Hospital Experienced Ransomware Threat, *Undetected by EDR*

PONDURANCE

CASE STUDY

RANSOMWARE ATTACKS SAW A YEAR-OVER-YEAR DECREASE IN 2022, BUT 2023 HAS SEEN A SIGNIFICANT SURGE IN ACTIVITY.

In fact, the number of victims in March was 1.6 times higher than the peak month in all of the prior year, according to Black Kite's *Ransomware Threat Landscape Report 2023*. Threat actors are continuously finding innovative ways to infiltrate company networks to execute malicious malware and extort high-dollar ransom payments.

A prime example of such innovation was a recent incident where a large hospital experienced a *ransomware* threat that was undetected by the endpoint detection and response (EDR) solution.

IDENTIFYING THE THREAT

In June, a hosting provider notified a large hospital that it was seeing suspicious activity coming from the network. Pondurance, the hospital's managed detection and response provider, quickly performed a full analysis. The team identified a malicious backdoor and found a remote access trojan on a system in the hospital's digital envelope that had been downloaded as a result of search engine optimization (SEO) poisoning.

With SEO poisoning, a threat actor creates malicious websites and uses SEO keywords to make the websites rank high in the search results as seemingly relevant and authentic search options. That way, an unsuspecting victim is likely to click on a website in the search. SEO poisoning allows threat actors to target victims within a specific audience such as healthcare.

In this particular attack, the victim entered keywords for a contract agreement template used by healthcare workers. The victim downloaded the file and opened it. Then, the file executed a backdoor and gave the threat actor an entry vector into the network.

"Unfortunately, the hospital computer that downloaded the file did not actually alert on the file, even though it was malicious," said the Principal Incident Response Consultant at Pondurance. As a result, the threat actor was able to take numerous actions to execute the threat, moving into an environment that was not monitored by an EDR solution and continuing to move laterally across the environment.

DEFENDING THE ATTACK

A potential threat in the cyber landscape requires a rapid incident response, and Pondurance was ready. One of the first challenges for the Pondurance team was making sure that the hospital could continue functioning with minimal disruption as the team worked to contain the incident.

"We found ourselves walking a tightrope," said the Pondurance Consultant. "We were balancing patient needs, electronic patient health records and system needs while still making sure we didn't let this ransomware actor — or what we believed to be a ransomware actor — get any further into the network and potentially encrypt or disrupt the environment." The hospital experienced a bit of an outage, a workstation was taken offline and had to be reimagined, and connections were taken down between certain groups, but overall, the disruption was kept to a minimum.

The Pondurance team gathered a copy of the various malicious payloads and sent it to the EDR vendor. The vendor also worked on the incident.

"From our perspective, we now had a really valuable piece of intelligence here, much the same way that an intelligence service conducts intelligence collection through all of the different channels that it uses," said the Pondurance Consultant. With that intelligence, the team entered the backdoor, did some reverse engineering on the malware, and built that logic within the Pondurance EDR console to automatically detect similar activity and alert on it moving forward.

Hospital Experienced Ransomware Threat, *Undetected by EDR*

PONDURANCE

CASE STUDY

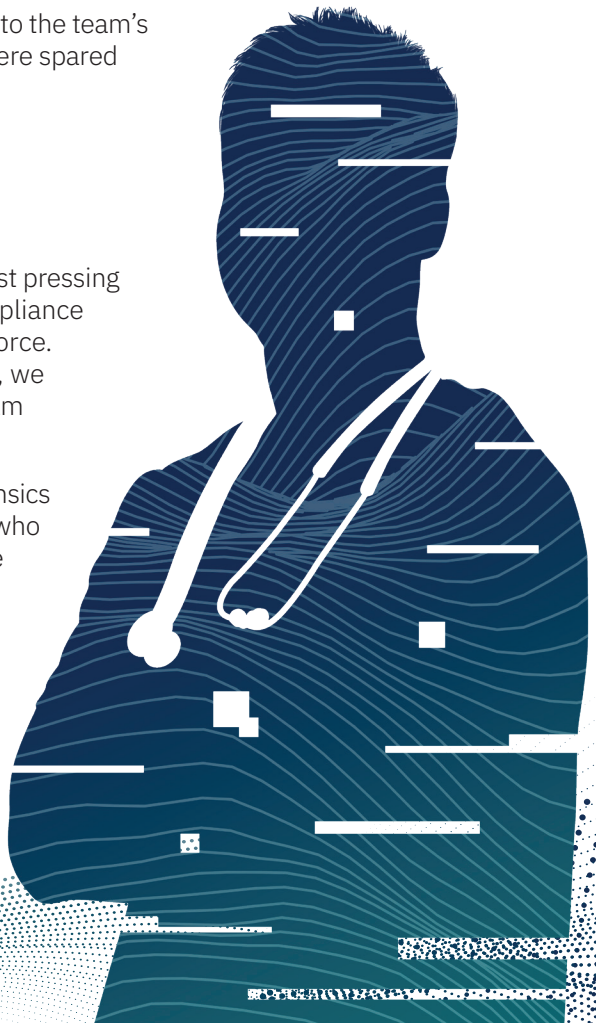
The team added the signature to the blacklist and rescanned its systems. Because the hospital belongs to a larger professional group that shares information and threat intelligence, many of which are Pondurance clients, Pondurance put out a communication to inform the entire group about the incident. The clients were pleased to hear that Pondurance had taken measures to contain the threatand improved its detection for the future.

AVOIDING FUTURE ISSUES

An EDR solution doesn't often miss malicious activity, but it can happen. When it does, a company needs a team of experienced humans to take control of the situation. Pondurance believes people are the most important component of any comprehensive cybersecurity service. Human attackers must be confronted by human defenders.

"A lot of people think that purchasing a cybersecurity tool like EDR is kind of a silver bullet," said the Pondurance Consultant. "And while in certain ways it is, you always need to have the people on the backend who are doing the things to make the tactics, techniques, and procedures a success."

The experienced humans on the Pondurance team made a difference. Thanks to the team's handling of the situation, the hospital and other potential healthcare victims were spared from further SEO poisoning and avoided extensive damage and high-dollar ransom demands.



ABOUT PONDURANCE

Pondurance delivers world-class MDR services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate, and contain threats so your own team can focus on what matters most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals, and compliance and security strategists who provide always-on services to clients seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

For more information, call 1-888-385-1702 or email us at info@pondurance.com.

pondurance.com