DARKTRACE
Evolving threats call for evolved thinking™

# Healthcare Threat Trends Report / 2022

## Industry Spotlight

DARKTRACE

## CONTENTS



# Executive Summary

Darktrace's early indicator analysis[1] of the threats facing the healthcare sector over the last year paints a picture of a global healthcare sector that remains a top target for cyber-criminals who are particularly hungry for patient data.

Security teams remain over-stretched and under-resourced in the sector, particularly as the recovery from a global pandemic continues. Cyber attackers continue to target the sector because of its reputation for low cyber maturity, and its wealth of sensitive data-stores. Attackers are not only seeking out protected health information (PHI) to conduct standard identity theft and extortion of victims but also seek to access prescriptions, other medical services and even to file false insurance claims.

Data exfiltration is a common technique used in sophisticated ransomware attacks – an attack method renowned for its ability to cause disruption to normal operations. The prominence of data exfiltration in the healthcare sector indicates a high risk of such disruption, which can directly impact patient care, as well as the risk of significant financial loss for a sector that already runs on tight budgets.

In 2022 the UK and Australian healthcare sector saw a notable rise in data exfiltration. In the US healthcare sector there was a decrease in data exfiltration threats, but the attack type remained in the top three most common malicious activities observed in the sector. Despite this, data exfiltration remained a significant challenge to the global healthcare sector in 2022.

1. Darktrace's data is developed by 'early indicator analysis' that looks at the breadcrumbs of potential cyber-attacks at several stages before they are attributed to any particular actor and before they escalate into a full-blown crisis.

# The Data

Darktrace's 'Unusual External Data Transfer' indicators were the **third most common threat** detected in the UK, US, and Australia, after 'Suspicious Network Scan' and 'Lateral Movement' indicators. Even in the US where the percentage of exfiltration threats seen in 2022 was less than in 2021, it remained the third most common indicator. 'Suspicious Network Scan' and 'Lateral Movement' are *always* expected to be the first and second most common indicators as they are the earliest actions a potential hacker takes to conduct the vast majority of cyber-attacks. Essentially, they are attempting to find a way in, then establish a foothold by infecting more devices which is the bread and butter of most attacks. It's what comes next that varies according to sector, threat type and environment and is therefore an important point of analysis.

If we take the ransomware attack deployed against Advanced Software Services to attack several NHS services including 111 in August 2022, as an example, the pathway becomes clear. Advanced's report of the breach states : "[after gaining access through a third party], the attacker moved laterally in Advanced's Health and Care environment and escalated privileges, enabling them to conduct reconnaissance, and deploy encryption malware. Immediately prior to encrypting systems, the threat actor copied and exfiltrated a limited amount of data."

In this context, the below data, taken from Darktrace's fleet, shows that both Australia and the UK are suffering with increasing proportions of exfiltration, while the US healthcare sector is faring better than in 2021, but still being burdened by data theft.

## Australia

1. The most observed cyber incident in the Australian healthcare sector was **Suspicious Network Scan Activity**, compared with the previous year when it was Multiple Lateral Movement Model Breaches.
2. The second most observed cyber incident in the Australian healthcare sector for 2022 was **Multiple Lateral Movement Model Breaches**.
3. The third most observed cyber incident in the Australian healthcare sector was **Enhanced Unusual External Data Transfer**. Data Exfiltration accounted for **1.42x more** of all cyber incidents in the sector in 2022 compared to 2021.

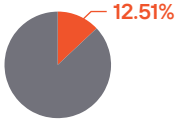

## UK

1. The most observed cyber incident in the UK healthcare sector was **Suspicious Network Scan Activity**.
2. The second most observed cyber incident in the UK healthcare sector was **Multiple Lateral Movement Model Breaches**.
3. The third most observed cyber incident in the UK healthcare sector was **Enhanced Unusual External Data Transfer.** Data Exfiltration accounted for **1.04x more** of all cyber incidents in the sector in 2022 compared to 2021.


## US

1. The most observed cyber incident in the US healthcare sector was **Suspicious Network Scan Activity**.
2. The second most observed cyber incident in the US healthcare sector was **Multiple Lateral Movement Model Breaches**.
3. The third most observed cyber incident in the US healthcare sector was **Enhanced Unusual External Data Transfer**.


The number of data exfiltration incidents as a percentage of overall incidents **decreased by 34.19%** between 2021 and 2022.




Despite this decrease, these incidents still **accounted for 12.51% of all incidents** seen in the US healthcare sector in 2022.

