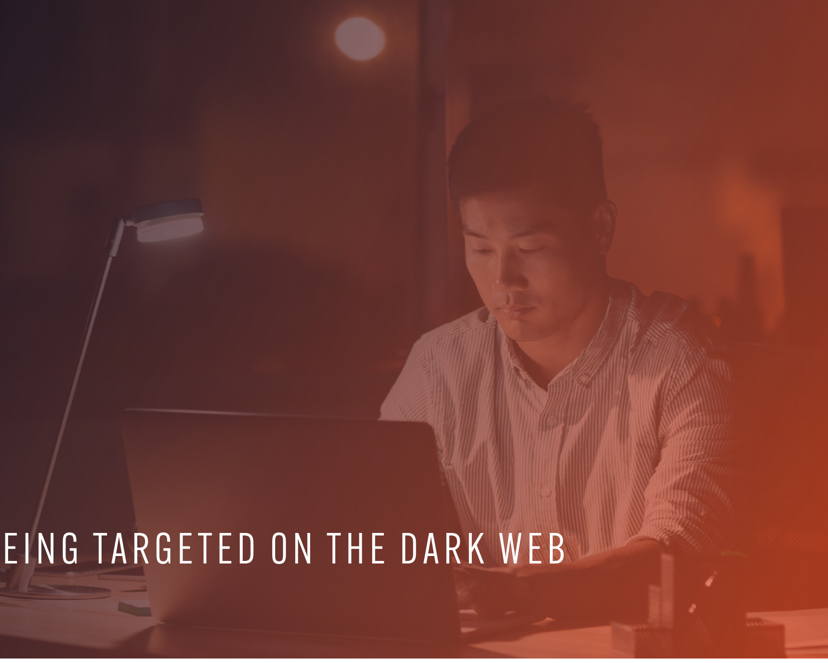
SEARCHLIGHT.
CYBER



EXECUTIVES UNDER THREAT

A CASE STUDY FOR IDENTIFYING STAFF BEING TARGETED ON THE DARK WEB

INTRODUCTION

The threat to executive personnel across all industries has been increasing over the past few years, with a notable spike coinciding with the pandemic.

In 2021 research from Ontic[1], 24 percent of physical security and IT leaders reported that their CEO or their family members had received threats and/or were harmed when working from their private residence or while traveling that year. A further 15 percent of respondents said that their company had received executive kidnapping threats since the beginning of 2021.

These statistics are certainly of concern. So too is the length of time that sensitive information about executives can be accessed on the clear web, on dark web forums, on paste bins, or on dox* sites before the individual or their organization is alerted to it. In some cases, they may never become aware of that data and it remains available online indefinitely for somebody to exploit.

> “
> **24 PERCENT OF PHYSICAL SECURITY AND IT LEADERS REPORTED THAT THEIR CEO OR THEIR FAMILY MEMBERS HAD RECEIVED THREATS.**

***DARK WEB DEFINED:** DOX/DOXXING

The practice of finding and sharing personal or identifying information about a person or organization on the internet, usually with malicious intent. Dox sites are websites specifically dedicated to sharing these details, which could include their full name, home address, or phone number.

This should not be considered the norm for executive roles. No one should ever feel that their personal safety is at risk because of their job and there are measures that can, and should, be taken to minimize the threat to executives.

Continuous monitoring of activity on the clear, deep, and dark web can alert organizations to when executive credentials and information is exposed, allowing action to be taken at the earliest opportunity to mitigate the threat or remove the data from the public domain.

Dr Gareth Owenson,
CTO of Searchlight Cyber

[1] https://ontic.co/2021-mid-year-outlook-state-of-protective-intelligence-report/

USE CASE: EXECUTIVE THREAT

A large healthcare organization located in the United States engaged with us to understand their digital risk footprint on the dark web.

The organization has an established security operations center (SOC), with teams monitoring their data 24/7, covering every aspect of security from individual endpoints to network communications.

As far as the security team was aware, the company had not been the victim of an attack, but they wanted to enhance their security posture further with a view to becoming more proactive at identifying potential threats earlier in the Cyber Kill Chain*.

Utilizing Searchlight's dark web threat monitoring solution, DarkIQ, the organization was able to specify certain company attributes that they wanted to search for and automatically flag if they appeared on the dark web.

These attributes included the organization's domains and subdomains, IP addresses associated with its corporate network, product names, and keywords associated with the organization.

Specific emails were added for additional monitoring of key stakeholders or executives within the organization, which is where we got a match. The personal email address of an executive was identified on a paste bin dedicated to doxxing.

*DARK WEB DEFINED: THE CYBER KILL CHAIN

The Cyber Kill Chain framework outlines the sequence of actions attackers have to take to achieve their ultimate objective.

