THE FUTURE OF RANSOMWARE

A few years ago, if the average person heard the term 'ransomware' they might have imagined the fashion ensemble of a kidnapper. Fast forward to today and most everyone one is now familiar with ransomware one way or another. Most ransomware infects target computers when unsuspecting users click on an attachment or link usually embedded in an email. This common method of delivery is called a phishing attack as it often lures in users to take the bait (the attachment) through an unsolicited (spam) email. When malware (malicious software) is dispensed on the target computer, local files become encrypted, with the hacker holding the only key for decryption. These phishing attacks are becoming more sophisticated because they are being created by specialists in the criminal field. Unfortunately, their targets (general computer users) haven't graduated to the same level of skill needed to counter these attacks. So where are all of these ransomware specialty attacks headed?

Popular ransomware variants like 'WannaCry' have the ability to easily spread across some variants of Microsoft Windows by exploiting a known bug. With larger networks, it's all about speed. Once the malware gets in, it spreads quickly and is therefore tough to stop before it spreads across entire networks. This recent strain of ransomware acts more like a 'worm' because it can effectively self-spread on its own by exploiting compromised NSA code called 'Eternal Blue'. Like much hyped AI and machine learning technology, ransomware and its creators continue to evolve tactics and approaches. Where else can we expect to see more attacks?

Hackers will soon set their sites on targeted medical implants. Imagine a politician, high net worth individual, or celebrity relying on a pacemaker for their heart. Physicians typically gather data and

receive updates wirelessly from medical implants to adjust settings for their patients as needed. A hacker needs only to tap into this wireless link to blackmail and threaten a patient's life by altering settings through known vulnerabilities. The bigger the target, the bigger the ransom. The hacker could easily send a warning message by triggering a series of low-energy electrical pulses forcing the heart into arrhythmias. The same pacemaker that controls abnormal heart rhythms could be used to injure the victim until the ransom is paid.

Hacking cars will soon get worse. A few years ago, white hat hackers Charlie Miller and Chris Valasek took control of a 2014 Jeep Cherokee by sending commands from their laptop through the vehicle's network (click to watch). This was a physical hack but it was also recently demonstrated remotely through the Internet connected to the Jeep's dashboard computer. All modern cars have integrated cellular modems that communicate wirelessly through the same cellular network as our cell phones. This wireless connectivity allows car manufacturers and dealers to remotely monitor and administer maintenance when needed. Drivers can get real-time navigation updates, find specific destinations and even host their own Wi-Fi hotspots to keep passengers entertained. These conveniences can pose security vulnerabilities. Recent research demonstrated remote control over windshield wipers, AC fans, radio and even the car's engine itself.

These hacks were used to demonstrate some security weaknesses in modern cars in the hopes that vehicle manufacturers will take automotive security more seriously. Newer cars are loaded with hybrid ECUs (Engine Control Units) that combine the functionalities of Advanced Driver Assistance Systems (ADAS), instrument clusters, rear camera parking assist and infotainment units to name a few.

Once hackers can exploit a wireless vulnerability, they move laterally throughout the vehicle and place malware that can be weakened to cause havoc later. Since no one in their right mind would knowingly enter a vehicle infected with malware, the handoff from the driver's control to the hacker's control must be swift and smooth. This would ensure the driver's full compliance as a victim trapped in their own speeding car and allow the ransom amount to be increased considerably.

Both ransomware and cyber security defenses will continue to evolve, leaving regular users particularly vulnerable. It is important that users of all levels avoid clicking on any unknown links or attachments lest they become victims of future ransomware attacks.

Click here to discover how to explore new security policies and strengthen your cybersecurity strategy.