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

intel471.com/blog/conti-leaks-ransomware-development

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.

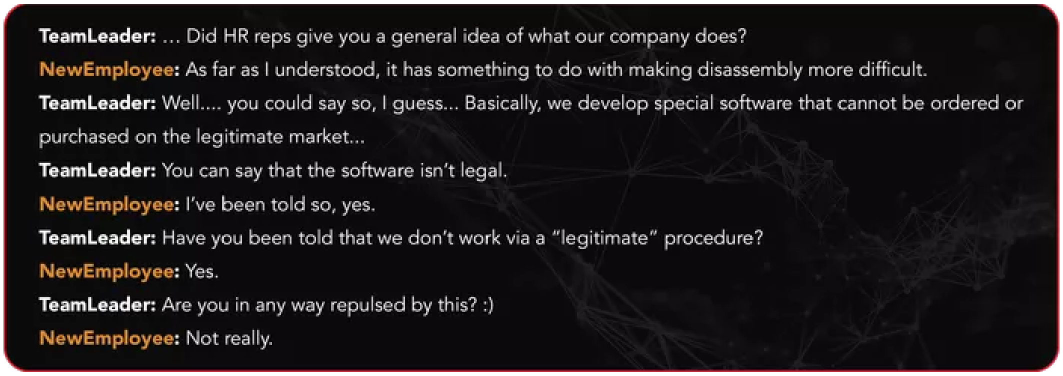
There were at least eight “senior” developers who were responsible for different ransomware builds, while also floating between teams responsible for other malware, crypting services, and support projects. Senior developers also reached out to various affiliates for “customer service,” discussing particular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

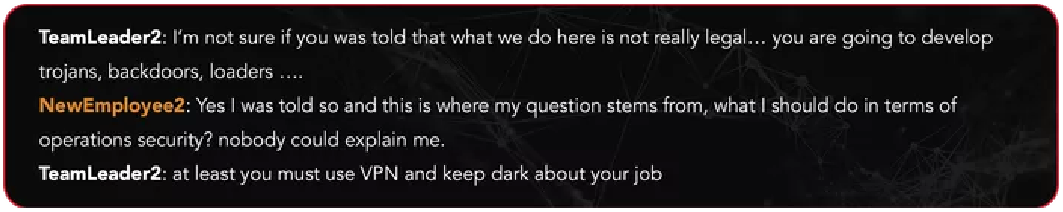
The development team also supported other semi-legitimate projects the group leadership promoted in addition to malware, including the idea of launching a “private social network” for cybercriminals and a blockchain platform similar to the BNB Chain exchange.

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:

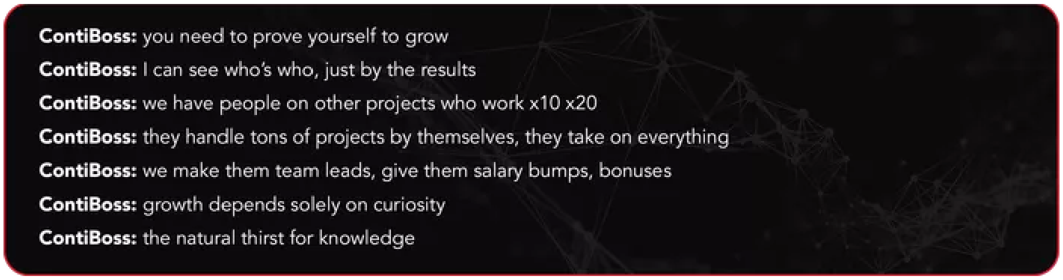


TeamLeader: … Did HR reps give you a general idea of what our company does?
NewEmployee: As far as I understood, it has something to do with making disassembly more difficult.
TeamLeader: Well.... you could say so, I guess... Basically, we develop special software that cannot be ordered or purchased on the legitimate market...
TeamLeader: You can say that the software isn’t legal.
NewEmployee: I’ve been told so, yes.
TeamLeader: Have you been told that we don’t work via a “legitimate” procedure?
NewEmployee: Yes.
TeamLeader: Are you in any way repulsed by this? :)
NewEmployee: Not really.

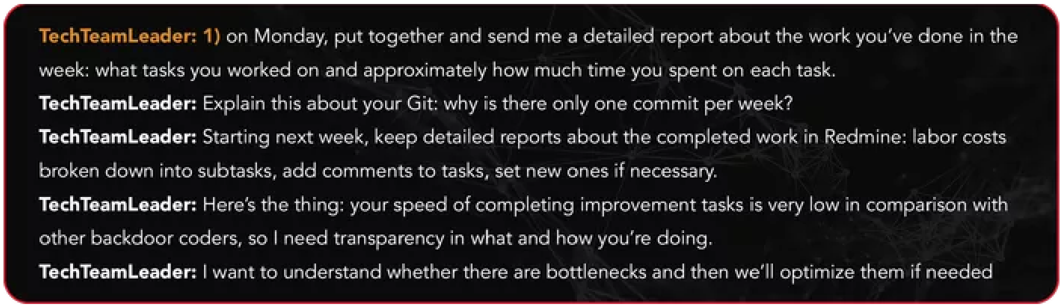


TeamLeader2: I’m not sure if you was told that what we do here is not really legal… you are going to develop trojans, backdoors, loaders ….
NewEmployee2: Yes I was told so and this is where my question stems from, what I should do in terms of operations security? nobody could explain me.
TeamLeader2: at least you must use VPN and keep dark about your job

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:



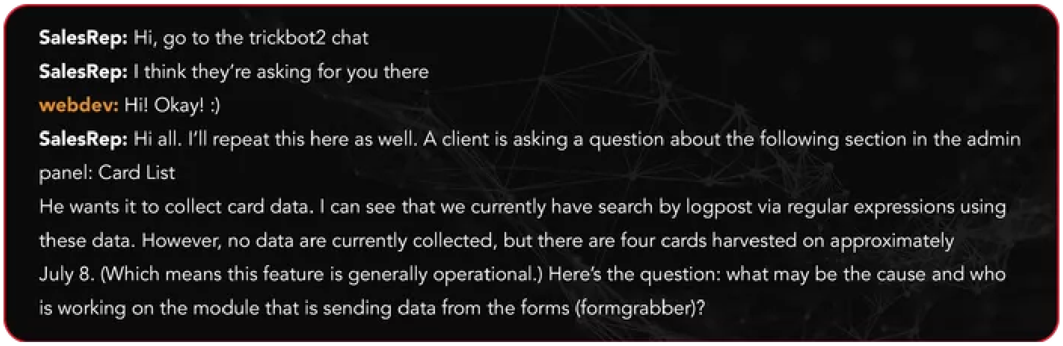
ContiBoss: you need to prove yourself to grow
ContiBoss: I can see who’s who, just by the results
ContiBoss: we have people on other projects who work x10 x20
ContiBoss: they handle tons of projects by themselves, they take on everything
ContiBoss: we make them team leads, give them salary bumps, bonuses
ContiBoss: growth depends solely on curiosity
ContiBoss: the natural thirst for knowledge



TechTeamLeader: 1) on Monday, put together and send me a detailed report about the work you've done in the week: what tasks you worked on and approximately how much time you spent on each task.
TechTeamLeader: Explain this about your Git: why is there only one commit per week?
TechTeamLeader: Starting next week, keep detailed reports about the completed work in Redmine: labor costs broken down into subtasks, add comments to tasks, set new ones if necessary.
TechTeamLeader: Here's the thing: your speed of completing improvement tasks is very low in comparison with other backdoor coders, so I need transparency in what and how you're doing.
TechTeamLeader: I want to understand whether there are bottlenecks and then we'll optimize them if needed

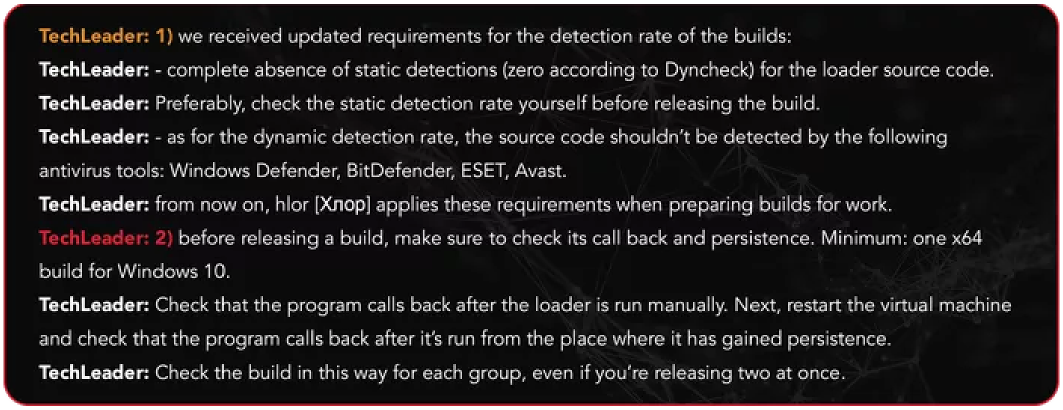
Even criminals have customer service

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



SalesRep: Hi, go to the trickbot2 chat
SalesRep: I think they're asking for you there
webdev: Hi! Okay! :)
SalesRep: Hi all. I'll repeat this here as well. A client is asking a question about the following section in the admin panel: Card List
He wants it to collect card data. I can see that we currently have search by logpost via regular expressions using these data. However, no data are currently collected, but there are four cards harvested on approximately July 8. (Which means this feature is generally operational.) Here's the question: what may be the cause and who is working on the module that is sending data from the forms (formgrabber)?

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:



TechLeader: 1) we received updated requirements for the detection rate of the builds:
TechLeader: - complete absence of static detections (zero according to Dyncheck) for the loader source code.
TechLeader: Preferably, check the static detection rate yourself before releasing the build.
TechLeader: - as for the dynamic detection rate, the source code shouldn't be detected by the following antivirus tools: Windows Defender, BitDefender, ESET, Avast.
TechLeader: from now on, hlor [Хлор] applies these requirements when preparing builds for work.
TechLeader: 2) before releasing a build, make sure to check its call back and persistence. Minimum: one x64 build for Windows 10.
TechLeader: Check that the program calls back after the loader is run manually. Next, restart the virtual machine and check that the program calls back after it's run from the place where it has gained persistence.
TechLeader: Check the build in this way for each group, even if you're releasing two at once.

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.