CASE STUDY

CryptoLocker: a modern-day bank robbery

Financial institutions carry a particular risk when it comes to cyberthreats. Because they're entrusted with such highly sensitive data, the damages caused by a security breach can reverberate through a bank for years.

Not only are banks subject to the same high costs associated with remediation as other businesses—as well as the corresponding regulatory penalties—but banks are also liable to take a far greater and costlier hit to their credibility and brand. Therefore, banks tend to be at the forefront in network security. They invest heavily in defense technologies and employ large staffs of IT security experts to keep their customers protected—and to keep themselves out of the news.

But when a large, international bank ("ABC Bank") was breached in 2014, it was the result of a distinct type of cyberattack known as CryptoLocker. CryptoLocker is a version of ransomware that encrypts the data on a victim's system and demands payment in order to unlock the data. Ransomware works by first getting past a network's defenses and then by prompting a user to open the infected payload, which often arrives in the form of a PDF or image attachment. From there, it can quickly spread to attached devices and across a network, bringing business to a grinding halt.

How "ABC Bank" was infiltrated by CryptoLocker

ABC Bank had a solid security infrastructure consisting of 40 physical and virtual web proxies from McAfee and Blue Coat, and it had made significant investments in firewalls, web filters, antivirus systems, and other security devices. But malware can bypass such protections, often entering a network through email phishing—the source of ABC Bank's breach.

The breach:

- **1,352** emails containing CryptoLocker were sent to ABC email addresses
- **114** emails evaded existing security controls and were received by employees
- **9** employees opened the email, which downloaded the malware onto their systems

The cost:

- All **9** employees were sidelined while their machines and profiles were refreshed and rebuilt
- **6,769** network fileshares had to be restored from backup
- **11** IBM resources had to be restored, a 121-hour effort
- **9** ABC CERT resources had to be restored, a 108-hour effort
- **4** executive briefings were held over 5 days
- **45** hours of management time was expended on the matter

THE ZSCALER SOLUTION

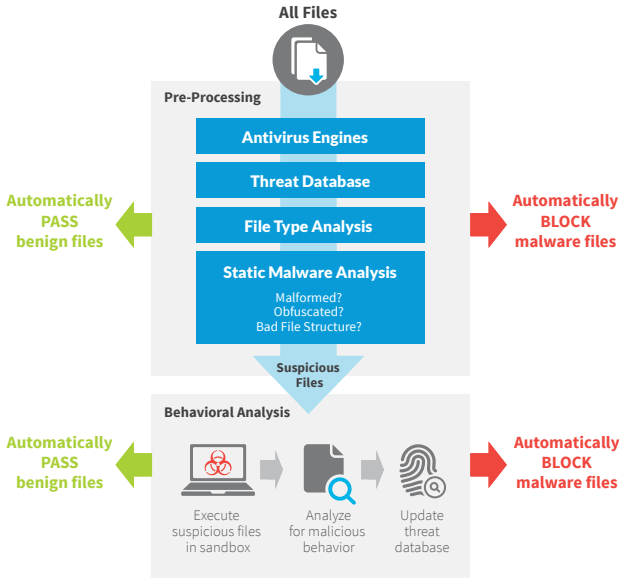
Following its breach in 2014, the bank sought to implement improvements, which could not be supported by its Blue Coat proxies. So ABC Bank selected the Zscaler cloud-based solution for its proxy services. Two days following its migration of 3,500 users to Zscaler, ABC Bank experienced another CryptoLocker run. As a result of Zscaler's advanced threat protection, not a single system was infected.

Why Zscaler can stop ransomware when other methods can't

While appliances, like firewalls and intrusion prevention systems, adequately perform individual functions, Zscaler delivers multilayered security from the cloud. It combines a broad set of security solutions into a single integrated platform. And a multilayered approach is what is needed to combat ransomware. For example, you need antivirus and sandboxing to detect and block infection, and you need an intrusion prevention system to interrupt delivery of the ransomware's payload.

With Zscaler, suspicious objects are automatically executed and monitored in a controlled sandbox, and because this occurs inline, malicious behaviors are recorded, analyzed, and blocked before they can infect an end-user's system. Many sandboxes operate in TAP mode, which means they similarly execute suspicious files, but they do so even as they pass along the potentially malicious traffic. If the sandbox detects a problem, it sends a warning. But that can be too late.

Zscaler also automatically blocks all Internet-bound traffic, including SSL, that contains unauthorized content, and locks down unauthorized ports, protocols, and cloud applications to make sure attackers can't use these channels for communications or data exfiltration. In the case of ABC Bank, Zscaler's inline scanning identified and automatically blocked attempts to communicate with botnet command and control (C&C) servers, thus rendering CryptoLocker powerless. If ransomware can't reach its C&C servers, it can't encrypt your files.



With multilayered security, Zscaler inspects all files, including encrypted files, before they have a chance to infect systems.

HOW ABC BANK WEATHERED A CRYPTOLOCKER RUN, BEFORE AND AFTER ZSCALER

BEFORE ZSCALER

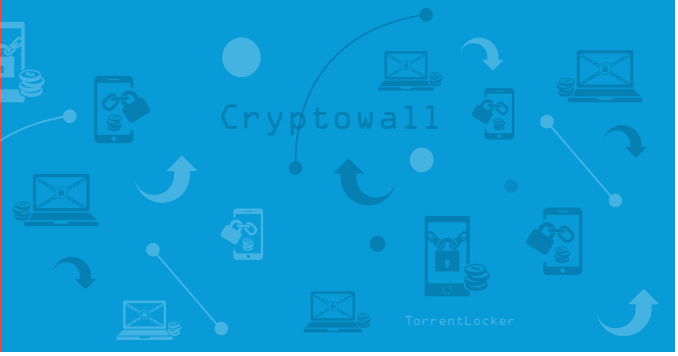
In a six-hour period:

- **1,352** emails containing CryptoLocker were sent to ABC Bank email addresses
- **114** emails evaded existing security controls and were received by employees
- **9** employees opened the email, which downloaded the malware

AFTER ZSCALER

In a six-hour period:

- **5,405** emails containing CryptoLocker were sent to ABC bank email addresses
- **169** of the emails evaded existing security controls and were received by employees
- **11** employees opened the infected email
- **0** downloads: the malware was blocked by Zscaler and downloaded onto no ABC systems



ABOUT ZSCALER

Zscaler is revolutionizing Internet security with the industry's first 100 percent cloud-based platform. Zscaler is used by more than 5,000 leading organizations, including 50 of the Fortune 500, protecting more than 15 million users worldwide against cyberattacks, while keeping organizations fully compliant with corporate and regulatory policies. With its multi-tenant, distributed platform, Zscaler effectively moves security into the Internet backbone, operating in more than 100 data centers around the world. Zscaler delivers unified, carrier-grade Internet security, next-generation firewall, web security, sandboxing/advanced persistent threat (APT) protection, data loss prevention, SSL inspection, traffic shaping, policy management, and threat intelligence—all without the need for on-premises hardware, appliances, or software. To learn more, visit us at **www.zscaler.com**.

CONTACT US

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

FOLLOW US

facebook.com/zscaler
linkedin.com/company/zscaler
twitter.com/zscaler
youtube.com/zscaler
blog.zscaler.com