# Ransomware: Overview, Prevention and Response Best Practices

## What is ransomware

**Ransomware is a type of malicious software that restricts access to an infected machine, typically via systematically encrypting files on the system's hard drive, and then demands payment of a ransom, usually in a crypto-currency (e.g., Bitcoin), in exchange for the key to decrypt the data. A very limited sampling of notable variants identified over the past three years includes:**

Cryptolocker: Trojan generating a 2048-bit RSA key pair, uploaded to a command-and-control server, and used to encrypt files using a whitelist of specific file extensions.

Cryptowall: Trojan distributed as part of a "malvertising" campaign; wherein the ads redirected to rogue websites that used browser plugin exploits to download the payload. Cryptowall 3.0 used a payload written in JavaScript as part of an email attachment, which downloads executables disguised as JPG images. It creates new instances of explorer.exe and svchost.exe to communicate with its command and control servers. When encrypting files (and file names), it also deletes volume shadow copies.

LeChiffre: Notable in that it needs to run manually on the compromised system. Attackers are automatically scanning networks in search of poorly secured remote desktops, cracking them, and after logging-in remotely, manually executing LeChiffre.

Locky: Spread through phishes containing Microsoft Word attachments. Each binary of Locky is reportedly uniquely hashed making signature-based detection is very difficult.

Maktub Locker: Spread via phishes with a .scr attachment that pretends to be a document with a Terms-Of-Service update. When the user opens the document, it really displays a fake TOS update in .rtf format, while in the background files are being encrypted.

MSIL/Samas.A: Attackers use vulnerabilities in JBoss application servers, Java-based web servers, with the publicly available tool JexBoss. If they find a vulnerability, they download an exploit to infect the server. With this foothold established, they look for attached hosts, move laterally through the network, and encrypt those systems. Additional functionality looks for backup files, stops backup processes, and deletes the backup files.

Petya: Spread by phishes targeted at HR staff containing a link to what appears to be a Dropbox account with an applicant resume; what it really contains is an executable. Once the user opens the file, the computer crashes, reboots, and then the user receives a message stating the computer is performing a disk analysis; this is when the ransomware overwrites the master boot record.

PowerWare: Ransomware exploiting PowerShell, a core utility of current Windows systems. By piggybacking on PowerShell, this ransomware attempts to avoid writing new files to disk and tries to blend in with legitimate processes. Typically delivered via a macro-enabled Microsoft Word document.

CBSL445_US_04/16

## Tips to prevent a ransomware infection

- Ensure anti-virus software is up-to-date.
- Regularly train employees to avoid phishing attempts.
- Periodically test employees through phishing campaigns, monitor the effect on response rates, and consider a formal sanctions policy (after consultation with HR and your legal counsel) for repeat offenders.
- Block emails with .js, .wsf, .zip extensions and/or macros at your email gateway level.
- If possible, disable the following commonly used attack vectors: Adobe Flash Player, Java and Silverlight.
- If you use JBoss, review the developer information on configuring and hardening it.
- Evaluate whether application whitelisting makes sense for your systems.
- Enable automated patches for your operating system and web browser.
- Robust network segmentation can often reduce the impact of ransomware.
- Enable strong identity and access management, with the use of established principles of least privilege ("need to know"), and limit local administrative rights.
- Invest in an intrusion detection system to monitor signs of malicious activity.
- Implement (and test) a data backup and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location (preferably offline). Backup copies of sensitive data should not be readily accessible from local networks.

## Tips on responding to a ransomware infection

- Infected machines should be disconnected from the network (wired and wireless) as soon as possible.
- Evaluate extent of infection, attempt to identify the type of ransomware variant, and whether the infected machine was connected to shared or unshared network drives, external hard drives, USBs, or cloud based storage. You may also want to check for a registry or file listing created by the ransomware.
- Clean the ransomware from impacted systems (a variety of free and paid disinfection tools exist for this purpose) and reinstall the operating system. Do your own due diligence on the tools you use. Beazley does not endorse products in any manner, but reputable tools can be found from, for example, BitDefender, Kaspersky Labs, Norton/Symantec, and Trend Micro.
- Proceed to restore from a reliable back-up. A well thought out back-up and restoration plan is one of the most important countermeasures against ransomware.

## Paying the ransomware: yes or no?

Without the ability to restore from a recent back-up or when faced with the prospect of operations grinding to a halt, many organizations elect to pay the ransom request, especially where the amount is relatively low. In doing so, organizations often struggle to procure the necessary amount of crypto-currency (e.g., Bitcoin), and some thought should be given by organizations on how they would go about doing so.

It important to consider, however, that paying the ransom essentially keeps the cyber-criminals' business model operational and profitable, encouraging additional attacks and further emboldening the attack groups. Indeed, once the victim organization is known to pay ransoms, other attackers (through "chatter" on the dark web) may look to launch additional attacks against the same organization. Lastly, keep in mind, that there is no guarantee of honor amongst thieves; the attackers might just take the money and run, or their decryption code might fail to work.

We recommend that before considering payment of any ransom you contact Beazley's Breach Response Services and Claims teams as defined in your Beazley Breach Response policy. You can contact them via email bbr.claims@beazley.com or telephone 866 567 8570.

KBA INSURANCE SOLUTIONS

**Chuck Maggard**
**502.736.2671**
***cmaggard@kybanks.com***

beazley

**www.beazley.com/bbr**