Mindstar Security & Profiling

Concierge Security Report
September 2015
Volume 1, Issue 3

Enhancing Physical Security: The Impact of Internet and Social Media Exposure

Protecting Your Home and Family

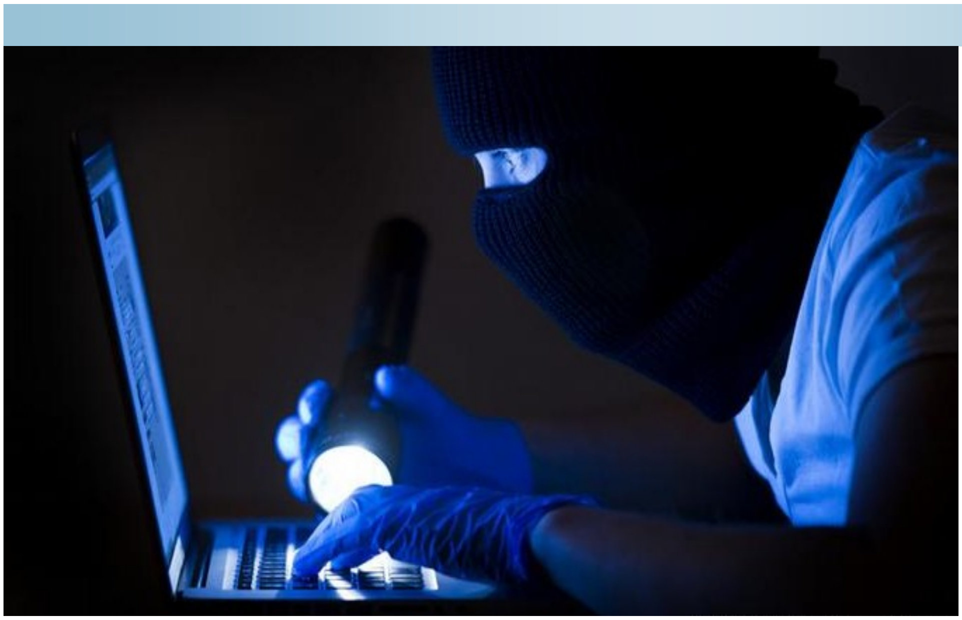
High net worth persons and executives are frequently targets of theft, burglary, scammers and hackers. While all types of people may be victims of a home burglary or a mass email scam, high net worth persons are sought out by sophisticated criminals because of their wealth and status. These criminals begin their targeting operations by scanning the Internet and social media for data and intelligence.

Discussions concerning the dangers of the Internet and oversharing on social media often end with warnings about potential embarrassment, possible risks to future employment, cyber-bullying, or warnings about identity theft. Often lost in these discussions are the serious threats to physical security caused by information that can be fairly easily obtained in the open source internet, whether the information has been posted by a third party or by the potential victim.

In order to better explain exactly how criminals can leverage open source information to better plan a physical attack, burglary, kidnapping, or other crimes, Mindstar Security & Profiling has created the following narrative from the perspective of the criminal. The security and intelligence analysts at Mindstar have over a decade of experience conducting threat assessments for business executives and high net-worth individuals. The targeting techniques included below are just a few of those observed by our analysts over the last several years and should not be considered a complete list of potential vulnerabilities. In the interest of brevity we have only included some of the more common threat vectors we routinely identify.

The goal of the criminal may be to commit a home burglary, robbery, home invasion or stalk/harass the target family. The motivation may stem from personal revenge, a disgruntled employee, an activist, someone making a political and/or social statement, or simply for financial profit. Here is an operational plan from a criminal's point of view of an executive and his family being targeted.

Inside this issue



“Burglars used Google Street View to scout out millionaire banker's mansion before carrying out jewelry raid.”

Learning About the Target Family From the Criminal’s Perspective

Please allow me to introduce myself. I am a thief, a burglar, and sometimes even a hacker. My job is to find vulnerable high net worth targets and exploit them. After choosing my target I need to develop a better understanding of the target and his or her family in order to better understand the vulnerabilities that exist for the family, each individual, and their home. The first step taken here is to run a rudimentary internet search of the target. This search typically yields several hits leading to different data aggregation websites. By comparing the consistencies in these sites I can confidently put together the names and ages of my target, his or her spouse, and their children. These aggregation sites typically provide an address as well but in the case they do not, and I am dealing with a high net worth individual, I will check political campaign contribution information for any donations made by my target. These contribution receipts are public and most contributors use their home address not realizing this information is public and easily accessible.

