To: All Distributors, Sales Managers, Customers

From: Wedge WeService Support Center

Subject: WedgeAMB™ - Protection Against WannaCry Ransomware

WedgeAMB Immediately Protects Your Network Against WannaCry Ransomware and Other Malware

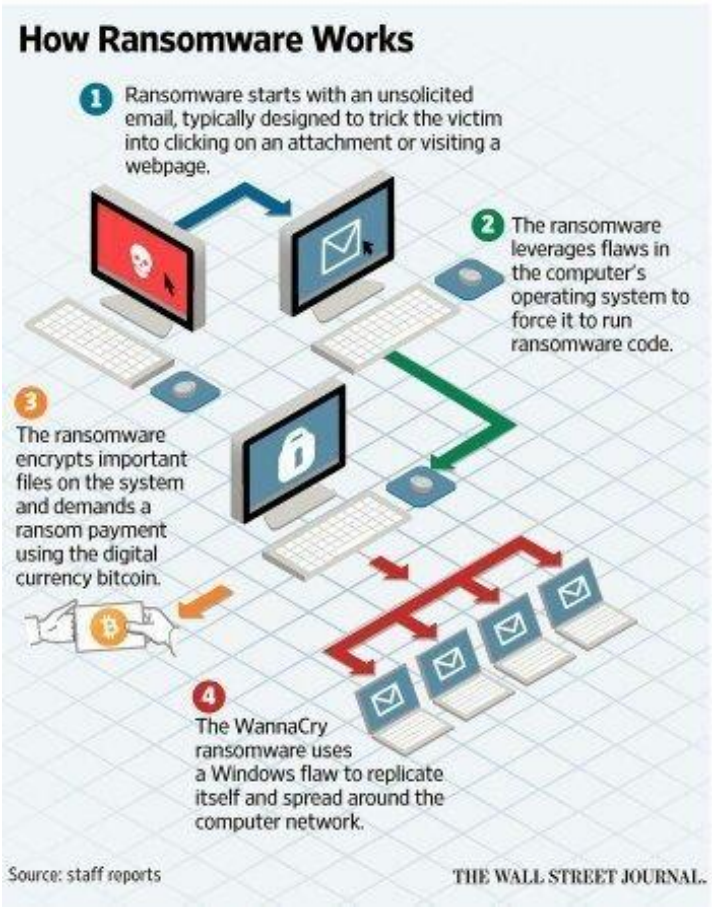
The WannaCry ransomware family of malware was unleashed across the globe last week in more than 150 countries; impacting more than 200,000 victims, as of Sunday, May 14th according to Rob Wainwright, the head of the European Union's law enforcement agency Europol. While security vendors globally have now identified and issued signature updates to protect against WannaCry, WedgeAMB's multi-layered security has proven instrumental in blocking this multi-vectored attack, without requiring software updates. WedgeAMB is uniquely positioned to detect and block future variants of WannaCry and other ransomware families using a combination of Wedge's patented real-time deep content inspection engine, working in concert with four different malware detection technologies, to block both known and new, never encountered before malware, in real-time.

Infection Vector

The attack used a multi-vectored approach consisting of the WannaCry/Wcry, a relatively new ransomware family that was discovered in April. In some cases, the exploit was delivered via a phishing attack and in other cases it was delivered using a worm that exploits a vulnerability in the Windows SMB 1.0 Server [CVE-2017-0144] which was identified in March. In the phishing scenario, the event begins when one end user in an enterprise's network clicks on a link which triggers the download of a dynamic link library (DLL) file which contains the WannaCry ransomware.

The infographic below provides a summary illustration as published by the Wall Street Journal.

In the SMB scenario, the exploit was delivered using a worm which operates without requiring end user activation. As a new version of malware, WannaCry evaded the detection by thousands of conventional signature and heuristic-based anti-virus and firewall security systems.



Wedge Solution

WedgeAMB also uses signature and heuristic-based AV technology, but, using its patented Deep Content Inspection Technology (USPTO 7,630,379) where network traffic is assembled in real-time into its constituting objects, WedgeAMB also analyzes executable content in using artificial intelligence anti-malware. WedgeAMB's AI-AM technology immediately recognized that the DLL file contained malware and blocked the file, in real-time, from being downloaded.

