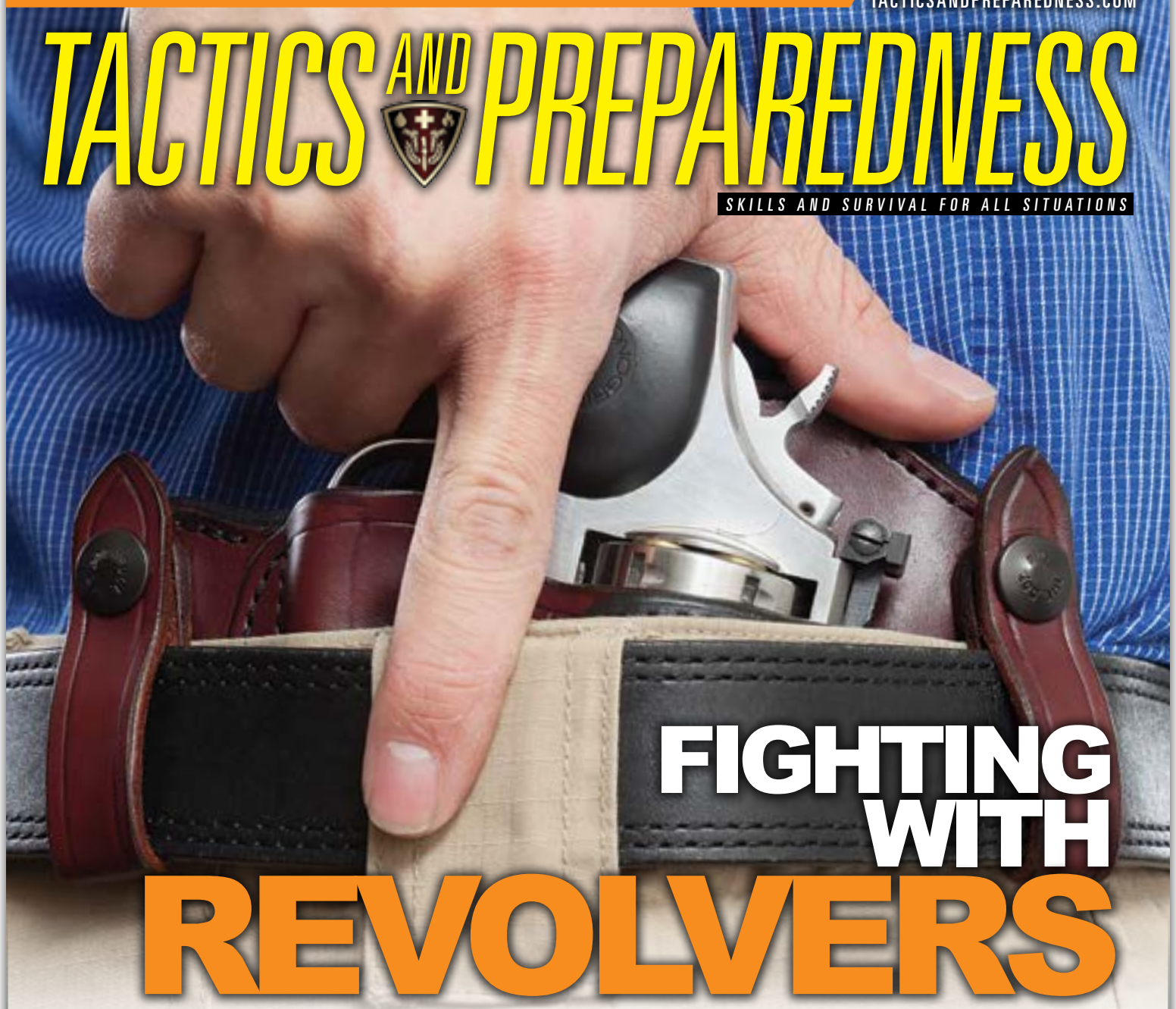
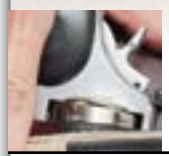
QUICK CHANGE | SUPPLY CHAIN ATTACKS | EAT SCORPION
NOVEMBER 2017 ISSUE 49
TACTICSANDPREPAREDNESS.COM

TACTICS AND PREPAREDNESS

SKILLS AND SURVIVAL FOR ALL SITUATIONS



FIGHTING WITH REVOLVERS



In the modern world, with modern things, we often wonder how in the world our fathers and grandfathers made do.

