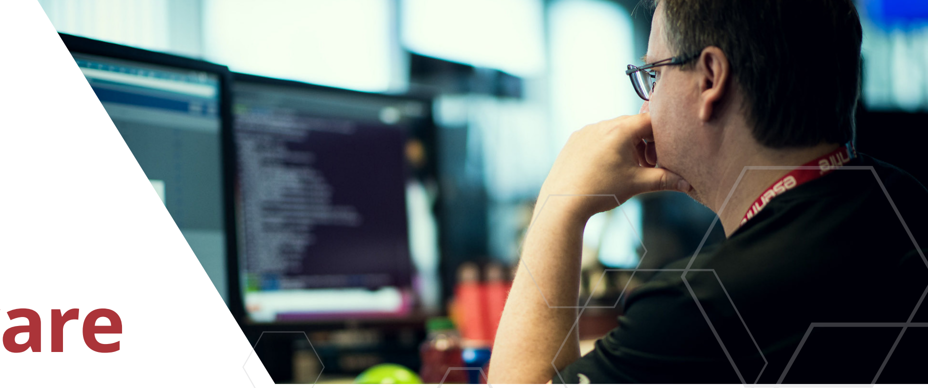

INCIDENT REPORT

Locky Ransomware Attempt

Ransomware has evolved over the last 20 years, with new strains being discovered regularly. "Locky" is a recent example of a highly effective ransomware variant. Released in 2016, Locky works by locking users out of their systems and is most commonly deployed by hackers using phishing campaigns that leverage Microsoft Word documents and malicious macros.

At the height of its distribution, a number of eSentire clients were targeted by Locky, but experienced no loss of data thanks to the detection capabilities of esNETWORK™.

Here's the full report.

Patient Zero

Our Security Operations Center (SOC) started to receive alerts that a computer on a client's network was displaying signs of post-infection viral activity. This particular user opened a malicious attachment that contained the Locky virus. SOC analysts quickly noticed file encryption on the client's network. Once a file is encrypted, it's nearly impossible to retrieve it. Even when a ransom is paid (and encryption keys are shared), there's no guarantee files will be unlocked.

Human Investigation

Upon detection, a forensic investigation was immediately launched. First, analysts applied an internal network block on the compromised host which prevented further infection, not only on the originating device, but on other devices on the network. The block also helped the client determine and isolate the infected device(s). At the same time, the malicious IP address was added to eSentire's blacklist. Within seconds, the IP propagated eSentire's ecosystem, protecting eSentire's global network of sensors from the threat. Analysts recommended that the client wipe the infected machine before putting it back online.

Ransomware Attempt Blocked

Thanks to the SOC's immediate detection, isolation and response, the client was able to control and minimize a potentially damaging breach event. In response, the client reported back that "eSentire saved the day."

Is your firm at risk?

Contact us to learn more about how eSentire Managed Detection and Response™ can help protect your network.

Uncovering threats quickly is critical to preventing widespread network damage.

At eSentire, our 24x7 team of elite security analysts live inside our technology – monitoring, hunting, and responding to threats in real time.