"BlackCat" attempts to up the pressure on Suffolk County; starts to leak data? - DataBreaches.Net

Published: 2022-09-25 · Archived: 2026-04-09 02:18:43 UTC

Since September 8, Suffolk County has been trying to recover from a cyberattack by a ransomware group known as “ALPHV” or “BlackCat.” The attack disabled the county’s 911 system as well as other services. The county reverted to older methods for handling essential county operations, dispatching, and paying bills. State police have also provided support for some services. Still, this incident will undoubtedly result in questions about whether county executives and legislators made prudent decisions about cybersecurity and cyberinsurance and were prepared for a ransomware attack.

On September 15, DataBreaches reported that BlackCat had claimed responsibility and provided some proof of access to county files.

A message posted by BlackCat attempts to pressure the county into paying them. Such messaging by threat groups is common.

But BlackCat did more than that. Shortly after that, they published a second statement to the county. Their second statement was typical of such statements by ransomware gangs: they talk about how the public's information will be dumped, how the executives will suffer politically, and how they (BlackCat) stand ready to help the county restore its systems if the county contacts them and negotiates a "SMALL REWARD FOR OUR WORK TO FIND VULNERABILITIES ON THE SUFFOLK COUNTY COMPUTER NETWORK."

Since the county first disclosed the incident, DataBreaches suggested that reporters who contacted this site ask the county, "Does the county have a usable backup that it can use to restore systems?" DataBreaches didn't suggest reporters ask the county if it has a cyberinsurance policy to cover the costs of recovery and mitigation, but it turns out they don't.

Did BlackCat know that the county had no cyberinsurance that would cover a ransom payment? Many ransomware groups research their targets or potential victims and know what cyberinsurance they have. What did BlackCat know? And how much ransom did BlackCat demand as a "small reward?"

DataBreaches is not suggesting that the county should have paid any ransom. But what will incident response and recovery from this attack cost? When they decided not to purchase cyberinsurance, did they accurately estimate the costs of an incident like this?

Which brings us back to my original question: does the county have a current and usable backup they can use to restore from? Some screencaps posted by BlackCat suggest that the answer to that question might not be encouraging.

Bill Toulas of Bleeping Computer recently reported on changes BlackCat has made as they upgrade and evolve. He reported:

> Another recent addition to BlackCat's info-stealing capacity is the deployment of a new malware called "Eamfo," which explicitly targets credentials stored in Veeam backups.
>
> This software is typically used for storing credentials to domain controllers and cloud services so that the ransomware actors can use them for deeper infiltration and lateral movement.

Looking at the screencaps posted by BlackCat on their leak site, DataBreaches noticed one in particular concerned with backups:


Backup infrastructure information

A screencap provided by BlackCat shows the backup infrastructure. Three backup proxies appear to be identified as "disabled," and 12 managed servers appear "unavailable." Names of servers and descriptions redacted by DataBreaches.net.

The image appears to be taken from a Veeam Backup & Replication tool — the very tool that would run backups and assist with recovery from a data disaster. If BlackCat got this far, what did they do next? DataBreaches sent an email inquiry to the county asking about the availability of usable backups, but no reply has been received as yet.

 Yesterday, BlackCat published another update. This one claims they are making 400 GB of county and contractor data available. DataBreaches could not confirm the claim because their site has timed out on all connection attempts. If they have leaked 400 GB of files, that would be 10% of what they claim to have acquired.

As Brett Callow of Emsisoft recently reminded people, at least 37 local governments in the U.S. have been hit by ransomware this year; over half of them had data stolen. According to a spokesperson for the county who gave a statement to *Newsday*, Suffolk has spent $6.5 million on cybersecurity since 2019 and has been collaborating with the New York State Association of Counties to explore the possibility of obtaining cyber insurance. Perhaps this incident will be a cautionary tale for all the other NYS counties that do not have cyberinsurance. Even when a victim decides not to pay any ransom demand, incident response and mitigation costs may be very costly. Taxpayers in Suffolk County will eventually learn how costly.

Suffolk County residents can obtain information on county services and updates at https://www.suffolkcountyny.gov/. The county advises residents to be vigilant about monitoring any financial or credit accounts for signs of fraud and offers information on placing fraud alerts and security freezes.

Update: Suffolk County did not reply to the inquiry about backups, but DataBreaches was able to contact BlackCat to ask them whether they had deleted all backups or if the county had any backups left by them. Their admin answered: " Hi, they should have removed everything, I can clarify now." Well, "should have" and "did" are not quite the same, but it sounds like their intention was to delete all backups.
