RANSOMWARE: CURRENT STRAINS, ATTACK VECTORS AND PROTECTION

By Steve Lawn, Senior Consultant at HALOCK

Staying ahead of security threats is no easy task. One threat that should definitely be on your radar is ransomware. From hospital heists to attacks on schools and other businesses, ransomware is costly and is projected to be one of the biggest threats in 2016. According to CNN, the FBI reported that it received 2,453 complaints about ransomware hold-ups last year, costing the victims more than $24 million dollars. And there's little the FBI can do about it, and so victims pay.

Ransomware is a variant of malware that encrypts files, mapped drives, and/or the Master Boot records. Typically, data is not exfiltrated off of the network or moved from the device, instead files are encrypted, making them inaccessible to anyone without the decryption key.

Ransomware is projected to be one of the biggest threats in 2016.

After the ransomware has infected a machine, the only way to recover from an attack is by restoring a validated backup or paying the ransom to obtain the decryption keys and process. Unless you pay for the decryption key held by the attackers, the ransomware developers (thieves) will destroy the private encryption key, making it impossible to recover your files.

Multiple forms of ransomware, as well as new variants, are continually being created. Some ransomware making the news, and that we have seen, include:

- **Locky** which encrypts your files just like all others and also changes the file extension to ".locky." Locky is an attachment-based attack.
- **SAMSAM** or Samas spreads through unpatched vulnerabilities in JBoss application servers.
- **TeslaCrypt** is a server compromise of WordPress impacting .js files hosted on websites.
- **Cryptowall** encrypts files on your PC and directs you to a webpage with instructions on how to unlock the files.

Other ransomware variants include:

- **Crowti.A** encrypts files on your PC and directs you to a webpage with instructions on how to unlock the files.
- **Tescrypt.A** is similar to Cryptowall. The threat is an HTML message that asks you to pay a ransom to regain access to the files encrypted by "Tescrypt."
- **Nymaim.f** can lock your PC and stop you from accessing your files. It shows you a "lock screen" that asks the victim to pay or provide sensitive information in order to gain access to the device again.
- **Reveton.V** locks your PC and displays a full-screen message, or "lock screen," and pretends to be from the FBI or a national police force and tries to scare the victim into paying a fine to unlock the PC.

Vectors of a Ransomware Attack

The top four vectors for initial infection of ransomware are email attachments, embedded hyperlinks within emails, internet browsing-type attacks, and web application vulnerabilities. For example,

- **Weaponized e-mail attachments** are carefully crafted "spear-phishing" emails with weaponized Word and/or Excel documents. Emails use highly persuasive subject lines and email body text which trick users into opening malicious attachments.

- **Embedded hyperlinks within e-mails** is the malicious practice of using email messages to lure the victim into following the hyperlink to an infected site.

- **Internet browsing (drive-by) attacks** occur when a user visits an unknown malicious web page, and the web server delivers a HTML document with malicious content that infects the user's device.

- **Web application vulnerabilities** currently have two known variations. The first exploits JBoss using an open-source exploit tool called JexBoss. The second attack involves WordPress and Joomla environments.

Ransomware Protection

With ransomware everywhere, how do you protect yourself and your organization against this threat? Since there's no silver bullet to protect against ransomware, a combination of end user security awareness training, proper implementation of security products, and incident response readiness can generally help defend against ransomware and malware attacks.

- **Security awareness training** is an ongoing process, not a one-time event. A comprehensive campaign of training classes, detailed e-mails about top threats, and printed literature strategically placed around the office should be developed and deployed on a regular basis.

- **Incident Response Readiness** is an overall program that organizations should adopt with the goal of hardening systems, creating incident response plans and gaining the skills necessary to respond appropriately if and when an incident occurs. Be sure your incident response plan incorporates first responder training as well as incident manager training.

- **A "Defense in Depth" strategy** should be strongly considered when deciding on security software and architecture. As illustrated by the different types of ransomware and the multiple methods for infiltration, there is no one control that will protect systems. A multi-layered approach provides a variety of protection to help stop infections. Consider the following:

  End-point Defense. Bolster your endpoints with anti-virus programs, end-point process monitoring capabilities, malware specific detection and removal tools. Ensure you have backups of critical assets, that you regularly test the restoration of the backups, and keep the backups offline when not in use. Do not allow users to map drive letters and replace it with UNC network shares. Ransomware will typically follow mapped drives but not UNC shares (for now, anyway). Finally, do not allow administrative shares to be created from servers or workstations beyond what is required for business functionality. This allows an attacker an easy mechanism for infecting a network from one compromised host.

  Email Defense can be enhanced through a security e-mail gateway. A security email gateway identifies targeted attacks that are occurring through email to users and provides information on the malicious content within the emails. This will drastically reduce the amount of Spam, Phishing, and weaponized emails, attachments, and URLs users are exposed to and also provide email encryption and data loss prevention capabilities.

  Network Defense using a next generation firewall, identifies applications that are operating on the infrastructure (internally or externally) and associates a risk rating based on the behavioral characteristics of the application. Additionally, be sure to restrict outbound access origination from servers at the firewall unless required for business or approved functionality. Malware generally relies on outside contact with a command control server to report infiltration success and receive the next set of instructions to complete a mission.

  Application Defense using a Web Application Firewall (WAF), identifies and acts upon dangers maliciously woven into innocent-looking website traffic and/or traffic that slips through traditional defenses. This includes blocking technical and business logic attacks like SQL injection, cross-site scripting and remote file inclusion. Business logic attacks include site scraping and comment spam, botnets and DDoS attacks, and preventing account takeover attempts in real-time, before fraudulent transactions can be performed. Using a WAF will limit the exposure to front-door exploits that allow ransomware such as TeslaCrypt and SAMSAM to infect your web servers.

  Advanced Malware Threat Detection. An advanced threat detection and prevention solution will detect, alert, and block malware and suspicious activities flowing into and out of your environment. These types of solutions help identify unknown (zero-day) threats that a traditional Intrusion Detection and Prevention (IDP/IDS) system may miss by analyzing all payloads that traverse the internet ingress/egress route.

It's important to note that the best chance to combat ransomware is to have the right protection in place before an attack. Once attacked, little can be done, particularly if back-ups are not segregated from the rest of your network.

About HALOCK
Founded on the philosophy of "Purpose Driven Security," HALOCK Security Labs is a new breed of information security professional services firms combining strategic security consulting and compliance with technical security architecture and implementation. HALOCK's services include Governance & Compliance, Penetration Testing, Technical Assessments, Workforce Staffing, Incident Response, and Compromise Assessments.