRE ATT&CK Framework:

- T1486 - Data Encrypted for Impact
- T1068 - Exploitation for Privilege Escalation
- T1083 - File and Directory Discovery
- T1140 - Deobfuscate/Decode Files or Information

- T1489 - Service Stop

Distribution:

- Microsoft Exchange Server CVE
- Cobalt Strike
- PowerShell

Persistency: Very High

Infection Rate: High

Decrypter: Not Released

Threat Assessment: Critical

BlackByte is a Ransomware as a Service (RaaS) group that encrypts files on compromised Windows host systems, including physical and virtual servers. As of November 2021, BlackByte ransomware had compromised multiple US and foreign businesses, including entities in at least three US critical infrastructure sectors (government facilities, financial, and food & agriculture), although the group has remained relatively uncentralized. In February of 2022, AdvIntel found evidence that BlackByte was working as a subsidiary group of Conti when the group was credited for a breach of the San Francisco 49ers.

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