Conti Internal Server Leak Research

Michael Twining

Department of Criminal Justice Studies, Utica University

[REDACTED]

[REDACTE]}

[REDACTED]

Conti Internal Server Leak Research

When thinking about ransomware groups, it is common to assume that it is merely a group of younger individuals that are hooded or cloaked, meeting at a local coffee shop and simply hacking into networks. However, the leak of 2022 from the Jabber chat server reveals the infrastructure of Conti Ransomware group, which is far from this common misconception (Check Point Research 2022). This leak helped break down the organizational structure, identify key roles, key individuals, hiring practices, and overall operational practices.

Conti Group's Org Structure with Roles and Responsibilities

Conti operated as a business with leadership teams, human resources, and technical employees, much like a legitimate business. Within the technical team, Conti utilized coders, testers, administrators, reverse engineers, and hackers. Coders we hired to write the malicious code, testers would test the code against security tools, administrators set up and tore down attack infrastructure like C2 servers, reverse engineers disassembled computer code to study and find ways to exploit vulnerabilities, and hackers simply were the front-line team stealing data and planting ransomware (Krebs on Security, 2022). Testers and crypters, worked closely together to ensure payloads were difficult to detect and maintained some form of obfuscation on a target machine (Check Point Research, 2022). Finally, the Conti group also had a staff of Open-Source Intelligence (OSINT) specialists and negotiation staff. OSINT specialists supported one of the most important pieces of the group's operations, which was to obtain as much information on a victim possible to determine key information on the victim's revenue, sector, and other factors to determine the ransom payment amount, while negotiators acted as the customer service team that communicates with the victim to obtain payment (Check Point Research, 2022).

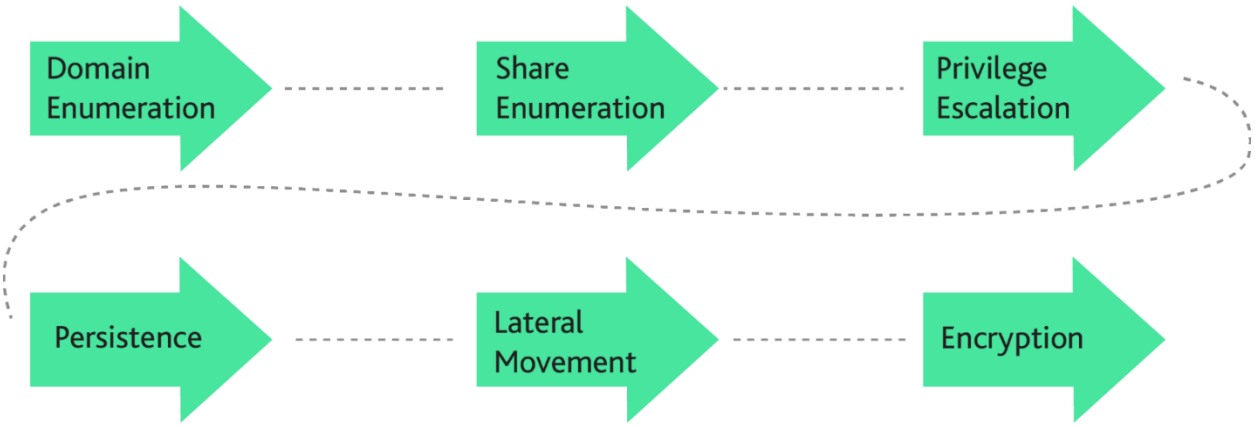
There are a few key members that held principal roles in the organization's success. Think of these individuals are directors or executive leadership. Stern is considered the big boss of the operation, developing high-level vision of operations and collaborations with affiliates, while also managing people and projects. Bentley is considered a technical lead for testing and evasion tactics and techniques of malware and payloads, over the crypters and testers. Mango's role was similar to the director of human resources, assisting the big boss, but also handed questions from team members and handled some payroll functions. Buza was responsible for the coders and the products they used, procuring any necessary tools needed for development. Target was another individual with human resource function, in charge of hackers, providing budgets, HR communication, and took part in social engineering campaigns. Lastly, Vernon was responsible for managing all campaign activities with Emotet, as an affiliate manager (Check Point Research, 2022).

Conti Group Operations

Operations of the cyber kill chain before ransom was demanded aligned with Figure 1, where the workflow of hackers were followed.

Figure 1

Conti Ransomware Operator Workflow. Source: ReliaQuest (Tirado, 2022)



The first stage was to determine the target's value, which was done by the OSINT specialists. Google Dorking was a technique used in obtaining this information that was available on the web. To obtain a foothold into the organization's infrastructure, hackers found ways to exploit any native Windows applications like net.exe or nltest.exe through Cobalt Strike Beacon's net module to enumerate any targets of interest and environmental protections that will help aid towards a successful attack. This also gave the hackers the potential access they needed to gain privileges in the target's environment. Next, they used tools to enumerate shares to identify files and directories of interest for holding ransom. Once they have a lay of the land, the next stage was to escalate their privileges by obtaining any credentials to administrative accounts using multiple tools. Once this has been successful, they use the administrative privileges to maintain persistence on the victim's network by exploiting windows accessibility features like sticky keys, execute backdoors in member, inject DLLs, and create scheduled tasks. This is not only to remain in the systems should one method be removed, but also to evade detection as they could be seen as legitimate activities from an antivirus program. Towards the final steps, the hacker then uses the privileges to run the locker program onto all domains and shares of interest which then encrypts them (Tirado, 2022).

Conti Group's Negotiation Strategy

One of the biggest things to consider is that the resources from Conti group's OSINT specialists have already determined their victim has the means to pay the specific ransom that was demanded. This is part of their pre-exploitation tasks, in fact the first. As part of the enumeration process, they are also looking for evidence of cyber insurance and bank statements to come prepared should the victim try to "low-ball" a counteroffer. Victims were usually double extorted to ensure they get something from their efforts should the victim refuse to pay. They were payment for the decryptor to unlock files and payment to avoid the dump from

being available to the public. They provide the victim with a link to their leaked site that contains a timer that the victim must make a payment (Krebs on Security, 2022b).

Negotiation Lessons to be Learned

Learning about the sophistication of the organization and the resources used by Conti, a negotiator may be able to take a few things into account when trying to successfully negotiate with them. The leak has brought to light the organizational and operational flow. The negotiator who sees the ransomware note from this group already can come to the table with an assumption that the group has identified the client with the ability to pay the demanded amount and has likely deployed techniques for maintaining persistence into their systems. The negotiator also knows that Conti is a Russian organization, so sanction rules may apply to their client who may not be able to pay due to regulations. Because of this leak, should an insurance carrier require information about the group or statistical data, this is readily available to the negotiator. The negotiator should try to buy time through a cadence of communications with the group, in this case asking for proof of life or proof pack and proof that the said decryptor will work. To start, the response after the initial demand has been made should be quick. The cadence afterwards does not have to be after each reply so long as communication does occur. The negotiator must also understand that the more time spent with the client is less time spent on another victim, which may increase their likelihood to settle for a lesser amount. Should the client want to offer a different amount, be sure there are plausible explanations to this, as we recall stage one of their approach is determining what the client can afford. This may lead to a response from them that alludes to what information they may know about the client's financial details if they have not already revealed it in their proof pack. These tips from the leaked chat may help to provide a successful negotiation.

References

Check Point Research. (2022, March 10). Leaks of Conti Ransomware Group Paint Picture of a Surprisingly Normal Tech Start-Up… Sort Of. *Check Point Research*. https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/.

Krebs on Security. (2022, March 2). Conti Ransomware Group Diaries, part II: The office. https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/.

Krebs on Security. (2022b, March 4). Conti Ransomware Group Diaries, part III: Weaponry. https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/.

Tirado, B. (2022, June 13). How the Conti Ransomware Gang Orchestrated Their Attacks. *ReliaQuest*. https://www.reliaquest.com/blog/conti-ransomware-gang-attack-methods/.