Move fast and commit crimes: Conti’s development teams mirror corporate tech

By Intel 471

Published: 2026-04-01 · Archived: 2026-04-06 01:02:39 UTC

There has been a long-lasting trope about cybercriminals for nearly two decades: young men sitting alone in a dark basement, hopped up on energy drinks and EDM basslines, crafting code into the wee hours of the morning in the hopes their malware will net them millions of dollars after they hack their way into the world’s leading companies. This idea has creeped into the information security industry’s mindset, mainly that it’s nearly impossible to stop these kinds of criminals, who work in small teams or by themselves, because they don’t have to follow the corporate norms that are put in place to protect organizations.

The recent Conti leaks flip this narrative on its head. Researchers with Intel 471 have found that the ransomware group’s development operations mirror that of most technology-focused companies: scores of employees separated by divisions, building “products" with commonly-used tools, and a focus on tech-savvy concepts like “continuous integration” and “continuous delivery.” By mirroring the corporate culture of most technology companies, it changes the paradigm for organizations that need to protect themselves. Instead of the idea that a rag-tag group of tech-minded marauders are outmaneuvering organizations’ security teams, the reality is that ransomware gangs are devoting time, effort, manpower and money on a business-like level for the sole purpose of extorting legitimate businesses.

Crime needs lots of code

Intel 471 estimates that at one point Conti included as many as 150 members, with different departments and teams working on a variety of projects. Conti’s backbone was the development team, with subdivisions responsible for building malware, testing its functionality, and recruiting and onboarding new employees. Each team has “subteams” responsible for their own tasks and projects, including a team specifically working on the BazarBackdoor and TrickBot malware. It also included coders developing malware crypters, front- and back-end environments, TrickBot web-injects and various other modules.

There were at least eight “senior” developers who were responsible for different ransomware builds, while also floating between teams responsible for other malware, crypting services, and support projects. Senior developers also reached out to various affiliates for “customer service,” discussing particular attacks and providing various ransomware builds and decrypters.

Team leaders placed specific focus on the crypting efforts, which was created to keep malware hidden from antivirus software and cybersecurity experts. As many as 13 developers worked on crypting services, from development to testing to source code review.

The development team also supported other semi-legitimate projects the group leadership promoted in addition to malware, including the idea of launching a “private social network” for cybercriminals and a blockchain platform

similar to the BNB Chain exchange.

Business as usual

The Conti group tasked team members to recruit developers on legitimate freelance marketplaces as well as underground cybercrime forums. Human resource representatives and respective team managers usually told newcomers they would be going to work on “illegal” projects and taught them about operational security measures. Some employees were comfortable with what was presented to them, while others struggled with finding the right level of operational security. Here is a sample of two conversations with new employees:

[Image: Conti Team Blog image1 Dialog]

[Image: Conti Team Blog image2 Dialog]

The average salary of a developer was about US $2,000 a month, and those who performed well and met project deadlines received bonuses. The group offered awards, bonuses and opportunities for career growth. However, bosses were vocal with those who underperformed and threaten to penalize developers’ earnings if they did not meet benchmarks:

[Image: Conti Team Blog image3 Dialog]

[Image: Conti Team Blog image4 Dialog]

Even criminals have customer service

The Conti team apparently had members who engaged with clients, discussing inquiries and eliminating bugs that would appear in the malware:

[Image: Conti Team Blog image5 Dialog]

The same person who chided poor performance among other developers was also tasked with reaching out to clients in a sales engineer capacity. The following conversation shows him instructing a customer on what to check before using new builds in future schemes:

[Image: Conti Team Blog image6 Dialog]

All in a day’s work

The conversations uncovered by Intel 471 could arguably be found in any legitimate organization that depends on code development to be operationally successful. Given that the conversations were happening in an organization devoted to cybercrime serves as evidence that ransomware gangs are not fly-by-night operations. These groups are organized enough to know that they need time to remain a lucrative endeavor and multiple levels of technical talent to meet those goals. By understanding how closely ransomware gangs mirror legitimate technology firms, security teams can formulate their defensive posture and establish to the rest of their organization’s operations what needs to be done in order to keep their enterprise safe.