BY **JAMES WASHINGTON**

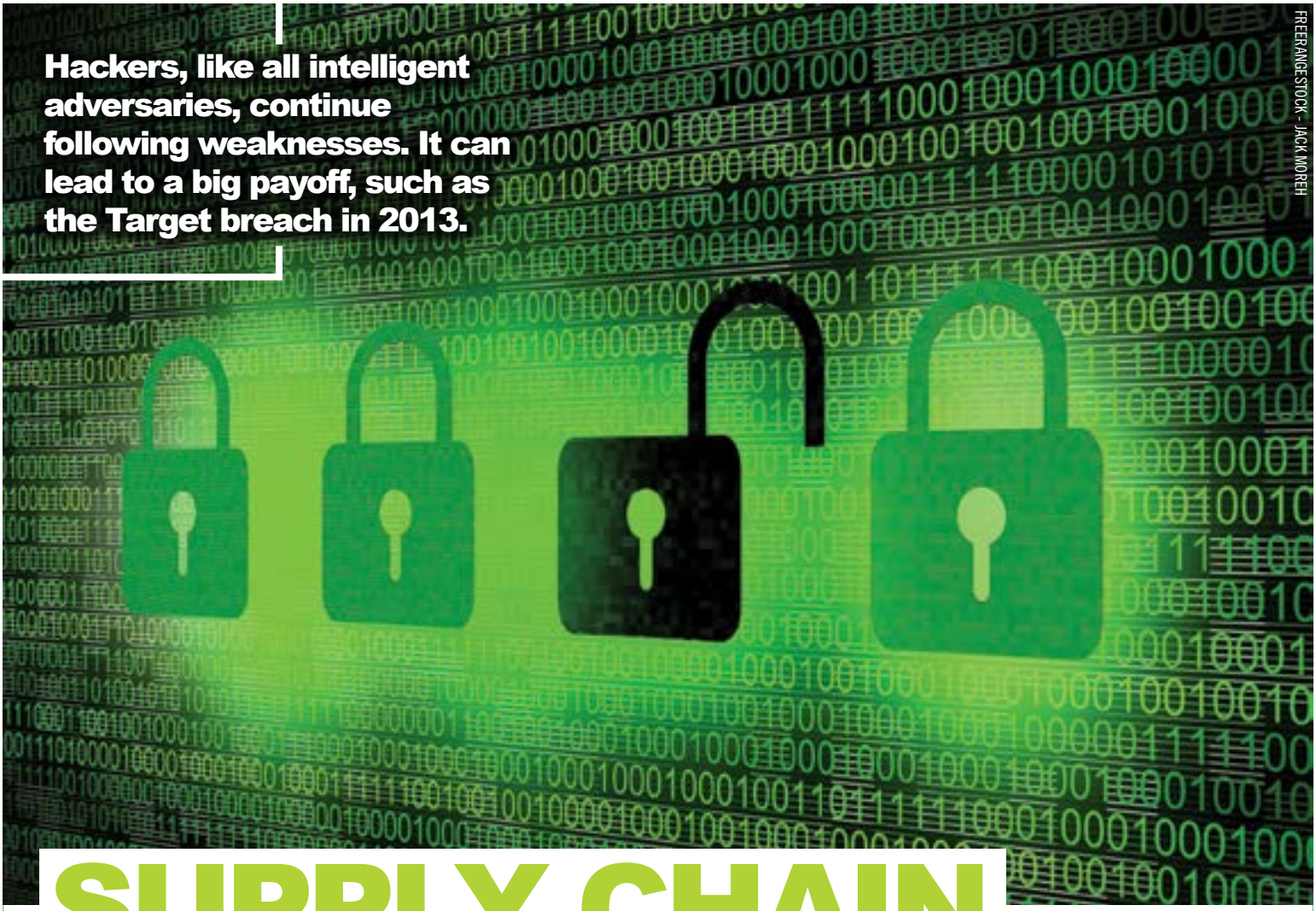
PHOTOS BY: OLEG VOLK / WWW.A-HUMAN-RIGHT.COM

