EGNYTE

Ransomware Checklist

Ransomware is a complex attack, and requires education for both IT professionals and end users. Each with a responsibility for protecting their company's sensitive and valuable data.

Ransomware kill chain

The term "kill chain" is used in the Cybersecurity community to describe the steps in a cyber-attack. It is helpful to understand these steps so that they can be individually addressed. Stopping ransomware at any point on this chain can completely disable or at least limit the damage. Ransomware typically goes through the following stages of a kill chain in order to complete an attack:

1. Initial vector infection: Typically, a small dropper file is introduced to an endpoint machine via a malicious website or email attachment.
2. The ransomware code itself is downloaded, installed, hidden, and executed on an endpoint machine.
3. The ransomware code does a quick inventory (directory structure, registry, etc.) of the target machine.
4. If the machine appears to be a likely target, the ransomware code reaches out to a Command & Control server on the Internet for encryption keys to be used.
5. The software waits for a period of inactivity, and then begins quietly encrypting accessible files on the local drive and any network drives accessible to the user.
6. The software uses SMB or Domain Controller attacks to infect other machines, to continue the process.

Best practices that will help you to protect your environment from a ransomware attack

IT/Cybersecurity staff:

- □ Lock down endpoints and prohibit usage of user installed software, or at least monitor it. Don’t allow PowerShell use by end users on Windows endpoints. (Blocks “2”)
- □ Keep up with Operating System patches and updates on end user machines. Make sure malware signatures are up to date in Endpoint Detection and Response (EDR) and Antivirus (AV). Also maintain currency with firewall rules, intrusion detection systems, and email protection systems. (Blocks “2”)
- □ Consider an automated Sandboxing tool or use VirusTotal to detonate possible malware before allowing it to be downloaded by users. (Blocks “2”)
- □ Install a secondary keyboard mapping for Cyrillic keyboards on endpoints and servers. To avoid infecting themselves, many ransomware programmers have their code check for Cyrillic keyboards and will not execute on a machine with those keyboards installed. (Blocks “3”)
- □ Use a Secure DNS provider to block the connections out to known Command & Control Servers on the Internet. Default DNS services provided by your Internet Service Provider (ISP) are typically insecure. (Blocks “4”)
- □ Maintain multigenerational backups of all endpoint and server data and test restoration of backup data regularly. (Mitigates “5”)
- □ Keep up with Operating System patches and updates on file servers and Domain Controllers. Use network segmentation or micro-segmentation to limit network domain access, and use Group Access Policies to limit server access. This helps to isolate an attack to one user.
- □ Continuously collect, monitor, and analyze logs to detect active attacks as quickly as possible. Have a quarantine process in place to isolate infected machines and servers quickly. Baseline typical network and server behavior to be able to spot unusual activity.
- □ Understand and manage risk introduced into your systems by third parties including partners, suppliers, user owned devices (BYOD), and customers.

Best practices to share with your end users so they can help protect against ransomware

End User:

□ Make sure your computer is kept up to date, and comply with restrictions established by your IT staff.

□ Don't open unexpected attachments. It's often safer to upload a document or spreadsheet to a file storage system and open it in your browser instead of on your desktop.

□ Don't click on suspicious links in emails. If you get an email from a known entity (your bank, for example), type the URL into the browser yourself. Don't trust the link in the email.

□ Forward any suspicious email to the address designated by your IT team to be checked.

□ Don't use your work computer for personal Internet browsing. Even legitimate websites can sometimes be compromised by hackers to send malware to your computer.

□ If you get a warning asking you to install browser add-ons or notifications, do not select it.

□ If a ransomware screen pops up, or you notice unusual changes in files in your computer, or it slows down, you may have an active Ransomware infection. You need to act quickly. Immediately disconnect the ethernet cable or disconnect from WiFi. Then immediately power down your computer. Don't follow the usual software shut-down process- use the power switch. Do not restart your computer, but take it to your IT staff to remediate instead.

Contact Us

+1-650-968-4018

1350 W. Middlefield Rd.
Mountain View, CA 94043, USA

www.egnyte.com