

Is KillSec3 Trying to Extort Victims Using Publicly Leaked Data?

 databreaches.net/2024/12/08/is-killsec3-trying-to-extort-victims-using-publicly-leaked-data/

Dissent

December 8, 2024



KillSec3 is a ransomware group, but is it really encrypting its victims these days? Recent data suggests that its affiliate(s) may be trying to extort victims using data that has already been publicly leaked.

The following was researched and written by Dissent Doe, [JayeLTee](#), and a third researcher who prefers to remain in the shadows. Contributions to the research were also made by [@Chum1ng0](#) and [@bucketchallenge](#).

Background

A recent report by SpyCloud indicated that nearly a third of companies that fell victim to ransomware last year had at least one infostealer infection in the 16 weeks prior to their attack. But correlation does not prove causation, and stolen credentials may not be the explanation for any one ransomware group's attacks. Today we consider another possible explanation for at least one group's attacks.

The threat actors called KillSec have occasionally been described as hackers who evolved into financially motivated criminals. In October 2023, they began to attract media attention and in June 2024, they announced that they would now be offering RaaS (ransomware as a service), penetration testing, and other services. By the third quarter of 2024, KillSec had started getting more attention as the number of their victims rose and appeared on the group's darkweb leak site.

But what was this group actually doing?

Casual Comments Inspire A Deeper Dive

In a chat with DataBreaches on November 28, JayeLTee linked to a post alleging Curenta had been attacked by RansomHub. He casually commented, "Another one that was exposing the data on a cloud server." Unaware that Curenta had been exposing their own data on a cloud server prior to RansomHub's claimed attack, DataBreaches asked, "So did RansomHub hack or just help themselves to what was freely offered?"

JayeLTee said he couldn't tell yet because RansomHub had not listed any files that could be compared to Curenta's data leak, but he added, "Nationwide Legal was the same thing. [Another researcher] emailed them months ago and I also emailed them a month later. We both got ignored. Then they got ransomed and the next day the s3 bucket was closed."

It sounded like the makings of an interesting post — about entities ignoring responsible disclosure attempts and then getting hit with costly ransomware attacks. When DataBreaches suggested the idea to JayeLTee, he mentioned that looking at KillSec's leak site, there were at least several recent listings where he knew the victims had previously had misconfigured and exposed data buckets.

Could KillSec (and other groups) just be finding exposed buckets or storage devices and claiming to have attacked the entity? It was certainly possible, but was it happening?

So We Started Looking

Because some exposed servers were subsequently secured after they were listed on KillSec's leak site, we could not always directly compare data threat actors leaked to what had previously been leaked by the entity itself. In some cases, we could compare it through matching other data points, but in almost all cases mentioned below, we could see that the data claimed by KillSec was either exactly the same or appeared to be the same or related to exposed buckets or data storage previously noted by researchers.

As noted below, some of the servers are still exposed even after the victims presumably received ransom demands and have shown up on KillSec's leak site, so we are not naming specific entities for now. JayeLTee has taken steps to try to protect recent KillSec victims from further exposure, but as of publication, dozens of victims still have exposed servers.

For purposes of this post, our attempt to correlate KillSec's victims with previously spotted server leaks was confined to the recent two-month period: October and November with one early December incident.

Findings

For the time period we sampled, we found that 39 out of KillSec's 68 victims had previous leaks of the same or almost identical data, and 36 out of their 44 currently active posts are linked to publicly exposed data.

In some cases, the leaks had gone on for years. Of five leaks that were first detected by researchers in 2019 and 2020, one was secured after KillSec claimed an attack on them; the other four remain unsecured to this day. In other cases, leaks had first been noted by researchers months before KillSec added them to their leak site.

Ten of the 39 entities for whom we found matches to previous leaks are U.S. entities. Two of them have since locked down their servers, but eight remain unsecured as of publication.

In total, 30 out of 39 previous leaks researchers had noticed remain unsecured even after the entities showed up on KillSec's site and presumably received ransom demands.

