Important Cybersecurity Update

Qakbot Malware

What is Qakbot Malware?

This malware has been installed in thumb drives that were manufactured in China. Upon investigation, it seems the thumb drives were infected prior to entering the United States. More specifically, these thumb drives are infected with the bank credential-stealing Qakbot malware variant.

Systems Affected

The systems affected are any and all devices. The malware has the ability to propagate through removable drives, network shares, and web pages. A common use is also through phishing emails.

Risks

Qakbot is known for its persistency and requires removal of all malware from every device. Failure to remove even one node of the malware may result in re-infection and thousands of dollars in malware removal and system downtime. In addition, the malware also has keylogging abilities and the ability to lock users out of active directory accounts.

Protection

Every device connected to the network and every piece of attached removable media must be scanned for malware and be cleaned of the infection. Additionally, employees must ensure that they are not clicking on unknown emails or inserting removable devices into the network that were not previously scanned for the variant.

Recommended Steps

1. Only purchase hardware from approved and trusted vendors.
2. Scan all hardware before insertion into a network environment.
3. Practice good browsing habits and alert employees.

What should you do?

Although this malware may seem alarming, it is important to counter the possibility of its insertion by constantly upholding all best practices within an organization. In addition, preventative measures are emphasized as this malware can be detected and remediated in a timely manner with the correct security and remediation steps.

Have questions or need help implementing these recommendations? Call us at (315) 525-6233.