1 **RECONNAISSANCE**

HARVESTING EMPLOYEE EMAILS ADDRESSES AND CREDENTIALS, PROBING THE NETWORK IN SEARCH OF VULNERABILITIES.

2 **WEAPONIZATION**

COUPLING THE EXPLOIT WITH A BACKDOOR TO CREATE A DELIVERABLE PAYLOAD.

3 **DELIVERY**

DELIVERING THE WEAPONIZED BUNDLE TO THE VICTIM, FOR EXAMPLE THROUGH EMAIL, WEB, USB OR CLOUD APPLICATION.

4 **EXPLOITATION**

EXPLOITING A VULNERABILITY TO EXECUTE CODE ON THE VICTIM'S SYSTEM.

5 **INSTALLATION**

INSTALLING MALWARE ON THE ASSET.

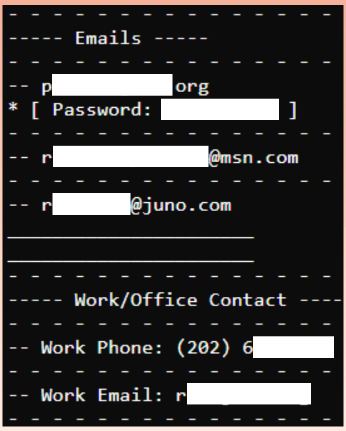
6 **COMMAND AND CONTROL (C2)**

ESTABLISHED A COMMAND CHANNEL TO AN EXTERNAL SERVER FOR REMOTE MANIPULATION OF THE VICTIM.

7 **ACTIONS ON OBJECTIVES**

FOR EXAMPLE, DATA EXFILTRATION, RANSOMWARE DEPLOYMENT OR CORPORATE ESPIONAGE.

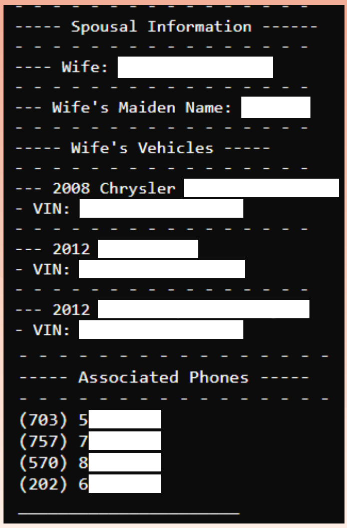
This dox had a significant amount of information relating to the executive in question, including business and personal email addresses and contact numbers.



```
- - - - - - - - - - - - - - - - -
----- Emails -----
- - - - - - - - - - - - - - - - -
-- p[redacted]org
* [ Password: [redacted] ]
- - - - - - - - - - - - - - - - -
-- r[redacted]@msn.com
- - - - - - - - - - - - - - - - -
-- r[redacted]@juno.com
___________________________
___________________________
- - - - - - - - - - - - - - - - -
----- Work/Office Contact ----
- - - - - - - - - - - - - - - - -
-- Work Phone: (202) 6[redacted]
- - - - - - - - - - - - - - - - -
-- Work Email: r[redacted]
- - - - - - - - - - - - - - - - -
```

Figure 1: Redacted excerpt from the dox showing personal and business contact information.

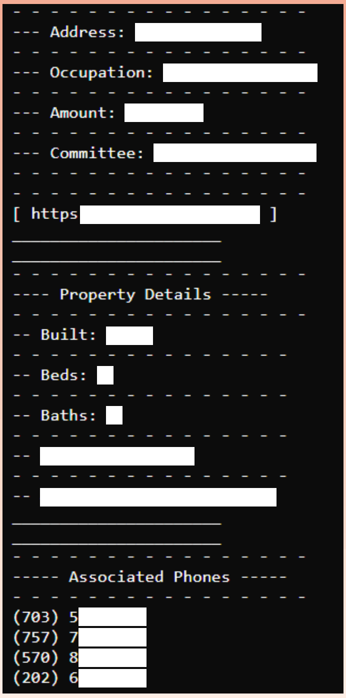
The dox also contained information relating to the executive's spouse, including name, contact numbers and vehicle information.



```
- - - - - - - - - - - - - - - - -
----- Spousal Information ------
- - - - - - - - - - - - - - - - -
---- Wife: [redacted]
- - - - - - - - - - - - - - - - -
--- Wife's Maiden Name: [redacted]
- - - - - - - - - - - - - - - - -
----- Wife's Vehicles -----
- - - - - - - - - - - - - - - - -
--- 2008 Chrysler [redacted]
- VIN: [redacted]
- - - - - - - - - - - - - - - - -
--- 2012 [redacted]
- VIN: [redacted]
- - - - - - - - - - - - - - - - -
--- 2012 [redacted]
- VIN: [redacted]
- - - - - - - - - - - - - - - - -
----- Associated Phones -----
- - - - - - - - - - - - - - - - -
(703) 5[redacted]
(757) 7[redacted]
(570) 8[redacted]
(202) 6[redacted]
___________________________
```

Figure 2: Redacted excerpt from the dox showing information relating to the executive's spouse.

