# Attivo Networks Deception Platform for Forensics and Incident Response

| Company | Situation | Solution |
| --- | --- | --- |
| Regional healthcare provider<br>Eastern Seaboard<br>Mulitple hospital locations | Qakbot Malware attack on Windows XP systems | Attivo Networks Delivered fast and detailed attack analysis, preventing a full-network malware attack |

## Overview

In early 2016, a regional healthcare provider experienced a cyberattack that had the characteristics of Qakbot, an extremely aggressive form of malware popular in 2011. While Qakbot had appeared to be eradicated, it recently resurfaced with new strains and unknown signatures. Known for its polymorphic behavior, Qakbot spreads quickly through a network to steal critical data from its target. The attack started on a few end-point machines and while the organization's traditional security measures were able to detect anomalies the information security team could not action the alerts as they were not specific enough. As more alerts surfaced, they became suspicious and deployed cybersecurity devices to gain additional visibility to the legacy domain in their network. Once these devices were in operation, they raised a large number of high-level alerts, revealing a full Qakbot attack that was rapidly spreading through their network.

With several new machines becoming infected every few minutes, the team knew they needed to immediately execute an incident response plan, but needed information to remediate. They needed to know where the malware came from, how it was moving laterally through their network, what credentials the malware had compromised, and much more.

## Challenge

The nature of Qakbot's constantly-changing code made it nearly impossible to lock down and analyze. Moreover, since Qakbot had not been seen since 2011, there was very little information on common signatures or attack patterns associated with this new strain.

## Solution

The information security team had exhausted traditional measures to identify the malware but remained unable to conclusively identify the attack. Luckily, the regional healthcare provider was completing a proof of value (POV) of the Attivo Networks ThreatDefend™ platform and had deployed an engagement server on multiple VLANs in their network. Having seen the BOTsink' solution's analysis and forensic capabilities, the security team detonated Qakbot inside of the deployed Deception Platform. As the malware moved laterally within the Attivo analysis engine, the Deception Platform showed which user accounts were used to deliver and execute the payload, exactly where the files were dropped, what processes were responsible for infection and lateral movement, and what the malware's next steps would be.

With detailed attack analysis and forensics, the information security team limited the spread of Qakbot through their network, block external communication to command and control, and wipe the virus off the already infected end-point devices. Additionally, now that they knew the attacker's signatures, they were well equipped to prevent Qakbot and similar strains from penetrating their network in the future.

## ROI

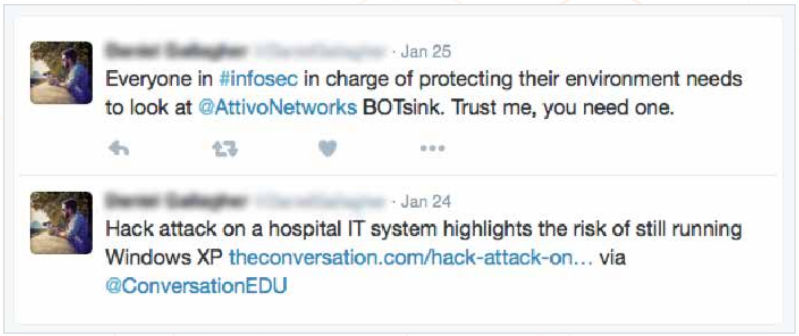
The security team spent several days trying to remediate the malware without the necessary information to do so. Infecting the BOTsink solution decoys had an immediate positive effect on their visibility into the issue. By installing the malware into the decoys, the security team was able to understand its nature, how it communicated with Command and Control, what changes it made to different Windows OSes, and more. Before the team used the BOTsink solution, the malware was able to spread, but with detailed attack forensics the BOTsink solution provided, the team was not only able to provide the AV vendor with a detailed report of the malware but more importantly, they were able to contain the outbreak and prevent further propagation.

*[The Attivo BOTsink] gave me the controlled environment for observation, allowed me to see lateral movement and the accounts that were compromised.*

Because the malware was infecting several new machines every few minutes, the ability to save days of work by using the ThreatDefend Platform was a momentous success. The organization was able to drastically reduce the number of infected machines in their network, stop data exfiltration, and, accordingly, saved significant money given that each stolen patient record costs an average of $363 for healthcare organizations.

## Outcome

When asked about the experience, the regional healthcare provider shared that they really wished that they would have had the Attivo Networks Deception solution on that VLAN. If they had, they would have saved significant time and energy in their initial assessment of the attack. They also shared that by the time their on-call Incident Response team landed, they had already identified and contained the attack, a true testament to the speed and efficiency of the Attivo Networks ThreatDefend platform.




## Attivo Products

ThreatDefend Deception and Response Platform

## About Attivo Networks

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response. www.attivonetworks.com