SEARCHLIGHT. CYBER

GOVERNMENT AGENCY TARGETED

A USE CASE FOR IDENTIFYING THREATS ON DARK WEB FORUMS

INTRODUCTION

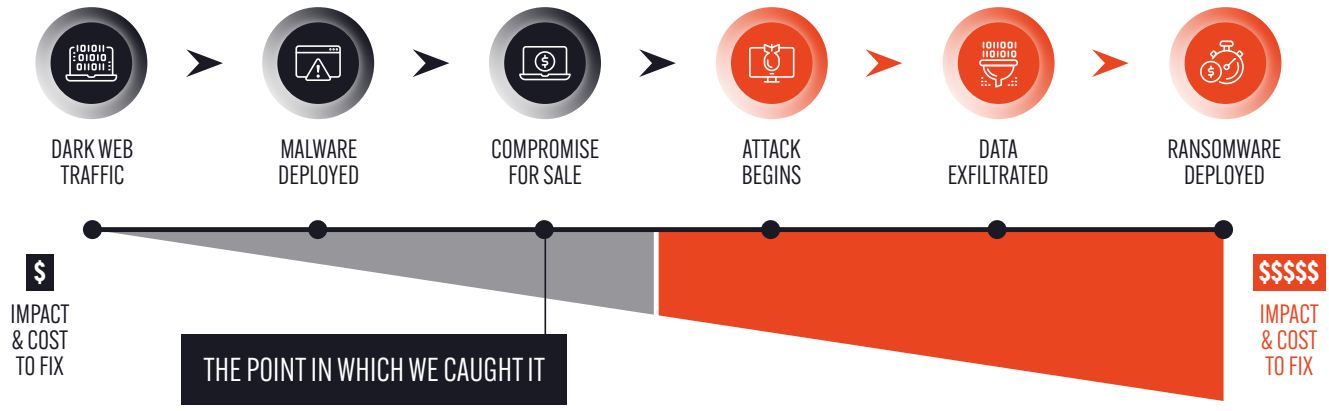
The Searchlight Cyber threat intelligence team spotted a threat actor targeting a European government agency on the dark web. The dark web post was shared with the government agency, who were able to find and remediate the webshell the threat actor had installed on their network before it was exploited - effectively stopping the cyberattack before it could begin.

The threat actor's post was spotted as part of an ongoing investigation into their activity across a number of dark web hacking forums. Further investigation of dark web traffic to the organization's infrastructure appeared to show indicators of when the malware was installed by the threat actor.

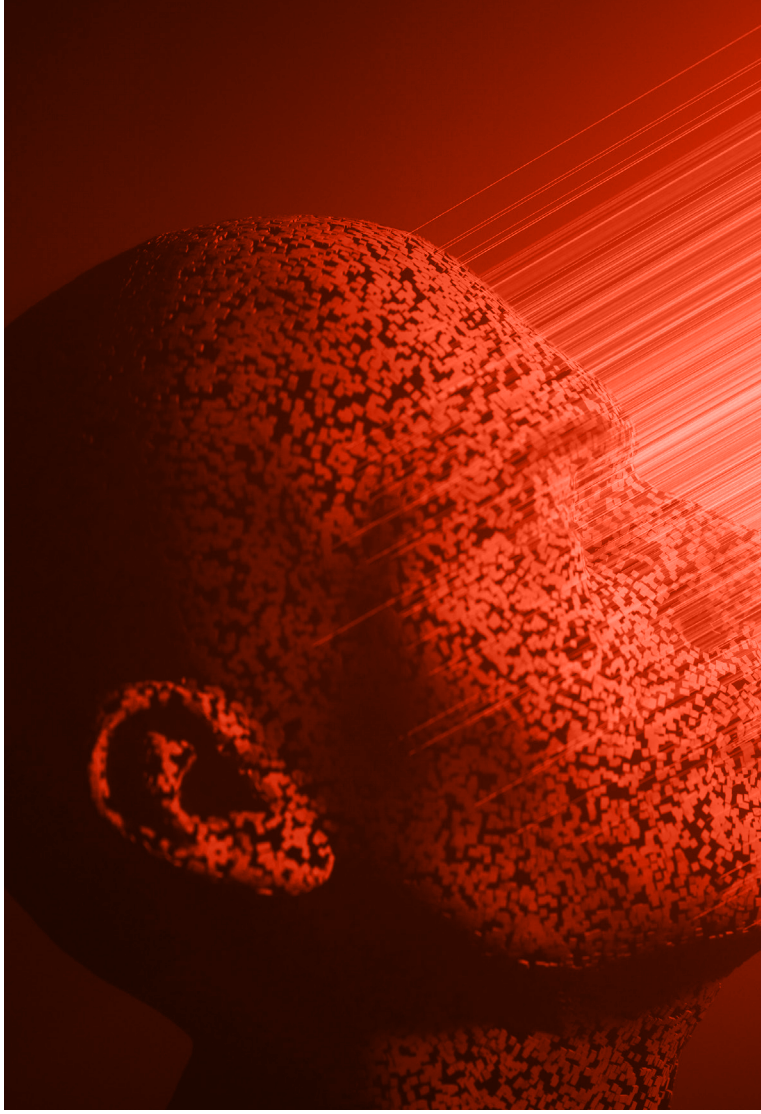
This use case demonstrates the value of the dark web as a source of "pre-attack" intelligence, providing organizations with a vital window of time for them to stop a cyberattack before it has been launched. It is an obvious but important point that the sooner an organization can act, the lower the damage and therefore cost of an attack will be.

