N-Dimension Solutions Quick Tips – Petya Ransomware

To defend your utility, first you must understand the nature of ransomware, versus phishing or other types of cyber attacks. Defined by TechTarget as a "type of malicious code that is used by cybercriminals to launch data kidnapping and lockscreen attacks. The motive for ransomware is monetary, and unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions for how to recover from the attack. Payment is often demanded in virtual currency to protect the criminal's identity."

In the case of the recent Petya global ransomware attack, ***Mihir Kapadia, VP of engineering at N-Dimension****, recommends the following quick tips on how to prevent and protect your utility and constituent IT properties from damaging ransomware effects.*

Quick tips to help you avoid being held ransom by Petya:

More Sophisticated Than WannaCry: it is similar to WannaCry, but much more advanced. It seems to be leveraging the same EternalBlue vulnerability in Microsoft Windows (which Microsoft issued a patch for back in March).

Don't Pay Because There's No Guarantee: as with WannaCry, there is no indication that paying the $300 in Bitcoin actually results in the infected machine being remedied. For any ransomware attack it is always recommended to not pay the ransom.

What To Do Right Now: ensure all Windows machines on the network are patched with the MS17-010 patch. It is also recommended to have a robust backup and recovery mechanism in place.

It's Not Over: this is an ongoing attack, which N-Sentinel will identify before an attack. If you do not have a cyber threat detection solution, learn more here.

www.N-Dimension.com
sales@n-dimension.com