Conti pivots as ransomware as a service struggles

Threat Research | April 8, 2022

Blog Author
Paul Roberts,

Cyber Content Lead at ReversingLabs. Read More...

The Conti ransomware group —a.k.a. Wizard Spider; a.k.a. TrickBot; a.k.a Ryuk—is one of the most prolific ransomware gangs around. It is believed to have been active, in various incarnations, since about 2016. Just in the last year, Conti is believed to be responsible for high profile attacks, including the city government in Tulsa, Oklahoma and Ireland's Health Executive service in May, 2021.

Even as leading ransomware groups like REvil and Darkside have folded in recent months, Conti is getting renewed attention from cybersecurity experts. The group, CISA warns, has been linked to more than 1,000 attacks on U.S. and international organizations while “Conti cyber threat actors remain active.”

2021: A ransomware extinction event?

The contrast is worth noting. In fact, 2020 and 2021 saw something like a mass extinction event among high profile ransomware gangs and ransomware as a service outfits. There was the digital takedown of infrastructure used by the REvil ransomware group, followed by the arrests of REvil group members by Russian authorities in January, 2022. In May, 2021, the Darkside ransomware group - which is believed to be responsible for the attack on the Colonial Pipeline - said it was ceasing operations as well. That announcement coincided with a coordinated law enforcement seizure of some of the group’s infrastructure and cryptocurrency from the wallets of some Darkside affiliates. In November, BlackMatter, another ransomware as a service group, said it was shutting down in the face of increased scrutiny from law enforcement.

Conti thrives amid chaos

Despite this, Conti has been thriving. Why? In our latest episode of the ConversingLabs Podcast I sat down with Yelisey Boguslavskiy, a co-founder of the threat intelligence firm AdvIntel, to talk about Conti's evolution in recent years, and why the group continues to be such a potent threat.

According to Boguslavskiy, Conti's continued vitality reflects a long-running practice of tightly controlled and highly vertical business operations. That runs counter to the predominant "ransomware as a service" model of "quantity over quality:" farming work out to pretty much anyone interested in making a buck and counting on a small number of scores from a large base of attacks. "This is something Conti never really followed in their methodology," Boguslavskiy said.

Conti's operations have always been "rigid and organized," by the standards of the criminal ransomware underground. "It was run like a strict business unit," he said. That meant doing a lower volume of more targeted attacks, while keeping its network of business and technology partners small.
"Conti established key business alliances with other cybercrime groups to remain successful," said Boguslavskiy. Rather than rely on others to provide tooling, Conti only uses tools that they've developed or taken control of. "They don't want to rely on others," he said.

Ransomware: It's strictly business

Coming into 2021, as most ransomware gangs were expanding operations, Conti took an opposite path: ejecting non-core members and making the organization smaller and more hierarchical. They also began rolling up key partners, like the group responsible for the TrickBot and Emotet malware - long suppliers to Conti. "They've been very deliberate and purposeful in their methodology," Boguslavskiy told me. "It's not a game. It's a business."

That strategy has proven to be decisive in keeping Conti operating in a new and more hostile environment for ransomware groups, he said. The last six months has shown that ransomware outfits that relied on large and diverse ecosystems of suppliers, infrastructure partners and affiliates proved easy for governments and law enforcement to disrupt. That fact was on display in May, when the Darkside group announced that it lost control of its blog, payment server and CDN (content distribution network), as well as wallets containing cryptocurrency ransoms paid by victims.

Conti: mind the R&D

One of the other key differentiators of Conti and ransomware as a service groups is the group's ongoing investments in research and development. Conti has consistently invested back into its operations as a way to stay a step ahead of the competition (and law enforcement). Right now, the group's R&D is focused in areas like discovering new, exploitable vulnerabilities and avenues for attack, Boguslavskiy said.

Among other things, Conti is looking for ways to leverage common and critical flaws like Log4j, Petit Potam and a recent, critical vulnerability in SonicWall's SonicOS. The group is also working on enhancements to the Emotet botnet and engaging with other ransomware groups, like those that developed the new BlackCat ransomware, to further its activities.

Know your adversary

The key for organizations concerned about ransomware is to not be complacent, Boguslavskiy told me. Reports of the demise of ransomware groups, or dissent within Conti's ranks over business disputes or the War in Ukraine shouldn't prompt organizations to let down their guard. Conti remains very active and has shown itself to be extremely resilient. "Even if they disappear they will come back stronger," he said.

Understanding how Conti is working to compromise victims and how it behaves once it has a foothold within organizations is the key to defending your organization, Boguslavskiy said. These days, that means paying special attention to precursors of Conti, including indicators of compromise linked to Emotet.

Questions? Talk to ReversingLabs

ReversingLabs continuously improves its detection mechanisms to keep up to date with malware trends. That includes threats related to ransomware, wipers and other threats.

ReversingLabs' Titanium platform combines Explainable Machine Learning technology with static analysis to reliably identify and extract wipers, malware and other indicators at scale. That allows our customers to detect such threats in their environment quickly and before they allow malicious actors to extend their reach within compromised networks.

Contact us if you'd like to learn more about how we help organizations combat threats like malicious wipers and ransomware or to schedule a demonstration.

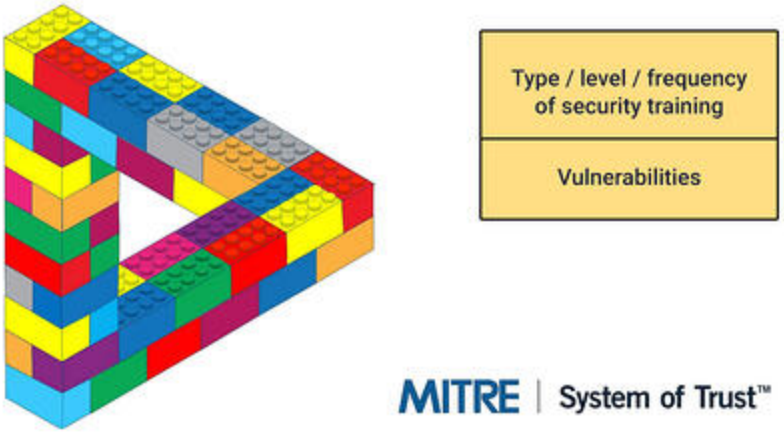
Watch ConversingLabs Episode 2: Putting Conti in Context

To view the full conversation with Yelisey Boguslavskiy, check out the latest episode of ConversingLabs, our new podcast. In addition to Conti, Yelisey and I talk about the Lapsus$ gang and the evolving cyber dimensions of Russia's war on Ukraine.

Register to watch the next episode of ConversingLabs: Emotet Unbound, happening live on Wednesday April 13 at 12 pm EST.

register here

MORE BLOG ARTICLES



RSA Conference 2022 | June 08, 2022
MITRE's System of Trust: A proposed standard for software supply chain security
MITRE's System of Trust framework is aiming to standardize how software supply chain security is assessed. MITRE's Robert Martin explains.

Read More

RSA Conference 2022 | June 08, 2022
Software supply chain security is no game. Or is it?
ReversingLabs delivered a game-show style review of its survey on software supply chain security at RSA Conference. Here are the questions and answers.

Read More

RSA Conference 2022 | June 08, 2022

A (Partial) History of Software Supply Chain Attacks

SolarWinds put supply chain hacks on everyone’s radar. But it was hardly the first such attack. In fact, hacks of software supply chains are older than you might suspect. How old? Here's an (incomplete) history of supply chain attacks and compromises.

Read More