## MITRE ATT&CK Category: Exfiltration

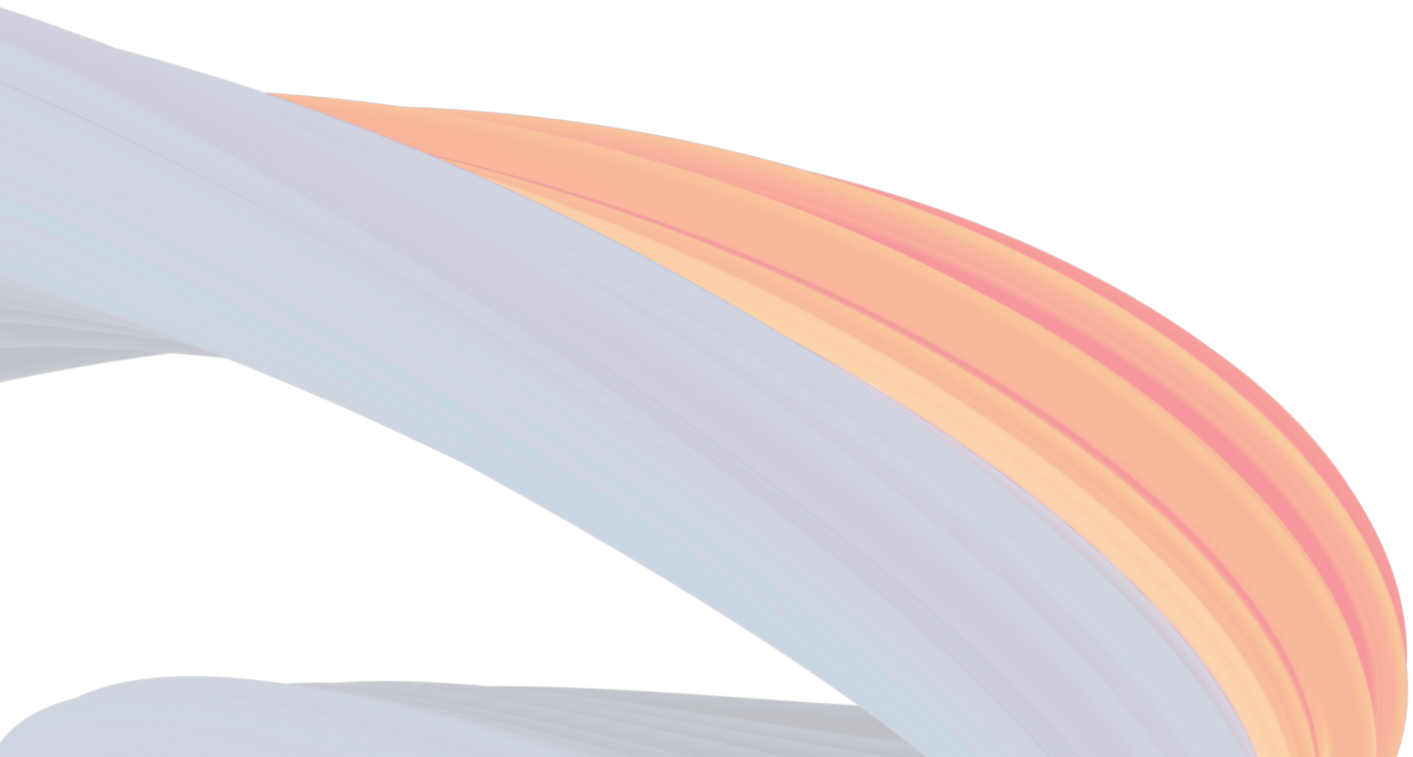
MITRE ATT&CK categories are the industry standard to group different attack-types.

The adversary is trying to steal data.

> " Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command-and-control channel or an alternate channel and may also include putting size limits on the transmission."

## Threat Story

In January 2022, a US healthcare customer saw a malicious PowerShell script deployed on one of their internal servers. Darktrace DETECT/Network immediately detected unusual activity. Darktrace revealed that the script was hardcoded to connect to a rare IP to create a 'reverse shell' session which, if successful, would have handed control to the threat actors. With a reverse shell they could have issued remote commands, opening the network to further lateral movement, data exfiltration and malware deployment. Ultimately this was unsuccessful as Darktrace RESPOND/Network ensured the connections were blocked.



