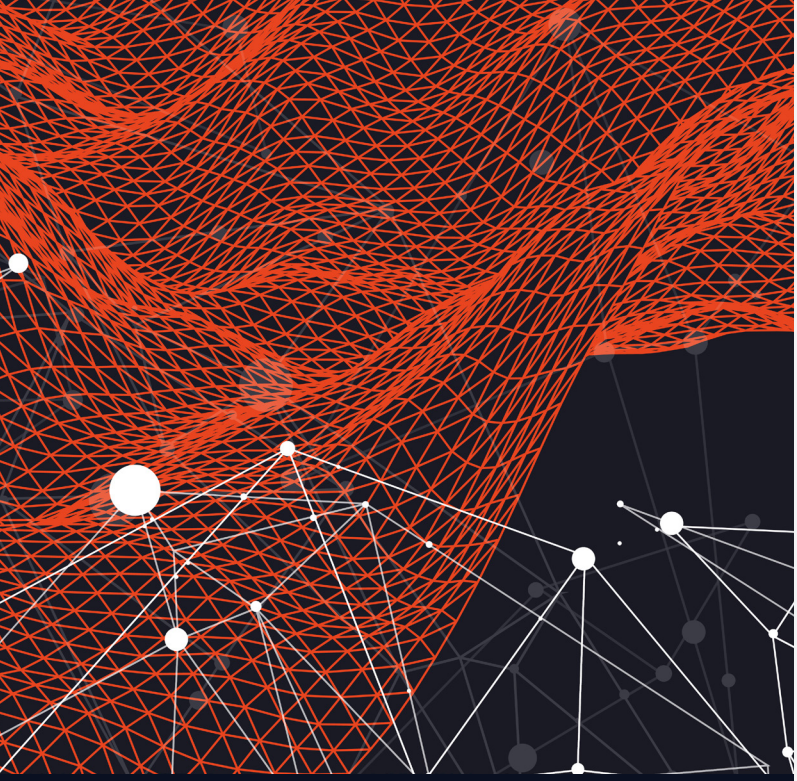
SEARCHLIGHT. CYBER

SHIFTING LEFT IN THE CYBER KILL CHAIN

HOW EARLY WARNING SIGNS OF AN ATTACK CAN BE IDENTIFIED ON THE DARK WEB

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CYBER ESSENTIALS



SEARCHLIGHT.
CYBER

Searchlight Cyber provides organizations with relevant and actionable dark web threat intelligence, to help them identify and prevent criminal activity. Founded in 2017 with a mission to stop criminals acting with impunity on the dark web, we have been involved in some of the world's largest dark web investigations and have the most comprehensive dataset based on proprietary techniques and ground-breaking academic research. Today we help government and law enforcement, enterprises, and managed security services providers around the world to illuminate deep and dark web threats and prevent attacks.

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CYBER ESSENTIALS

> DARK WEB MONITORING AND INTELLIGENCE GIVES ORGANIZATIONS THE CAPABILITY TO STRIKE BACK AGAINST THREAT ACTORS EARLIER IN THE CYBER KILL CHAIN - BEFORE THE NETWORK IS BREACHED.

INTRODUCTION

Organizations around the globe continue to invest in their defenses against cyber threats, proven by the market value standing at an estimated $139.77 billion in 20211. With an ever increasing number of capabilities and methodologies on offer for security teams to deploy, the focus has generally evolved around identification of malicious activity within a network. Should such activity be detected, the lengthy task of remediation begins, not only to ensure that damage to the company is limited, but that business-as-usual can return as soon as possible, in a secure environment without risk of further compromise.

However, the concept of monitoring activity within the network perimeter, whilst a vital component in securing infrastructure, is a reactive approach to security. That is, a malicious actor or cyber criminal usually needs to be operating inside of the network before they are detected, resulting in a signature match for an Intrusion Detection System, for example. Or it could be the detection of new network communications being established, potentially identified during the reach back to a staging server during data exfiltration. Unfortunately, in both of these scenarios, the organization has already been breached.

The importance of having these security measures in place cannot be stressed enough, as without them the likelihood of attacks in general would increase and for many organizations the impact of falling victim to a cyber attack can be catastrophic. However, is monitoring of internal networks sufficient? Is there another capability organizations can add to their arsenal in order to further enhance their security?

