CONFIDENTIAL

Analysis of Collection of DarkWeb Exposures (Redacted)

Writing sample

Table of Contents

1. Introduction

On RedactedDate, I was presented with a collection of screenshots of appearances on the DarkWeb of 7 keywords. Malicious actors published this data both freely and in some cases for sale between RedactedDate and RedactedDate. I was asked to examine each screenshot, determine what happened, and the level of risk posed to the entity to whom the keyword refers.

The keywords appear in contexts ranging from email addresses to a script that takes a list of the client potential usernames and passwords and automates the process of testing them against a server. These appearances, though, also range in the level of risk they pose to the businesses to whom they refer, and to businesses that experienced multiple exposures of their name. For example, Client1 experienced the most frequent appearances, only one of which constitutes a significant risk. Meanwhile, Client2 experienced the least significant exposure.

This document describes what occurred in each case, the implications for current and future risk posed by these appearances, and potential ways to mitigate any risk. It contains an executive summary, appearance matrix, list of the keywords, as well as of the dark web marketplaces where the keywords were found, details about each exposure and where appropriate, recommendations.

2. Executive Summary

Starting in RedactedDate, seven businesses saw the name of their website appear in leaks of information onto the dark web that were released freely or put up for sale by malicious actors. No relationship or pattern was observed between the seven businesses, the forms of attack, the likely attackers, or the sites where the data was made available.

The exposures provided for comment in this collection of screenshots do not contain direct personal or business information related to the keywords. The keywords appear in advertisements for tools that malicious actors seek to provide to other malicious actors that could be used to enable them to extract information that could potentially damage the website, customers, or business to which the keyword refers.

Consequently, the determination of such an appearance as high or low risk depends on the likelihood and facility with which a bad actor could leverage the information being offered for sale (or freely) to perform direct financial, reputational or destructive harm to the business or to its customers.

The dark web appearances presented in the screenshots in this collection range in the amount of risk to which they expose the companies, from low likelihood of any potential damage to high risk. They also range in frequency. While Client1's name appears in six different releases in this screenshot collection only one appearance shows potential for high risk. The other five mentions pose minimal amounts of risk to Client1 or to the REDACTED (CLIENT1), even if they may pose risk to people associated with CLIENT1. Site2.com's name appears in twice in this collection, once on its own, and once in conjunction with an exposure Site1, one of its clients, experienced. Its risk is high not only because the seller is providing usernames, IDs, cookies, and API information but because both Site2 and Site1 work with REDACTED.

Site3.com and Site4.com both have medium level risk appearances in this collection of screenshots. A malicious actor offered a script that they claim could provide someone with access to the backend that controls Site3.com's website. If this script works, it would pose significant risk. However, the relative ease and speed with which the risk can be mitigated reduces the overall threat. Malicious actor, "BadActor," published the details behind Site4.com's payment page. This exposure is considered medium level risk because a malicious actor could use leverage these details to break into the payment application database, or to build a copycat page that steals users' personal identification including credit card information. Information about Site2.com's API configuration was also made available in a dump of information posted about one of its vendors. This appearance was rated as medium risk because Site2 works with REDACTED.

Five of Client1's six appearances in this collection of screenshots bear comparatively low risk to the institution. Site5.com, and Client2's appearances also are rated low risk. The exposure Client2 experienced in RedactedDate has been mitigated via corporate merger, name change, site infrastructure change, and redesign. The URL (address on the web) is no longer is in use and it is unlikely that Client2 could be harmed via any of the information provided. While a list of Site5.com's subdomains was published, thereby also revealing a list of its customers, no other information about the website, its customers, or the structure of the login page was made available. Consequently, the Site5.com's risk was rated to be low.

While these screenshots show that data was released onto the dark web that could enable a malicious actor to do harm, a malicious actor would still need to take additional steps and action in order to harm these businesses. At the minimum, they would need to buy the compromising data in a transaction that itself bears risks. The seller and marketplace need to complete the sale and the seller needs to deliver the information which it might not do. Marketplaces have been known to abscond with funds, as have sellers. Furthermore, the product needs to work, the buyer needs to understand how to use it, and then needs to act upon the data they collect or access they gain in a way that compromises the target. Regardless, these leaks show that each client has some element of weakness in its digital security procedures or architecture which should be addressed to avoid future exposure.

While some of the leaks were due to possibly misconfigured web applications or potentially unpatched software, other exposures happened because one of the business' vendors experienced a leak. Consequently, such risks could be mitigated by alerting the vendor.

3. Threat Rating and Appearance Matrix

The risk these mentions and data leaks posed to the companies that experienced them was determined according to two factors along three dimensions. The first factor was to consider how much of an immediate effect the mention or leak could directly have upon the keyword owner. The second factor considered was the level of effort a malicious actor would need to employ in order to leverage the information to do harm to the keyword owner in one or more of these three dimensions:

- Risk to reputation (**R**),
- Financial loss (**F**),
- Damage to technical infrastructure or further data leaks (**TD**)

The level of risk was determined to be **high**, **medium**, or **low** based upon the likelihood of a current risk at the time of writing (RedactedDate).

In short:

- Client1: **High risk** of technical infrastructure damage in one case, otherwise, **low risk**
- Site2.com: **High risk** of reputational, or technical infrastructure damage
- Site1.com: **High risk** of reputational, financial, or technical infrastructure damage
- Site3.com: **Medium risk** of technical infrastructure damage
- Site4.com: **Medium risk** of reputational, financial, or technical infrastructure damage
- Site5.com: **Low risk** of reputational, or technical infrastructure damage
- Client2: **Low risk** of reputational, or technical infrastructure damage

Appearance Matrix:

Who	Threat Level	Type	Where	When	What
Client1	High	TD	DumpSite, DumpSite1, DumpSite2	All dates redacted.	High: Username, password, cookie Low: subdomains, email address, script.
Site1.com/Site2	High	R, F, TD	DumpSite2	All dates redacted.	Login information, session cookies
Site2.com	Medium	R, TD	DumpSite2	All dates redacted.	UserID, port number, API details
Site3.com	Medium	TD	DumpSite	All dates redacted.	Web-shell
Site4.com	Medium	R, F, TD	DumpSite3	All dates redacted.	Database structure
Site5.com	Low	R, TD	DumpSite1	All dates redacted.	Subdomain dump
Client2	Low	R, TD	DumpSite4	All dates redacted.	Partial credential exposure

4. List of Keywords and Marketplaces/Data Dumps

Dark web marketplaces were searched for the following terms:

- Client2
- Client1
- Site1.com
- Site2.com
- Site4.com
- Site3.com
- Site5.com

These terms were found in these marketplaces or dumps:

- DumpSite1
- DumpSite
- DumpSite2
- DumpSite3
- DumpSite4

---

5. Client1 (High) (post 10 of pdf)

While Client1's name was published on six different occasions in this collection, the most of any of the companies provided in the list of keywords, only one appearance poses any significant risk. The other five mentions occurred as a side consequence of other people's exposures, are already public information or easily deduced, or require additional materials and tools in order to constitute a threat. As a result, they have been rated as low risk.

The following mention is significant:

- **High:** On RedactedDate, "BadActor" posted a list of links, logins, and passwords on **DumpSite** which they are selling for $Price. Included in this list is a link to the login form for the administration controls Client1 uses to manage user identities:

    - Client1

    This affects Client1 directly. This management console controls how Client1 manages which users have been given permission access the different parts of its website and system. For $Price, BadActor offers buyers on the dark web a login, password, and cookie which will give them access to this system. With this access, an attacker could create a new identity for themselves that gives them complete access to all areas of the system and the ability to change any other person's access permissions. They could also lock out rightful administrators. The risk to Client1 is rated as high because of the damage a bad actor could do, and the ease with which they could do it given the login, password, and cookie that BadActor has made for sale.

    Mitigation entails changing the password immediately and installing two-factor verification.

The following five darkweb appearances of the term “Client1” are all rated as low risk, listed here for convenience, and are reviewed in date order.

- Low. (**post 3 of pdf**) On Redacted, **BadActor1** published a list of Outlook Web Access points on **DumpSite**:
    - owa.Client1
    - owa5.Client1
    - owa3.Client1
    - bss.myClient1

  The first three subdomains listed above provide users with a Web browser-based version of Microsoft Outlook which they can use to access their email. The last subdomain, bss.myClient1 provides the user with a login form to access to their account on Client1’s platform.