How awful it must have been talking on a telephone attached to the wall by a rubbery coil of wires. Cars without remote starters forced you to get dressed at 2:00 am, in 10 degree weather to let your car run for fifteen or twenty minutes so your engine wouldn't freeze. Worse yet, televisions weren't high definition flat screens, and not having DVRs with one terabit memories was pure agony. Revolvers may seem like a holdover too, but it pays to have a wide range of skills.

Not only have large numbers of revolvers been manufactured and distributed around the world over the years, but revolvers can be the perfect defensive gun; deployable without fully drawing them from a pocket. One does not have to worry about hindering the slide function, blocking the ejection port or causing some other interruption of the firing cycle. There are no immediate action drills for stoppages to practice dry or on the range. Whether you like revolvers or not, you may find one to be the tool-at-hand or the best solution for a specific defensive need.

When choosing a pistol, you want to stick with a major caliber and not an underpowered cartridge in projectile diameter or speed (velocity). You want continued on next page

Hackers, like all intelligent adversaries, continue following weaknesses. It can lead to a big payoff, such as the Target breach in 2013.



FREERANGESTOCK - JACK MOREH

SUPPLY CHAIN ATTACKS

In the digital age, more and more of our economy is powered by the Internet and related technologies.

BY: DR. BRANDEN R. WILLIAMS

Not only have companies started to derive actual value from intangible assets (such as source code) over tangible assets (such as buildings and machinery), but there are entire businesses that derive their entire value chain through online activities. We can all laugh at properties such as Instagram, Pinterest, Facebook and Twitter, but they command real value in the marketplace. Who would have thought that sharing a picture of your dog online could be part of a multi-billion dollar concern?

The challenge for we consumers is that increasingly, the "old way" of face to face business is being phased out in favor of cheaper digital methods that provide their firms with much farther reach. It's the difference between opening a small antique shop in Richmond that relies on foot traffic and starting a website from Boise that relies on Google AdWords and eBay. The shop in Richmond may have a devoted, local following, but with high overhead costs. The shop in Boise could be shipping all over the world from the owner's garage or from a storage unit. It has much lower overhead and much farther reach.

That is one big reason why digital commerce is significantly displacing physical store fronts. We are past the point of excluding some consumers because the only way a firm does business is digitally. Since there is no going back, let's take a look at a very real attack that you are vulnerable to today. The Business Email Compromise attack—a class of supply chain attack.

YEAR OF THE SUPPLY CHAIN ATTACK

2017 has reminded companies big and small

that their informational supply chain, or the parts of the value they create that are digital and informational based, are at risk for compromise. A recent example is the CCleaner utility, which is used to keep computers safe from malware. Hackers compromised the development and build environments of the parent company, Avast, and inserted code into the application without the company's knowledge. The version with the malware was built and signed automatically, then distributed to over two million users.

This summer, the NotPetya worm spread throughout Ukraine through the MeDoc software—a government approved accounting package. Similar to the CCleaner example, hackers leveraged MeDoc's auto update feature to spread the malware automatically. Given the software package and the amount of damage it did to Ukraine, some speculate it was a state sponsored attack from Russia.

A more recent—and possibly more significant example—is the news that Kaspersky's anti-virus tool was being used by the Russian Government to look for specific keywords and steal sensitive information—including state secrets. The reason we know about it is an Israeli state-sponsored cyber group broke into Kaspersky and found a Russian cyber group already there. Cyber war is real, and it is here. Only vigilance on our part will keep us from becoming collateral damage.

Trust in technology must be limited, because all parties must be working together to secure the experience from end to end.

