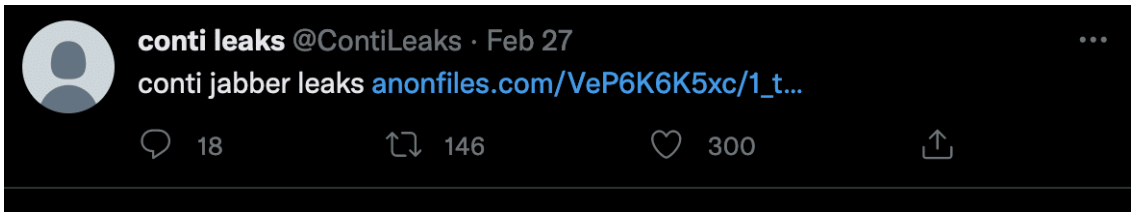
Consequences - The Conti Leaks and future problems

By Silent Push Threat Team

Published: 2022-03-16 · Archived: 2026-04-05 16:45:35 UTC

On 27th February 2022 a new Twitter account was opened called @contileaks and started to post information from the chat logs of a cyber criminal organization called The Conti Group.

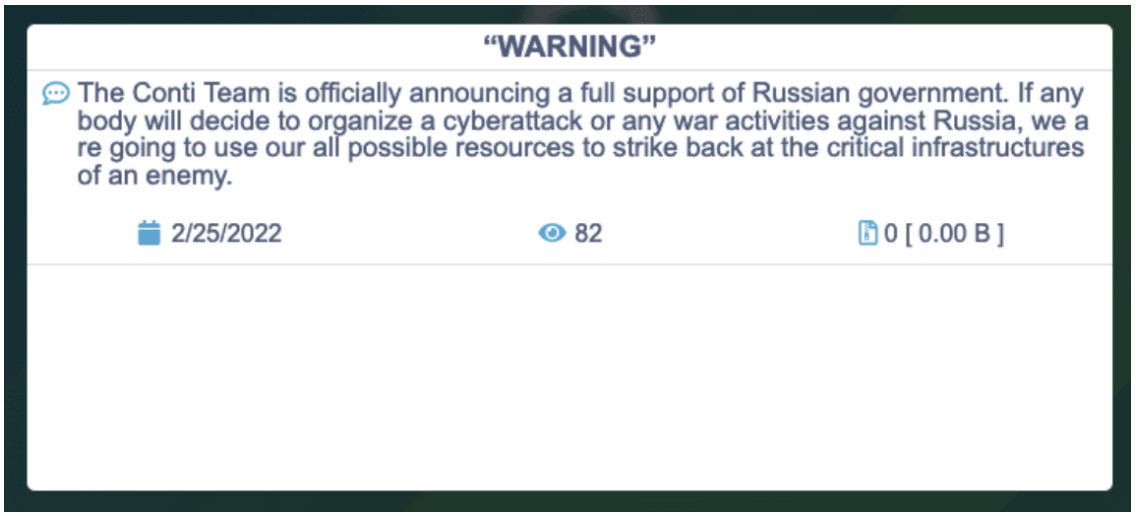


The Conti Group is renowned for being a very successful Ransomware operator and the gang have terrorized businesses worldwide by encrypting their networks for a ransom and also threatening to leak data if not paid.

Their list of victims is long and sometimes very tragic, such as when they ransomed the Health Service of the Republic of Ireland during the early Covid pandemic. We've linked to the full report.

The leaked information is reportedly coming from a Ukranian who was upset that the Conti gang had publicly declared on the side of Russia.

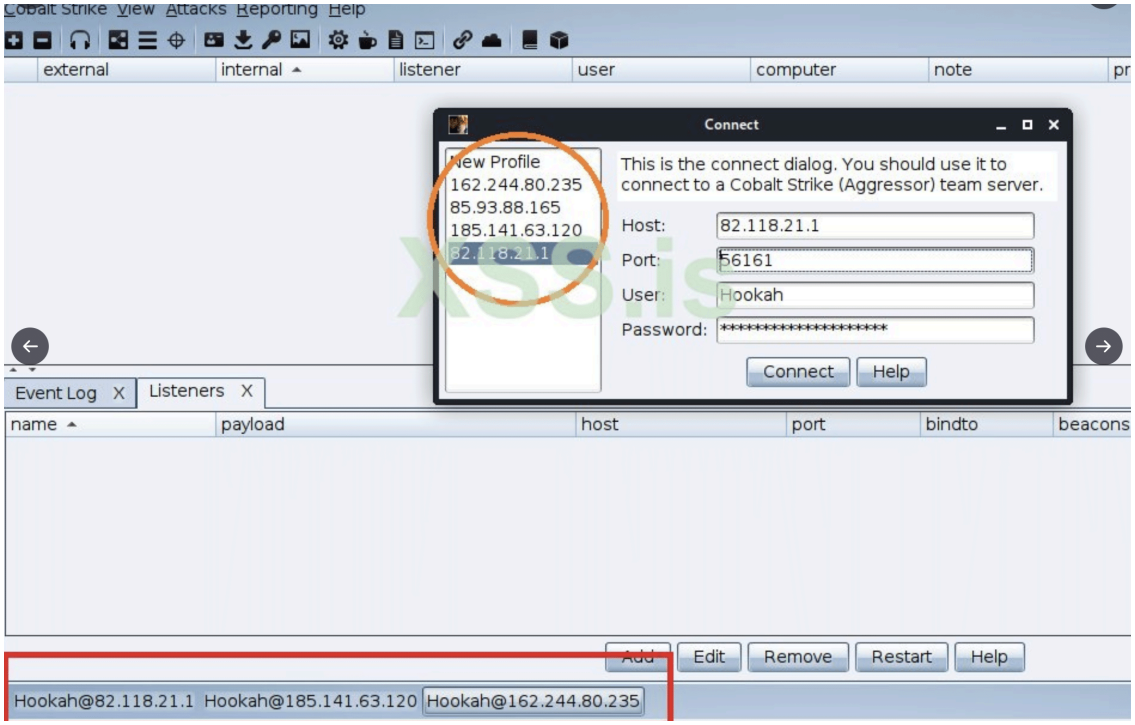
Credit:Twitter



Original message on the Conti site supporting Russia.

Included in the leaks were source code of tools used by the gang as well as chat logs and quite a lot of infrastructure was revealed. Also included was a lot of internal coaching and advise as to how to manage the operation and how to work your way through each intrusion and receive payment. Coaching tips from senior staff to junior staff and links to useful training videos and open source tools are included.

This is not the first leak of Conti material as training materials were also previously leaked in 2021



Concerns

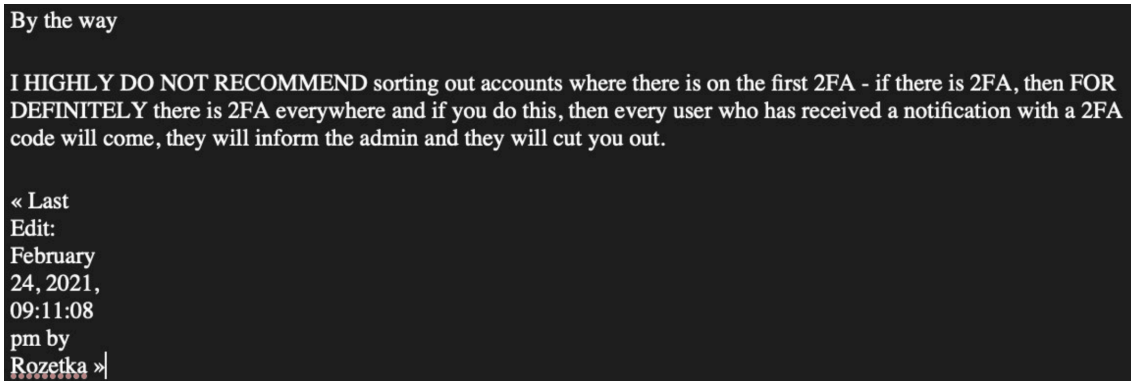
Most reporting on this subject focuses on the short term gain for security researchers and threat intelligence analysts. The view is that there is enough insight into the tactics, techniques and procedures of the gang to assist in tracking them and helping defenders.

The problem with this is that the content is far more useful to ‘wannabee’ ransomware operators or even currently less successful ransomware operators. The information contained in the leaks is an insight into running an operation like this and will inevitably lead to a proliferation of the problem. Current operators will learn from the material be able to improve their operations.

