Cybercrime: Ransomware Attacks Surging Once Again

Lockbit, Conti, Hive and Alphv/BlackCat Tied to Greatest Number of Known Victims Mathew J. Schwartz (euroinfosec) • April 28, 2022

Lockbit 2.0 ransom note (Source: Trend Micro)

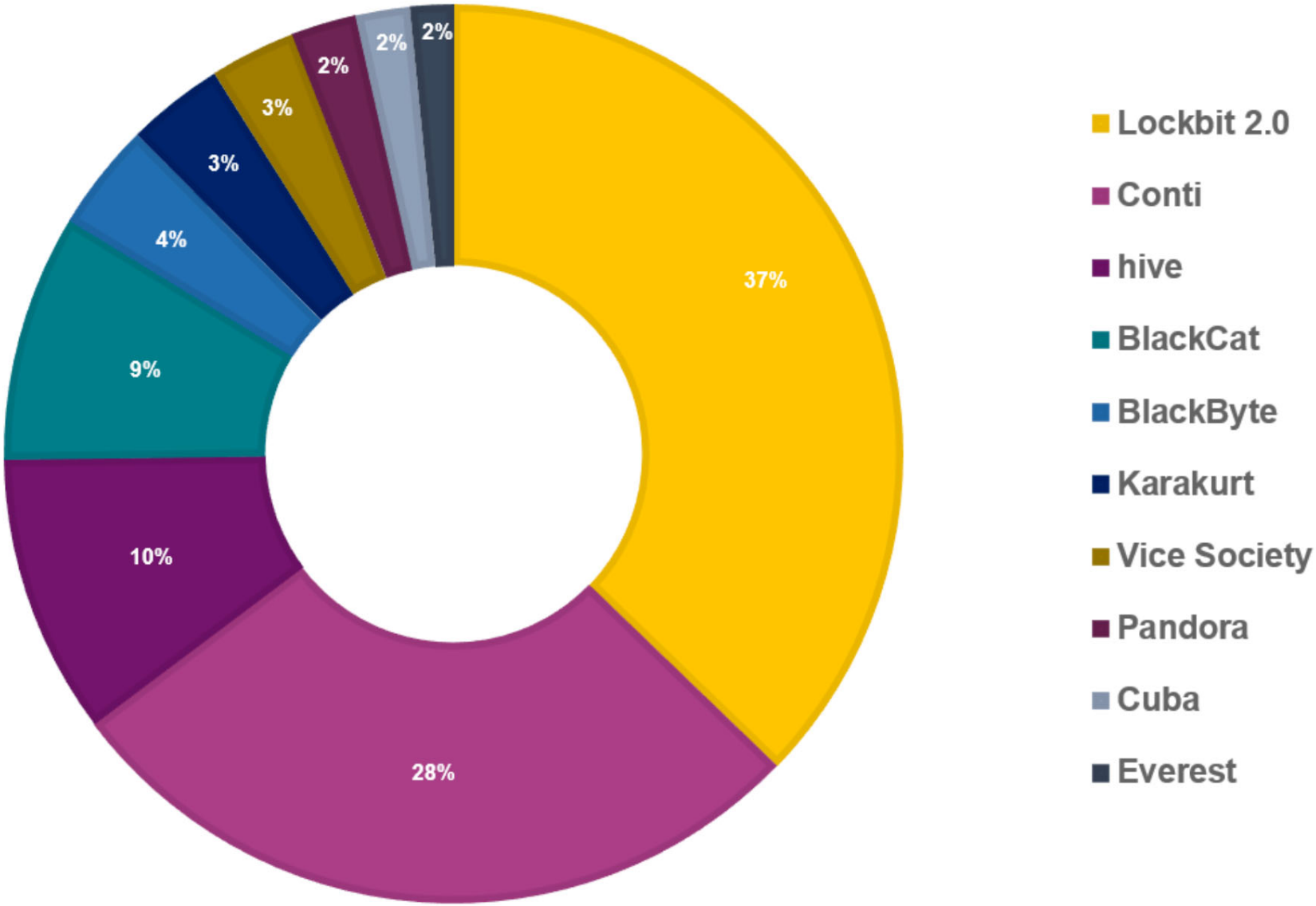
Ransomware attacks have come storming back after experiencing their typical end-of-the year decline, security researchers report.

See Also: The Ransomware Files, Episode 3: Critical Infrastructure

From February to March, the number of known ransomware victims surged from 185 to 283, consultancy NCC Group reports.

Based on attacks that have come to light, Lockbit 2.0 was the most prolific, accounting for 96 of the 283 attacks, followed by Conti with 71 attacks, Hive with 26 attacks and BlackCat, aka Alphv, with 23 attacks, NCC Group says. Of the known victims, 44% are based in North America, followed by Europe with 38% and Asia with 7%, it adds.