In addition to this information, the dox went on to provide personal email addresses and phone numbers for the executive's children, as well as their home address.



```
- - - - - - - - - - - - - - - - -
--- Address: [redacted]
- - - - - - - - - - - - - - - - -
--- Occupation: [redacted]
- - - - - - - - - - - - - - - - -
--- Amount: [redacted]
- - - - - - - - - - - - - - - - -
--- Committee: [redacted]
- - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - -
[ https[redacted] ]
___________________________
___________________________
- - - - - - - - - - - - - - - - -
---- Property Details -----
- - - - - - - - - - - - - - - - -
-- Built: [redacted]
- - - - - - - - - - - - - - - - -
-- Beds: [redacted]
- - - - - - - - - - - - - - - - -
-- Baths: [redacted]
- - - - - - - - - - - - - - - - -
-- [redacted]
- - - - - - - - - - - - - - - - -
-- [redacted]
___________________________
___________________________
- - - - - - - - - - - - - - - - -
----- Associated Phones -----
- - - - - - - - - - - - - - - - -
(703) 5[redacted]
(757) 7[redacted]
(570) 8[redacted]
(202) 6[redacted]
```

Figure 3: Redacted excerpt from the dox showing information relating to the executive's home address.

Now armed with the knowledge that this information was available on a paste bin, the organization was able to implement the necessary extra security measures required to protect the executive.

It was also able to use DarkIQ to continue to monitor conversations on the clear, deep and dark web for any reference to the organization and the individuals mentioned in the dox, which would highlight if cybercriminals were discussing them on a forum and planning an attack. Alerts were put in place to notify the relevant security teams in the event this occurred.

Ultimately, this information prompted the creation of a more proactive posture from the security team, by preparing them for the potential threat (a targeted attack on the executive and/or their family) before criminals could act on the information they could access. This gave the organization time to apply the necessary mitigations and enhance security where required, including the physical security space beyond their networks.

SUMMARY

While traditional cybersecurity solutions provide an element of protection for the network, by their nature they are reactive to an incident and rely on the identification of suspicious or malicious activity inside the network perimeter.

By utilizing dark web monitoring capabilities, organizations are able to extend their visibility beyond their network and into the conversations and discussions happening within the criminal underground.

This additional visibility enables security teams to proactively search for or monitor conversations that pose a risk to organizations and individuals alike before they can become a threat.

This not only enhances the security posture of an organization in regards to protecting the network and its infrastructure, but enables an additional layer of protection around a key asset for any business: the personnel that enable the organization to run day-to-day.

USE SEARCHLIGHT TO TACKLE EXECUTIVE THREAT

Searchlight Cyber helps you to proactively protect infrastructure, people and digital assets across your organization with relevant, actionable dark web intelligence:

UNDERSTAND YOUR DARK WEB RISK EXPOSURE

Get a health report of your organization's exposure on the dark web, along with context and guidance on the actions you need to take to prevent malicious activity.

CONTINUOUSLY MONITOR FOR SPECIFIC THREATS AGAINST YOUR ORGANIZATION

Create automated alerts on attributes that are specific to your business - including domains, networks, assets, and executive credentials - to cut through the noise and receive intelligence on threats that are likely to directly impact your organization.

PREVENT DATA BREACHES

Stop staff credentials from being breached and leaked in the first place by identifying the early warning signs of an attack - such as company IP addresses, open ports, and compromised devices for sale on the dark web, or dark web traffic to and from the company network.

THREAT INTELLIGENCE AND INVESTIGATION

Enhance your threat intelligence and threat monitoring capabilities with an unmatched window into activity on dark web forums, marketplaces and conversations, without any risk to your analysts.

INCIDENT INVESTIGATION AND RESPONSE

Forensically examine the chain of events on the dark web that led to an attack or data breach to inform incident mitigation and response.

SEARCHLIGHT.
CYBER

VISIT **WWW.SLCYBER.IO** TO FIND OUT MORE OR BOOK A DEMO NOW.

UK HEADQUARTERS
Suite 63, Pure Offices,
1 Port Way, Port Solent,
Portsmouth PO6 4TY
United Kingdom

US HEADQUARTERS
900 16th Street NW,
Suite 450, Washington,
DC 20006
United States