DNS history of a conti domain

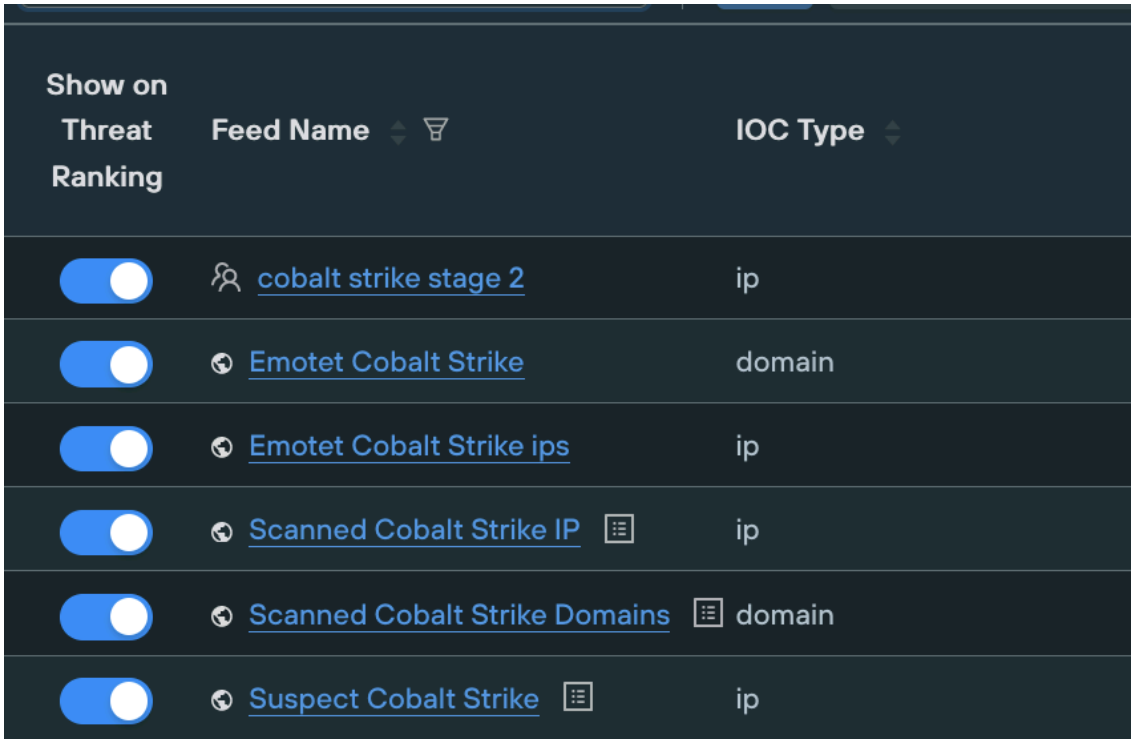
Some of the surprising things about the leaks are how little was already known in the general legacy security industry of the infrastructure used. Searches across common security tools showed most of the mentioned infrastructure in the leaks as being safe and not suspicious. This highlights the need for the industry to move towards a new approach to evaluating what is suspicious infrastructure. Focusing on key parts of the attack kill chain to disrupt attackers is also useful.

The leaks inadvertently also contain some key security tips like below(inferred of course). So everyone should take their advice and turn on Two Factor Authentication everywhere.



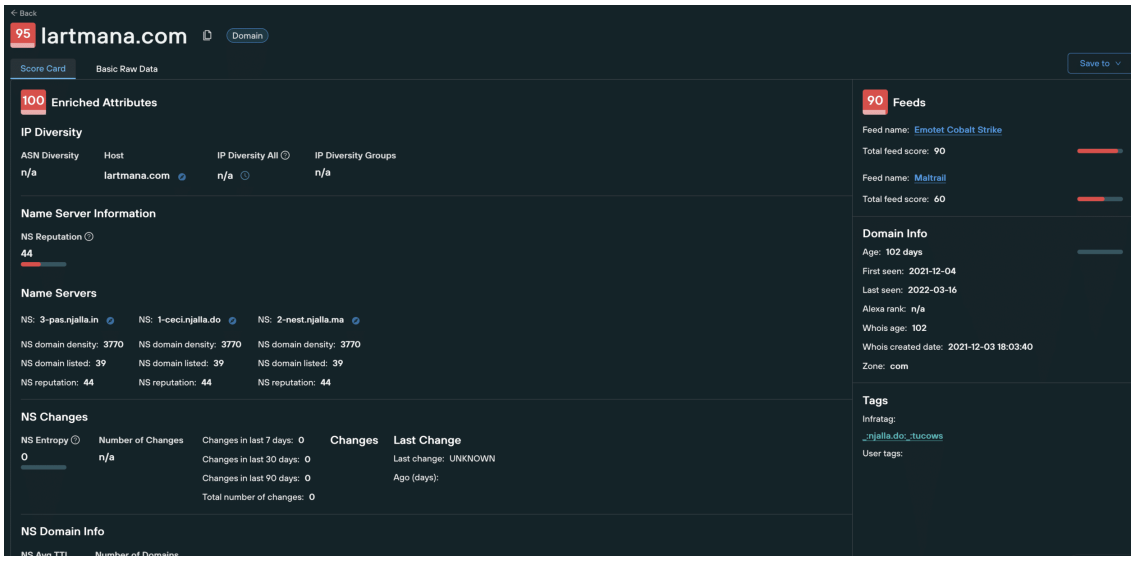
Some important things to track on the back of this leak to help defend your network.

1. Cobalt Strike servers. Some associated infrastructure is listed by [CISA here](). But it is possible to get quite comprehensive lists tracking new Conti infrastructure based on their TTPs. Lists of Cobalt Strike IPs and associated domains are available, such as in our threat feeds.



2. The cybercrime community consists of overlays of complementary tools and services including access brokers, infrastructure providers and tool providers for the different parts of an intrusion. Many of these are tracked

separately and information is readily available, even from open source providers. A good example associated with this group is the use of Emotet. Use the available services that provide this information or include them in your Threat Management Platform.



Together we can share not just information about the IPs and Domains used, which can all be changed, but share the management methods that allow us to block all of what gets set-up and requires a bigger effort for the attacker to change.

Source: https://www.silentpush.com/blog/consequences-the-conti-leaks-and-future-problems