Digital Asset Redemption

DRK_MDR

The DAR Team Intervenes To Protect Patient Records on the Dark Web

Executive Summary

Despite paying a very substantial ransom to prevent the public release of sensitive patient data, a large US-based network of urgent care clinics and pharmacies couldn't rely on the promise of criminals to keep the information private. They decided to harness The DAR Team's DARK_MDR product for its ability to infiltrate, intercept, and interdict on behalf of their clients on the dark web.

Leveraging their established dark web presence, DARK_MDR dark web operatives discovered the company's data for sale on a small, invite-only Telegram channel. This channel was operating as a covert secondary market for stolen information that can't be listed on "public" leak sites and forums.

The DAR team went to work. They confirmed the data was legitimate, provided a recommended course of action (COA), and obtained permission from the customer to act on their behalf. The DAR Team operative discreetly purchased the data set as part of a larger bundle for a mere $2,000, effectively removing it from criminal circulation.

The customer praised DARK_MDR's rapid response, discretion, and cost-effective approach, which resolved a significant threat for a fraction of the original ransom.

This strategic intervention yielded several benefits:

- Prevented further exploitation of sensitive patient information
- Mitigated potential HIPAA compliance issues
- Reduced the risk of additional attacks using the stolen data
- Allowed for uninterrupted recovery without fear of retaliation

Customer Introduction

Who: A large, US-based network of urgent care clinics and pharmacies. The data they hold is highly lucrative for threat actors and includes protected health information (PHI), pharmaceutical and prescription information, and other private information about patients.

The Incident: The company had recently experienced a breach and extortion event that compromised 20 million patient records. During this event, the victim chose to negotiate with the threat actors and pay a reduced ransom demand, hoping to:

- Prevent the data set with tens of millions of patient records from being published on the threat actors' leak site
- Shorten incident response and recovery time
- Allow for continuity of care for their patients and pharmacy customers

The Mission: After the incident, the victim decided to use The DAR Team's DARK_MDR product to monitor and covertly respond to further proliferation of their data, unauthorized access into their environment, or exploitable vulnerabilities on the dark web.

Challenges

There are still rules and codes of conduct ransomware group members generally must adhere to in their own communities. One of the most fundamental rules for ransomware operators and affiliates is simple: once they receive payment from a victim, they are not allowed to then resell that data they stole. Doing so jeopardizes the entire operation, and *ransomware writ large*. Once a threat actor does not uphold their end of the bargain, they cease to get paid and will most likely be kicked out of the community as a whole. (You might think of this as ransomware groups' general brand management strategy.)

These dark web ecosystems self-police and breaking this code of conduct can result in consequences such as:

- Expulsion from the threat actor/ransomware group and losing the support/infrastructure/social community
- Exclusion from other groups in the future who know he might undermine their business
- Harassment and intimidation
- Doxed identities

That said, these *are* still criminals who like the idea of making a quick, easy buck. So while they might now publish stolen data on a main ransomware group's leak site, there is still a secondary market for re-selling the data. That secondary market takes place entirely in the most inner circles of these criminals' networks on places such as invite-only Telegram channels. These private channels are small – maybe a dozen or so members – and invitations are extended only to people that the threat actors truly trust - those with yearslong histories of activity and discretion.

The customer's data was being sold in one of these private, invite-only Telegram channels for other threat actors to conduct more targeted attacks. In the case of this network of urgent care clinics and pharmacies, it's likely this data set could have been parsed out by the purchasing criminals to commit crimes such as pharmaceutical fraud. Any further wide scale leaks of this data could have put this customer at further risk, continued to add to their incident response costs, and, of course, put patients at risk.

The Solution

Since these secondary data set markets are more discreet, the purchasers in these scenarios act more like "chop shops", buying wholesale data they can't use right away, but rather need to parcel out for other uses or sales. This type of transaction also avoids any alerts to victims so the criminals can take them more by surprise.

One established identity of a DAR Team operative was a member of this private Telegram channel and saw that this DAR customer's data was up for sale again behind the backs of their main ransomware group.

This type of dark web data purchase is often the "last on the line" for these types of data sets in this ecosystem. Since the sellers can't/don't want their main groups to know they're going behind the group's backs to resell and the buyer will have to do a lot of work to make a profit, the prices for these types of purchases are often quite reasonable. The trick, of course, was getting there.

The DAR Team contacted the customer immediately, provided a recommended Course of Action, and informed them of an opportunity to take quick action to remove this data set from this secret, secondary market. This would mean purchasing that data set in this private Telegram channel while ensuring they wouldn't raise suspicions about The DAR Team operative's identity and motives.

After a briefing about the situation, the customer agreed to The DAR Team's proposed Course of Action. This resulted in the operative purchasing the data and removing it from further proliferation. In order to maintain their cover, The DAR Team operative knew how to communicate with the seller because of their long standing "relationship" and what would appear as suspicious behavior.

Since the seller was listing quite a few data sets meant for what they perceived as various dark web data "chop shops", The DAR Team operative couldn't appear *too* interested in the customer's data set in particular. They asked to "look at" a few of the data sets, knowing they were only interested in the DARK_MDR customer, but keeping up appearances to the seller. The seller provided a small sample of the data to the operative, who worked behind the scenes to confirm the data was, in fact, the stolen data set from the prior breach.

Results
Once approved by the customer, DAR Team operative negotiated a bundle deal for a few data sets. **The cost for the data was approximately $2,000**.

The purchase of this data on a secret, secondary market was well worth the cost for the victim for a number of reasons:

- Safeguarded sensitive and exploitable patient data
- Significantly reduced the risk of their sensitive data from falling into another criminal's hands
- Allowed recovery to continue without fear of retaliation from the threat actor

The company was ecstatic with how DARK_MDR saved both their patients and company more agony for pennies on the dollar of the original ransom. They were especially happy with The DAR Team's:

- Knowledge of the secret data sale
- Responsiveness to the threat
- Intelligence report and accurate summaries
- Discreet communications with threat actor to avoid their detection
- Speed

At the purchase price, this transaction of $2000 was a "no-brainer" as a risk mitigation strategy for the customer. They were thrilled with this outcome, and have continued as a DARK_MDR customer since

Conclusion

When dealing with criminals there is always – *always* – inherent risk involved. While there is no honor among thieves, there is a way to mitigate the impacts of their dishonorable actions. DARK_MDR proved to be that exact mitigation.

By infiltrating the private dark web channels, intercepting the knowledge of the data sale, and interdicting by purchasing it before anyone with bad intentions could, The DAR Team was able to identify and neutralize a significant threat to their client. The speed and discretion of their response, coupled with the cost-effectiveness of the solution, highlight the value of continuous dark web monitoring and the ability to take decisive action.

For the client, this operation not only protected sensitive patient data from further exploitation but also safeguarded their reputation and regulatory compliance. The relatively minimal cost of the data recovery compared to the original ransom underscores the efficiency of The DAR Team's approach.

This managed detection and response for the dark web – The DAR Team's DARK_MDR – shows how any company's threat surface extends far into places traditional security tools and teams can't go. By responding at the source of the threats, The DAR Team helped keep both patients' and the company's data from falling into the wrong hands once again at a fraction of the cost. This prevented massive amounts of potential damage if the data had fallen into another set of wrong hands.