Maze Ransomware is Dead. Or is it? | Webroot

By Justine Kurtz

Published: 2021-01-13 · Archived: 2026-04-05 17:47:11 UTC

“It’s definitely dead,” says Tyler Moffitt, security analyst at Carbonite + Webroot, OpenText companies. “At least,” he amends, “for now.”

Maze ransomware, which made our top 10 list for Nastiest Malware of 2020 (not to mention numerous headlines throughout the last year), was officially shut down in November of 2020. The ransomware group behind it issued a kind of press release, announcing the shutdown and that they had no partners or successors who would be taking up the mantle. But before that, Maze had been prolific and successful. In fact, shortly before the shutdown, Maze accounted for an estimated 12% of all successful ransomware attacks. So why did they shut down?

I sat down with Tyler to get his take on the scenario and find out whether Maze is well and truly gone.

Why do you think Maze was so successful?

Maze had a great business model. They were the group that popularized the breach leak/auction website. So, they didn’t just steal and encrypt your files like other ransomware; they threatened to expose the data for all to see or even sell it at auction.

Why was this shift so revolutionary?

The Maze group tended to target pretty huge organizations with 10,000 employees or more. Businesses that big are likely to have decent backups, so just taking the data and holding it for ransom isn’t much of an incentive.

Now think about this: those huge businesses also would’ve been subject to pricey fines for data breaches because of regulations like GDPR; and they’re also more likely to have big budgets to pay a ransom. So, instead of simply saying, “we have your data, pay up,” they said, “we have your data and if you don’t pay, we’ll expose it to the world – which includes the regulators and your customers.” Most of the time, paying the ransom is going to be the more cost effective (and less embarrassing) option. We don’t know if the Maze group invented this tactic, but they definitely set the trend, and a bunch of other ransomware groups started following it.

Other than the leak sites, did they do anything else noteworthy or different from other groups?

One of the bigger threat trends we saw in 2020 was malware groups partnering up for different pieces of the infection chain, such as Trojans, backdoors, droppers, etc. The botnet Emotet, for example, was responsible for a huge percentage of ransomware infections from various different groups. Maze, however, was pretty self-contained. We saw them working with a few other groups throughout 2020, but they had their own malspam campaign for delivery and everything else they needed in-house, so to speak. They were like a one-stop shop.

Do you think the move to remote work during the pandemic contributed to their success?

Absolutely, though you could say that about any ransomware group. Phishing and RDP attacks really ramped up when people started working from home. Home networks and personal devices are generally much less secure than corporate ones, and cybercriminals are always looking for ways to exploit a given situation for their gain.

If Maze was doing so well, why did they shut down?

Probably because they'd gotten too much attention. The more notoriety you get, the harder it is to operate. We see this with a lot of malware groups. They shut down for a while, either to lie low because the heat is on, or to just spend the money they've gotten from their payouts and enjoy life. Or, sometimes, they don't lie low at all but just rebrand themselves under a new name. Either way, they tend to come back. For example, a ransomware variant called Ryuk went dark and came back as Conti. Emotet went away for a long time too and then came back under the same group name.

How can you tell when an old group has rebranded?

Unless they announce it in some way, the only way to really tell is if you can get a sample of the malware and reverse engineer it and look at the code. One of our threat researchers did that with a sample of Sodinokibi and discovered it had "GandCrab version 6" in its code. So, that's an example of a rebrand, but it can be hard to spot.

Do you think Maze is done for good?

Not a chance. They attacked huge targets and got massive payouts. Most ransomware groups attack smaller businesses who are less likely to have strong enough security measures. Even the ones that targeted larger corporations, like Ryuk, still attacked businesses one-fifth the size of a typical Maze target. Now, the Maze group can relax and take a lavish vacation with all the money they got. But I'd be pretty shocked if they just abandoned such a winning business model entirely.

The verdict: Maze may be gone for now, but experts are fairly certain we haven't seen the last of this virulent and highly successful malware group. In the meantime, Tyler advises businesses everywhere to use the lull as an opportunity to batten down their cyber resilience strategies by implementing layered security measures, locking down RDP, and educating employees on cybersecurity and risk avoidance.

Stay tuned for more ransomware developments right here on the Webroot blog.

About the Author

Justine Kurtz

Senior Copywriter

Justine Kurtz has crafted the voice of Webroot for nearly a decade. As senior copywriter, she partners with clients across the organization (and the globe) to communicate the value Webroot solutions bring to businesses, consumers, and technology partners alike.

Source: https://www.webroot.com/blog/2021/01/13/maze-ransomware-is-dead-or-is-it/