ATM Losses BLOWIN' UP!

Anyone with a passing familiarity with teens or social media (or social media-obsessed teens for that matter) knows that, apart from war zones, when something 'blows up' it's going, or has just gone, viral.

We've probably all heard "OMG, X is totally blowing up!" with "X" usually being a hot new band, a just released video, or another head-scratching scandal from this year's increasingly absurd presidential campaign, for example.

In this case, we'll go back to the original meaning of the phrase. It turns out, in Europe, especially for the last six months or so, criminals have settled on a new-old technology hybrid approach to separate banks – particularly bank ATMs – from their customers' money. The new technology portion is, as you might expect, primarily malware-based while the old technology is more "Bridge Over The River Kwai" and less "Mr. Robot."

Let's back up a step.

Studies have repeatedly shown that many ATM networks across the globe are running on outdated technology and are thus ripe for manipulation and raids with or without malware even entering the equation. More proactive banks have started beefing up their ATM cyberdefenses (with biometric identification, chip and PIN combos, etc.) and in response, criminals are going old school where necessary and supplementing cyberattacks with more blunt force brick-and-mortar (with a distinct emphasis on the *mortar*) attacks.

In fact, nearly 500 European ATMs were literally blown up by criminals for their cash in the first six months of 2016 alone, which was nearly a 50% increase from the same period in 2015.

So between non-malware attacks, skimming attacks, "Cash Out" or "Jackpotting" style malware attacks (where malware causes the machines to start dispensing cash, and lots of it), Transaction Reversal fraud, and now a spike in physical attacks (Kaboom!), it's no wonder that ATM losses in Europe, and across the globe, are mounting.

Some research estimates have ATM fraud costing banks over $221 million in Europe this year alone. Which sounds like a lot. Until you realize that skimming alone costs the industry somewhere in the neighborhood of $2 billion worldwide each year.

Chip cards are a help, though not an iron-clad solution, and so is covering your PIN when you type it in as many skimmers will just be able to grab the magnetic stripe info but not the PIN and simply covering the keypad may foil a strategically placed camera from recording your keystrokes.

Hackers have an easier time installing skimmers in unattended street ATMs, convenience store locations, etc. To at least reduce your risk of falling victim to a skimming attack, try and use only

ATMs in banks or bank vestibules over those located on the street or in convenience stores as it will almost always be harder to compromise those located on bank premises.

As far as malware-infected machines go, that’s a bit harder to protect against, but it’s a good idea to check your bank statements regularly and look out for any small charges (or, obviously, large ones) that you don’t recognize; as criminals will often float a small ‘test charge’ to see if they can then go in for a bigger score.

And if you see some dodgy looking folks in flak jackets fixing a blob of C4 onto the screen the next time you hit the ATM, you might want to keep moving.

Just sayin’.