The Rise of Foreign Cybersecurity Threats

Our industry must do its part to address asymmetrical hybrid warfare in critical communications.

By Rex M. Lee
August 2019
MissionCritical Communications

The U.S. government, telecommunications providers and operating system (OS) developers must address cybersecurity and privacy threats from adversarial countries such as China and Russia. These threats are centered on intellectual property (IP), telecommunications, smartphones, tablet PCs, connected products, Internet of things (IoT)/industrial IoT (IIoT) devices and PCs that use the Android, Apple iOS and Microsoft Windows OS.

Joint Chiefs of Staff Chairman Gen. Joseph F. Dunford said in March that countries such as China enable U.S. technology companies to sell U.S. products and services to Chinese citizens, which is good for our economy. However, the Chinese government then adopts the U.S. technology to oppress its citizens and enables the Chinese military to use the technology against adversaries such as the United States.

The Chinese government legally and illegally acquires the IP for such technology for nation-state smartphone and social media app and platform developers such as Baidu and Tencent to compete against U.S. companies such as Google and Facebook.

We are seeing a re-rise of great power competition from adversarial countries in competition with western countries such as the United States and the European Union.

“Companies are waking up to the fact they have been squarely in the gray area between peace and war,” says T. Casey Fleming, CEO of BLACKOPS Partners, a cybersecurity mitigation firm. “They are finding that current strategies and tactics (cybersecurity and business) are ineffective and must give way to more proactive measures rooted in adversarial intelligence.”

Great power competition is nothing new. There were threats associated with great power competition pre-World War II from Germany, Japan and Italy.

We are seeing a re-rise of great power competition from China, Russia, Iran and North Korea, which are competing against the U.S. for global economic and military power.

Global competition from these adversarial countries presents cybersecurity and privacy threats coupled with unprecedented risk associated with asymmetrical hybrid warfare (AHW) that the U.S. government and U.S. companies associated with the defense, technology, critical infrastructure and enterprise business industries need to address.

Unprecedented Risk

U.S. companies are making billions selling products to adversarial countries while enjoying cheap labor by manufacturing U.S. goods and services in China and other

countries. CEOs, board members and senior executives of U.S. multinational companies need to realize nation-state companies from adversarial countries do not compete at the same level as U.S. companies. U.S. firms compete on an individual basis, but nation-state companies compete to advance their host countries' political agendas.

Nation-state companies from China and Russia apply AHW as a means to compete. During the Black- Energy malware attacks in the Ukraine in 2015, state-sponsored Russian hackers used NotPetya ransomware to cause blackouts to Ukraine's grid, affecting about 1.4 million people.

The Crash-Override malware, as it is known, targets industrial control systems (ICS), affecting critical infrastructure including IoT/IIoT devices. The BlackEnergy malware was believed to be installed via Windows and Linux plug-ins and remained dormant until activated, a sign the malware was related to military or state-sponsored techniques rather than an individual hacker.

In similar attacks on Saudi oil refineries in 2017 and 2019, Triton Trisis malware attacked industrial control systems centered on safety at Petro Rabigh refinery and another unnamed oil refinery. Fortunately, nobody was injured or killed in either attack.

Similar to the BlackEnergy malware attacks, Triton Trisis, according to FireEye, is likely linked to Russian state-sponsored hackers believed to be linked to the TeleBots group.

Russian officials deny responsibility for such attacks, but malware such as Crash-Override and Triton Trisis are so sophisticated that it can probably only be developed by military and/or state-sponsored Russian hackers associated with groups such as TeleBots and Sandworm.

The modern battlefield is no longer limited to warfare between military forces alone. The battlefield now includes non-military and trans-military warfare targeting civilians, companies and critical infrastructure. AHW poses huge threats to national security, cybersecurity, privacy, safety and critical infrastructure associated with telecommunications networks and hardware.

Networks and hardware at risk include 4G and 5G networks, licensed and unlicensed private networks, smartphones, tablet PCs, connected products, IoT/IIoT devices and PCs manufactured by Chinese companies such as Foxconn, ZTE and Huawei. Additionally, platforms that support social media services plus software such as apps,

widgets and other content developed by nation-state companies include Baidu, Tencent and Prisma Labs.

