

Improving Protections Against Healthcare-Focused Attacks

The healthcare sector has emerged as the primary target for cyber threats. The need for modern, reactive protections paired with proactive guidance is increasingly critical.

Traditional tooling like EDR, XDR, and firewalls are no longer enough on their own. Network Detection and Response for Healthcare (NDR-H) tools are vital to stop advanced attackers in their tracks, and defend vital systems and data. Unlike traditional solutions, NDR works by monitoring and analyzing all network traffic, not just incoming requests or endpoint activity. This lets you defend all the devices connected to your network, regardless of device manufacturer, OS, or BDR protection status. It's the next level of protection for your healthcare network environment.

Cynerio's Network Detection & Response technology is tailored for the unique needs and staffing challenges of healthcare settings. NDR-H is designed for rapid deployment, and enables response times measured in seconds even with minimal resources.

Designed specifically for healthcare environments



■ Tailored For Healthcare

Cynerio's NDR-H tooling knows what 'normal' traffic should look like in a healthcare setting, so there are fewer false positives and false negatives.

■ Day 1 Protections

Immediately identify and protect against dormant, ongoing, and future attacks, ensuring swift response and mitigation.

■ Comprehensive Coverage

Address attacks on all connected technologies, including IT, IoT, IoMT, and OT systems, creating a unified defense against diverse threat vectors.

■ Remediate With CSA Playbooks

Cynerio NDR-H allows you to remediate threats immediately to stop attacks in their tracks. CSA Medical Device Playbooks are provided to guide further action.

■ Supported Response

Receive clear attack details, guidance, and support within minutes, empowering decisive, efficient action.

■ Validated Findings

Remove the noise generated by traditional systems, focusing on verified threats for more efficient and accurate response efforts.

■ Get Access To All Your Data

At Cynerio, we don't blackbox your data. You'll have full access to your logs, including full forensic details, tracing the origin and flow of data, and providing crucial insights for comprehensive investigation and response.

■ Fits In Your Existing Ecosystem

No matter which firewall or EDR/XDR vendor you're currently using, Cynerio NDR-H is a complementary solution that plugs the gaps in your network security.

■ Full Integration

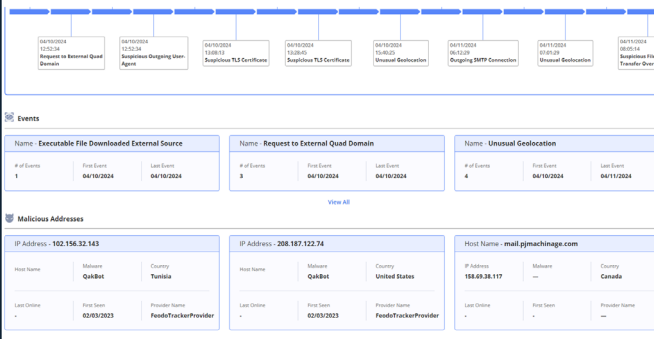
Seamlessly view results in the Cynerio Platform or integrate with existing in-place systems, ensuring a cohesive cybersecurity infrastructure.

■ Embrace Generative AI

Harness the power of advanced feedback loops, fueled by insights from a diverse array of healthcare environments.



Ongoing, Real-Time Protections



Events

Name	# of Events	First Event	Last Event
Executable File Downloaded External Source	1	04/10/2024	04/10/2024
Request to External Quad Domain	3	04/10/2024	04/10/2024
Unusual Geolocation	4	04/10/2024	04/11/2024

Malicious Addresses

IP Address	Host Name	Malware	Country
102.156.32.143	QakBot	Turla	United States
208.187.122.74	QakBot	Turla	United States
158.69.38.117	mail.pjmachine.com	Turla	Canada

Identify Exploitation Attempts
Uncover verified exploit attempts and remediation guidance.

