CASE STUDIES

THE CODER

DECODING THE CRIMINAL CODER

When a highly-popular online apparel retailer started receiving dozens of calls from customers who claimed their credit card information had been compromised, company management suspected their systems had been breached. They knew they had a problem. They just didn’t know what kind of problem they had.

As is often the case, the online retailer asked their developers to conduct an internal investigation, which revealed malicious code had been injected on to their site. Upon this discovery, the retailer quickly contacted their law firm, who enlisted SpearTip to uncover the source of the problem and mitigate the breach.

Our team of operatives meticulously analyzed the retailer’s site and discovered a highly sophisticated custom attack that was used to compromise the server. Even more impressive, the code was designed in such a fashion that it would not crash the retailer’s systems and was nearly undetectable.

SpearTip discovered the breach, of Ukrainian origin, obtained root access to the retailer’s server and “back doored” its way into the company database. Once entrenched within the retailer’s server, criminals inserted code on pages requiring credit card information.

With speed and precision, the SpearTip team uncovered how the code was inserted and closed all doors it used for penetration and initiated 24/7/365 security monitoring.

During lockdown and monitoring, we encountered the Ukrainians again, as they attempted more breaches. With each attempt, the criminals were blocked and repelled in real time. The retailer’s crisis was over. Once again, SpearTip outmaneuvered the adversary.

The retailer has encountered no further breaches and employs SpearTip to handle managed security services for the company. So next time criminals attempt to breach the retailer’s server, and there will always be a next time, whether they’re Ukrainian, Chinese, Russian or any other nationality, SpearTip will be in place waiting to repel their every advance.

(As a matter of privacy and confidentiality, SpearTip never names clients when providing case studies.)

SPEARTIP®
CYBER COUNTERINTELLIGENCE
Outmaneuver Your Adversary™

1-800-236-6550

speartip.com