In this case it was a government agency targeted but no organization is immune from being targeted by cybercriminals. All companies should be monitoring the dark web for "early warning signs" of threats against their organization which - as this use case shows - can help them to prevent cyberattacks.

Dr. Gareth Owenson,
Co-Founder and CTO of Searchlight Cyber



THE PERPETRATOR



Magnetic Wolf is the alias given to an actor tracked by Searchlight Cyber's threat intelligence team who is associated with numerous dark and clear web cybercrime profiles. Magnetic Wolf appears to have operated under linked profiles from early 2023, and the actor has shown they're a credible and capable threat both through their posts and independent intelligence obtained by analysts within Searchlight Cyber. The real-world identity of Magnetic Wolf is currently unknown.

Magnetic Wolf is primarily an initial access broker, a type of criminal who provides access for third party criminals into an organization. Imagine the online equivalent of the person who sells the front door keys to a burglar. As well as acting as an initial access broker, Magnetic Wolf has demonstrated the capability to build their own malware, and has shown evidence of developing malware in the kernel space.

WEBSHELL FOR SALE

On March 19 2023 at 01:49 am (UTC) Magnetic Wolf published a post on a dark web hacking forum, offering a webshell exploit for the national government agency of a European country.

A webshell is a malicious script used by threat actors, and is uploaded to a remote server. This webshell can then be used as a backdoor into the system they have compromised. This backdoor allows them to return to the system to launch further attacks or - in this case - to sell the access for other cybercriminals to exploit.

Through their tracking of Magnetic Wolf, Searchlight Cyber analysts observed the post and alerted the government agency, who were then able to find and remediate the webshell before it was exploited. This effectively prevented a cyberattack from taking place.

DARK WEB TRAFFIC

Following the discovery of the dark web forum post Searchlight Cyber researchers investigated further and discovered an anomalous pattern of traffic to the government agency's network from the dark web network The Onion Router (Tor).

Traffic from Tor to an organization can suggest potentially suspect activity as it indicates an individual is visiting from the dark web. While this could just be a curious onlooker, patterns in data can indicate whether the visitor is attempting to do something malicious.

This graph (**Figure 1**) shows dark web traffic to the organization's network since December 2022. When drilling down into this data, Searchlight Cyber analysts investigated traffic around the time of the post on the dark web forum on March 19.

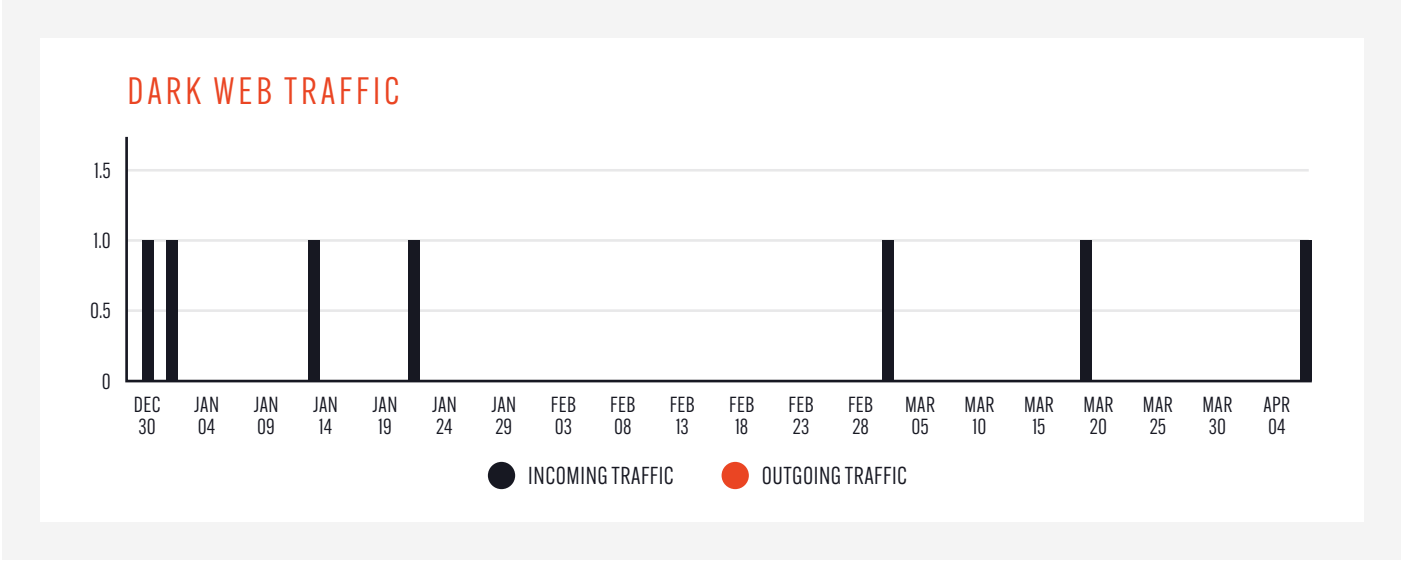


Figure 1: Dark web traffic relating to the government agency's network, displayed in Searchlight Cyber's dark web monitoring platform, DarkIQ.

Examining this connection on March 18 in closer detail (**Figure 2**) demonstrates that there was incoming traffic from the dark web less than four hours before Magnetic Wolf posted about the webshell on the dark web forum, which is highly indicative that the Tor activity relates to the actions of the threat actor.

DATE	TYPE	PORT	TOTAL CONNECTIONS	DATA REQUEST (BYTES)	DATA RESPONSE (BYTES)
2023 - 01 - 21	Incoming	443	1	2441	6786
2023 - 03 - 02	Incoming	443	4	2715	19178
2023 - 03 - 18	Incoming	443	1	13675	6350
2023 - 04 - 07	Incoming	443	1	1817	6922
2023 - 05 - 30	Outgoing	-	-	-	-
2023 - 05 - 31	Incoming	443	1	372	0

