American Technology Services

2017-04 ATS Security Advisory

WannaCry Ransomware Attack

Summary

On Friday morning, a widespread Ransomware attack began spreading across the globe. Going by the name “WannaCry” and some variations, this attack takes advantage of a vulnerability in the Server Message Block (SMB) in Microsoft’s Windows operations system. Once infected, the malicious software operated like typical ransomware and encrypted non-system files and presented the user with instructions for decryption. It is highly suggested to **not pay the ransom** if your machine is infected.

Details

The vulnerability being exploited in this case was released by The Shadow Brokers on April 14, 2017 and is believed to be a tool used by the National Security Agency (NSA). Microsoft released a patch (MS17-010) for this vulnerability a month before the disclosure, on March 14, 2017.

The vulnerability itself is with SMBv1 on all versions of the Windows Operating System since Windows NT. For the initial infection, an attacker must have access to TCP Port 445, either by open ports on a firewall or from a previously infected computer on the same network. Once infected, the malware checks for the existence of a ‘kill switch’ domain. If the domain does not exist, it continues execution. When executed the malware encrypts non-system files, installs a persistent backdoor (called DOUBLEPULSAR), presents payment instructions for the user and begins scanning internally and externally for more vulnerable systems. Infected systems should ensure the backdoor has been removed even if the files have been decrypted.

Security researchers quickly learned that the ‘kill switch’ domain was unregistered. When they registered the domain, and pointed it to a server that responds to requests, the malware stopped infecting new systems. This effectively stopped the spread of this strain of the virus. It is reasonable to expect a new strain to address this weakness and be released in the near future.

Risk Mitigation Steps taken by ATS

As part of our Managed Services offering, ATS keeps your servers and workstations up to date with Windows patches. The patch for this vulnerability, MS17-010, was released on March 14th and was installed on workstations almost immediately. Servers received the patch the following weekend as part of our regular patch policy.

For any clients that had previously request to be excluded from our regular patch policy, we pushed the relevant patches as an emergency policy over the weekend.

When Microsoft released the patch for the unsupported Server 2003 operating system, it was approved immediately and pushed out to any remaining Server 2003 servers we have in our monitoring system.

Additionally - We are running reports every hour today and will manually install patches for any servers that may have been unavailable when patches were pushed. It is also suggested to ensure unused protocols, such as SMB, are blocked externally at the firewall. Allowing traffic from the ‘kill switch’ domain is suggested, however, to prevent any new infections.

Future Risk Mitigation

These types of attacks are on the rise. While this instance has been mostly resolved, it is a reminder that we can expect more, similar attacks in the future. Having automated patching for servers and workstations is critical to maintaining a secure environment.

Understanding current threats and the security posture of your organization is important and ATS can help by providing a Vulnerability Assessment and Penetration Test (VAPT). For more information, reach out to your ATS Account Manager or send an email to security@networkats.com.