In very infrequent cases where my target’s family members are not disclosed on data aggregation websites, I will find the target’s social media accounts, typically Facebook, and run searches within their Friends List to pinpoint a potential spouse and children. More often than not I am able to find the family members either within the Friends List, or if that is unavailable for search, tagged within the target’s photos.

In cases where my target’s address is not easily accessible via data aggregation websites (which is almost never the case) or campaign contributions, I search specific real estate websites that often provide the name of the buyer and seller of properties. There are certain sites that are notorious for providing information of this nature, regardless of how long ago the property was purchased. These are the three main (and easiest) ways in which I am able to connect my target with his or her physical address. These steps can be done by anyone with even the most rudimentary understanding of the Internet.

No Social Media Presence?

Many people have told Mindstar, “I do not use social media, I do not have a Facebook page, a Twitter presence, or even a LinkedIn page. So I cannot possibly be exposed on the Internet.” The fact that there is no social media presence initiated or used by an individual does not mean that there is no social media or Internet footprint.

Even if you do not have or use social media, everyone around you probably does. These secondary parties can and do post information about you, your family’s activities, likes, dislikes, photos, and a variety of other information.

Your family members, your friends, your colleagues, and those who have special access and privilege as service providers inside your home (i.e., personal chefs, au pairs, dog walkers, pool cleaners, house keepers) collectively may be posting bits and pieces of information that when collected and viewed together can provide a very robust profile.

Tertiary parties such as real estate sites, PeopleFinder sites, alumni associations, genealogy sites and philanthropic organizations are also providers of rich data about your home and activities.

Even people you do not even know well such as your children’s friends, their parents, coaches, teachers and the like can be posting information about schedules, activities, or personal contact information with the intent of being “helpful” and sharing. However, in concert with other secondary party information, the profile only grows with a greater breadth and depth of detail and accuracy.

Learning More About My Target's Home

Once I have obtained my target's address I begin the process of learning as much about his or her home and property as I can. The first step of this process is a simple Google Earth search of the property. This allows me to gain a better understanding of the property and neighborhood surrounding it. I can map potential routes into and out of the neighborhood, identify potential breach points for the target property, as well as search for wooded or otherwise uninhabited areas near the home where I can conduct further surveillance without drawing attention from my target or neighbors. These areas can also be used during the actual breach of the property. By utilizing satellite imagery of the home I am able begin mapping my points of ingress and egress both onto the property and into the home.

The satellite imagery of the property is a great start but I always try to find images of the interior of my target home. In many cases, I am able to find at least some photos taken from the interior of the home via the social media accounts of my target and his or her family members, most often by the un-privatized accounts of a spouse or the couple's children. The family members could have blocked me from access by simply privatizing all of their social media accounts.

Gaining Valuable Home Images

Another way I am able to gain valuable images of the interior of my target's home is to conduct a simple Google search on his or her home address. A typical Google search on an address of a private residence typically yields several pages of results but by narrowing the focus of those results to just the online real estate websites I am able to quickly search these listings for any photos that have been left online by the site, even if the home has not been on the market for several years. This is something that many home owners do not realize. Many of these real estate sites (e.g., Zillow, Trulia, Homesnap) contain a massive amount of data and are often poorly managed. They often provide incorrect information about current listings and sometimes fail to take down photographs posted of homes that were put on the market several years earlier. While the furniture and décor is likely to be different, these photographs provide me with valuable information about the interior of the home that allows me to plan my breach and movements within the home once a breach has been made.

"Nearly 80% of 50 ex-burglars surveyed strongly believed that Facebook, Twitter and Foursquare were being used by current criminals to target homes."

Planning the Breach

Once I have done my due diligence searching for photographs of the interior of the home and possibly some light surveillance from a safe area nearby, I begin the next phase of my targeting process: using information found online to accurately predict when the home is most likely to be either unoccupied or occupied by children only. This is the longest phase of the entire targeting process. During this time I do extensive online research in order to gain a better understanding of the target and his or her family members. This search begins with social media and focuses mainly on Facebook, Twitter, and Instagram.

Burglars Use Google Street View to Target Homes

In January 2014 thieves burglarized the home of Robin Bowie, founder of British investment bank Dexion Capital, likely after gaining intimate knowledge of the layout of his sprawling property from the use of Google Street View.

The burglars made off with a haul of expensive jewelry and several thousand dollars in cash. Due to the speed and efficiency in which they conducted their operation, Mr. Bowie believes they used the online mapping service to conduct reconnaissance on his home before burglarizing it.