In short, yes.

Dark web monitoring and intelligence gives organizations the capability to strike back against threat actors earlier in the Cyber Kill Chain - before the network is breached - enabling them to take a much more proactive approach to cybersecurity. This report explains where the dark web fits in the Cyber Kill Chain and uses the real life example of a university breach to demonstrate how dark web intelligence could have helped to prevent the attack.

Dr Gareth Owenson
CTO of Searchlight Security

SHIFTING LEFT IN THE CYBER KILL CHAIN

The Cyber Kill Chain is one of the more commonly referenced frameworks in cybersecurity. Originally developed by the aerospace and defense company Lockheed Martin2, the framework is a part of the Intelligence Driven Defense model for identification and prevention of cyber intrusion activity, highlighting the different stages of an attack a threat actor must complete in order to achieve their objective. There are seven stages in the Cyber Kill Chain:

> TO GIVE THE BEST CHANCE OF DISRUPTING A CYBERCRIMINAL'S OPERATIONS, ENTERPRISES NEED TO STRIKE EARLIER.

The general consensus amongst cybersecurity teams is that the earlier, or further to the left in the kill chain, that cyber threat actors can be identified then the less likely they are to be successful in their operations. For example, if phishing emails can be identified by the end user and the malicious link within is not opened then the chain will be broken at the Delivery phase. Unfortunately, as threat actors continue to evolve their capability and their skill sets to bypass existing security solutions, identification of an attack is not always that simple.

Therefore, to give the best chance of disrupting a cybercriminal's operations, enterprises need to strike earlier by "shifting left" of the Delivery phase.

To the left are Weaponisation and Reconnaissance. Weaponization will almost certainly be done in a threat actor's own environment. With no reason for them to connect to the network before delivery, identifying and disrupting this stage is pretty much impossible for an organization.

However, cyber criminals do create a footprint during the Reconnaissance phase on deep web and dark web marketplaces and forums, which creates an opportunity for organizations to be proactive and move their defences to the start of the Cyber Kill Chain.

There are several key opportunities here for organizations to identify potential risk from threat actors during the Reconnaissance phase:

IDENTIFICATION OF LEAKED CREDENTIALS

Organizations are often completely unaware that their data has been leaked and potentially published on leak sites or pastebins. In some cases this is the result of third party organizations being breached where individuals have used their business emails and passwords to create accounts, such as for mailing lists.

Identification of this data on the dark web can enable organizations to enforce password changes on the compromised accounts to prevent access through exploiting these credentials. It can also inform the implementation of additional layers of authentication, if not already in place.

SALE OF CREDENTIALS

Batches of an organization's credentials for sale are commonplace in dark web markets, enabling lower tier criminals to monetize the data they have gathered, whilst the criminals buying the data will often seek to exploit the organizations further. Not only can this activity be observed through market listings, but breached credential trading also takes place on dark - and clear - web forums and via channels such as Telegram and Discord.

Identification of batch credential data can indicate a previous breach, prompting security teams to conduct a thorough investigation into their networks to identify and patch any vulnerabilities. It may also be possible to associate forum, market, or chat usernames with threat actors, providing an indication of which adversary may be targeting the company. In turn, this can enable the security team to alter their risk position and prompt a review of the mitigation approach or incident response playbooks.

DARK WEB TRAFFIC

Communications between the corporate network and Tor nodes is a red flag of criminal activity. Cyber criminals, advanced persistent threat groups and hacktivists have all utilized Tor in the past to anonymize their activity. From Tor, they are able to scan an organization's networks for vulnerabilities, open ports and unsecured systems, helping to identify the most efficient avenue of attack through which they can conduct their operations.

Incoming network activity from Tor nodes to a company's network can indicate possible Reconnaissance activity such as port or vulnerability scanning. The ability to see which ports are being actively targeted at any given time can have a dramatic impact for businesses in helping to prioritize defenses on the most likely paths of attack.

Outgoing traffic from an organization's network towards a Tor server is a potential indicator of an insider threat, or even a compromised device communicating back to Command and Control (C2) servers. Again, this visibility can help security teams to take swift action in disconnecting systems calling out to the dark web and begin their investigations to find the cause.