BUSINESS EMAIL COMPROMISE

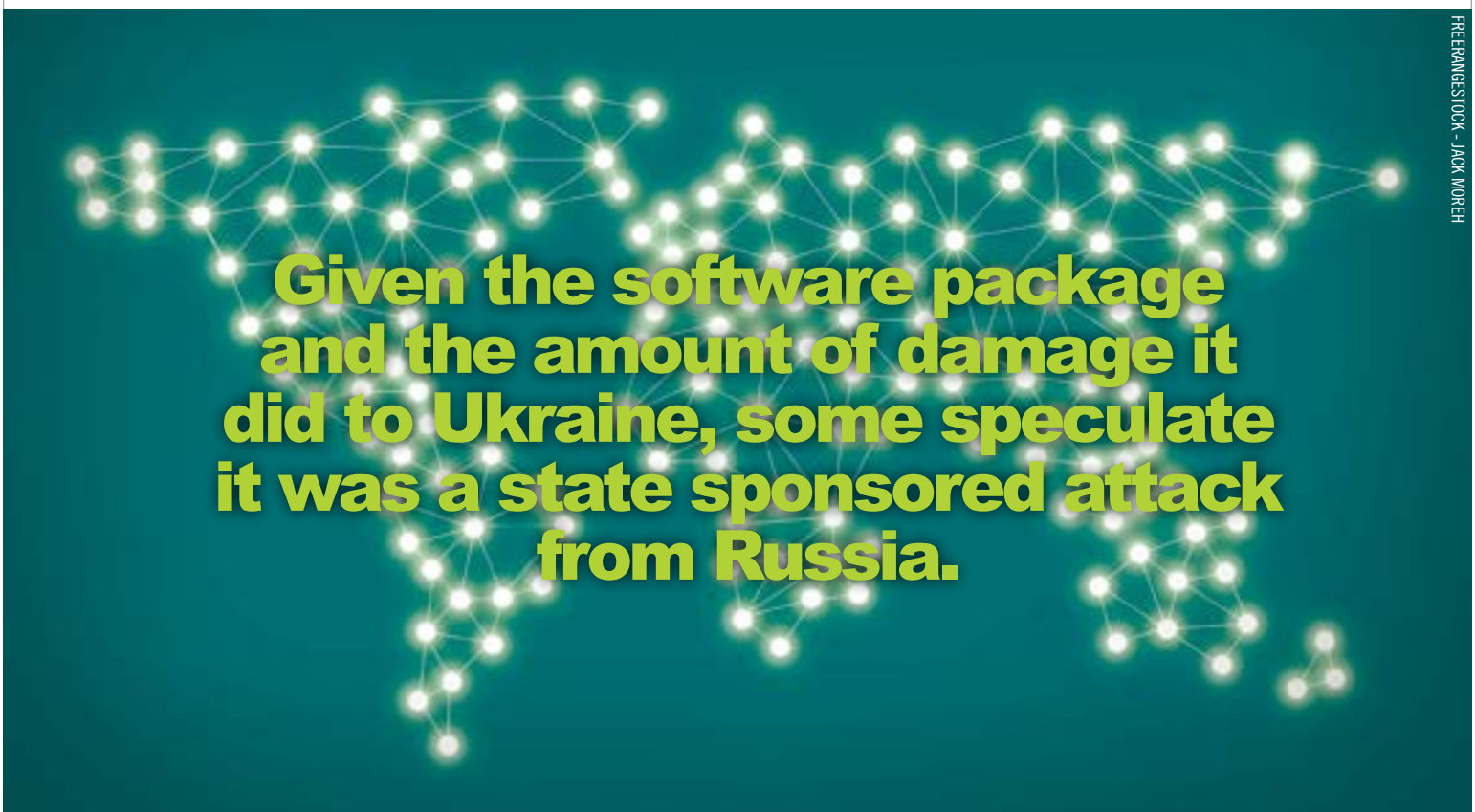
Imagine one of the best days of your life. You are able to buy your dream home; your forever home. You have been nervously giddy all morning as you wait in the Starbucks around the corner for your appointment at the title company. After picking up your second refill, your phone rings. It's the title company. They didn't receive the funds you wired.

This scenario is happening all over the country and it could happen to you. As we get better at security in general—and firms *are* getting better—cyber crooks also get more creative. While they prefer to steal and hack without any human intervention, many of those avenues are closing—or at least they are getting much more difficult to do. What used to be done through automated tools and exploit kits freely available for download now require much more reverse engineering for a big bang hack.

