Conti puts the ‘organized’ in organized crime

intel471.com/blog/conti-leaks-cybercrime-fire-team

Combing through business intelligence platforms to find new prospects. Deciding whether to focus on huge multinational companies or small- and medium-sized businesses. Finding the right person to contact in the organization. Developing a script that will land information that’s critically needed for success.

The above scenario is one that may seem familiar to anyone that works in sales. However, this set of actions has also been adopted by organizations which make money by less conventional means, particularly criminals who are responsible for ransomware attacks.

Due in part to the leak of information tied to the Conti ransomware group, Intel 471 was able to piece together the inner workings of the notorious criminal syndicate. With this information, researchers were able to understand how Conti conducted its actions, which often mirrored processes used by countless legitimate businesses.

Intel 471 discovered communications tied to one division of Conti which had its own dedicated mission. This team was responsible for collecting information on targets for ongoing and future attacks, drafting phishing scripts that were used over the phone and sent via email, and applying multiple forms of pressure in the course of ransomware negotiations. The team had access to several open-source intelligence (OSINT) and business intelligence tools, as well as a legal “expert” who provided advice on how to threaten victims with litigation or official complaints that would be sent to government authorities. In chats found by Intel 471 researchers, some team members were unaware they were working for criminals, instead believing they worked for a company providing competitive intelligence to their customer base.

Team Building!

The division, known inside Conti as the “Fire Team,” started in July 2021 as a way for the gang to invent cover stories for phishing phone calls to targeted personnel, as well as randomize spam letters to potential victims. By November 2021, the team consisted of 10 people, which prepared operational and revenue reports on potential targets. The team leader allegedly made US $3,000 per month while members were paid US $2,000 per month. In addition to their salary, team members also received a one percent cut of any ransom they helped negotiate. While ransom cuts were dispersed via cryptocurrency, some salaries were paid via prepaid bank cards.

Despite initially being stood up to do reconnaissance on future targets, the team started ransomware negotiations as more members were brought on board.

I'm going to need those TPS reports... ASAP

The reports put together by the team contained general information on targeted companies that included operations and revenue. However, the team focused heavily on the target's personnel. The reports were required to include phone numbers, email addresses and social media accounts of the company's leadership, mid-level employees, and some information technology personnel. Leaders requested contact information of at least 20 personnel per report, with encouragement to focus on female employees.

Some people were also tasked to collect open source information on a target's network infrastructure following directions that included:

- Internet domains
- WHOIS data like IP notations, domain registrar, age, and who purchased the domain.
- Subdomains, with IP addresses if possible
- SSL certificates in raw format, open TCP ports, and vulnerabilities found using OSINT tools

"Remember, any information about the company may be useful for its competitor (our client), therefore, do not disregard any nuances that may seem insignificant at first glance. We need EVERYTHING!," a team leader posted in a Russian-language chat discovered by Intel 471 researchers.

The team apparently utilized several tools and subscription-based services to gather the information required. Those most frequently mentioned included the SignalHire contact information platform, the SpiderFoot OSINT tool and the Shodan search engine. Another team member brought on in November 2021 apparently also had access to a paid version of the ZoomInfo business intelligence platform.

Companies that made the cut

In the early stages of standing up the division, the higher-level leaders of Conti asked for draft reports on a variety of high-profile technology, pharmaceutical and finance industry companies. However, a month later, the team changed direction, focusing on organizations in the aerospace, chemical, defense, energy, hospitality and medical equipment industries, particularly those with an annual revenue from US $500 million to US $5 billion.

As affiliates launched attacks, reconnaissance assignments changed. Actors from other parts of the group told the team to find information on dental clinics and online stories, as they were considered to be the "best" targets. Preference also was given to insurance, law and logistics companies.

Circling back on deliverables

The Fire Team's leader took the information gathered in the reports and used it for various ransomware negotiations, often collaborating with other people working within the syndicate. Some of these actors managed calls to Conti victims and potential targets, while others would jump into ongoing conversations and leave messages for victims, even if they did not start the negotiation process. Additionally, an alleged "lawyer" familiar with U.S. and European legislation sought additional ways to pressure hacked companies with threats of litigation from customers or employees, or official complaints that would be sent to government authorities. This set of actors would also have side conversations about ransomware victims, primarily focused on data that would be posted on the Conti name-and-shame blog from time to time.

Over the course of the conversations Intel 471 researchers observed, other actors gave the Fire Team feedback on what types of companies it should reconnaissance on in the future. One actor specifically mentioned that they were having trouble convincing JP MorganChase employees over the phone to install malware. In turn the actor suggested targeting smaller companies with less strict security policies.

No job is perfect

Even criminal syndicates can't avoid office politics. Despite the structure set up by Conti, team members still complained to their bosses and one another about time spent working and the amount of money each member made. One team member who received 0.5% of ransom payouts often claimed to have a much higher workload compared to the team leader and complained about being exploited. The team leader often called this actor "greedy" and actively sought to give this person more work and pay the actor less.

Ransomware, Inc.

One of the biggest mysteries for years when discussing ransomware was wondering how these criminal groups conducted operations. With the Conti leaks, the information security community now has the best look it's ever gotten at what makes these criminal groups tick. As Intel 471's analysis shows, these groups are set up to conduct crimes as if they were a legitimate business. There are divisions dedicated to examining every facet of a potential target — no matter the size — in the hopes that the information can help them extract more money post-attack. The stereotype of young men in a basement coding their way into international crime sprees is woefully inaccurate. Ransomware-as-a-service groups operate like corporate entities, with payroll, revenue goals and salary bonuses worked into their operations. By understanding their inner workings, security teams can better adjust their threat models and take the necessary steps to make sure that security measures make similar reconnaissance efforts worthless.