10 STEPS TO MITIGATE WANNACRY DAMAGE

Code Red:
You've Been Infected

On Friday, May 12, 2017 the WannaCry ransomware was unleashed, infecting more than 300,000 computers in 150 countries and demanding ransom payments in bitcoin in 28 languages. WannaCry is a ransomware program targeting Microsoft Windows operating systems using multiple methods, including phishing emails and unpatched systems as a computer worm. Because of its success infiltrating systems, the software is already inspiring imitators, meaning we're all at risk.

The guidance regularly touted is to simply update your operating system with Microsoft's patch, but that's only the beginning of the story.

Infrascale™

WHAT SHOULD YOU DO IF YOU YOU'RE INFECTED WITH WANNACRY?

How can you begin to mitigate the damage and limit the downtime right now—as soon as the first ransomware symptom rears its ugly head? How do you avoid paying the ransom? What do you do after the attack to restore your data and mission-critical systems?

MINIMIZING THE DAMAGE

Steps to Take During a WannaCry Attack

01 Deploy the Microsoft Security Update Immediately

In March, Microsoft released a security update which addresses the vulnerability that was exploited by the WannaCry ransomware. Those who have Windows Update enabled are protected against attacks on this vulnerability. For those organizations who have not yet applied the security update, download Microsoft Security Bulletin MS17-010 immediately.

02 Set the BIOS Clock Back

Resetting the BIOS clock back to a time before the ransom expiration window might help delay the expiration deadline. But the programmers are getting smarter, so this tactic may only work with certain strains of ransomware.

03 Patching and Plug-ins

Keeping applications like Adobe Reader, Java, and other plugins up to date greatly reduces security vulnerabilities that may bypass your antimalware defenses. Ad and pop-up blockers also greatly reduce user error, stopping users from inadvertently clicking fake dialogs that download ransomware.

04 Download Latest AV/AS Signature

Even though you've just been infected by ransomware, it's still a best practice to update your antivirus software to ensure you don't get re-infected down the road. To maintain the highest level of protection, configure your antivirus software to check for updates as often as it will allow. Keeping the signatures up to date doesn't guarantee a new virus will never slip through, but it does make it far less likely.

05 Educate your Employees

It takes one bad decision by a user to unleash the spread of a costly ransomware attack. Ransomware is often let in through a phishing email. Prevention isn't possible 100% of the time, but in many cases attacks can be stopped if users are educated about what to look for. If attacked, ensure that all employees are aware that a ransomware attack is in process and direct them to the procedures needed to protect their data and provide a time frame for restoration of affected systems.

Infrascale™

RESTORING THE DATA

Steps to Take After You've Been Infected by Ransomware

01 Use System Restore & Decryption Tools

If system restore was enabled on your windows machine, you should attempt to restore to a known clean state. Also, see if your anti-virus solution offers free decryption tools that can help decrypt files.

02 Identify a Safe Point In Time

Determine the point in time when ransomware infected your data, and restore the most recent files/VMs from a clean backup. Determining the date of infection and restoring clean copies of infected files with traditional backup solutions is cumbersome and time consuming; with disaster recovery as a service (DRaaS), this entire process is far easier and faster.

03 Test Boot Your Virtual Machines (VMs)

It's quite possible your backups and VMs may have also been corrupted during the attack. With DRaaS, admins can more quickly browse a disk image to quickly determine if the files contained in the image have been encrypted. Generally speaking, if the VM boots up, you have a clean ransomware-free image; if it doesn't, the VM is probably infected.

04 Restore Infected Systems

If a production database or mission-critical application has been infected, leverage a DRaaS solution to spin up an image or virtual machine in minutes-- ensuring your users stay productive.

05 Failback Workloads & Breathe

If you're using a DRaaS solution, the failback process is critical. You must consider how to move data back to production as quickly as possible. During the actual failback, data is re-synchronized — halting I/O and application activity once again — before operations are restored to the original location.

FINAL NOTE:

It pays to keep up with ransomware developments. Some ransomware strains have been cracked, but these are limited successes. Ransomware, like all malware, will continue to evolve. The more informed you are, the better equipped you are to protect your data and systems. A comprehensive backup and disaster recovery solution is your number one defense against ransomware. Be sure to practice restore processes and know that your actual data can easily be retrieved.

LEARN MORE:

Read the FBI's outlook and recommendations on ransomware prevention — featuring detailed reports tailored to the separate interests of CEOs and CISOs.

10 STEPS TO MITIGATE WANNACRY DAMAGE

Infrascale™

About Infrascale

Infrascale provides the most powerful disaster recovery and cloud backup solutions in the world. Founded in 2006, the company aims to give every organization the ability to recover from a disaster- quickly, easily and affordably. Combining intelligent software with the power of the cloud, Infrascale cracks the disaster recovery cost barrier by removing the complexity and cost of standby infrastructure to restore operations in minutes with a push of a button. Infrascale equips businesses with the confidence to handle the unexpected by providing less downtime, greater security, and always-on availability.

Gartner VISIONARY Disaster Recovery as a Service (DRaaS)

Gartner 2015 CoolVendor

CRN COOLEST CLOUDS STORAGE VENDOR 2016

LOGO HERE

About Your Company

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec quam felis, ultricies nec, pellentesque eu, pretium quis, sem. Nulla consequat massa quis enim. Donec pede justo, fringilla vel, aliquet nec, vulputate eget, arcu. In enim justo, rhoncus ut, imperdiet a, venenatis vitae, justo. Donec quam felis, ultricies nec, pellentesque eu, pretium quis, sem. onec quam felis, ultricies nec, pellentesque eu, pretium quis, sem. Nulla consequat massa quis enim. Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

Your Company Name, Inc.
8000 Aenean commodo, Suite 100
Los Angeles, CA 90066
Phone: 888.888.8888
Email: sales@yourcompanyname.com
Web: www.yourcompany.com