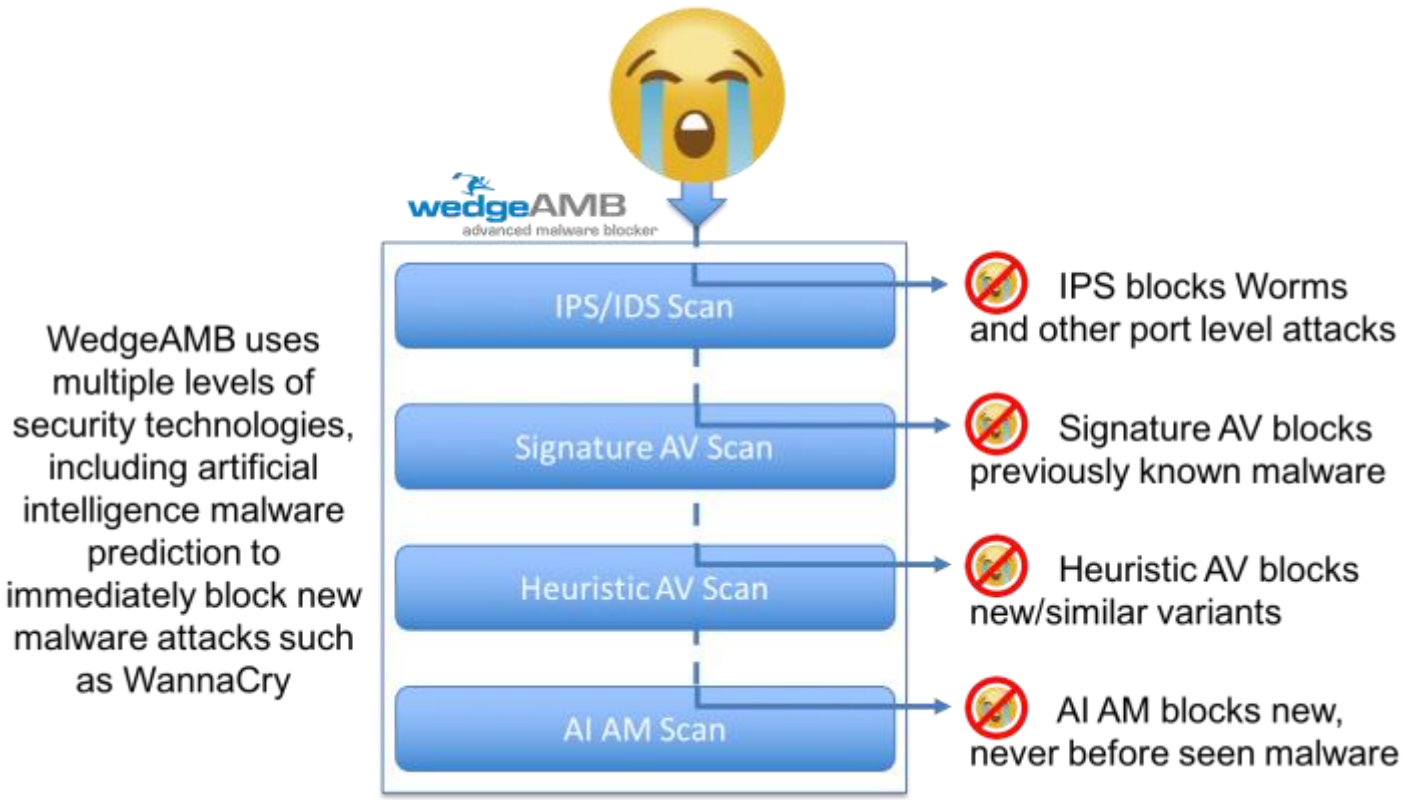
Even before such a threat is detected by the AI-AM technology, WedgeAMB scans packets as they first enter the system. In the SMB worm based scenario, the WedgeAMB Packet Inspection function blocked the worm that would have exploited CVE-2017-0144, thus eliminating the potential for dissemination of the ransomware. As such, WedgeAMB's real-time, orchestrated malware threat scanners blocked both vectors of the WannaCry cyberattack, in real-time – the "worm" or the propagation vector using its packet inspection scanner, and the worm or phishing "payload", the infecting vector, using its AI-AM deep content inspection scanner with AI-AM.

Defending Against The Next Ransomware Attack

The recent WannaCry attack is just one more example of the increasing frequency and intensity of new cyber threats. The following steps are recommended to mitigate future ransomware and malware attacks in general.

- Ensure all conventional anti-virus software is up to date. If possible, deploy new AI based AV endpoint protection software, such as Cylance PROTECT®, which does not rely on signature updates to detect and block new malware.
- Implement a data backup and recovery plan which includes storage of critical data in remote locations that are not readily accessible to the local network.
- Educate and encourage all network users to follow best practices regarding web and email interactions, to minimize the potential for user activated threats.
- Enable automated patches for your operating system and Web browsers.
    - As an example, according to Microsoft, service packs, hotfixes and security patches are updates to products to resolve a known issue or workaround. Moreover, service packs update systems to the most current code base. Being on the current code base is important because that's where Microsoft focuses on fixing problems. Security patches minimize security risks and other vulnerabilities. These are analogous to hotfixes. Microsoft, primarily offers different routes for obtaining client software security patches for its products. It is important to be current on how to patch your product.
    - The WannaCry Ransomware exploits were all covered by different security patches. This link provides a summary: https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/
- Scrub your network data with multi-level threat prevention systems which include AI powered, advanced threat prevention, such as WedgeAMB™ to block threats before data is delivered to endpoints.

The following infographic provides a summary of how WedgeAMB uses multiple levels of malware scanning technologies to detect and block not only known and heuristically similar threats, but also new, never before encountered threats such as the original WannaCry attack. This platform architecture combined with WedgeAMB's patented deep content inspection, orchestration and SubSonic Engine™ uniquely positions WedgeAMB to protect enterprise networks from the next, new global ransomware attack.



Security Bulletin References

- US Cert **Alert (TA17-132A) I**ndicators Associated With WannaCry Ransomware
  - https://www.us-cert.gov/ncas/alerts/TA17-132A
- Microsoft: "Microsoft Security Bulletin MS17-010"(link is external)
- Forbes: "An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak"(link is external)
- Reuters: "Factbox: Don't click - What is the 'ransomware' WannaCry worm?"(link is external)
- Microsoft: "Microsoft Update Catalog: Patches for Windows XP, Windows 8, and Windows Server 2003", (KB4012598)(link is external)