Ransomware taking digital data hostage

Marc Koscieljew says that ransomware attacks are becoming more frequent and brazen.

Digital data from around the world is being taken hostage. The data is freed only if victims pay ransoms.

Taking digital data hostage is one of the most common and worrisome trends in the dark virtual world of cybercrime.

In May and June of this year, governments, corporations, and individuals across the globe fell victim to two rounds of sophisticated cyberattacks. Both cyberattacks used the same hacking tools that were stolen from the US National Security Agency within the last year by a mysterious group of hackers known as the Shadow Brokers.

The first cyberattack in May featured ransomware that attacked networks. The attacker encrypted data, locked users out, and demanded a ransom. Although it is nothing new, ransomware is a growing problem. IBM's security research unit, for instance, estimated that in 2015 less than one per cent of spam was ransomware, but by 2016 it comprised 46 per cent of spam.

These recent cyberattacks will probably raise the percentage even higher for this present year.

Ransomware attacks can occur in different ways. Almost half involve phishing e-mails persuading recipients to click on links or open attachments. Another method involves hackers scanning for and exploiting various digital, software, and password vulnerabilities of an organisation to then seize and encrypt as much as possible. Hackers also establish so-called watering hole attacks by infecting a website with ransomware and, whenever a user visits it, ransomware is downloaded onto their computer.

Taking digital data hostage, instead of stealing it, is becoming increasingly profitable. Ransomware has become an effective means by which to make money in a short time.

Ransomware has a few costs associated with it. There are some useful steps that both individuals and institutions can take to help protect against these new cyberattacks.

First, update software. As Care, Gartner's research director, argues, "it is safe to assume that all complex software is vulnerable to malware". Do not be complacent about computer or network security. Remain vigilant by regularly updating software to install the latest security features.

Second, install antivirus software. Care emphasizes the need for detection, advising "to make sure your malware detection is updated and that your intrusion detection systems are operating and examining traffic". Antivirus software helps detect and prevent different kinds of malware from infecting or infiltrating computers and networks. But only use antivirus software from reputable providers and ensure that it is continuously updated as well in order to block the latest and emerging threats.

A number of dubious e-mails and pop-up windows are the reason why people are increasingly susceptible to phishing e-mails and pop-up windows. Ensure e-mails are trustworthy by checking the sender's address to determine if its legitimate; spotting spelling, grammatical, or formatting errors; and hovering over hyperlinks (without clicking on them) to see if they lead to dubious websites. Also be aware that e-mails from reputable sites, such as banks or credit card companies, will not ask for sensitive information such as personal identification numbers or passwords.

Further, be suspicious of most pop-up windows that advertise antivirus software services or other products that guaranty against malware. It is advisable not to click on any feature featured on these pop-ups and instead trustworthily by checking the sender's address to determine if its legitimate; spotting spelling, grammatical, or formatting errors; and hovering over hyperlinks (without clicking on them) to see if they lead to dubious websites. Also be aware that e-mails from reputable sites, such as banks or credit card companies, will not ask for sensitive information such as personal identification numbers or passwords.

Fifth, create a digital security plan as part of routine information management practices. There should be specific scheduling of checking for and installing the latest software updates. For institutions and businesses, this scheduling should apply across the enterprise and be implemented at times best suited to avoid interruptions. For individuals, this scheduling could perhaps be done automatically for them by most reputable antivirus software providers.

Sixth, isolate infections. If already infected with ransomware, isolate the device and limit network connectivity. Make sure to disconnect the computer from both your internal network and the internet to prevent its spread. Report the crime to law enforcement and immediately seek assistance from legitimate information technology professionals specializing in data recovery.

The May cyberattack was eventually halted by a British security researcher, known as MalwareTech, who purchased a domain to help track it and that ended up acting as a kill switch.

Yet many victims affected by the ransomware remain unable to access their data. But the June cyberattack showed that this had only been a temporary reprieve. Indeed, there are indications that other similar cyberattacks are brewing that will possibly be even more stealthy than either of these two rounds.

As Jonathan Care, research director at the information technology consultancy Gartner, states "right now you are in the swamp, and the alligators are still lurking beneath the surface." These cyberattacks are most probably signs of what more is to come.

These cyberattacks are alarming not only because of their global reach and impact but also because they illuminate the significant vulnerabilities of most computers, networks, and the Internet.

According to Robert Pritchard, a former cybersecurity expert at the UK defense ministry, "this vulnerability still exists, other people are bound to exploit it. The current variant will make its way into antivirus software. But what about any new variants that will come in the future?" Or as the cybersecurity expert Justin Harvey warns, "these types of attacks are just going to keep happening, and we've known this since we first saw how big WannaCry was going to be last month. The real question is whether these are all just practice runs for the big one."

There are some ways to help guard against future threats, including updating software, installing antivirus software, avoiding suspicious e-mails and pop-up windows, backing up data, creating digital security plans, and isolating infections. Although these steps do not guarantee perfect security, implementing them is better than doing nothing.

The consequence could be valuable digital data being taken for ransom.