The intruders used a ladder to scale a six foot high perimeter wall at the front of the property before forcing open an upstairs window. A wheelbarrow found on the property was used to transport a stolen safe to a waiting getaway car.

A recent survey of 50 convicted burglars by UK security firm Friedland Response and reported by the United Kingdom's Sky News argues that Google and social media tools are being used extensively to target people. Nearly 80 percent of the 50 ex-burglars surveyed strongly believed that Facebook, Twitter and Foursquare were being used by current criminals, and nearly 75 percent stated that they thought Google Street View was also involved in theft planning.

Home Networks and Wifi

Information found off of social media and the Internet can also impact your home network security. For example, birthdays are frequently posted on Twitter and Facebook, and the same dates are sometimes used as easy to remember passwords for home networks, email, banking credentials and other user login information.

Personal information scraped from online sources can be used by scammers, spammers, spear phishers, and ransom ware hackers to target specific individuals with a great deal of authentic data. These online scammers can target you by:

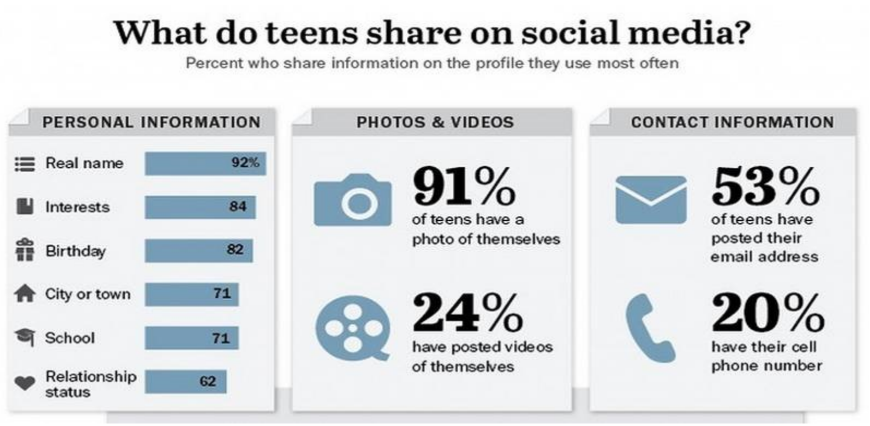
- Scanning your home network to assess if it is password protected.
- Using basic password cracking tools on a home network that is password protected to attain the login credentials.
- Brute forcing passwords on your home network by using easy guesses such as your address, your birthday, your anniversary, or date of graduation.
- Sending you targeted emails that appear to come from friends or family members with infected attachments or malware infested.

Part of a thorough examination of your online profile should include how online criminals and burglars could use exposed data to target your home network and gain complete access to your personal computers, tablets, phones, and other devices.

Planning the Breach, cont.

Social media accounts often provide information about groups or organizations the target is affiliated with. Examples of information I am looking for during this step include:

- Are there any patterns of movement the parents appear to do regularly? Maybe they go out to dinner every Thursday night and one of them “checks in” on Facebook when they do so. Are they members of any social groups that might have a website or Facebook account with a schedule of events they’re likely to attend?
- Charitable organizations? Does the couple appear to attend some sort of fundraising dinner or gala every year for the same cause? If so, is that event coming up in the near future?
- Does the target participate in any recreational sports? Local basketball or softball league? Avid golfer? Theatre junkie? If so, are there any events coming up that he or she is likely to attend?
- What extracurricular events are the children involved in? If I see a lot of social media posts showing the parents at their son’s hockey games I can assume they are likely going to be attending some of his home games. A simple search for that school’s hockey schedule will provide me with times that his parents are likely to be away from the home attending his game.
- Are any of the family members posting Facebook statuses or tweets about an upcoming vacation? Teenagers often post countdowns to vacations on social media: “Costa Rica in two weeks!!”, “Can’t wait for South Beach next week!!”, “t-minus three weeks until Paris!” This is a very common occurrence and provides me with a specific timeframe, often several days long, where I can breach the home and operate without fear of being interrupted by a family member.



