Conti (Ryuk) joins the ranks of ransomware gangs operating data leak sites

By Catalin Cimpanu

Published: 2020-08-25 · Archived: 2026-04-05 21:41:19 UTC

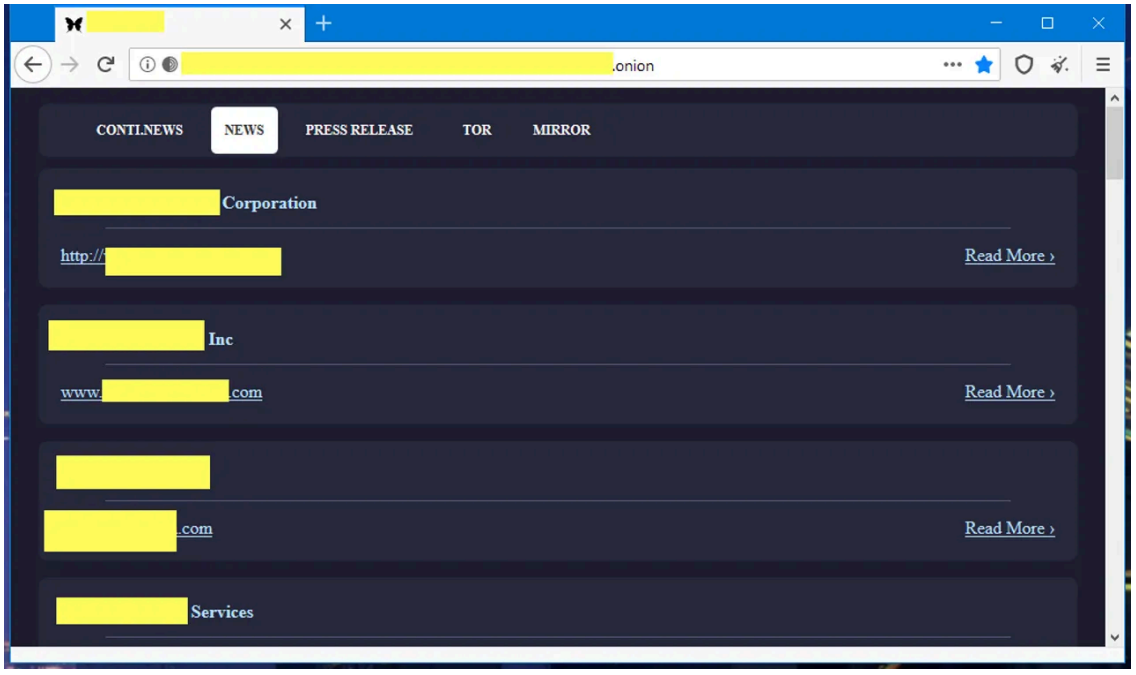

Image: ZDNet

It has now become a mainstream tactic for big ransomware groups to create so-called "**leak sites**" where they upload and leak sensitive documents from companies who refuse to pay the ransomware decryption fee.

These "leak sites" are part of a new trend forming on the cybercriminal underground where ransomware groups are adopting a new tactic called "**double extortion**."

The perfect example of how ransomware gangs are currently using "leak sites" and "double extortion" to put pressure on victims to pay is the case of the University of Utah.

Last week, the university's management admitted to paying $457,000 to a ransomware gang even if they recovered their encrypted files using previous backups.

In a statement posted on its website, the university justified its payment by revealing that the ransomware gang threatened to leak files containing sensitive student data online if the university did not agree to pay regardless if they recovered their original files.

Dozens of ransomware groups operate leak sites

Such incidents are becoming more common these days as more and more ransomware groups shift to operating a leak site to put additional pressure on victims.

The good news is that not all ransomware gangs operate leak sites.

However, this number has been steadily growing since December 2019, when the operators of the Maze ransomware launched the first-ever leak site.

Today, the list of ransomware gangs who operate leak sites includes the likes of Ako, Avaddon, CLOP, Darkside, DoppelPaymer, Maze, Mespinoza (Pysa), Nefilim, NetWalker, RagnarLocker, REvil (Sodinokibi), and Sekhmet.

Some of these groups are small-time operators that even malware analysts have barely heard of, but some, like Maze, DoppelPaymer, REvil, and NetWalker, are some of today's largest ransomware threat actors, responsible for a large chunk of ransomware attacks.

Other groups, like BitPaymer, WastedLocker, LockBit, ProLock, and the Dharma family, have not yet adopted leak sites. The reasons are unknown, but malware researchers have told this *ZDNet* reporter in previous conversations that some criminal groups like to operate without drawing too much attention to themselves -- and leak sites tend to draw way too much attention from journalists, cyber-security firms, and law enforcement officials alike.

Conti launches leak site

But last week, we had another major ransomware group shift to this double-extortion tactic and launch a leak site.

Know as Conti, this is a relatively new ransomware strain. However, reports from Arete, Bleeping Computer, and Carbon Black claim that Conti "is being operated by the same group that conducted Ryuk ransomware attacks in the past" -- with Ryuk being one of the most active ransomware operations from the past two years and one of the biggest players on the ransomware scene.

Discovered by a malware analyst going by the pseudonym of BreachKey, the Conti leak site is available at different URLs on both the public internet and the dark web.

BreachKey says the site already lists 26 companies that have fallen victim to the group's attacks and have declined to pay the ransom, and that for each company listed on the site, the Conti group has leaked documents obtained from their networks.


conti-leak.png
Image: ZDNet

All in all, the launch of yet another leak site shows that the double-extortion scheme is here to stay with ransomware gangs.

This new trend also means changes need to take place in how companies treat ransomware attacks. While in the past, victim companies only had to recover files and get back to day-to-day operations, today, ransomware attacks almost always involve the theft of sensitive corporate data, employee or customer personal details.

This, in turn, means that most ransomware incidents also require an in-depth incident response and broad network audits to discover lingering backdoors that could be used for future attacks, but also public disclosure and data breach notifications, which are necessary when any type of personal user/employee data has been stolen.
