News > Security > Organizational Ransomware Attacks

# Organizational Ransomware Attacks

2016-12-02 - Burner EOAS - Security

Ransomware can be localized to target individual users or systems, or expanded to larger groups and even organizationally focused with the intent of paralyzing an organization.  Recently, there have been a number of ransomware attacks that exploit unpatched vulnerabilities on servers connected to the internet, resulting in an attack against the **entire organization**,impacting all operations; in higher education this affected the ability to teach and do research. Some examples include the University of Calgary, San Francisco Municipal Transportation Agency, Hollywood Presbyterian Medical Centre, and Carleton University.

Below are some similarities and recommended solutions we have been able to draw between these recent organizational attacks:

1. *Vulnerabilities are exploited to gain an initial foothold*

Solution:

We strongly encourage everyone to **patch** all networked systems; focus first on all internet facing servers, paying special attention to java-based servers as they are frequently targeted. If you require assistance in patching your servers, please contact your department’s IT Administrator. If you are unable to patch your server or get help from your department, please contact security@ubc.ca.

2. *Keyloggers are installed to steal administrative credentials, which are used to map network shares and deploy ransomware*

Solution:

For critical accounts that have control over multiple servers/systems (e.g. root, Administrator, etc.), use a privileged account manager that checks in and out the account, changing passwords for each usage.  Privileged accounts should have limited access to only those who need it and used only when necessary.  These accounts must not be used for checking email or web browsing or any other user related activity.

Anti-malware software must also be installed and kept up-to-date on all operating systems, such as Windows, Mac, and Linux.

3. *Ransomware encrypts critical files needed for research, teaching or administrative activities.*

Solution:

Use network file shares that are backed up regularly (e.g Home Drive, Teamshare, or Workspace) for the storage of critical files.  Keep backups off-line and accessible only via specific privileged accounts that have restricted usage.

In addition to the above recommendations, we strongly encourage everyone to review and ensure they have the latest patches for their servers.