



Deloitte Cyber Risk Services team aids FBI in disrupting major ransomware

Deloitte's Cyber Risk Services was recently acknowledged by the [FBI](#) for its assistance in disrupting the CryptoLocker ransomware, a sophisticated tool that hackers and organized criminals use to encrypt data on personal and corporate computers, rendering their files inaccessible unless a ransom is paid.

"The leading cyber intelligence and analysis capabilities of Vigilant by Deloitte were instrumental in assisting the FBI with their investigation. This is a great example of how we are not only serving the public good, but also enhancing our profile as leaders in the increasingly important field of cyber risk and security," commented Ed Powers, principal, Deloitte & Touche LLP and U.S. leader for the Cyber Risk Services practice.

About CryptoLocker

CryptoLocker first appeared on the Internet in September 2013, primarily targeting users through spam emails sent to corporate email addresses. Once CryptoLocker encrypts the targeted files, it demands a ransom from the user within a set period of time in exchange for a decryption key. According to the FBI press release, sources estimate that as much as \$27 million in ransom payments were made to unlock the malware in just the first two months after it emerged.



Cyber Risk Services at work

Sample message generated by CryptoLocker once files have been encrypted.

The Vigilant by Deloitte cyber research team began working on the CryptoLocker issue shortly after it appeared, and helped organize the CryptoLocker Working Group – a consortium of vendors, academic institutions, and individuals who contributed to an analysis of the malware and its patterns of proliferation. In January 2014, the Deloitte team published a Threat Advisory Bulletin on CryptoLocker to help organizations understand the threat architecture, disseminate detection techniques, and warn organizations of the need for widespread data backup processes.

“We emulated the main mechanism CryptoLocker uses to evade detection and survive a takedown. This enables us to help clients detect CryptoLocker activity in their environments and thwart its ability to encrypt a user’s files,” said Lance James, head of Cyber Intelligence at Deloitte & Touche LLP.

This high-profile example is just one of the ways that Deloitte’s [Cyber Risk Services](#) professionals help organizations be more *secure, vigilant, and resilient*. Whether a client’s primary concern is protecting intellectual property, ensuring the integrity of critical applications and data, defending business operations and critical infrastructure, or managing complex compliance programs, our industry-tailored solutions can help them be more confident in strategically leveraging technology for competitive advantage, improved business performance, and more efficient service to their customers and constituents.

For more information about CryptoLocker, please send a request to cyberriskinfo@deloitte.com.

To receive ongoing threat intelligence updates, join our Security and Cyber Risk email list at <https://subscriptions.deloitte.com>.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2014 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited