Daixin Team Ransomware Group Protection | Portal26

By lsdigitalmarketing

Published: 2022-11-28 · Archived: 2026-04-05 15:31:23 UTC

How to protect against the Daixin Team Ransomware Group

Ransomware attacks are common and becoming more creative. However, as attackers evolve, so do their decisions of targets and methodology. As of October 2022, the FBI's Internet Crime Complaint Center (IC3) holds victim reports across all 16 critical infrastructures, but the healthcare and public health sector made up 25% of ransomware complaints.

This year, the Daxin Team Ransomware Group has caused chaos for healthcare data security teams. If you are looking to research the Daixin Team ransomware attacks on the healthcare sector, investigate solutions that can be put in place to minimize these attacks from happening again, or learn more about how to prevent their encryption-based attack, look no further!

What is the Daixin Team?

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and HHS (Department of Health & Human Services) has warned in a cybersecurity advisory that "The Daixin Team ransomware and data extortion group is an active threat to the healthcare sector." Since June 2022, the group has been targeting businesses and primary healthcare organizations. What makes them so dangerous to healthcare organizations is that they have deployed ransomware to encrypt the essential servers of healthcare professionals.

How do they work?

The Daixin Team is not unique in the way that when they target a hospital, it is to steal this sensitive information. They complete this task by encrypting the servers responsible for running the place. Another goal these healthcare cyber attackers may have is to exfiltrate PII and patient health information (PHI), then threaten to release the data if the organization refuses to pay the demanded amount of ransom.

While healthcare data has become a target for ransomware, Daixin Team's technical approach and note at the end leaves you with no mystery in wondering who has your PHI. Here's their methodology.

Step One: Daixin Team actors will use a virtual private network (VPN) server to gain access to their target's systems. This exact infiltration method has ranged from getting credentials through phishing emails and then getting in through a lack of Multi-Factor Authentication (MFA) or cybercriminals exploiting an unpatched vulnerability in the target organization's own VPN server.

Step Two: Once they are in the system, Daixin actors can move throughout via Secure Shell (SSH) and Remote Desktop Protocol (RDP) with software based on Babuk Locker source code. According to the agencies in the advisory, the privileged accounts allowed the attackers to get into VMware vCenter Servers. Once they reset account passwords for ESXi servers, they deploy their ransomware.

Step Three: Once they are freely moving about the network, Daixin actors look for PII/PHI to exfiltrate. Data is exfiltrated before Step Four and used as additional leverage to collect ransom.

Step Four: Daixin actors then proceed to encrypt the system and the victim sees a note such as:

What differentiates healthcare cyberattacks?

For providers, their services are no longer safe to host personally identifiable information (PII) or personal health information (PHI) aspatients' records are at the mercy of the Daixin Team. Hospitals are already vulnerable locations, as their clientele are patients who may need critical care.

Given the volume of sensitive data they store, the number of connected devices they utilize, and the possibility that a disruption in crucial treatment could force organizations to pay the ransom. Also PHI fetches very good prices on the dark web and Daixin actors are motivated by this additional revenue stream as well. For these reasonshealthcare data and their facilities have grown to be a popular public sector target of ransomware and extortion operators.

If it has already happened to your organization, it is not your fault, and you are in the right place to protect your organization moving forward. Let's discuss preventing these dire consequences and keeping your patients' care going throughout a Daixin Team attempt.

What does the US healthcare system suggest regarding data protection and cybersecurity?

Some of the suggestions for how to keep healthcare data secure, according to the warning advisory, include:

- Keeping operating systems, software, and firmware updated
- Securing and monitoring RDP
- Requiring MFA as much as possible
- Implementing network segmentation
- Turning off SSH are all ways suggested by the three advisory agencies to keep healthcare data secure.
- The advisory also suggested ensuring that healthcare organizations must secure PHI as required by HIPAA to prevent the initial introduction of bad actors into the system. HIPAA data is typically required to be secured via encryption.
- Traditionally, encryption of healthcare data was only available while data was at rest i.e. not being actively utilized. This meant that when bad actors such as Daixin attackers successfully broke in, they could easily decrypt it using stolen credentials. However, now there are other solutions offering encryption-in-use, that can ensure that even if attackers have access to admin credentials, they cannot get to PII and PHI in unencrypted form. These systems promote immunity to the attacks to further protect organizations.

Ransomware prevention: How can I further prevent my organization from Daixin Team Ransomware?

Portal26 solutions support all sectors including Healthcare and other sensitive verticals. with their data security. Using Portal26, organizations can secure existing systems against data exfiltration and extortion, as well as build new ransomware-proof products from scratch.

