Issued 3/7/18

Locked Windows machines Can Be Compromised through Cortana

Compromising locked Windows computers that have the Cortana voice-activated virtual assistant enabled is relatively easy – or it was until Microsoft made a simple tweak. This attack requires the attacker to have physical access to the target computer so that he can plug a network adapter in the locked machine's USB port. The next step is to hail Cortana and instruct it to visit a non-HTTPS site. (In Windows 10, Cortana responds by default to any voice. Making it respond to just the owner's voice requires a short "training.") The network adapter intercepts the web session, which can then be modified by the attacker. A reply can then be sent to the computer telling it to visit another site, which has been booby-trapped to deliver malware to visitors. In enterprise environments, this one compromised computer can be made to "attack" others on the same local network, the researchers told Kim Zetter. If, for example, the first computer is made to download malware that allows it to perform ARP poisoning, it can force the other computers on the local network to send all traffic through it. If equipped with the Newspeak proxy – a tool created by the researchers that monitors all Cortana requests and responses on every machine on a network – the attacker can, as before, intercept and redirect this traffic to send those computers to malicious pages. And, if waiting for users to use Cortana seems like too much trouble, the attacker can force the nearby machines to start a Cortana session by simply playing instructions over the original compromised computer's speakers. If done by

night, when offices are empty, this lateral move could easily pass undetected.