## Expert Analysis

The global healthcare sector has historically been characterized by high rates of technology obsolescence, and while recent years have seen a deliberate push within the industry to resolve these cyber security 'black spots', some regions have been faster than others in their digital transformation, and the sector remains a top target for data exfiltration attacks.

### How does Data Exfiltration work?

In plain English, data exfiltration is the theft of data, to either then be sold on as a commodity or held to ransom as a form of extortion. Sometimes this is via an attacker gaining access to an organization's network and exfiltrating that data back to their own storage equipment. Other times there could be an insider who is either stealing that information for themselves or being paid by an attacker to use their legitimate credentials and abuse the trust of their employer.

Data exfiltration attacks have proliferated in recent years with the rise of first double and then triple extortion ransomware actors. Attackers are looking to get the maximum ROI for a successful compromise of a network, and if backups are reducing the impact of business disruption due to data encryption, reputational damage and potential threats from information regulators has proven to be just as good leverage.

### Why the Healthcare Sector?

Hospitals and other healthcare organizations can be seen as a 'soft target' for unscrupulous threat actors. With the impact of covid still being felt most keenly in healthcare, hospitals remain over-stretched and under-resourced. With digital infrastructure in hospitals spanning everything from back-office networks and patient record systems, to connected medical devices and IoT equipment, the challenge of defending critical data and building resilience is more daunting than ever. We see a lot of medical devices using embedded operating systems which are either difficult to patch or cannot be patched at all. Many organizations in the healthcare industry run a "flat network" where equipment, admin systems, front-line workers and patient information are all stored in the same area instead of segmenting networks. As such, the reality of an attack such as ransomware on hospitals can be devastating, with disrupted IT systems leading to ambulances being rerouted, urgent surgeries being postponed, and treatment options being scaled back - ultimately jeopardizing human life.

The sensitivity of patient data is a massive factor in why the healthcare sector gets targeted. It is also not unheard of for nation-state actors to try to illegitimately acquire intellectual property. Or alternatively, as we have seen, it could be part of a ransomware attack where the threat of blackmail is used to coerce a ransom payment, meaning that sensitive data will be uploaded if the victim does not pay the ransom. Whether that's through triple extortion (first demonstrated in the attack against the Finnish Psychotherapy firm, Vastaamo, and the onward extortion of the individual patients), or as demonstrated against Australia's Medibank, the higher privacy stakes and subsequent greater reputational risk is leveraged by opportunistic hackers to ensure payment.

Hospitals and other healthcare organizations are extremely rich data-sources. Data is being described today as "the new gold" as it is critical for an organization to survive, with insights it provides offering a competitive edge. This data is highly lucrative for attackers, as we have seen with a multitude of high profile breaches this year. Attackers can make a profit from selling customer or patient information such as medical records, credit cards or banking details.

### Differing levels of compromise indicators in different regions

Interestingly this year we saw a rise in the proportion of data exfiltration threat indicators in the UK healthcare sector, and a larger (more concerning) rise in Australian healthcare, but the US has seen a reduction in the proportion of data exfiltration indicators compared with 2021. It's a difficult art to say exactly why the US healthcare sector seems to be faring better than last year, but one factor could be the increasing cyber maturity of the US healthcare sector.

It is important to note that exfiltration indicators still account for the third most frequent alerts seen by Darktrace in the US healthcare sector, after Suspicious Network Scan Activity (34%); and Multiple Lateral Movement Model Breaches (22%). Network scans and lateral movement are always to be expected be the first and second most common indicators which our AI will flag because those are the first and second things which almost any potential attacker will start with. Network scans are carried out on almost every organization daily, as hackers look for any easy way in. Pentesters will also carry out network scanning as part of their work. Greater cyber maturity in the US healthcare sector could well mean that potentially suspicious activity is being stopped in these early stages, before any attempt at data exfiltration can be made.

## List of Contributors

**Toby Lewis,** Global Head of Threat Analysis

**Tony Jarvis,** Director of Enterprise Security APAC

## About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. It is delivering the first ever Cyber AI Loop, fueling a continuous end-to-end security capability that can autonomously prevent, detect, and respond to novel, in-progress threats in real time. Darktrace employs over 2,200 people around the world and protects over 8,100 organizations globally from advanced cyber-threats.

Scan to LEARN MORE

DARKTRACE

Evolving threats call for evolved thinking™

North America: +1 (415) 229 9100
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
Latin America: +55 11 97242 2011
info@darktrace.com
darktrace.com