  By itself, the release of this list does not pose a great risk to Client1. However, a list of Outlook Web Domains could be used in conjunction with leaked user names and email name formats (firstname.lastname, for example), in a brute force password attack, or alternatively in a phishing attempt. This would give them access to the user’s email account. The platform login form could be used similarly, and if hacked successfully would give a malicious user access to their account on the platform. However, only one email address was found in a later dump, no email passwords were reported available, and any risk would be to the email accounts of individuals who use Client1’s mail server. Therefore, the risk from this has been rated as low.

- Low: **(post 2 of pdf)** On RedactedDate, a Redacted credit card number issued to Redacted was posted on **DumpSite1** by a user named “**BadActor2**”. The following information was included:
    - Cardnumber: RedactedNumber
    - Expiration Date: RedactedDate
    - CVV: RedactedNumber
    - Date of Birth: RedactedDate
    - Address: Redacted
    - Phone: RedactedNumber
    - Email: Redacted

  The only connection to Client1 is the email address, “Redacted@Client1”. Unless this was a corporate card issued to Redacted for use and managed by “Redacted@Client1”, there is no direct risk to Client1 as a result of this exposure. Furthermore, as the card has already expired the risk of financial exposure is low. Note, however, the card was available and valid for 4 years before expiry.

  The email address for Redacted@Client1 provides a potential malicious actor with both email login name convention information as well as a username that could be used in a brute force attack. The personal information posted in regard to Redacted could be used in social engineering or phishing attacks against her personally or Client1 if she is an employee. However, there is little risk of immediate compromise from Client1’s perspective.

- Low: **(post 11 of pdf)** On or after RedactedDate, a malicious actor posted details about information they had captured from a currently unknown individual’s computer and were selling

on **DumpSite** for $Price. Included in this list are logins and passwords for this person's accounts on the following Outlook Web servers:

- https://owa.Client1
- https://owa3.Client1

If this person is a CLIENT1 employee, this would give a malicious actor access to their corporate email account and addressbook. Otherwise, the risk to Client1 is low, while the risk to the individual personally is considerable.

- **Low: (post 9 of pdf)** On RedactedDate, "**BadActor3**" uploaded credit card transaction information obtained from a possible Redacted leak to **DumpSite**. According to the information provided, the card was issued in the name "Redacted", in Redacted, in zip code Redacted and lists "@Client1" as the email domain. It was last used at Redacted on RedactedDate in the amount RedactedAmount. The seller offers the credit information for "2.5", but does not mention a currency.

  The risk to Client1 is low unless "Redacted" is an employee, and the credit card is a corporate one. It is worth noting that some students may list their school email addresses for professional or financial purposes.

- **Low: (post 12 of pdf)** On RedactedDate, someone posted a Redacted script to **DumpSite2** that targets Client1. This script takes a list of logins and passwords, tries to login with them, and returns a list of those that are successful. While seemingly concerning, this script contains a low level of risk for these reasons:

  1. It requires a separate list of credentials, i.e. login names and potential passwords to function, which is not included in this posting.
  2. Any such list must contain at least one working login pair for it to be a threat. Given such a working login/password pair, this script would identify and return it, and an unauthorized user would be able to access an account on Client1. Even without such a pair, this script could pose a DDOS (denial of service) threat by consuming site resources, but no other threat.
  3. The URL posted for the login form is incorrect, though this error could easily be fixed.

---

6. Site1.com and Site2.com (High) (post 4 of pdf)

On an unverified date (potentially RedactedDate), someone exposed a username, userID, session cookies along with the URL for the page on Site1.com's site where healthcare providers log in to their accounts to **DumpSite2**. Ordinarily, the web utility "cURL" is used in a non-malicious way to access webpages from the command line instead of going through a web browser. It is commonly used during site builds. However, in this case someone leveraged a username, "Redacted", and that user's userID, "Number" to acquire cookies for their session on the system.

The risks in this situation are that a malicious actor could employ this information to steal both the user's information, but the patient personal information (PII) and health related details to which they have access as a health care provider. In addition, an attacker could attempt to use the login portal to escalate their privileges on the site and potentially gain access to the entire system. Since Site1.com's patient information appears to be stored on Site2.com's system accessible through a gateway, this poses significant risk to both businesses. Suggested mitigations include canceling all cookies thereby forcing a password reset, strengthening the requirements for passwords, and denying access to cURL to all users except authorized administrators. Site2.com should examine its API logs and check for unexpected access.