Identifying the early warning signs of attack through dark web intelligence aligns not just to the Cyber Kill Chain framework, but also the Reconnaissance phase of the MITRE ATT&CK3 framework, including techniques such as Gather Victim Identity Information4 (T1589) and Gather Victim Network Information5 (T1590).

With this intelligence in hand, organizations can be notified at the earliest opportunity of a potential risk to their networks, make the corrective actions required and put themselves in the best position possible to mitigate an attack before adversaries gain initial access to the network. Without it, organizations are literally already two steps behind criminals in the Cyber Kill Chain.

> THE ABILITY TO SEE WHICH PORTS ARE BEING ACTIVELY TARGETED AT ANY GIVEN TIME CAN HAVE A DRAMATIC IMPACT FOR BUSINESSES IN HELPING TO PRIORITIZE DEFENSES ON THE MOST LIKELY PATHS OF ATTACK.

CASE STUDY: UNIVERSITY BREACH

In 2021 a university in the United Kingdom was the victim of a serious ransomware attack. The attack caused the university to close for several weeks, with some IT systems remaining offline and under investigation for much longer to ensure all traces of the ransomware had been removed.

The university dealt with the situation very efficiently and kept downtime to a minimum. Nevertheless, the attack had a significant negative impact on the university, staff and students alike.

Not only were students' emails leaked, but access to key services required for their studies such as the university library were severely limited, with students living on campus being advised not to log into the network. In addition to the disruption caused for the students, the university was inevitably hit by costs associated with the attack, from the downtime in the services offered, the costs associated with incident response activities, to the ransom demand itself.

The reality is, as with most situations following a breach, security teams find themselves in a reactive position. They are trying to understand what has happened, how it happened, the extent of the attack and how the attackers gained initial access, which can be a timely process.

However, in the year prior to this attack there were a number of indicators on the dark web which, if properly monitored, could have highlighted the potential for an imminent attack. With access to dark web threat intelligence relating to the university and its digital assets, it is highly likely that the actions of the ransomware gang would have been spotted in the Reconnaissance phase of the Cyber Kill Chain.

The security teams could have been alerted on at least three separate occasions that data had been leaked and that suspicious connections to the network were ongoing. This would have in turn enabled necessary security preventions to have been put in place prior to ransomware deployment.

TIMELINE OF ATTACK

MONTHS PRIOR TO ATTACK

TWELVE

ELEVEN

TEN

NINE

EIGHT

SEVEN

SIX

FIVE

FOUR

THREE

TWO

ONE

ZERO
DAY OF ATTACK

TWELVE MONTHS PRIOR TO ATTACK

THREAT ACTORS' RECONNAISSANCE

- A year before the attack, more than 3,100 email address and password pairs (also known as "combos") belonging to staff and students of the university appeared on leak sites.
- This information is invaluable for attackers as a combination of this data can allow easy access to networks.

POSSIBLE DEFENSIVE ACTIONS

- Monitoring for leaked credentials across the dark web would have provided an early indication that potential access to the network was available to malicious actors.
- Security policies could have been updated to ensure that affected users - if not all users across the campus - updated their passwords at the earliest opportunity, rendering the leaked email address and password combinations useless.

FOUR MONTHS PRIOR TO ATTACK

THREAT ACTORS' RECONNAISSANCE

- A significant increase in network communications between Tor nodes and the university IP addresses associated with Virtual Private Network (VPN) accounts can be observed in the months prior to the attack.
- Approximately four months before the incident, 47 separate connections were made from Tor nodes to individual IP addresses associated with VPNs.
- This activity may have been reconnaissance to ensure that connection with the network could be established using the leaked combinations of university email addresses and passwords.

POSSIBLE DEFENSIVE ACTIONS

- Identification of access from Tor nodes to VPNs' associated IP addresses could have initiated stricter monitoring of these addresses.
- The security team could have enhanced the security and monitoring of the affected VPNs to minimize risk of exploitation.
- Investigations could have identified the IP addresses associated with the Tor nodes, enabling the security team to add them to firewall blacklists so that future Tor communications were blocked.

LESS THAN ONE MONTH PRIOR TO THE ATACK

THREAT ACTORS' RECONNAISSANCE

- In the weeks leading up to the attack, discussions on hacker forums increased regarding access to a number of organizations within the European Union, including this university.
- Threat actors claimed to have access to hundreds of different organizations across multiple industries, including aviation, healthcare, technology, and education.
- In one listing 'Fooble', an active user on the forum Exploit, offered 'valid access' to more than 200 EU organizations for 20K (the currency was not specified). **See Figure 1**.