Hackers, like all intelligent adversaries, continue following weaknesses. One way is to build a series of compromises that lead to a big payoff, such as the Target breach in 2013, which started with an HVAC system account compromise. The other way is to go after people who are unaware of proper security techniques or are ignoring them for convenience sake.

The Business Email Compromise attack is not new, but it has seen a huge uptick in money movement and theft in the last year. Fraudsters target individuals who may have knowledge of pending money movement, such as real estate agents, accounting professionals, title company employees and business development professionals. These folks tend to have lots of information about high dollar transactions and money movement within their email files. Many companies fail to adequately protect this information.

Good security around email requires both a password and a second element, such as a security token, text message or push alert through an app on your smartphone. The second element is not always available in every setup, but it is available in popular email services such as Gmail and ProtonMail. You should be using a service that offers a second factor of authentication. Many firms, such as local title companies, are not sophisticated enough to have dedicated security and technology professionals guarding their networks. Couple that with the human tendency to pick easy to remember passwords



FREERANGESTOCK - JACK MOREH

and reuse those over multiple websites and it's a recipe for a hack.

The problem with these types of hacks is that you have zero control over this. You can pick your title company, but you can't dictate their security policy or how their users transmit and access information electronically.

THE ATTACK

An attacker has compromised an email account and is looking through all the emails sent and received, being especially careful not to make any changes to the account to tip off the victim. When he sees a pending financial transaction, he will send out the typical wire instructions to the victim (i.e., the prospective home owner) via email, but include his beneficiary and bank account information, not the title company's. He will then use other tricks to prevent a legitimate email coming from the title company with different wire instructions to be visible. Sometimes the attacker will just send the email with the wrong wire instructions a few days in advance of when wire instructions are normally sent.

If he's good, he's been crawling through the victim's emails to understand the process of how things work. Ideally, they will find a day where there are lots of closings and try to get as much money as possible at once. Considering that wire transfers for payments on houses tend to be sizable five, six, or even seven figure wires, being patient and timing this just right could easily yield an attacker a multi-million dollar payout. Then it is up to him to ensure he's got the right logistics in place to start wiring those funds out of his target bank to launder it and remove the ability to reverse the wire.

Being patient and timing just right could easily yield an attacker a multi-million dollar payout.

According to the 2016 Internet Crime Report from the FBI Internet Crime Complaint Center, Business Email Compromise attacks topped the categorical losses at over $360 million. It's the most lucrative type of attack in play right now, and you can easily become a victim.

KRACK ATTACK

You may have heard of a new attack dubbed KRACK, which stands for Key Reinstallation Attack. If you ever trusted Wi-Fi, with WPA2 encryption of-course, you now have a reason to distrust it. Attackers found a flaw in the underlying Wi-Fi protocol that allows them to inject new keys into your session, which would allow an attacker to see and alter all traffic to and from your device. Be it a laptop, desktop, tablet, phone, or gaming system, if it is not patched, it is vulnerable.

There is a long tail on this particular vulnerability because both sides of the connection must be patched. It is time to check your home Wi-Fi router and upgrade the firmware so that you can at least be safe in your own home. Using public Wi-Fi should always be done with caution, but now it should be done with Virtual Private Networking (VPN) software to keep your sessions safe.

WHAT CAN YOU DO?

As with most kinds of social engineering and confidence scams, skepticism is your best ally. If you assume that everyone else's email is compromised when it comes to important things like financial transactions, then you will take emails with wire instructions with a grain of salt.

Your best bet is to take the email and call the person directly who is giving you the wire instructions. If you can meet face to face, that is even better. Confirm every aspect of the wire from the account numbers, to beneficiaries, to bank names. If you are calling to validate, be sure you know the person on the other end of the phone. Cellular networks are vulnerable to call redirection depending on the sophistication of the attack, so for a large sum it is conceivable that your phone connection would not be trustworthy either. ✓

BIO

Branden R. Williams (brandenwilliams.com) DBA, CISSP, CISM is a seasoned security executive, ISSA Distinguished Fellow, and technology executive sought after by global companies to consult on their digital business initiatives. His latest book on PCI DSS v3.2 Compliance is available on his website.