In March, attacks involving Hive, which first appeared in June 2021 and which often targets the healthcare sector, increased markedly compared to it being tied to only nine known incidents in February, which "begs the questions as to whether we are looking at a new, dominant threat actor," NCC Group says.



Percentage of known ransomware victims by group in March 2022 (Source: NCC Group)

Studies that compare the number of victims tied to different ransomware operations carry several caveats:

- Not all ransomware groups run data leak sites where they attempt to name and shame victims or threaten to leak stolen data, which are double-extortion tactics.

- When groups do have a data leak site, they rarely list every last victim. Cybersecurity firm Group-IB estimates that only 13% of a ransomware group's victims, on average, get listed.
- Some victims pay a ransom - sometimes quickly - precisely to avoid being listed on a data leak site. Group-IB estimates that about 30% of ransomware victims pay a ransom, although some studies suggest that figure may be much higher. Regardless, ransomware groups prefer victims to pay quickly and quietly, to make the scale of their operation more difficult to track.

But however ransomware victims get counted, the count of known victims has been increasing. That also goes for the Conti operation, despite a late-February leak of internal communications and code from the group. While the leaks have provided security researchers - and no doubt law enforcement agencies - with detailed intelligence about how the 100-strong criminal enterprise functions, at least so far they haven't disrupted its ability to take down fresh victims (see: *Leaks Fail to Dent Conti's Successful Ransomware Operation*).

REvil/Sodinokibi Disrupted

Compare the findings for February and March with newly published research from cybersecurity firm Trellix - formerly known as McAfee Enterprise - which looked at ransomware trends for the fourth quarter of last year. Lockbit 2.0 was also the most prevalent ransomware family detected in that time frame - accounting for 21% of all ransomware detections - followed by Cuba with 18% and Conti with 16%.

In a welcome development, from Q3 to Q4 of last year, Trellix says the quantity of ransomware attacks being detected by its U.S.-based clients declined by 61%.

Another big change in that time frame was the exit of REvil, aka Sodinokibi, from the ransomware scene. "REvil left the stage after a coordinated takedown of their infrastructure, several internal disputes, and members being arrested," says Trellix, which itself "assisted in the REvil investigation by providing malware analysis, locating key infrastructure and identifying multiple suspects."

But the members and affiliates of REvil who remained at large "most likely have found a new home" with other major ransomware families, Trellix says. Also, earlier this month, someone - perhaps a former developer - appears to have been trying to reboot the REvil operation, as spotted by Brett Callow, a threat analyst at security firm Emsisoft, and other researchers.

'Black Basta' Debuts

Meanwhile, the ransomware landscape continues to rapidly evolve. Since March, for example, a new group called "Black Basta" has emerged, recently claiming as a victim the American Dental Association

On Wednesday, Black Basta listed 10 new victims on its data leak site, reports Israeli threat intelligence firm Kela.

"Black Basta is a new operation that seems to be picking up pace," Emsisoft's Callow tells Information Security Media Group. "The ransomware appears to be unrelated to other strains and, unfortunately, is secure - meaning that the only ways to recover encrypted data are by replacing it from backups or by paying the ransom."

Repeat Target: Schools

In the first four months of the year, nearly 50 known - and successful - ransomware attacks against U.S. schools have come to light, reports Allan Liska, an intelligence analyst at Recorded Future.

Callow says that "at least 9 U.S. school districts with 234 schools between them have been hit" already this year. "Last year, 26 universities/colleges and 58 districts with 1,681 schools were hit."

Many Victims Pay a Ransom

One simple explanation for the recent surge in ransomware attacks and the steady appearance of new groups is that such efforts continue to be lucrative. A new study from cybersecurity firm Sophos reports that a sizable proportion of organizations admit to having paid a ransom after getting infected with ransomware.

Specifically, it found via a recent survey of 5,600 midsized organizations across 31 countries that two-thirds said they'd been targeted with ransomware in 2021 and that 46% of victims whose data was encrypted did pay a ransom.

But the Sophos survey also found that 83% of the surveyed organizations carry cyber insurance, and that "in 98% of incidents, the insurer paid some or all the costs incurred."

For the study, 965 organizations shared the exact amount their organization paid as a ransom in 2021, which averaged $812,000. That was a nearly fivefold increase compared to what 282 respondents had told Sophos for its study of 2020 ransomware attacks. In 2021, it found that 11% of the 965 victims paid a ransom of $1 million or more.

One cautionary note from Sophos is that victims who pay a ransom in return for a decryptor often cannot restore all crypto-locked data. In some cases, groups will fail to furnish a decryptor. In other cases, the decryptor may not function reliably, or the crypto-locking malware may have failed to correctly encrypt some files before deleting the originals, leaving victims unable to decrypt what's left.

"While paying the ransom almost always gets you some data back, the percentage of data restored after paying has dropped," according to the Sophos study of 2021 attacks. "On average, organizations that paid got back only 61% of their data, down from 65% in 2020. Similarly, only 4% of those that paid the ransom got all their data back in 2021, down from 8% in 2020."