CASE STUDY

SHINING A LIGHT ON THE DEEP DARK WEB

In order to combat the rise of worming malware and ransomware attacks, ECS is monitoring the deep dark web to actively hunt and protect against sophisticated cyber threats.

SHINING A LIGHT ON THE DEEP DARK WEB

In order to combat the rise of worming malware and ransomware attacks, ECS is monitoring the deep dark web to actively hunt and protect against sophisticated cyber threats.

Recently, an ECS customer in charge of delivering healthcare solutions to senior and assisted living facilities came under threat. Using the falsified email of an executive account manager, malicious actors sent around a message designed to look like a company invoice. Attached to the message was a Word document that, when opened, injected a dangerous malware called Emotet into the recipient's system. Routinely sold between cyber criminals, this hard-to-detect malware is often used as a stepping stone to more devastating ransomware attacks. The company's entire customer base was at risk. Unbeknownst to attackers, however, ECS had been monitoring their plans on the deep dark web. Before the spear-phishing campaign threatened the company and their customers, ECS experts had already enacted a response.

DARK WEB. CLEAR VISIBILITY.

The company was exposed, and so too were their customers and industry peers. As healthcare professionals, a ransomware attack could disable critical medical services or compromise the protected heath information (PHI) and personally identifiable information (PII) stored on their servers. Fortunately, the company protected their network using ECS' Advanced Research Center (ARC) Intelligence service, which combines managed security solutions with active threat intelligence.

As part of the service, ECS maintains visibility into the underground networks where malicious actors buy, sell, and trade criminal products such as account credentials, malware, and ransomware. Over 100+ custom keyword alerts and programs called "watchers" monitor these shadowy networks, automatically scanning for and recording any information potentially indicative of a security breach. These indicators include references to a company's domain or high-value employees.

During a routine security sweep, ECS uncovered that a financially motivated group was using fake emails to target the networks of healthcare companies, likely ransoming them at a later date. Over 100 industry emails had been false, including those of the executive account manager.

(Continues page 4)

Sophisticated Malware Requires Active Intelligence

The offending malware, a well-known worming program called Emotet, is a tricky piece of code. If it identifies cybersecurity experts observing it within a virtual or sandbox environment, the malware lays dormant in an attempt to avoid detection. If the healthcare company relied solely on a security operations center (SOC) and security information and event management (SIEM) solution, they may have overlooked the threat until it was too late.

THE DANGERS OF
EMOTET

Opens a path for trojans, ransomware, and information stealers into infected systems

Uses polymorphic code to help avoid detection

Spread through Word documents and email attachments

Leveraged to sell access to infected environments for ongoing attacks

ECS sprang into action. The early detection of deep dark web monitoring enabled ECS to quickly isolate the incident, preventing the spread of dangerous malware. After securing the employee's email account, our cyber experts notified the attack's targets and monitored all correspondence to guard against any potential spear-phishing threats. ECS investigators then scoured the company's network for traces of the malicious code. None were detected, and only one customer had been exposed to the doctored message. ECS reached out to their IT team to secure any potential breach.

Through ECS' efforts, our client's system remained uncompromised. Much of the remediation process took place automatically using our built-in security orchestration and response (SOAR) tools. Afterwards, ECS analysts generated a threat intelligence report detailing the attack, its vector, and our remediation process. Our final recommendation to the company: no action needed. The threat had been contained.

- **Custom Designed Intelligence Requirements**
- **Compromised Credential Monitoring**
- **Brand Monitoring**
- **Potential Breaches**
- **Vulnerability Intelligence**
- **Threat Hunting**
- **Automated Response/Escalation**

SECURITY BEYOND THE SIEM AND SOC

In order to defend against cutting-edge malware, companies like our healthcare customer are turning to ECS to augment their SIEM and SOC with active threat intelligence. As secure as SIEM and SOC solutions can be, they are not sufficient on their own. Alert fatigue can allow threat actors can slip past perimeter security. Sophisticated malware has become more and more adept at avoiding the oversight of these systems. Effective protection requires layering different tools to create a complimentary security system.

By choosing to support their networks with deep dark web monitoring, the healthcare company was able to generate a proactive response to a potentially crippling malware threat. This choice protected not only their own systems, but the sensitive data of their partners and customers. With our ARC Intelligence deep dark web monitoring, active threat hunting, and 24/7 managed SIEM and SOC solutions, ECS will continue to ensure the company maintains the capabilities needed to guard against cyberattacks, no matter the threat or its vector.

With over 40 million indicators of compromise (IOC), 50 intelligence sources, and an advanced team of cyber investigators and analysts, ECS can solve even the most difficult threat intelligence challenges. Interested in learning more about our ARC Intelligence program?

Reach out and talk to an expert today.

ECS is a leading information technology provider delivering solutions in cloud, cybersecurity, software development, IT modernization, and science and engineering. The company's highly skilled teams approach and solve critical, complex challenges for customers across the U.S. public sector, defense, and commercial industries. ECS maintains partnerships with leading cloud and cybersecurity technology providers and holds specialized certifications in their technologies.

CONTACT OUR EXPERTS