CERT-MU Security Alert

CERT-MU

ADYLKUZZ CYBER ATTACK

Original Issue Date: 18th May 2017

Severity Rating: High

Description:

Another cyber-attack known as **"Adylkuzz" (Trojan:Win32/Adylkuzz)** is underway and takes advantage of the same Microsoft Server Message Block (SMB) exploit used in the WannaCry ransomware attack. However, unlike the WannaCry Ransomware, it does not encrypt users' files or announce its presence. The attack is carried out in the background of infected computers and uses their computing power to "mine" a digital currency called Monero.

Unlike the WannaCry Ransomware, the Adylkuzz attack demands no money from victims; rather users will only notice their Windows machine running slowly and will not have access to shared Windows resources.

Affected Systems:

Systems that are vulnerable to Adylkuzz are those running older versions of Windows.

Users are advised to take the following precautions:

i. Aggressively patch and update Anti-Virus signatures with a priority on those in the last 60 days (including MS17-010).

ii. Warn users not to open attachments/enable macros on suspicious emails. This may be the entry vector so diligence is warranted.

iii. If you suspect you may be a victim, install Windows Defender; and run to remove the malware on systems.

iv. If patching is not possible (i.e. if the machines cannot be updated with the March MS17-010), temporarily block SMB connections to limit the spread. This will likely impact your organization's services. The following workarounds may be helpful in your situation:

- Disable SMBv1

For customers running Windows Vista and later, see Microsoft Knowledge Base Article 2696547

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu