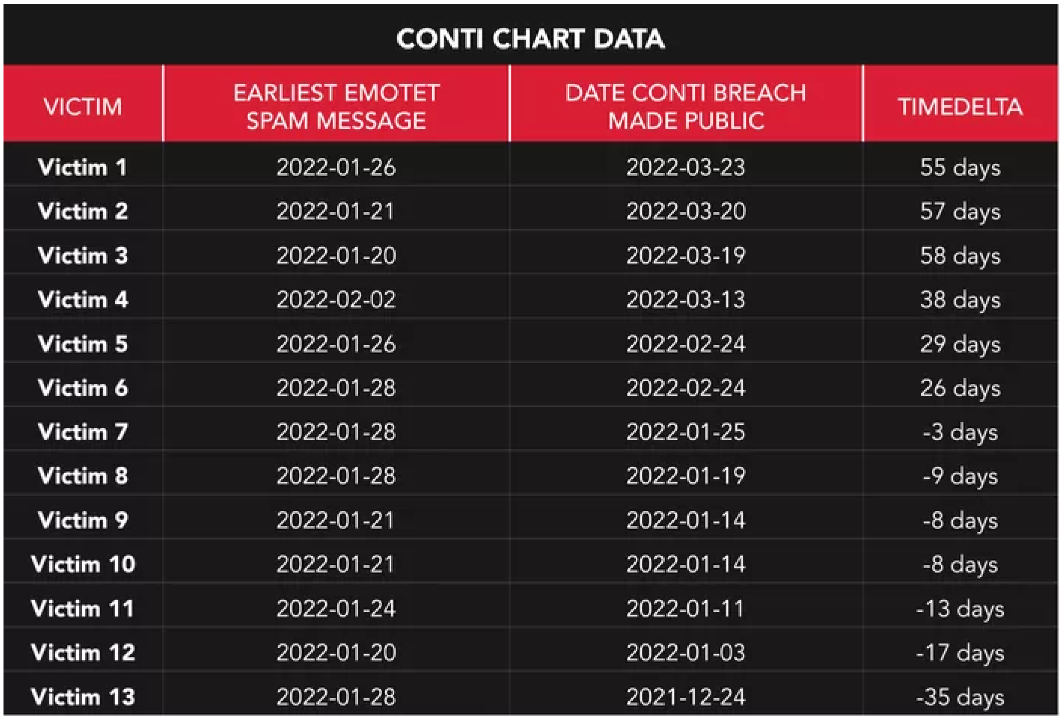
Conti and Emotet: A constantly destructive duo

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

The relationship between Trickbot, Emotet and Conti has been well documented, with many security researchers showing how threat actors have used the malware combination to launch a plethora of schemes. This relationship has come into greater focus in recent weeks, as the Conti Leaks show just how interdependent Conti affiliates are on Emotet. Through a combination of information pulled from those leaks and Intel 471's technical monitoring of Emotet campaigns, we now have a clearer understanding on how criminals are using Emotet in concert with Conti.

Intel 471 assesses with high confidence that Emotet malware operators' spam targets will enter a pool of potential Conti victims. Intel 471 analyzed Conti ransomware incidents from Dec. 25, 2021, to March 25, 2022, and discovered over a dozen targets that were recipients of Emotet malspam. While what Intel 471 measured was based on known attacks, the true degree of correlation between Emotet spam recipients and Conti ransomware breach victims may be greater, since not all Conti victims are publicly listed on the name-and-shame blog for a variety of reasons, including victims opting to pay ransoms to remain anonymous. Intel 471 believes it's likely that Emotet is highly relied upon by Conti ransomware operators to find their current victims.

The chart below shows the dates of Emotet showing up on systems, followed by a ransomware attack where Conti was used.



CONTI CHART DATA

VICTIM	EARLIEST EMOTET SPAM MESSAGE	DATE CONTI BREACH MADE PUBLIC	TIMEDELTA
Victim 1	2022-01-26	2022-03-23	55 days
Victim 2	2022-01-21	2022-03-20	57 days
Victim 3	2022-01-20	2022-03-19	58 days
Victim 4	2022-02-02	2022-03-13	38 days
Victim 5	2022-01-26	2022-02-24	29 days
Victim 6	2022-01-28	2022-02-24	26 days
Victim 7	2022-01-28	2022-01-25	-3 days
Victim 8	2022-01-28	2022-01-19	-9 days
Victim 9	2022-01-21	2022-01-14	-8 days
Victim 10	2022-01-21	2022-01-14	-8 days
Victim 11	2022-01-24	2022-01-11	-13 days
Victim 12	2022-01-20	2022-01-03	-17 days
Victim 13	2022-01-28	2021-12-24	-35 days

The negative numbers on the table above indicate that some victims were still receiving Emotet malspam after a ransomware incident was already listed on Conti's blog. This is an important point to highlight as it gives great insight to the overall operation of the Conti ransomware group and Emotet operators.

While Emotet has been linked in concert with Trickbot and Conti, Emotet does not operate under the same leadership umbrella (unlike Trickbot, which Conti "acquired" earlier this year) as the other two forms of malware. The Emotet malspam operation is independent and massive, with some parts running in an automated manner. What's likely occurring is that most Emotet spam recipients are not strictly targeted by a ransomware affiliate using Conti. Instead, Emotet is used by Conti affiliates to gain initial access. Once access is obtained, the organization is placed into a pool of potential ransomware targets, where ransomware operators can select their next victim based on the system information extracted by Emotet.

Even though Emotet operates outside the boundaries of Conti's leadership, the ransomware group has made it a key part of their attack chain, specifically as part of the relaunched Emotet we observed in November 2021.

The previous Emotet operation consistently launched malspam campaigns that dropped several malware families including IcedID aka Bokbot, Qbot and Trickbot. However, the updated Emotet malspam operation has been observed dropping only Cobalt Strike payloads or intermediary payloads, such as SystemBC, to drop Cobalt Strike. We know due to the Conti Leaks that the group leveraged Cobalt Strike: independent journalist Brian Krebs reported that Conti invested US $60,000 in acquiring a valid Cobalt Strike license in 2021.

The leaks further revealed evidence that certain members of the Conti team were responsible for handing Trickbot and Emotet development. The leak revealed the actor "veron" aka "mors," who directs the Emotet malware spam operation, reports to a senior manager in the Conti organization, who uses the "stern" handle. This information aligns with our own observations and long-term monitoring of Emotet and TrickBot malware campaigns. In past campaigns, only bots with the Trickbot group tag (gtag) "mors" received commands to download and execute Emotet. This suggests "mors" added the gtag to Trickbot.

When any organization finds a successful operational process, it leans on it as much as possible. The Conti Leaks have shown how this group conducts itself like a legitimate business, adopting well-worn practices that allow it fulfill its goals. These leaks show just how crucial Emotet has been to Conti's ransomware schemes. While not every instance of Emotet means that a ransomware attack is imminent, our research shows that there is a heightened chance of an attack if Emotet is spotted on organizations' systems. By being proactive against Emotet, defenders can save their organizations from further issues that could cause substantial damage to their operations.