Threats posed by ZTE and Huawei have been highly publicized in the news during the past two years. In fact, in May, President Donald Trump signed an executive order to bar U.S. communications firms from acquiring technology from foreign companies. He later backed off the order during trade talks with China.

We have also heard of threats posed by Russian software companies such as Kaspersky Labs, which develops antivirus/malware software that millions of American citizens and companies use.

However, we have not heard many government warnings regarding nation-state companies that produce intrusive apps sold by and used on Google, Apple and Microsoft hardware and smartphones, tablet PCs, connected products, IoT/IIoT devices and PCs supported by Android, iOS and Microsoft Windows OS.

Apps can be classified as a legal form of malware that enables the app developer to monitor, track and data mine the app user. Chinese app developers Baidu and Tencent have this capability. Why are the Crash-Override and Triton Trisis malware relevant to apps distributed by Google, Apple and Microsoft?

Apps that support connected products such as smartphones are also capable of launching distributed denial of services (DDoS) and man-in- the-middle (MITM) attacks.

BlackEnergy malware was originally designed to launch DDoS attacks but morphed into sophisticated Crash-Override ransomware, with a KillDisk component. Theoretically, the malware could be launched from a disguised app, enabling the malware to be distributed.

Google, Apple and Microsoft apps that can launch attacks are not being developed by the everyday hacker but by state-sponsored hackers from both Russia and China. Consider the required investment in research and development (R&D) coupled with the amount of knowledge needed to develop such intrusive and destructive apps while meeting all of the quality control criteria imposed by Google, Apple and Microsoft. Other than a state-sponsored hacker, who could afford to develop apps that can launch DDoS and MITM attacks knowing the apps are not designed to make a profit but instead to find holes in our nation’s cybersecurity?

Attacks through apps are a serious cybersecurity and safety threat that needs to be addressed immediately by chief information officers (CIOs), IT professionals, telecom providers, app developers, the FCC and other relevant agencies.

Surveillance and Data Mining

What is concerning is that some U.S. tech giants, telecom providers and government agencies are enabling companies from adversarial countries to monitor, track and data mine U.S. citizens via smartphones supported by protected telecom infrastructure regulated by the FCC.

Enabling nation-state companies to surveil and data mine U.S. citizens via apps is an existential threat to our national security and economy while posing cybersecurity, privacy, civil liberty and safety threats to smartphone users.

This flaw in U.S. cybersecurity is a greater threat to our national security and economy than Huawei and ZTE combined because companies such as Baidu and Tencent can distribute legal malware as apps through Google Play, Apple and Microsoft app stores. For example, these three app stores actively distribute intrusive apps such as Baidu's DU-Browser, Tencent's WeChat and Prisma Labs' Prisma Photo Editor apps.

In essence, companies from China and Russia are able to lawfully hack confidential personal and professional information, including IP. If you are skeptical, read the app permissions for verification.

Google, Apple and Microsoft enable these app developers to virtually collect, use, share, sell, store and aggregate nearly 100% of all location data and sensitive user data from the use of a smartphone, tablet PC, laptop PC or even a desktop PC. Tencent, a Chinese nation-state company, can collect nearly 100% of the OS user's location and sensitive user data, including biometric data.

It is clear no oversight, policies or regulations are in place to protect app users from predatory surveillance and data-mining business practices employed by tech and telecom giants.

The United States needs to confront these threats. Company boards of directors and IT and cybersecurity experts must do the same by implementing best practices and policies concerning smartphones, tablet PCs, IoT/IIoT devices, connected products and bring your own device (BYOD) programs. Best practices need to include a total review of all preinstalled apps, plus the terms of use that support smartphones and all products and services concerned.

All organizations, including government entities, should eliminate all BYOD programs. The Apple iPhone is the most secure smartphone on the market, but not all personal and professional information can be secured on iPhones or any smartphone supported by the Android OS, according to T-Mobile, Verizon and My Smart Privacy research.

Rex M. Lee is a tech journalist and cybersecurity and privacy advisor for My Smart Privacy. For more information, go to www.MySmartPrivacy.com. Email feedback to editor@RRMediaGroup.com.