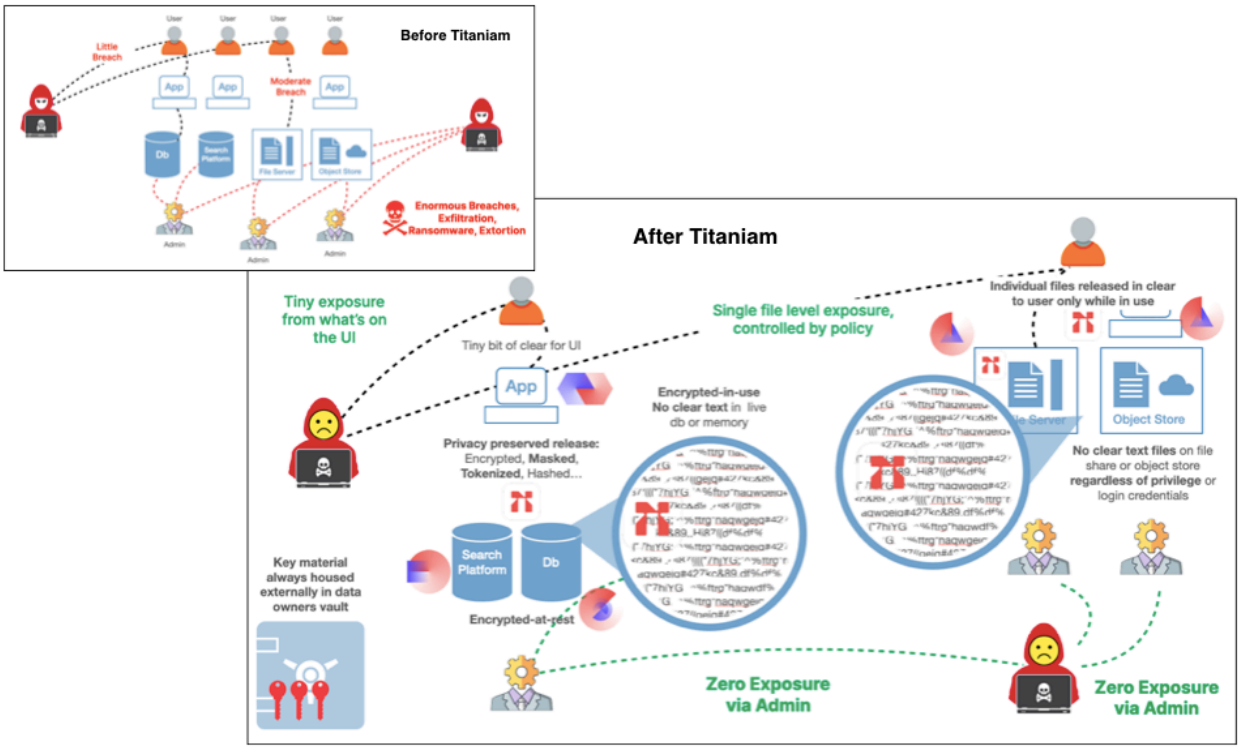
How Portal26 Works for Ransomware Defense

When a data store is protected using Portal26, the primary attack path being defended is the admin attack vector. The idea is to not interfere at all with end user activities and business flows but to ensure that if attackers get admin privileges and manage to get to large volumes of data, they should not be able to leave with it in clear text. Without a sizable amount of stolen data as leverage, attackers would be unable to use it as leverage for ransom demands.

1. Portal26 is deployed on a fileshare via agent or in front of it via proxy. For object stores, Portal26 is deployed as a proxy. For Enterprise search platforms, as a plugin, and for structured databases, Portal26 enables sensitive data to be substituted with either format preserving tokens or other privacy preserving formats.
2. Sensitive data in Portal26 protected systems is encrypted using NIST FIPS 140-2 certified encryption, without loss in functionality. Search is preserved in search platforms and for databased using tokens, full querying is supported in a companion vault.
3. When Portal26 encrypts files the encryption includes the data itself as well as names of files and folders as well. This makes it challenging for bad actors to traverse these repositories to pick and choose the data they want to take.
4. For data in search platforms, Portal26 encrypts both the source data as well as the reverse index.
5. When attackers break in and try to steal large volumes of data from file servers, object stores, databases and search platforms, they cannot access the data in unencrypted form even if they get to it using admin credentials. Even sensitive data in memory retains encryption.

By eliminating large scale data exfiltration and limiting clear text data to what individual users need at the time, Portal26 dramatically reduces the blast radius from ransomware and extortion based attacks.

Find out more about ransomware defense by exploring our top 3 ransomware defense strategies and mistakes to avoid.



The following is a list of Portal26's offering:

Portal26 FileShare Security: Portal26 provides always-on encryption for file servers and other file-sharing platforms. Portal26 ensures that all files are always secured with NIST FIPS 140-2 validated strong encryption and unencrypted data is not available directly from the file share regardless of privilege. Since data is encrypted before it lands, ransomware actors cannot access unencrypted data even if they are inside the firewall and moving laterally without restriction. The data release is strongly governed via policy, can be released in a number of private formats, can be rate limited, and can be plugged into other access controls as required.

Portal26 Object Store Proxy: Portal26 Proxy provides transparent application-level NIST FIPS 140-2 validated encryption for cloud object stores. Whereas native cloud platform encryption secures data from compromise on the cloud provider, encrypting with Portal26 ensures ransomware protection and complete data security if the enterprise themselves are victims of an attack. Portal26 supports privacy-enabled data release in nine secure and private formats as well as full-featured searches on encrypted data. The Portal26 Proxy bolts onto the non-extensible legacy, or fragile, systems and transparently directs sensitive data in and out according to security or privacy policy. Portal26 Proxy is available for both AWS and Azure environments.

Portal26 Vault: Portal26 Vault is a stand-alone data vault that can store and analyze structured and unstructured data, all while retaining strong NIST FIPS140-2 encryption without decrypting data at any time, including in memory or under the hood. With backup in place and strong encryption-in-use, Portal26 Vault is immune to cyberattacks, including ransomware. The Portal26 Vault also wins against traditional tokenization solutions by providing all the capabilities of tokenization with the added benefit of rich data usability. If used for tokenization, the Portal26 Vault can secure any type of existing datastore or existing applications and also build ground-up systems that are natively immune to data compromise. Data can be released from the Vault in nine different

privacy-preserving formats so that downstream systems are also protected from ransomware attacks and insider threats.

Portal26 Plugin: Portal26 Plugin protects sensitive data inside major enterprise search platforms without limiting full-featured search capabilities or deprecating search performance. Portal26 Plugin is available for all versions of Elasticsearch, OpenDistro, and OpenSearch on AWS/Azure. The Portal26 plugin can be up and running on enormous big-data clusters within hours. Data inside the Portal26-protected platforms cannot be exfiltrated in clear text, even if the cluster is compromised during a ransomware attack, insider attack, or left exposed by accident.

Portal26 API/Translation service: Portal26's API service can stand alone or integrate with any of the other Portal26 products to yield a high-performing data translation service. The Portal26 Translation Service can be used independently to make existing applications resistant to ransomware and other data-related cyberattacks. It can also ensure that protected data leaving other Portal26 products can be easily translated into clear text or other private formats by downstream applications. From the nine secure and private formats (including searchable encryption) and types of data, including keywords, text, numbers, dates, IP Addresses, Binary and PII-specific data types, the Portal26 API enables other Portal26-protected systems to be completely locked down, aligned with the Zero Trust Data security standard.

Portal26 Studio: Finally, the Studio provides an interface for managing other Portal26 products. It provides dashboards, reports, and granular compliance certifications in the event of a successful attack. Uniquely, the Portal26 Studio gives CISOs critical post-attack documentation as they can use Portal26 Studio reports as auditable evidence that their data retained encryption throughout the attack.

Highlights of the product's capabilities include:

- Protection from the most common and highly damaging types of ransomware attacks involving data exfiltration. These include large-scale unstructured and structured data exfiltration using privileged credentials.
- Strong security benefits without performance penalty. Portal26's data ingest overhead is under 5% when compared to clear text and Portal26 runs search with 0% overhead. Depending on the volume of data, the storage overheads are typically 15%. Portal26's closest comparable solutions, suffer from exceedingly large compute (500% overhead) and storage (10,000% overhead) requirements.
- Portal26's ability to release data in an application-friendly manner minimizes the need for application changes.
- Portal26 has been built to perform at an enormous data scale without loss of performance, handling petabytes of data and millions of keys with ease.
- Portal26 provides post-attack support for those who suffer a cyber attack. Uniquely, in the event of an attack, the software provides a report with visibility into any data that was observed, accessed, or exfiltrated. This offers auditable evidence that the data retained encryption. This helps avoid ransom payouts and also reduces liability, penalty, and notification obligations for regulated industries, private companies, and all who have a duty to their users to protect data.

Looking To Protect Yourself Against The Daixin Team Ransomware Group?

Portal26 can help!

Until Portal26 the typical ransomware defense strategy involved prevention/detection technologies on the endpoint (EDR/XDR) to identify and stop ransomware attacks as well as back up/recovery solutions to recover systems without being forced to pay the ransom. ***Both these approaches do not account for stolen data, and time after time, victims were forced to pay the ransom because their defense plan did not account for the leverage attackers gained by stealing data.***

Portal26 addresses this problem. Portal26 prevents the loss of unencrypted data thereby eliminating attacker leverage from data exfiltration. This closes a critical gap in ransomware defense today.

Portal26 Provides a Crucial Element for Ransomware Defense

To see a demonstration of how these products work, click to schedule a demo today.

Schedule a Demo >
