SUMMER 2019 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss smartphone discovery and key gotchas. We also explore case law involving monitoring employee activity on smartphones.

Smartphone Horror Incidents Increasing - SIM Card Hijacking

If you're a horror movie buff, you've seen a movie or two where the first thing the villain does is cut the telephone line so the scream queen can't call for help. Now, with an increasing number of homes relying on cellular service as their primary, and often only, residential telephone service, those old horror moves are showing their age. So, what's a screen writer to do with modern telephone technology? Enter SIM card hijacking, one of the fastest growing smartphone horrors.

SIM Card Basics

A SIM, or Subscriber Information Module, is a small card that contains a microchip that stores information prescribed by a cellular telephone service carrier. The exact information stored on a SIM card varies by carrier, but at the very least the SIM will contain enough information to identify the carrier and account owner associated with a telephone number. This information can also include approximately 250 contacts, a small quantity of text messages, and the authorized services for the account. SIM cards are removable, but not always interchangeable with all phones and carriers.

Hijacking Hijinx

SIM card hijacking, also called SIM hacking, SIM jacking, SIM swapping, and port out scamming, is the unauthorized transfer of SIM card data from the original SIM card to a duplicate SIM card and allows the hacker to take control of a cellular service account. SIM hacking is simple and is one of the fastest growing cybercrimes. Although mobile service carriers are reluctant to release the actual figures, law enforcement agencies are stepping up their awareness campaigns, investigations, and enforcement actions in response to the trend.

SIM card hacking begins with hackers identifying attractive victims: cryptocurrency traders, celebrities, and those with desirable social media handles. Once the victims are identified, the cybercriminals exploit various security protocol weaknesses to persuade the cellular services provider to execute the data swap between SIM cards. Those weaknesses include bribing or

blackmailing carrier employees and impersonating victims by phone or in person. The process has been documented to be as simple as calling up the customer service line of a carrier, and using data purchased from the dark web, or stolen via a database hack, pretending to be the customer and requesting the data be sent electronically to a replacement SIM card. Because many customers use the last four digits of their Social Security Numbers, birthdates, or even the last four digits of their telephone numbers to secure their mobile service accounts, this easily stolen data allows the SIM swap to take place quickly and easily. Next, the hacker inserts the SIM card into a new phone, and the scam continues.

Once the new SIM is controlling a new cellular device (SIM card enabled tablets can also be SIM card hijacked), the hacker can now access many of the accounts of the authentic account holder. In the case of cryptocurrency investor Michael Terpin, two SIM card hijacks led to the loss of $24 million in cryptocurrency, over which Terpin is suing the cellular carrier, AT&T (*Terpin v. AT&T Inc.*, No. 2:18-cv-06975, Central District of California, 2018). For celebrities, the stolen data is often compromising photos, emails, or text messages. In a particularly harrowing case, a woman with a very marketable Instagram and Twitter handle, @Rainbow, received a threatening, profanity-laden phone call designed to frighten her into releasing the social media identities so they could be resold. In addition to controlling her cell phone account, the hackers also gained access and changed passwords to other social media, email, entertainment, and even financial services accounts.

The Fight Against SIM Hackers

In 1997, California's Department of Justice founded the Regional Enforcement Allied Computer Team (REACT), and they've been fighting computer fraud and cybercrime ever since. Recently, REACT's efforts led to the decade's long sentencing of Javier Soto Ortiz, aka Joel Ortiz, the first convicted SIM hijacker in the US (https://www.mercurynews.com/2019/02/04/cryptocurrency-thief-cops-to-million-dollar-hacking-scheme-as-tech-squad-builds-rep/). Still, law enforcement can only do so much, and consumers and businesses must protect themselves, as well, by employing effective security practices. A few simple precautions can help deter SIM card hackers:

1. Add a unique SIM card password or PIN via most carrier's website self-service portals.
2. Limit the number of accounts secured with Social Security Numbers, telephone numbers, and dates of birth.
3. Change passwords and PINs frequently so that if personally identifiable information is out on the dark web, it's not valid forever.
4. When trading in or upgrading cellular devices, wipe the device of all data and be sure that you remove the SIM card.
5. If you suddenly lose cellular service, immediately contact the carrier. Do not rely on the carrier service to send a text notification of a SIM card change – you may not receive it in time to stop the hacker.

So many of us keep our business and personal information stored conveniently on accounts we can access quickly and easily from cellular devices, and that creates an attractive opportunity for SIM card hijackers. An electronic discovery and data forensics firm, such as Digital Mountain, can help deter cybercrime by investigating how much of your business or personally identifiable information is out on the internet, helping you create unique security protocols for your cellular devices, and making recommendations about how to mitigate your risks. Cellular devices have made mobile communications and productivity a dream, but SIM card hijacking is a real nightmare.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

BLACK HAT USA 2019
Las Vegas, NV: August 03-08, 2019

ABA ANNUAL MEETING
San Francisco, CA: August 08-13, 2019

ILTACON 2019
Lake Buena Vista, FL: August 18-22 16, 2019

PFIC 2019 CYBER SYMPOSIUM
Park City, UT: September 10-12, 2019

THE SEDONA CONFERENCE WORKING GROUP 11 MIDYEAR MEETING 2019
Montreal, Canada: September 18-19, 2019

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: