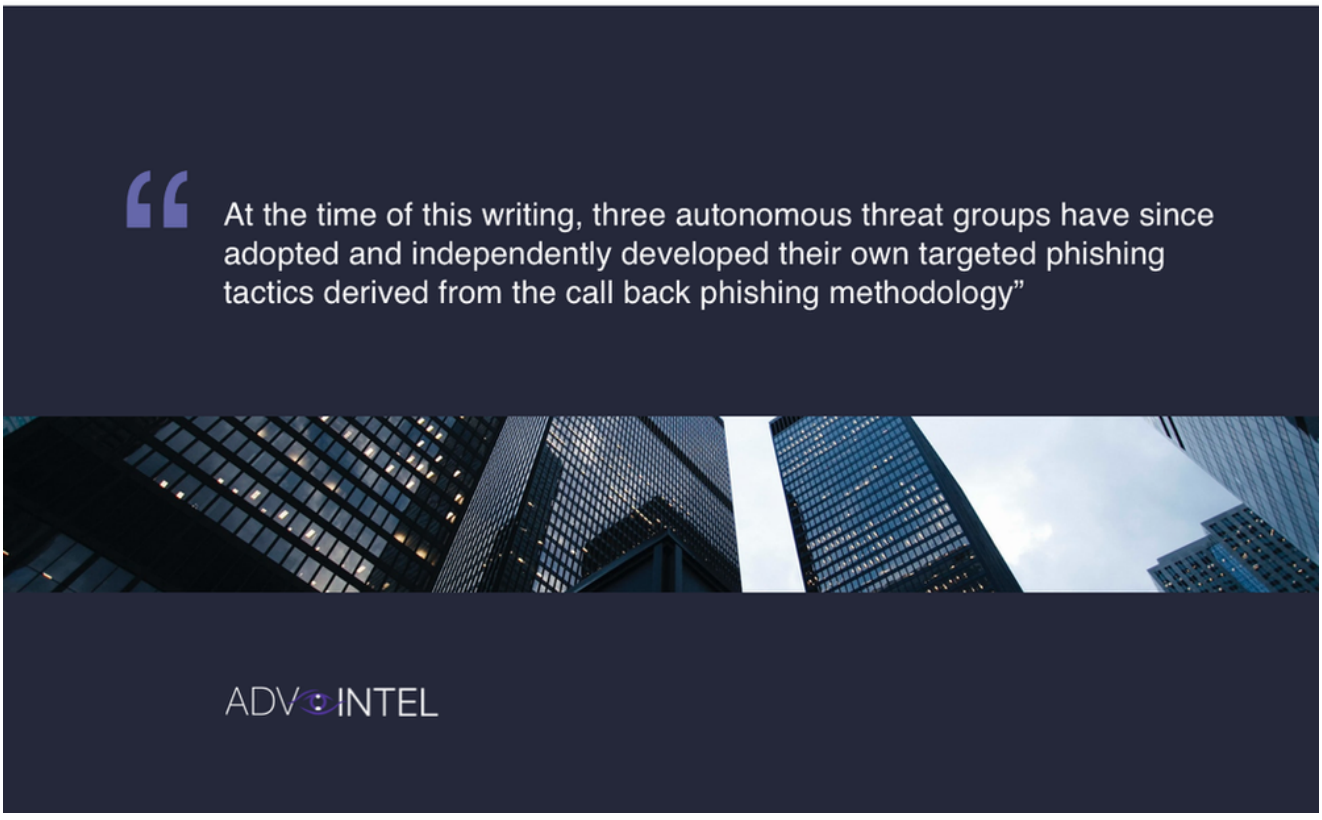
“BazarCall” Advisory: Essential Guide to Attack Vector that Revolutionized Data Breaches

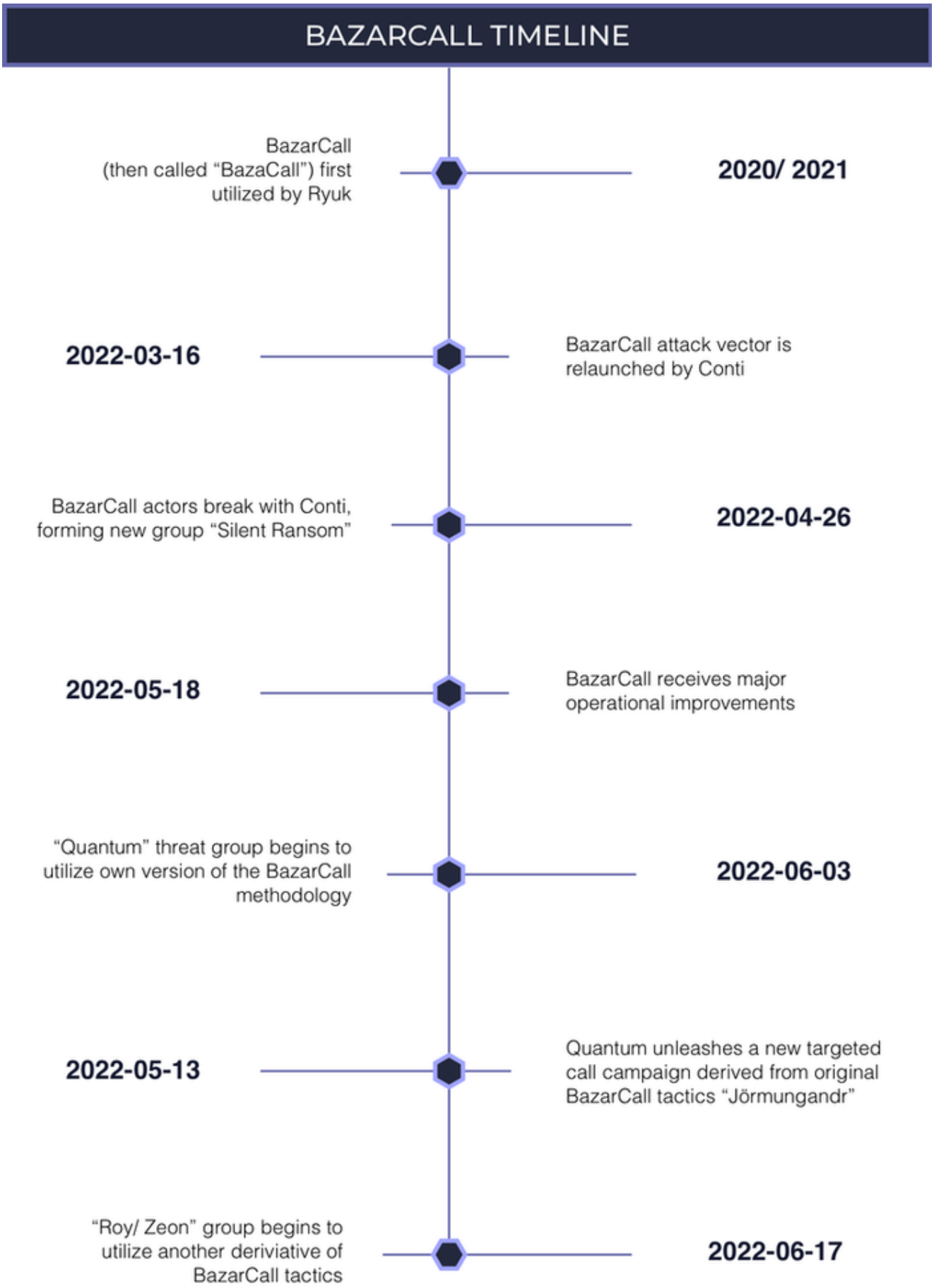
advintel.io/post/bazarcall-advisory-the-essential-guide-to-call-back-phishing-attacks-that-revolutionized-the-data

AdvIntel August 10, 2022

- Aug 10
-
- 5 min read

“BazarCall” style attack, or call back phishing, is an attack vector that utilizes targeted phishing methodology and that first emerged in 2020/2021 as a tool of Ryuk (later rebranded Conti).

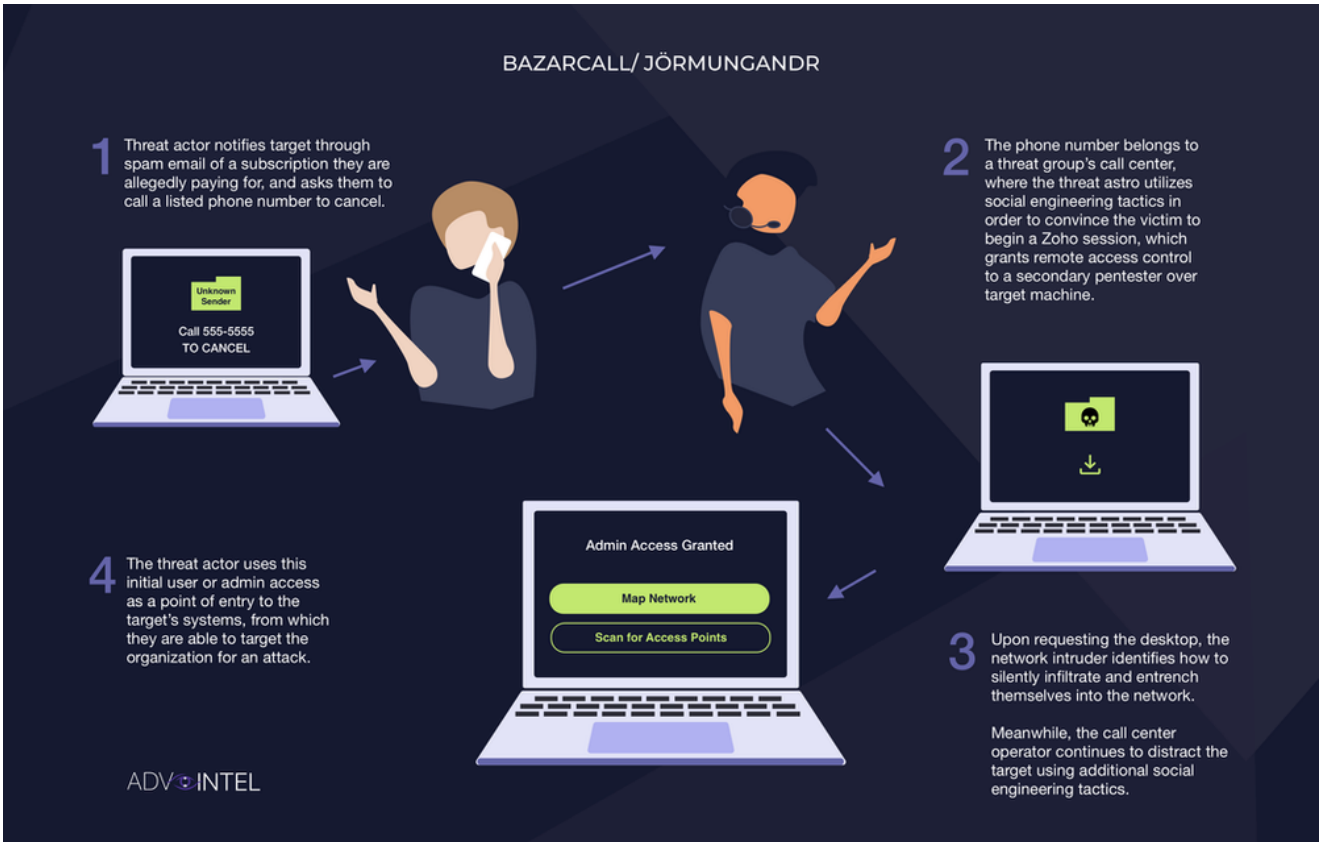



BAZARCALL TIMELINE
BazarCall (then called "BazaCall") first utilized by Ryuk
2020/ 2021
2022-03-16
BazarCall attack vector is relaunched by Conti
BazarCall actors break with Conti, forming new group "Silent Ransom"
2022-04-26
2022-05-18
BazarCall receives major operational improvements
"Quantum" threat group begins to utilize own version of the BazarCall methodology
2022-06-03
2022-05-13
Quantum unleashes a new targeted call campaign derived from original BazarCall tactics "Jörmungandr"
"Roy/ Zeon" group begins to utilize another deriviative of BazarCall tactics
2022-06-17

The tool has proven useful and malleable enough to fit an entire lineage of criminal hands. Callback phishing tactics have widely proliferated, completely changing the current threat landscape. At the time of this writing, three autonomous threat groups have since adopted and independently developed their own **targeted phishing tactics derived from the call back phishing methodology:**

1. Silent Ransom
2. Quantum
3. Roy/Zeon

BazarCall is notable for reversing the dynamic of a typical phishing operation with an advanced understanding of social engineering and targeted phishing (otherwise known as **Spearphishing**) and for quickly improving and adapting its operational tactics after only a three-month period.



Infographic detailing the BazarCall process. After splitting from Conti & becoming an autonomous group, Quantum formed their own version of the BazarCall campaign named "Jörmungandr". ***[Source: AdvIntel]***

How BazarCall Works

- **Stage One.** The threat actor sends out a legitimate-looking email, notifying the target that they have subscribed to a service for which payment is automatic. The email gives a phone number that targets are able to call to cancel their subscription.
- **Stage Two.** The victim is lured into contacting a special call center. When operators receive a call, they use a variety of social engineering tactics, to convince victims to give **remote desktop control**, ostensibly to help them cancel their subscription service.
- **Stage Three.** Upon accessing the victim's desktop, a skilled network intruder silently entrenches into the user's network, weaponizing legitimate tools that were previously typical of Conti's arsenal. The initial operator remains on the line with the victim, pretending to assist them with the remote desktop access by continuing to utilize social engineering tactics.
- **Stage Four.** In the final stage of BazarCall, the initiated malware session yields the adversary access as an initial point of entry into the victim's network. This initial access is then used and exploited in order to target an organization's data.

How BazarCall Revolutionized the Threat Landscape

The targeting capabilities of call back phishing have been revolutionary for post-Conti and the larger ransomware community since the operations resurgence:

Traditionally, ransomware has been reactive. Targets are random, decided by which ones happen to fall prey to infection. Hypothetically, a ransomware collective could send out 1,000 Emotet infections that are able to yield access for just ten organizations. The collective cannot afford to pick and choose in regards to their victims' revenues, jurisdiction, industry, etc. This cost/benefit ratio was severely limiting the potential of successful ransomware deployment, and therefore potential profit.

BazarCall leaders (as previous members of the Conti/TrickBot/Bazar alliance) were also aware that one of the challenges that led to the downfall of older ransomware groups was the repetitiveness of their attack patterns, which allowed for mitigations to be developed and honed against them as well as eventually leading to earlier and earlier detections.

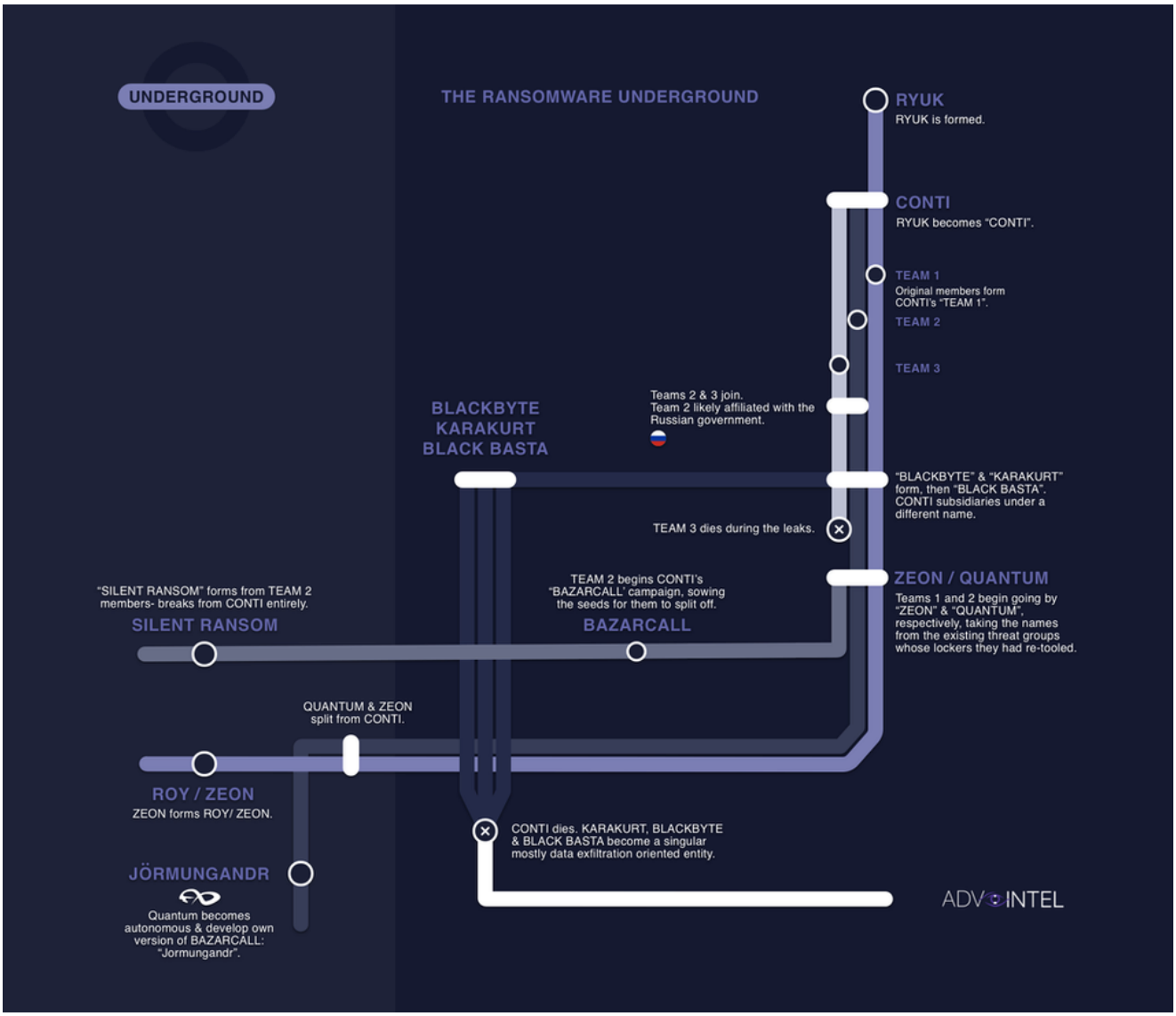
This all led to a natural business crisis among ransomware operators as the defenses and compliance became more rigid and effective. Said by a member of Conti during internal communications:

> *"We can't win the technology war because on this ground we compete with billion-dollar companies, but we can win the human factor".*

Callback phishing was the tactic that enabled a widespread shift in the approach to ransomware deployment. This is what made the approach so unique and effective:

1. Instead of automated botnet infections, a targeted selective approach is employed when the victim or victim industry is chosen before the attack campaign begins.
2. Instead of generic Emotet-style spam, a sophisticated phishing campaign is tailored for a specific industry/victim.
3. Instead of chaotic extortion strategies, a conceptualization of how to weaponize/maximize risk frameworks for the targeted victim is developed.
4. Instead of reliance on the same methodology each time, constant changes are made to the campaign's content- no repetitions.
5. And finally, instead of focusing on data encryption, there is a definitive shift in focus to data exfiltration.

Who Uses BazarCall



Infographic depicting Conti's splits, mergers, and dissolution into the set of groups now leveraging call back phishing tactics.

The callback phishing attack vector is intrinsically embedded into the Conti organizational tradition. It was conceptualized during the initial phase of Conti's operational crisis, between December 2021 and February 2022, and was actualized during the prime of this crisis in February-March 2022.

Today it is used by three separate but connected post-Conti groups:

- Silent Ransom

- Quantum
- Roy/Zeon

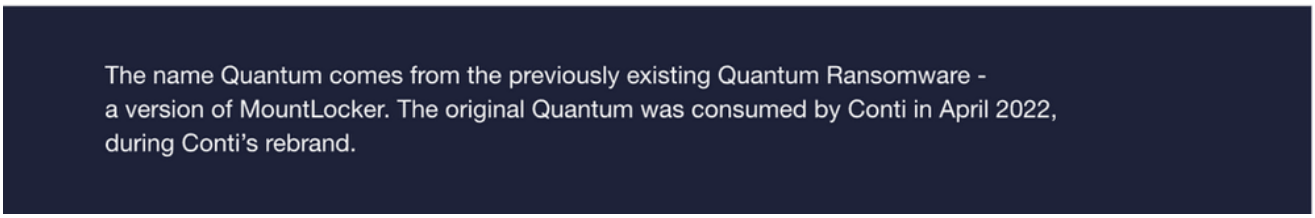
Silent Ransom

In March 2022, call back phishing experts split from Conti and created “Silent Ransom” when it became an autonomous group. They were operating for several months, and their tactics proved to be a success. Silent Ransom realized they could successfully avoid sanctions, regulations, and poor branding associated with the dying Conti.

AdvIntel graph charting target revenue for Silent Ransom, the progenitor of all current post-Conti phishing campaigns. Note that the average revenue stays close to the $10 billion USD revenue mark, which Roy/Zeon has made their target demographic.

Quantum

However, this understanding also came for Silent Ransom's previous bosses - Conti Team Two - the main Conti subdivision, allying with the Russian invasion into Ukraine and responsible for the **Costa Rica attack.**



Enraged by the "betrayal" and subsequent success of their subordinates, the Conti Team Two, at that point rebranded as Quantum, began their own version of call back phishing operations. On June 13, 2022, AdvIntel identified the launch of a massive novel operation called **"Jörmungandr"**.

It involved large investments into hiring spammers, OSINT specialists, designers, call center operators, and expanding the number of network intruders. As a highly skilled (and most likely government-affiliated) group, Quantum was able to purchase exclusive email datasets and manually parse them to identify relevant employees at high-profile companies.

Roy/Zeon

The third and the last iteration of the BazarCall group came in late June 20 by Roy/Zeon. This group came from the old-Guard members of Conti's "Team One" responsible for the creation of Ryuk itself. They demonstrated the best social engineering capabilities of the three groups.

The "Roy/Zeon" name comes from the use of two lockers, named Zeon and Roy respectively.

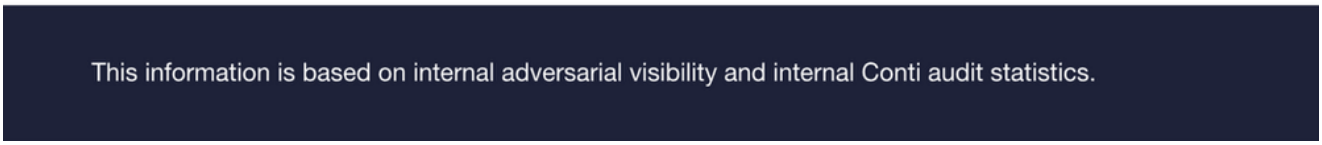
As Conti Team One, this group was responsible for major attacks such as:

- **JVCKenwood hit by Conti ransomware claiming theft of 1.5TB data**

- **Graff Gets Hit by Ransomware Attack**

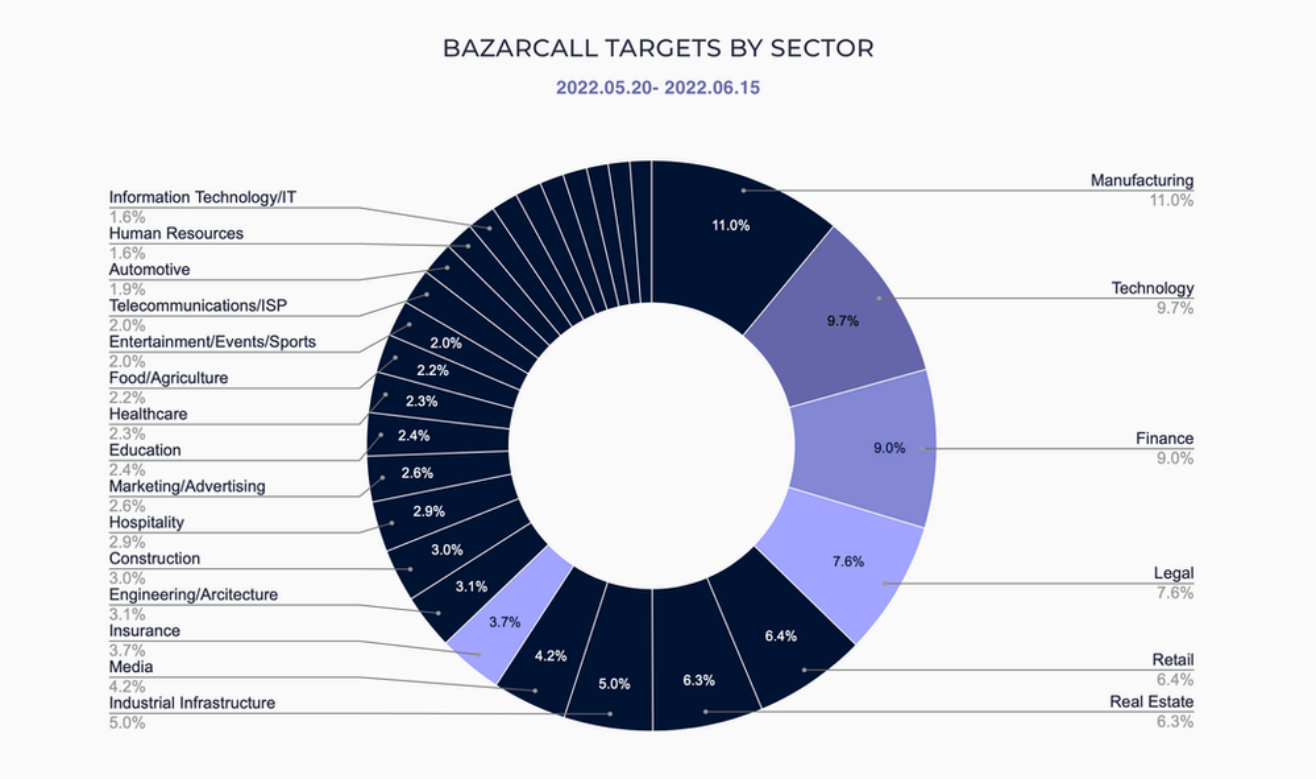
The group has been extremely selective in its approach and tends to engage in **Big Game Hunting** (judging by the high average revenue and/or sector and industry value of their targets).

Victimology of BazarCall

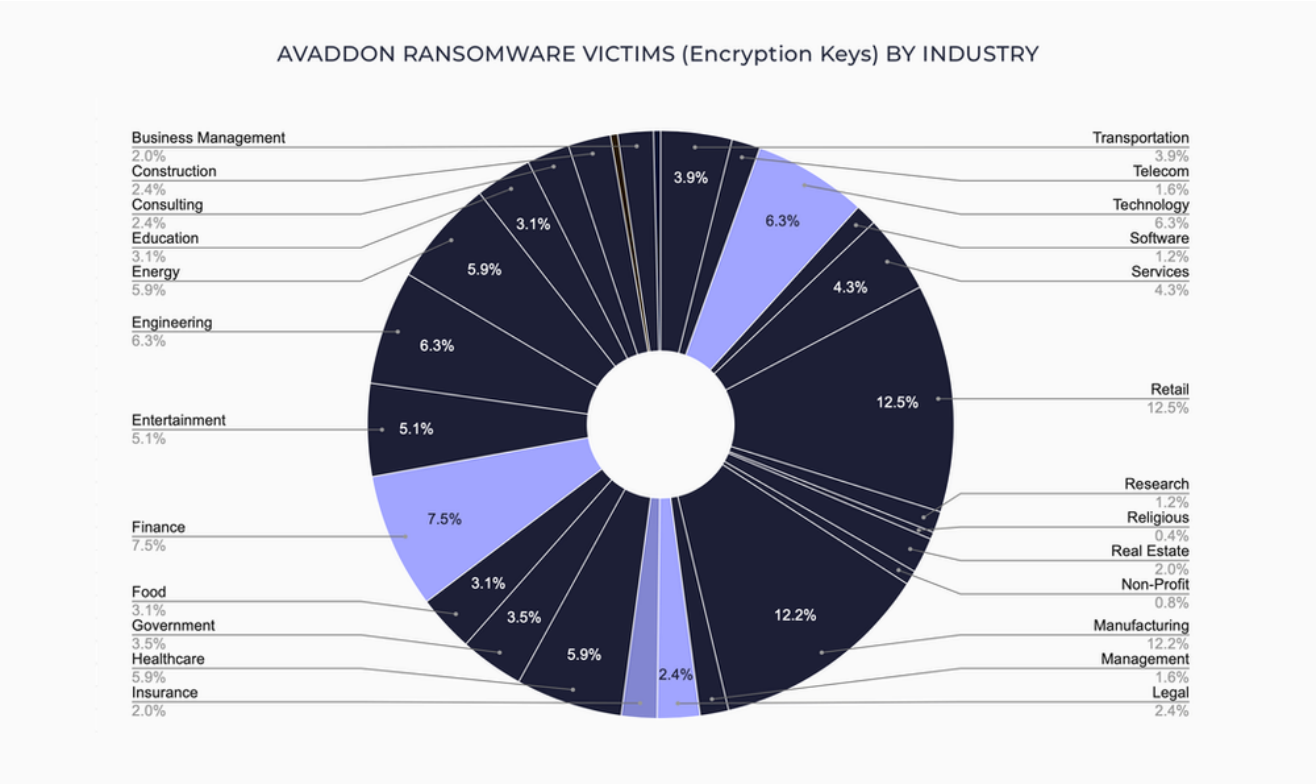


Callback phishing campaigns have shifted ransomware's victimology drastically. Compared to pre-Bazar groups such as **Avaddon** (for example), there are visible changes in the sectors targeted.

The targeted nature of these campaigns substantially increased attacks against **Finance**, **Technology**, **Legal**, and **Insurance**. These are four priority industries that were listed in almost all internal manuals, which were shared between ex-Conti members.



For Silent Ransom and Roy/Zeon, there is an evident increase in legal, finance, and Insurance targeting compared to Avaddon or other non-Bazar groups.



Conclusion

Since its resurgence in March earlier this year, call back phishing has entirely revolutionized the current threat landscape and forced its threat actors to reevaluate and update their methodologies of attack in order to stay on top of the new ransomware food chain.

Although the first to begin using this TTP as its primary initial attack vector, Silent Ransom is no longer the only threat group utilizing the highly specified phishing operations that they pioneered. Other threat groups, seeing the success, efficiency, and targeting capabilities of the tactic have begun using reversed phishing campaign as a base and developing the attack vector into their own.

This trend is likely to continue: As threat actors have realized the potentialities of weaponized social engineering tactics, it is likely that these phishing operations will only continue to become more elaborate, detailed, and difficult to parse from legitimate communications as time goes on.

*** Request White Paper on BazarCall Deep-Dive Report below:**

Request White Paper