SRG Security Resource Group Inc.

Professional Consultants committed to excellence

The three “R’s” of Ransomware

This article will provide advice to our customers on some of the most common points of awareness in dealing with the increasing frequency of Ransomware threats. With predictions of Ransomware to reach new levels of infections for 2016, your organization should be prepared in the event of an outbreak. These predictions are based on the “reported” known attacks; keeping in mind many organizations do not publically disclose an infection. With this increase in attacks and Ransomware variants changing almost weekly, having up-to-date Antivirus solutions may not simply be enough to fend off zero-day exploits and attacks. Below are some tips to aid in protecting your environment from blackmail attempts.

1. **Reduce** – Reduce the potential of attack vectors by implementing various practices such as user awareness training, system hardening/patching and strict Group Policy Object designs to name a few.
2. **Re-Image** – Re-Image any system that falls victim to a successful Ransomware attack. Ransomware variants are ever evolving to be more persistent that its predecessors. The old adage remains true, “Never trust a compromised system”.
3. **Recover** – Recovering from an infection or outbreak will take the most time. Whether this is due to a file recovery solution or the simple feeling of being violated, having sound recovery solutions in place will lessen the impact.

Proactive Approaches

- Ensure that an Incident Response plan is in place in the event of a successful attack. Backup solutions not only need to be in place, but regularly tested for effectiveness and resiliency. This includes having a single management point, whether an individual or team, to manage and oversee the outbreak and remediation efforts. The later reduces the risk of miscommunications between several individuals potentially missing pertinent information as well as an expedited recovery.
- The two most notable attack vectors are users being targeted by email phishing (emails that appear to be from legitimate sources) or visiting potentially harmful websites. Continued user awareness education (more than annually) is key in reducing the potential of a network wide outbreak, or just one system. “If it looks suspicious or unsolicited, second guess it”.

- Important data files should never be stored on the local machine where backups are not possible to be made. Files on a Network Share can easily be restored from a backup solution, and thus avoiding a major data loss as well as not giving in to ransom demands. Equally important, limit write access to critical files to only those with a business need — read access permits many business functions yet with far less risk
- Limit the amount of users that require Local Administrative rights where possible. If no other solution(s) is available where Local Administrative rights are required, users should be made aware to limit opening of documents or web browsing while these elevated rights are effective.
- Reducing attack vectors in known popular applications such as Flash, Silverlight, Office and browsers by patching systems as soon as possible. This closes those "holes" attackers use to gain a stranglehold in the environment.

Reactive Approaches

- The individual or team assigned to the outbreak should determine the "ground zero" system. This can be done by reviewing any affected shares and which user had last made modifications and have that system removed from the network immediately. It is also recommended to review any other systems that would have access to these affected shares for signs of Ransomware to reduce the potential of re-infection.
- Determine the attack vector and Ransomware variant if possible and implement necessary blocks of IP addresses, Web and Email Domains, Filenames, etc. at Perimeter and Internal Infrastructure Defenses. This includes a review of email logs of identified infected systems to determine if any malicious emails have been sent to infect other systems.
- Performing a search on all network shares for the infected files to determine what other systems may have been infected with access to those shared resources.
- Once the system(s) have been identified and removed from the network, they should be re-imaged to ensure that no chance of a re-infection can occur.
- Network shares that have been compromised can now be restored from a last known good backup with a reduced concern of re-infection.
- Affirm or re-affirm user awareness with those systems involved. While "ignorance is bliss", "not being aware is a crime" and thus increases the potential for another attack.