To: All Distributors, Sales Managers, Customers

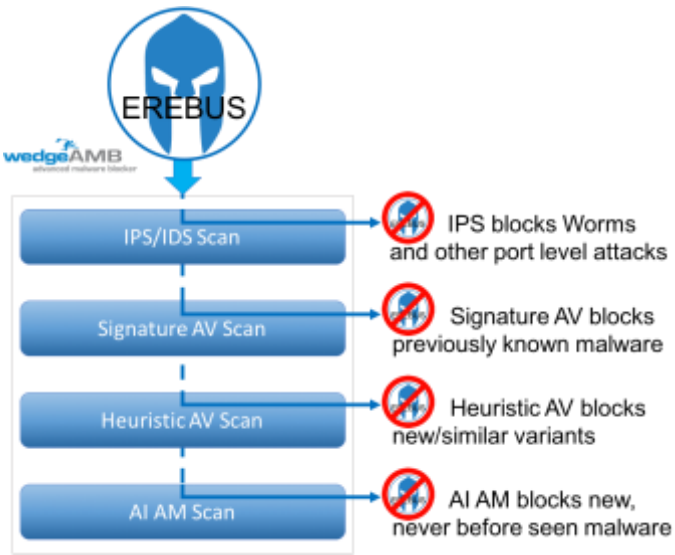
From: Wedge WeService Support Center

Subject: WedgeAMB™ - Protection Against Erebus Ransomware

WedgeAMB Immediately Protects Your Network Against Erebus Ransomware and Other Malware

NAYANA, a major web hosting company in South Korea, has reportedly paid over 1.3 billion South Korean won (~ $1.15M USD) in ransom to secure a decryption key to unlock 153 Linux servers which affected the websites of approximately 3,400 businesses [Source: News Article]. The Erebus ransomware attack, launched on June 12, 2017, gained widespread attention due to the large number of affected businesses and NAYANA's decision to pay the ransom.

While security vendors globally have now identified and issued signature updates to protect against this particular form of ransomware, this attack highlights the ability of cyber criminals to materially modify their malware to bypass conventional signature and heuristic based security alone. WedgeAMB's multi-layered security has proven instrumental in inline blocking of new ransomware attacks like WannaCry and Erebus, without requiring signature updates. WedgeAMB is uniquely positioned to detect and block future variants of Erebus 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 Erebus family of ransomware appears to be the work of an APT group which Kaspersky Labs refers to as ScarCruft. They believe ScarCruft is behind both Operation Erebus and Operation Daybreak. Daybreak was first launched in March 2016 and employed a previously unknown (zero day) Adobe Flash Player exploit. Operation Erebus employs an older exploit, for CEV-2016-4117 and leverages watering holes. A patch for that exploit was available in April 2017, so it is not clear if NAYANA had not implemented the patch or if a newer zero-day exploit was deployed.

The Erebus exploit may be delivered by a phishing attack, or using the watering holes in which a legitimate website is hacked and exploits are inserted into Adobe Flash Player downloads. A second stage download is encrypted differently each time, to prevent detection by signature based AV scans.

Erebus also uses a bug in the Windows Dynamic Data Exchange (DDE) component to avoid AV detection. It is well known that anti-malware systems trigger on special system functions that are invoked to provide deeper analysis of API calls such as CreateProcess, WinExec or ShellExecute. For example, many AV defense technologies trigger if a potentially vulnerable application such as Adobe Flash starts other untrusted applications, scripts interpreters or even the command console. In the case of Erebus, the threat actors used the Windows DDE interface to make payload execution invisible to conventional AV scans.

Wedge Solution

WedgeAMB uses a multi-layered AV scanning approach that is built upon Wedge's patented Deep Content Inspection (DCI) Technology (USPTO 7,630,379) where network traffic is assembled in real-time into its constituting objects. The ability to inspect content at the network layer gives WedgeAMB the visibility of network content that is currently only possible at an endpoint device, without the risk of downloading threats to the actual endpoints. When an end user clicks on a link provided via an email phishing attack or a website watering hole, the signature AV scan will detect any malware with an existing signature. The changing encryption nature of Erebus will likely bypass any known signature scan. Next, the heuristic scan will detect and block variants, including HTTPS encrypted content. There is a high probability that WedgeAMB's heuristic scan will block modest variants of Erebus. If the malware has undergone more dramatic modification to avoid heuristic detections, WedgeAMB also analyzes executable content using artificial intelligence anti-malware. WedgeAMB's AI-AM technology will analyze the executable code to immediately detect and block the payload, in real-time, before the payload is downloaded.

Defending Linux Servers Against The Next Ransomware Attack

The recent Erebus 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.

- Update system and server patches routinely. Routine patch management policies should ensure that the system and server have the latest available patches, fixes, and kernel updates.
- Use discretion when adding third-party or unknown repositories or packages. If possible, remove or disable unnecessary components or services in the server to further reduce the attack surface area.
- Restrict permissions and privileges to help reduce the threat of unauthorized use.
- 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.
- 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.
- Apply network segmentation to minimize the risk of spreading infections to other machines.