Executive Summary

A vulnerability scan has alerted us that our Microsoft Office 2016 software is currently critically vulnerable to CVE-2017-11882. This exploit is high risk, allowing attackers to embed trojans in Word and Excel files leveraging the Equation Editor to trigger buffer overflow through OLE objects. The Word and Excel files are delivered via phishing/spearphising. It further allows them to remotely execute code to enumerate networks, steal user information like passwords and download additional malware and spyware. If the vulnerability is exploited, it can be difficult to identify through static antivirus software/scans as it uses encoding to blend into normal processes. To mitigate the risk, we should implement the official Microsoft patch for the vulnerability. If the vulnerability has already been exploited, the affected machines must immediately be isolated, malicious processes be killed and the machines should be wiped clean and patched before continued use.

Question 1 - Is this a legitimate vulnerability? What does it do?

This is a legitimate remote code execution vulnerability in the Equation Editor in Microsoft Office. It allows attackers to execute arbitrary commands with the user's privileges, install malware or spyware, steal credentials or sensitive files and gain full system control if the user has admin rights.

Question 2 - Under what conditions can it be a vulnerability?

Systems that haven't applied the Microsoft Security Update that removes or disables the Equation Editor (available since Nov. 2017) are vulnerable. The vulnerability is exploited when victims open malicious Office files like Word or Excel documents that contain embedded OLE objects that trigger buffer overflow.

Question 3 - Any notable threat actors involved using this?

There are several notable threat actors involved in using the CVE-2017-11882 exploit: APT 41, APT34 (Allegedly Iranian), BITTER (T-APT-17, South Asian), Tonto Team, Sidewinder, Leviathan, Patchwork, Tropic Trooper and Saint Bear as well as a number of smaller groups associated with them.

Question 4 - What other indicators should we look for on our network if we become compromised from this vulnerability?

After being compromised from this vulnerability, we should be seeing C2 traffic. The vulnerability has been used for reconnaissance by downloading a grayware product called Agent Tesla. Agent Tesla contains a number of questionable functions including

password stealing, screen capturing and the ability to download additional malware. Through these functions we may see HTTP exfil routines, POST requests and encryption before sending. The malware attempts to download the program 225 times at which point it will launch or exit based on whether or not it is successful in downloading.

Question 5 - What else should we be concerned about based on your findings?

This vulnerability, when exploited, is very difficult to find via normal antivirus products and methods. It used encoding techniques to obfuscate strings to hide its behavior from static tools.

Question 6 - What are the top 3 things in order to do to respond to this?

The top 3 actions to take in order to respond to this vulnerability are:

1) immediately contain and isolate the machine from the network, kill the malicious Office process with task manager and block the known malicious IP/hashes at the firewall/EDR.
2) Dump the memory before shutting down and save:
    a) Temp files
    b) Office recent file list
    c) Event logs
    d) Prefetch/Amcache for Equation Editor execution traces
3) Eradicate and recover the machine:
    a) Reimage
    b) Apply official Microsoft patch before reconnecting to network
    c) Scan all Office files with updated EDR signatures before running Office.

Additionally, check EDR/SIEM for Equation Editor spawning from winword.exe as this is the main IOC for the compromise.