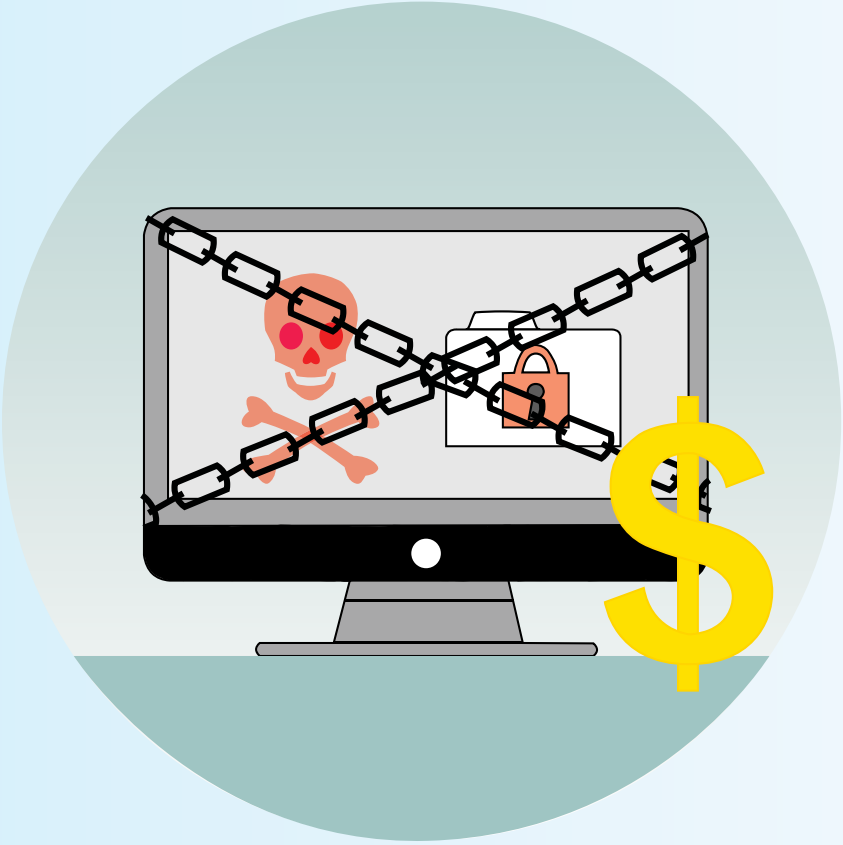
Best Practices in RansomWare Remediation

Including an Incident Report Describing CRA'S Resolution of a HELP_ DECRYPT RansomWare Incident

White Paper



Computer Resources of America

Best Practices in RansomWare Remediation

Introduction

Ransomware is malicious software that locks down files or computer systems until the victim pays the ransom. One of the modern iterations of this is cryptoviral extortion, in which the ransomware encrypts the user's files and asks for money in exchange for the decryption key. These are most often propagated via Trojans, in which users click on bad links or files and unknowingly initiate infection of their systems.

May 2017 also saw the emergence of a ransomware cryptoworm called WannaCry which could travel between computers running Windows OS without user interaction. Even more powerful versions continue to emerge, too. Analysts of the recent NotPetya ransomware said it appeared to be professionally developed and designed such that the programmers receive a cut of the ransom.

Given that it's nearly impossible to decrypt without a key, these schemes have been enormously lucrative for the criminals involved. It's estimated that the CryptoLocker ransomware attack which ran from September 2013 to May 2014 gained the perpetrators $3 million before it was taken down. The FBI estimated in 2015 that CryptoWall collected $18 million. In the last five years, these scams have been on the rise, too. Between January and September 2016, the number of ransomware incidences increased threefold. 62% of malware infections in Q1 of 2017 were ransomware attacks. Experts estimate that the damages of such attacks in 2017 will exceed $5 billion.

RansomWare Remediation Best Practices

Businesses and organizations across all industries are potential targets for RansomWare. Individuals may also find their computers infected and their files encrypted. Here we present best practices for ransomware remediation relevant to anyone affected.

Do Not Pay the Ransom

It may be tempting to pay for the decryption key for a quick solution, however there's absolutely no guarantee that the criminals will restore your files. In 2016, one in five small and mid-sized businesses that paid the ransom did not receive their data back.

There is also the risk that any provided decryption resources could introduce additional malware. Sharing of any financial or personal information could enable the perpetration of addition fraud, too.

Best Practices in RansomWare Remediation

Isolate the Ranomware Infection

It's vital to work quickly and communicate the issue to anyone whose computer or profile may be infected. Then:

- **Take the infected computer off the network.** Shut down the wireless capabilities and/or remove the ethernet cable.
- **Inform anyone using a connected computer or files to close files and disconnect.** This will permit you to further isolate yet unknown infections and prevent further spread.
- **Take read-only snapshots of the data.** This not only protects undamaged data, it preserves the crime scene.
- **Perform a deep scan for infected files and/or profiles.** Examination of audit logs will help you trace the source files and profiles, too.

Assess the Source and Extent of Infection

Your scan results will certainly show you the areas where you need to clean up and restore files. They also hold the key to preventing future ransomware infections, so it's important to analyze:

- **Infection source.** When and where did initial infection occur?
- **Infection pattern.** Did the infection stay relatively confined or did it have a more extensive reach?
- **Unexpected system or file changes.** Were there any other changes to the system during the attack? Were files or filenames altered? Examination of audit logs will help you trace the source files and profiles, too.

Recover the Data

Using the information from your analysis of the system scans, build a recovery plan. Then, choose an ideal restore point and recover the data from an external backup. Do not be tempted to roll back to a restore point on the same servers since they might be infected, too.

Protect Your System From Future Ransomware Attacks

It's important to address any system weaknesses once you know the cause of the ransomware attack. Some good general practices that will help protect you include:

- Keeping all software up to date, especially antivirus software.
- Implementing security tools that create recovery points if they detect triggering of ransomware.
- Maintaining data backups offsite, taking advantage of cloud storage where applicable.
- Disabling macros in documents received via email.
- Never opening unsolicited attachments, even from known senders.
- Regularly hosting staff training sessions and discussing current trends in cyberattacks, including ransomware.

Incident Report: Isolation and Remediation of the HELP_ DECRYPT RansomWare Virus

In April 2015, CRA investigated and quickly resolved an incident involving the HELP_DECRYPT ransomware virus. This component executes the Cryptowall virus, which scans for files with extensions such .doc, .docx, .xls, .ppt, and .jpg and encrypts them. It then adds files help_decrypt.txt, help_decrypt.html, help_decrypt.png and help_decrypt.url to the folder. Once this is complete, the HELP_DECRYPT window opens and presents the user with the payment process for restoring their files.

Here we present the root cause analysis of the incident, including a timeline of our response to the infection.

Best Practices in RansomWare Remediation

Event Summary

On Wednesday 8/19/15, CRA received notification that a user had lost access to some files.

- We investigated and noted infection by the CryptoWall HELP_DECRYPT ransomware virus.
- To isolate the issue, we immediately notified all users to close open files. We requested that they also log out of all Citrix sessions and workstations and stay off until further notice.
- We initiated intensive searching and antivirus scanning of all servers, including Citrix servers, and found the following:
    - ServerName1: Fifteen affected folders (in the public share folder) and one infected Citrix profile.
    - ServerName2: one entirely infected folder.
    - ServerName3: one infected Citrix profile.

Timeline

Our investigation revealed that the infection occurred at 1:54pm. The remainder of the timeline proceeded as follows:

2:35 PM – Received notification from User1 that certain files could not be accessed.

2:37 PM – CRA started assessing the extent of the problem/infection.

2:40 PM – Received a call from User2 that the booking department files are infected and cannot be accessed.

2:45 PM – Started a full scan of ALL servers and network shares.

2:47 PM – Requested to User1 to instruct all users to save and close all opened files, log out of Citrix and their workstations, and stay logged off until further notice.

3:20 PM – Completed searches and scans, identifying all infected files and folders.

3:30 PM – Mounted a restore point from 1PM on 8/19 on our backup server. Then moved all infected folders/shares to a secure location. Began restoring all infected folders/shares.

5:30 PM – Mounted a restore point from 1PM on 8/19 on our backup server. Then moved all infected folders/shares to a secure location. Began restoring all affected folders/files.

6:15 PM – Notified User1 of file restoration progress and asked her to verify access to a few folders/files.

6:19 PM – Notified User1 via email that the restore was complete.

Findings and Root Cause

Based on our investigation, the virus originated from one user's folder in the form of a PDF attachment. A hidden executable in the PDF encrypted all files and shares the user accessed from the time of infection.

Recommendations and Corrective Actions

- Users should **never open files from unknown sources** or click on unsolicited attachments. They should consult CRA if there's any doubt about file integrity.
- A **software restriction policy** to block CryptoWall virus has been created and is currently being tested.
- Look into **external filtering options** prior to reaching Opus Fortinet Firewall.

Innovative Security Solutions by CRA

How does your organization rate when it comes to security? Are you prepared for a cyberattack?
Whether you need a security check-up or implementation of all new security solutions, CRA is ready to help. Let us help you protect your assets so you can focus your personnel and resources on your business goals. For a free evaluation, visit www.consultcra.com and submit your contact information. To speak to our consultants directly, please call 212-376-4040 or email sales@consultcra.com.

CRA Transform IT
Computer Resources of America

Corporate Headquarters

64 West 48th Street, New York, NY 10036 – 212-376-4040 – www.consultcra.com – sales@consultcra.com