BEYOND WANNACRY: How Prepared Are You?

Organizations were **safe** from WannaCry – *but only if* they followed security best practices that were matured a decade ago, when worm outbreaks like this were more frequent.

So why did WannaCry cause **so much chaos,** including disabling hospital networks and automobile production facilities?

HOW QUICKLY MUST ORGANIZATIONS RESPOND TO THREATS?

Let's put WannaCry in **historical perspective.** Consider the amount of time in prior events from when a patch was made available and when the outbreak/spread occurred.

While many organizations have patched their systems and software, some either **did not patch** or are running unsupported Operating System versions.

What else do the SHADOW BROKERS have in store?

The **Shadow Brokers** are a criminal group who have leaked several hacking tools that were stolen from the U.S. National Security Agency. The WannaCry malware was based on code that the Shadow Brokers leaked to the Internet. What upcoming threats is the group proclaiming?

"Data Dump of the Month" Service
A subscription-based model where paying members can access unauthorized data such as:

- Web browser, router, handset exploits and tools
- Ops disks, including exploits for Windows 10
- Network data from SWIFT providers and Central banks, as well as from nuke and missile programs

4 THINGS YOU SHOULD BE DOING NOW

Recommendations for Good Security Hygiene

1 PATCH ON TIME, EVERY TIME

Keep all systems and software updated with the latest patches. Systems that were affected by WannaCry were either **not patched** or are running unsupported Operating System versions.

2 SEGMENT YOUR NETWORK

Segment and isolate systems on your network in order to **limit the impact** of a successful compromise. This is particularly important for legacy systems that cannot be patched.

3 ALWAYS MAINTAIN BACKUPS

If you do become victim to Ransomware or other attacks, **backups can be your lifeline** to help maintain business operations and minimize the impact of attacks.

4 PROTECT FROM EXTERNAL AND INTERNAL THREATS

The Internet is a hacker highway, requiring **strong, integrated protection and policy enforcement** – network access control, monitoring, threat detection, and other essential security controls that must work in concert with each other.