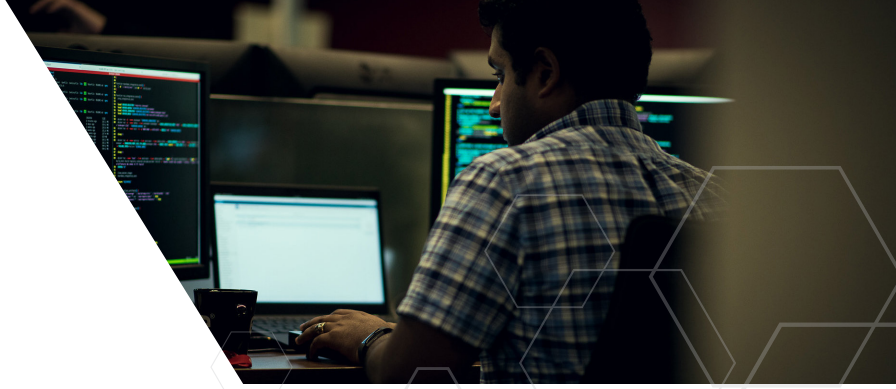
esentire®



INCIDENT REPORT

Vawtrak Banking Trojan

A proof of concept (POC) is a demonstration or trial period of a product or service which can benefit both a security provider and its potential clients.

One of these potential clients experienced the value of esNETWORK™ and esENDPOINT™ firsthand when the eSentire Security Operations Center (SOC) detected abnormal activity on an individual's computer and quickly took action to investigate.

Here's the full report.

The Initial Incident

On October 12, the SOC detected an individual logging into an inappropriate site with clear text credentials. This was a significant security concern because anyone could see the user's credentials if sniffing the traffic. The SOC alerted the POC client of the activity and worked with them to resolve the issue. The next day, the POC client requested to increase the number of endpoints they had installed.

Investigation and Response

On October 19, the additional endpoints were installed. At 11 AM the same morning, the SOC detected a malicious process on the CEO's computer. By 12:24 PM, the SOC had isolated the machine and sent the client a virus alert (Vawtrak Banking Trojan). At 12:45 PM, the client responded to the alert by calling the SOC, and an investigation was opened to gather additional details.

At 1:13 PM, the SOC provided information as to how the banking trojan infects a machine and attempts to steal banking credentials for later use. Given the attack vector of Vawtrak, the SOC indicated that the infection was most likely caused by a malicious email or attachment. At this point, the SOC removed the machine from the network and communicated to the client that a full OS restore was still required. Once completed, the SOC placed the machine back on the network and removed the isolation.

Crisis Averted

Without the additional esENDPOINT installation, the SOC may not have detected this infection, and the CEO's banking information would have continued to be exfiltrated, putting the company – and his own finances – at risk. This client put eSentire Managed Detection and Response to the test, and before the POC was even finished, they signed on to be a full-time client.

Are you at risk?

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

Sometimes it takes a real-life scenario to understand the risks associated with a cyber-attack and how prepared you are to defend against them.

At eSentire, our 24x7 team of elite security analysts live inside our technology – detecting, hunting and responding to threats around the clock.