Attack Description

On 2024-04-10 at 13:52 UTC, a Windows computer DESKTOP-SX3EYDP was infected with Qakbot (Qbot) malware. The Qakbot infection may have spread to another computer on the network DESKTOP-AM7UTX. The infected machine DESKTOP-SX3EYDP was also observed connecting to multiple SMTP servers, which is indicative of spambot activity.

[Click for more info](#)

SOS Action

1. Isolation - Disconnect the affected systems from the network immediately.
2. Check if other devices were affected, and try to estimate the size of the attack.
3. Identify suspicious Programs or processes running on the affected devices, and remove them. Consider using a suitable scanning software for this process.
4. Policy - Block all traffic from the malicious domain the file was pulled from (if known).

Quarantine

Attack Schema

First Seen - 04/10/2024 12:...

7 External

In-App Remediation with CSA Playbooks
Easily take remediation steps within the Cynerio dashboard to remediate and isolate attacks (requires integrations).

Malware - Lateral Movement **QakBot Malware Spreads on Network**

Attack Description

On 2024-04-10 at 13:52 UTC, a Windows computer DESKTOP-SX3EYDP was infected with Qakbot (Qbot) malware. The Qakbot infection may have spread to another computer on the network DESKTOP-AM7UTX. The infected machine DESKTOP-SX3EYDP was also observed connecting to multiple SMTP servers, which is indicative of spambot activity.

Cynerio Live - Analyst Note

A CynerioLive analyst validated the detections and assessed that the machine DESKTOP-SX3EYDP is indeed infected with Qakbot. AKA Qbot. The indicators observed are consistent with Qakbot, including TLS certificates, and the external SMTP connections that indicate spam-sending activity. We have yet to see indications that DESKTOP-AM7UTX is also infected, but it is usually preferable to err on the side of caution so it should be treated as such.

[See Detailed Records](#)

Detailed Threat Intelligence
Gain insights into the nature and origin of detected threats for informed decision-making.

7 Bad Actor

Bad Actor	Severity	Time	Module	Event	Details
Bad Actor 1 (158.69.38.117)	High	04/10/2024 13:28:45	NDR	Suspicious TLS Certificate	Host: 208.187.122.74
Bad Actor 2 (122.155.171.181)	High	04/10/2024 13:08:13	NDR	Suspicious TLS Certificate	Host: 102.156.32.143
Bad Actor 3 (64.29.145.194)	Medium	04/10/2024 15:40:25	NDR	Qakbot C2 Activity	Server IP: 23.111.111
Bad Actor 4 (23.111.114.52)	Medium	04/11/2024 07:01:29	NDR	Unusual Geolocation	Geolocation: Thailand
Bad Actor 5 (102.156.32.143)	Medium	04/11/2024 07:01:29	NDR	Outgoing SMTP Connection	Host: wwm171-181
Bad Actor 6 (208.187.122.74)	Medium	04/11/2024 06:12:29	NDR	Outgoing SMTP Connection	Host: mail.pjmachine.com
Bad Actor 7	Medium	04/11/2024 06:44:29	NDR	Outgoing SMTP Connection	Host: mail.console
	Medium	04/11/2024 08:05:14	NDR	Suspicious File Transfer Over...	Filename: umtqgk...
	Medium	04/10/2024 12:52:34	NDR	Executable File Downloaded E...	File Type: Executable

Forensic Details for Additional Investigation
Access detailed forensic data to support further investigation and response efforts.

Stop Attacks Today

Healthcare environments are breeding grounds for undetected attacks that persist for months. Relying on traditional tools like EDR or firewalls may not be enough to stop attack from spreading. To identify and address these threats in your environment, contact Cynerio today at info@cynerio.com

Cynerio's Healthcare Cybersecurity Platform is tailored to safeguard medical environments against constantly evolving threats. From real-time detection of malicious network activity to strategic microsegmentation guidance, Cynerio delivers a robust suite of proactive and reactive protections. Elevate the security of healthcare facilities and ensure the safety of the patients they serve. Learn more at www.cynerio.com

