2017-05 ATS Security Advisory

Petya Malware Attack

Summary

On Tuesday, June 27th, reports of a new, widespread malware outbreak appeared on security forums and eventually mainstream media sites. The malware at the center of this outbreak, known as "Petya", appears to have first attacked organizations in Ukraine, before spreading to other Eastern European countries, and eventually other parts of the world. This malware uses infection techniques like those found in last month's WannaCry ransomware outbreak. It also introduces a few new techniques to facilitate lateral movement within a network.

Ostensibly, this malware acts like ransomware. It modifies the master boot record of a Windows machine with custom code that prevents the operating system from starting. It displays a "ransom note" requesting that $300 worth of bitcoin be sent to a specific address. However, these aspects of the malware are less sophisticated than other, more damaging ransomware. To a growing number of researchers, it seems likely that the ransomware aspects of the outbreak may be acting as smokescreen for a more sophisticated, targeted attack on the Ukraine government.

Details

It has been reported that the initial attack vector for this malware is through email, with malicious Office Documents that leverage vulnerability CVE-2017-0199 to gain local execution. However, due to the large amount of compromised systems at the onset of this attack it is unlikely that email was the only, or even primary, attack vector. Many sources, including Microsoft, are saying a Ukranian accounting software company - MEDoc – had their updater process compromised which caused it to spread the malware. This furthers the theory that Ukraine, and companies that do business in Ukraine, were the primary targets of this attack.

Once the malware gains execution on the local host, it then uses multiple techniques to **encrypt** local files, and **propagate** to other Windows hosts.

To **encrypt the local file system**, the malware enumerates files on the local C drive, and then encrypts files with specific file extensions, except for those within C:\Windows. The malware also overwrites the master boot record, preventing Windows from completely booting. Instead, a ransom note is displayed to the end user. The malware creates a scheduled task to force the local machine to reboot.

To **propagate to other machines,** this malware uses several techniques of varying sophistication.

- The malware uses a password dumping tool to extract passwords from system memory.

- If the infected host is a Domain Controller, the malware will use the local DHCP database to enumerate hosts.
- The malware uses extracted passwords to gain SMB access to discovered hosts.
- The malware will attempt to use known SMB exploits to gain access to other machines.
- With access, it will copy itself and then use the Psexec tool to execute remotely.

The propagation methods seem to only attack locally available subnets, rather than attempting to propagate to hosts on the internet. The propagation technique uses re-purposed penetration testing and system administration tools. These techniques make propagation more likely.

However, the encryption and bitcoin payment techniques are not at all sophisticated. The malware relies on a single Google Mail email address for victim communication. Researchers have noted that decryption may not even be possible. It may be more accurate to describe this malware as a "wiper" rather than ransomware. Its intent is to destroy data on infected systems. It is also speculated that this malware was intended to "hit" a specific target.

Risk Mitigation Steps Taken by ATS on Behalf of Customers

As part of our Managed Services offering, ATS keeps your servers and workstations up to date with Windows patches. The two vulnerabilities used for initial infection, and further propagation, Office vulnerability **MS17-010**, and Windows vulnerability **CVE-2017-0199** were patched shortly after their disclosures in March and April 2017, respectively.

For any clients that had previously requested to be excluded from our regular patch policy, we pushed the relevant patches as an emergency policy as a response to the WannaCry outbreak in May 2017.

When Microsoft released a 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.

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.

What Can You Do?

At this time, there are no actions that needs to be taken by our clients. It remains important to be vigilant about security, and skeptical about incoming emails that appear even a little suspicious. Feel

free to contact security@networkats.com with any questions or concerns. As always, we value hearing from our clients about general, and specific security concerns so that we can provide the best possible services.