And it's not just KillSec. A quick check of just some of RansomHub's recent listings also uncovered some claimed attacks where we could find matching data in previously discovered leaks, but such instances represented a much smaller percentage of RansomHub's listings. For RansomHub, 11 incidents we spotted involved entities that had previously noted leaks that were still exposed at the time of the claimed breaches. Of those 11, one had been exposed since 2021, one had been exposed since 2022, and three had been exposed since June and July 2023. At least three of them had been notified by researchers attempting responsible disclosure, to no avail. Because we did not investigate all of RansomHub's 184 listings for the time period, we do not know how many they would have in total. But after the 11 entities were added to RansomHub's leak site, four of the exposed servers were subsequently locked down, while seven remained exposed.

We do not know how many researchers had tried to notify any of the KillSec or RansomHub entities before they were breached.

Implications

Why should any victim pay an extortion demand when they had already leaked their own data before threat actors acquired a copy of it? And how many others found the same leak and are already in possession of the victim's data or are sharing it?

Take-home Message #1: If you are contacted by KillSec (or any threat actor for that matter), check to find out if you do have an exposed server somewhere and lock it down. And **don't bother paying the threat actor to delete data** because many others likely have your data already.

Take-home Message #2: It shouldn't need to be said in 2024, but here we are again: Make sure you have contact information on your web site for people to alert you to any data leaks they discover, and then monitor those emails or contact forms to respond to responsible disclosure attempts. At least two of KillSec's victims had been contacted months before KillSec presumably attacked them. Two of them were even mentioned on a social media platform when they did not respond to a researchers's attempts at responsible disclosure.

Is KillSec the Ransomware Emperor Who Has No Clothes?

One of the other intriguing observations we made this past week is that we could not find a single victim of KillSec in the past two months who confirmed that they had their files encrypted at all. KillSec reportedly has a locker. But is it even being used? Or is a KillSec affiliate just finding exposed data and then attempting to extort the victims while claiming to have hacked them? None of the servers found still exposed contained any encrypted files.

KillSec's Response

DataBreaches contacted KillSec to ask them about the observations. The following is a transcript of the chat on Tox, redacted to mask identifying information. Note that KillSec Supp asserted that the affiliates are **locking data directly** and they **do not use previously leaked data**:

KillSec Supp: Hello, all data belongs to our affiliates and undergoes a thorough verification process by our management team. We do not use previously leaked data, as it would provide no financial value and is not possible when our affiliates are locking data directly on client servers.

Dissent Doe: OK, but I've got dozens of things that are on your leak site that have already been leaking in misconfigured storage. Are you sure your affiliates aren't just finding leaks on [redacted service] or somewhere and then trying to extort them? I can show you some links to compare what you are listing and what was previously leaked — and is still leaking, in some cases.

KillSec Supp: No, we had a problem and links weren't inserted in. We are working to fix that.

Dissent Doe: Let me give you a few things to compare so you will see what I am talking about. Give me a minute and I'll pull a few for you. You list [victim1]. It was already exposed/leaking at [http://\[victim1bucketurl\]](http://[victim1bucketurl]). You list [victim2] and it was already leaking at [http://\[victim2bucketurl\]](http://[victim2bucketurl]) You list [victim3] and it was already leaking at [https://\[victim3blob\]](https://[victim3blob]). And from what you leak or show as samples, it's the same data.

Dissent Doe: For everything you have listed recently, we have found a previously exposed or currently exposed bucket or cloud storage, etc. In fact, even back in July we could find such similarities.

KillSec Supp: Data belongs to affiliates, is not my problem.

Dissent Doe: OK. I didn't want to embarrass you by just publishing our findings without giving you a chance to respond. If you think it's not your problem that your affiliates are trying to get people to pay for data that's already leaking, well.... ok.

Dissent Doe: Thanks for replying.

KillSec Supp: +

Conclusion

DataBreaches has written many posts over the years with the theme, “No need to hack when it's leaking.” Today's post offers a current example suggesting that cybercriminals may be simply finding exposed data sets and then attempting to extort entities by claiming to have hacked them and posting some data as “proof.”

KillSec and other groups may have experienced or talented hackers, but there's really no need for them to use advanced or time-consuming skills when victims will just fall for a get-rich-quick approach of claiming they've hacked you when they just helped themselves to

data you conveniently left out for them.