Pondurance Incident Response, Threat Hunting, and MDR for Retailers

PONDURANCE

CASE STUDY

THE CHALLENGE

Russian hackers, identified by the FBI, stole millions from banks, schools, and individual companies over the course of several years. The bad actors utilized sophisticated phishing attacks, where opening an email installed keylogging software onto computers with every keystroke being recorded, eventually obtaining passwords, login information, and security questions to use and gain access.

One retailer, an intended victim of the attackers, was visited by the FBI with overwhelming evidence that the retail system had been recently breached. The retailer was told, based on information the FBI had on the history of this type of breach, that the bad actors would start encrypting data within 24 to 72 hours and would eventually ask for a ransom.

OUR SOLUTION

The breached retailer immediately reached out to an IT infrastructure partner who in turn contacted Pondurance for help. Pondurance quickly met with the retailer, IT partner, legal representatives, and other stakeholders to map out an incident response plan, and Pondurance threat hunters were in the retailer's environment within hours to begin the process of thwarting the attack.

Our incident response team quietly found the breach, isolated it, and worked with the retailer to eradicate the threat, while the Pondurance managed detection and response (MDR) threat hunters continued to monitor the network. The team then blocked the bad actor's access from the system, without alerting the assailant to their presence. The bad actor who originally gained access to the system had already sold that access to other cybercriminals, and those cybercriminals immediately recognized that the access they were sold was no longer open. Then, the two groups of cybercriminals together set off on a mission to reestablish a beachhead and were met time and time again with the Pondurance threat hunters. This resulted in human cybercriminals working together to gain access and Pondurance threat hunters in a keyboard-to-keyboard combat that lasted several days. Eventually, the cybercriminals gave up, and the impending ransomware attack was stopped in its tracks.

THE RESULT

No data was lost, and no ransomware was paid.

After the incident, Pondurance provided digital forensics support and communicated with all appropriate stakeholders. The Pondurance team documented key learnings and began the onboarding of the retailer into our MDR service.

The Pondurance MDR offering integrated with our retailer's existing infrastructure and now provides 360-degree visibility across networks, endpoints, logs, and the cloud. We provide 24/7 security operations and continue to "stand ready" with closed-loop incident response, should the need arise again.

THE BENEFITS OF PONDURANCE MDR

- Stop security incidents through 24/7 detection and response
- Maximize internal resources and security investments
- Improve compliance through reporting
- Increase visibility into alerts that require action
- Rapidly accelerate security program maturity
- Lower total cost of ownership

ABOUT PONDURANCE

Pondurance delivers world-class MDR services to industries facing pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation. Our advanced platform with our experienced team of analysts continuously hunts, investigates, validates, and contains threats so your team can focus on what matters most.

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

pondurance.com