This incident's risk level is rated as high since the data involved concerns patient health. Exposure of such records would also be subject to HIPAA rules. It is also rated as High because it involves three entities:

1. The Site1.com client whose user name, "Redacted" and id, "Number" was used to access a cookie to gain access to the system,
2. Site1.com, whose website was used to make an attack against all three parties, and
3. Site2.com, whose gateway leads to a store of records.

The screenshot does not provide information to suggest when this attack occurred.

---

7. Site2.com (Medium) (post 5 of pdf)

On an unknown date after RedactedDate, an unknown actor gained access to a service provided by **Redacted**, which Site2.com uses to Redacted. Details about Site2.com's use of Redacted's service were posted to DumpSite2 redacted. The incident's risk level is considered medium because it might be possible for a malicious actor to launch an additional attack against Site2 using the information provided, and because Site2 works with Redacted. However, this data appears to have been released in a collection of data gathered in an attack against Redacted, which bears the responsibility for protecting and hardening its API.

---

8. Site4.com (Medium) (post 6 of pdf)

On RedactedDate, seller **BadActor4**, posted the configuration for a login form on the site **DumpSite3.** This post exposed the address of the form on Site4.com's website, the API which gives access to the customer database, as well as the variables it uses to refer to users' stored data including their userID, password, and credit card information.

This exposure is rated as medium because of the significant risk it poses to customers should a malicious actor be able to leverage this data and stage a successful attack against the ecommerce website. For example, such an actor could potentially create a fake page that appears and behaves like the real site, gathers emails and passwords, and forwards users to the real site.

This risk can be mitigated by securing the form and access to the site and obfuscating the address of the API. Note, this risk is reduced as of this writing as the DumpSite3 site is currently down pending redesign.

---

9. Site3.com (Medium) (post 7 of pdf)

On RedactedDate, someone posted an offer on **DumpSite** to provide malicious code that gives an attacker remote access to Site3.com's web server in return for $Price. The seller offered no verification that the script, a web-shell, they are selling works, providing only the date the domain name was registered, which is public information, and an id number, Number.

If the script in fact works, the risk is that it would give the user access to the site's webserver which they could use to deface the site, get access to the database of content and customers, and possibly escalate to the rest of the system, as well. As a result, this poses potential reputational, financial and technological risk.

However, this could be mitigated by buying the script for the price asked, $Price, and testing to see if it works in the first place. If it does not, there is little risk from this exposure. If the script does work, further remediation would likely involve patching the web application. The overall risk is rated as medium due to the uncertainty surrounding the veracity of the claim and the efficacy of the script, weighed against the level of damage it could do if both are positive.

---

10. Site5.com (Low) (post 8 of pdf)

On RedactedDate, someone posted a listing of subdomains belonging to Site5.com on the dump site, **DumpSite1**. As a Redacted, this Redacted. It also inadvertently provided a listing of all their clients.

There are two risks in this case, one in terms of business, and one in terms of technological risk. The business risk is that a competitor could target their customers and solicit their business away from Site5. The technological risk is that if the login page is poorly managed on the back end, or if the site allows weak passwords, or some other credentials leak occurs, a malicious actor could attempt a brute force attack against the form. However, using the customer list, a bad actor could also approach each customer in a phishing or social engineering attack in an attempt to gain information which could assist them in their attack against this form.

The technological risk in this case is low as attacks would mainly depend upon additional exposures and a high level of effort. Mitigation efforts consist of potentially asking DumpSite1 to remove the data, in making sure that Site5.com maintains superior password requirements and in enforcing those across its customer base, and in sending advisory letters to its clientele warning of phishing attempts.

11.Client2 (Low) (post 2 of pdf)

On RedactedDate, a black-hat hacker named **BadActor5** exposed a likely userID and database number for an article in one of Client2's online collections of press releases on the dumpsite, **DumpSite4**. The present risk from this exposure is low as the website has been completely restructured. The domain name does not exist as a result of the corporate merger, and the technology used to build the site has changed. No additional mitigations are necessary to reduce risk.