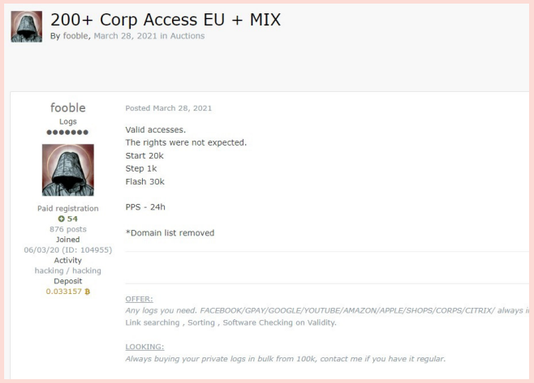


Figure 1: A threat actor under the alias "fooble" claims to have access to more than 200 EU organizations, including the UK based University

- This listing contained information around the organizations on offer - which included the UK University - with links to D&B Business Directory6 so that potential customers could see the estimated value of the compromised organizations.
- Additionally, there were more communications between Tor nodes and university IP addresses associated with VPN accounts in this period, likely to test the validity of access to these IPs.

POSSIBLE DEFENSIVE ACTIONS

- Knowledge of the dark web chatter around the university, the listing of access for sale, and the increase in activity against VPN associated email addresses for sale, would have undoubtedly led the security team to take a defensive security posture and prepared them to respond to a breach.
- The security team could have isolated the accounts associated with the compromised VPNs from the network to prevent the attacker from delivering and executing the payload.
- This would have also given the security team valuable time to update security policies and reset the associated passwords.

> "THE SECURITY TEAM COULD HAVE ISOLATED THE ACCOUNTS ASSOCIATED WITH THE COMPROMISED VPNS FROM THE NETWORK TO PREVENT THE ATTACKER FROM DELIVERING AND EXECUTING THE PAYLOAD.

SUMMARY

Organizations are continuing to be compromised in spite of investing in security solutions to protect their networks. In order to break this cycle, security teams need to view their existing capabilities as a solid foundation of security infrastructure, but also seek to augment them with intelligence that alerts to the possibility of attack earlier in the Cyber Kill Chain.

Dark web threat intelligence should be considered as an integral component to enhancing an organizations' security posture.

As the University case demonstrates, monitoring the dark web for the presence of information relating to an organization can provide early indicators of potential avenues of attack or potential threats. This monitoring can also be extended to an organization's supply chain to further increase security.

Employing a dark web monitoring capability can help to move an organization from a reactive posture and into a proactive security posture, identifying potential threats before cybercriminals can compromise the network.

USE DARK WEB INTELLIGENCE TO ILLUMINATE THREATS AND PREVENT ATTACKS

SEARCHLIGHT CYBER HELPS YOU TO PROACTIVELY PROTECT INFRASTRUCTURE, PEOPLE AND DIGITAL ASSETS ACROSS YOUR ORGANIZATION WITH RELEVANT, ACTIONABLE DARK WEB INTELLIGENCE.

MANAGE DARK WEB RISK EXPOSURE

Get an instant health report of your organization's exposure on the dark web and make decisions from Searchlight's intuitive, easy to use interface.

PREVENT DATA BREACHES

Identify early warning signs of attack through continuous monitoring of indicators of malicious activity such as leaked credentials, IP addresses, open ports, compromised devices, and dark web traffic.

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.

SUPPLY CHAIN MANAGEMENT

Remotely monitor the exposure of your third party suppliers and partners on the dark web without the need for an agent on their systems, to prevent supply chain attacks and prove compliance.

INCIDENT INVESTIGATION AND RESPONSE

Forensically examine the chain of events in the dark web that led to an attack to inform incident mitigation and response.

REFERENCES

PAGE 3

1. https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

PAGE 4

2. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

PAGE 6

3. https://attack.mitre.org/matrices/enterprise/
4. https://attack.mitre.org/techniques/T1589
5. https://attack.mitre.org/techniques/T1590

PAGE 9

6. https://www.dnb.co.uk/

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