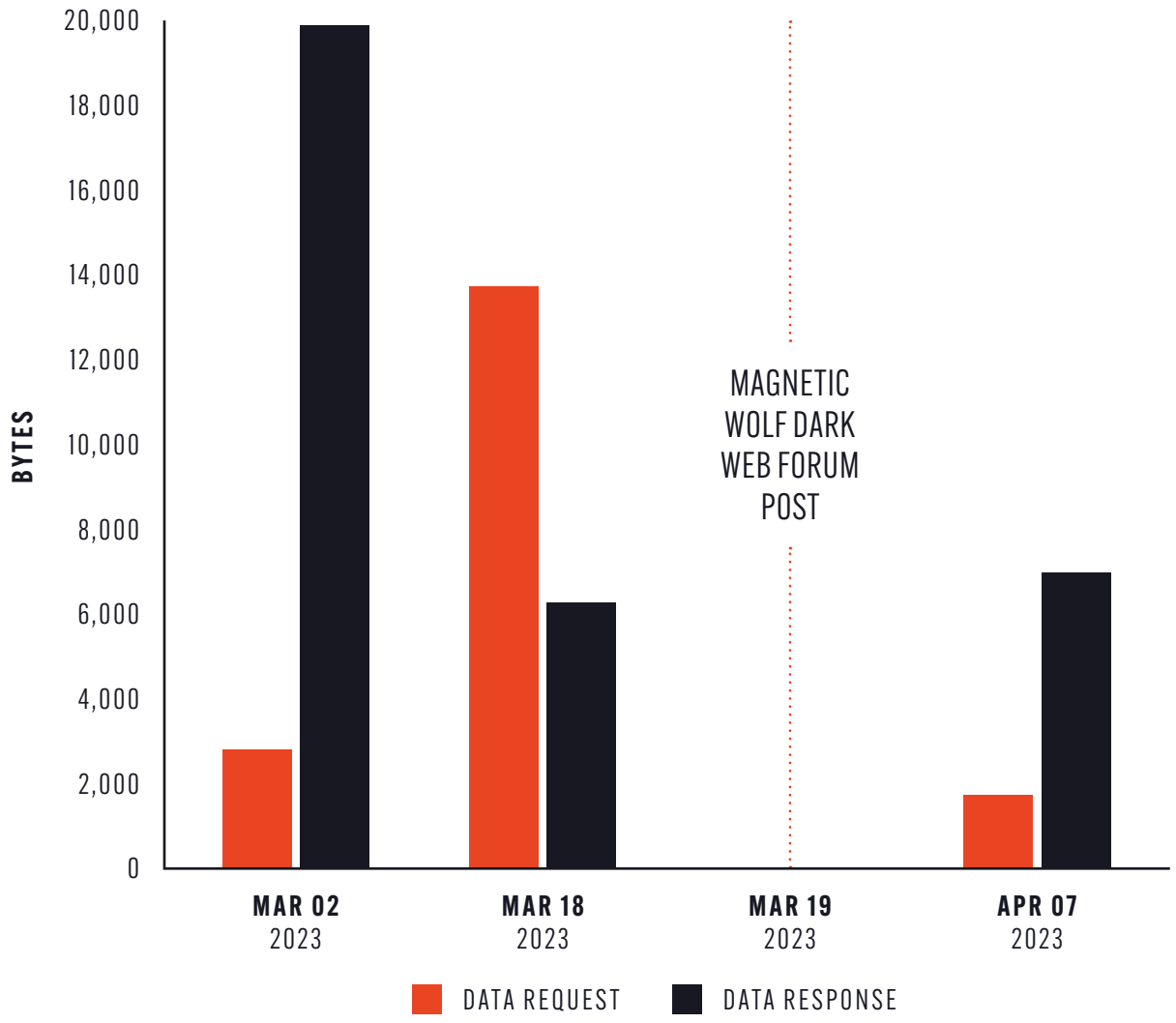


Figure 2: Dark web traffic activity around the time of the Magnetic Wolf post on the dark web forum. The gap between an anomalous Tor connection and the sale of a webshell is 3 hours and 37 minutes.

This hypothesis is supported by the fact that data sent into the server over Tor on March 18 is larger than would be anticipated in comparison to the size of the response. Usually, response data is larger than data into the server. For example, the connections on March 18 and April 7 were likely benign due to the data behavior.

However, the size of the data request into the server from the Tor network on March 18 suggests anomalous activity such as something downloaded onto the network - potentially the actor uploading the webshell before attempting to sell it hours later. Seeing a relatively large upload to your infrastructure from the Tor network should be the subject of close analysis. Based on our examination of a sample of webshells, the upload size via Tor (13.6 kB) is consistent with the approximate size of a webshell file, which typically range from 5 kB, through to 50 kB in size.

An alternate hypothesis could be it is a legitimate file upload to the network but this is unlikely for a number of reasons. Firstly, it is unlikely for a member of a government agency to be uploading a file to their network via Tor. Secondly, there is little evidence in the other dark web traffic to suggest this was a common - and therefore non-anomalous - occurrence.

Monitoring dark web traffic to the network would have almost certainly triggered further investigation by the security team had the dark web forum post not been spotted first. This means there are two potential “early warning signs” in dark web data that could have led the government agency to identify the attack.

SUMMARY

Cybercriminals commonly target organizations on dark web forums. As this case demonstrates, this includes numerous examples of threat actors selling access to organizations to other criminals to orchestrate more serious attacks.

This is an established part of the cybercriminal economy and threat actors conduct this activity brazenly, with the belief that the dark web offers them a degree of anonymity that organizations won't be able to spot that they are being targeted until it's too late.

Dark web monitoring changes that status quo. This case demonstrates how inbound dark web connections can be used by security teams to stop emerging attacks in their tracks.

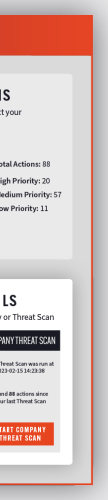
However, that can only happen if organizations are continuously monitoring for the early warning signs that their organization is being targeted. That is where we come in.

USE DARKIQ TO IDENTIFY THE EARLY WARNING SIGNS OF A CYBERATTACK

Our dark web monitoring platform DarkIQ continuously searches the dark web for early indicators of an attack against your organization.

- Receive alerts for dark web mentions of your organization, employees, or technologies.
- Spot cybercriminals in the reconnaissance stages of their attack.
- Interrogate dark web traffic to and from your network.
- Continuously monitor marketplaces, forums, onion sites, code repositories, social chats, CVEs, domains, phishing sites, and more.

- Assess your dark web exposure over time.
- Take mitigative action against attackers earlier in the Cyber Kill Chain.



> ALL COMPANIES SHOULD BE MONITORING THE DARK WEB FOR "EARLY WARNING SIGNS" OF THREATS AGAINST THEIR ORGANIZATION.

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