Source: PEW STUDY
http://www.csmonitor.com/The-Culture/Family/Modern-Parenthood/2013/0521/Facebook-waning-social-media-may-have-plateaued-among-teens-Pew-study-says

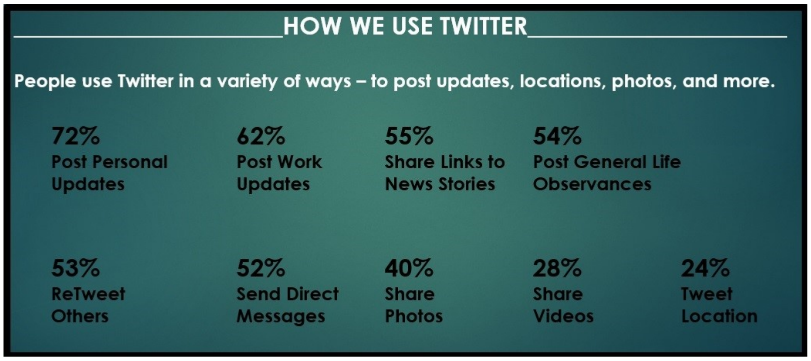
Criminal’s Note

While all of the collected data points are individually very important to me, the real power of the information is when I see the data collection as a whole. Over time, connecting all of this information can reveal real and accurate individual and familial patterns that I can use to predict a family’s whereabouts. By collecting the data my targets have posted over several years, I can easily map where they go, when they vacation, who they know, and other information that is likely increase the effectiveness of my plan.

Targeting Family Members Away From the Home

Much of the information I gather to identify the target family's patterns and movement (as outlined in the previous section) can also be used to target specific family members or the family as a whole while they are away from the home. If I wanted to target the family outside the home I would want to do it in a place that is both isolated and provides me an easy escape route.

The information I gain about the family's movements, whether it be their involvement with a specific golf course, horse stable, vacation home, church, or any other activity identified online is all I need in order to begin planning a potential isolated ambush of my target. Readily available open source resources like MapQuest and Google Earth can be used to identify the likely route the family would take to get to these places. From there it is as easy as simply identifying the most isolated places along that route, as well as potential choke points within the route from which I can launch a potential ambush.



HOW WE USE TWITTER

People use Twitter in a variety of ways – to post updates, locations, photos, and more.

72% Post Personal Updates

62% Post Work Updates

55% Share Links to News Stories

54% Post General Life Observances

53% ReTweet Others

52% Send Direct Messages

40% Share Photos

28% Share Videos

24% Tweet Location

Source: http://www.kumailhemani.com/how-twitter-can-make-you-a-better-seo/

Debrief and Recommendations

Based on the targeting tactics of the criminal, Mindstar has put together a review of the criminal's planning behaviors and presents recommendations for preventative strategies below. The methods highlighted in this narrative can, have, and will continue to be utilized by sophisticated criminals to target their victims. None of the steps outlined above require more than a basic understanding of the open source Internet and it is imperative that individuals do their due diligence to assure that sensitive personal information is not readily available in the open source. Some personal information is difficult or impossible to remove. Examples of this include address information found on data aggregation websites and access to satellite images of neighborhoods and properties. Beyond very basic information of that nature, most people have the opportunity to significantly limit potentially sensitive information on the open source Internet. Unfortunately, many people are unwilling or unable to invest the time or money it may take to do so.

There are three steps that need to be taken in order to ensure that there is not information in the open source internet that could potentially create security vulnerabilities.

1) The first step is conducting a comprehensive assessment of what information is already out there. This is basically a current state of affairs reading for your online footprint. This step allows you to gauge what information is currently out there and what (within that sample) needs to be dealt with.

2) The second step is to take what is learned from the initial comprehensive threat assessment and deal with the issues that cause concern and need to be eliminated from the open source. In cases where there is sensitive content posted that needs to be removed, a simple takedown request is sent to the site's webmaster. If this tactic does not work and the content is either posted illegally or is creating an immediate security issue, a lawyer then sends the site a cease and desist order. There are times where content is unable to be removed but more often than not it is. In cases where it is not, simply knowing that the content is out there can be of value. Much of the work done during this step is conducted by the subject of the threat assessment. Privatizing (fully or at least partially) all social media accounts, addressing social media issues among family members, and deleting accounts that have not been used in years or that were created without the subject's knowledge is vital during this step. After potential issues have identified and addressed the subject of the assessment should have a clear understanding of their current Internet footprint.

3) The third and final step in this process is maintenance. Your current and recently polished Internet security stature needs to be maintained in order to assure that new vulnerabilities do not appear after the assessment was conducted and addressed. The work in this step is most often done by the subject's security team (should the subject be a high level executive) or by a third party vendor hired by the subject or security team. Maintenance involves regularly searching the open source for re-posts of old issues and the creation of new content that is of concern. This allows any new issues to be identified immediately and dealt with swiftly rather than pile up and possibly lead to a bigger issue later.

Conclusion

In order for an executive and his/her family to reduce the odds that sensitive information is not available to those that may target them, various strategies must be implemented proactively and over time. Overall, it is important to consider:

- Understand your individual and family's current and ongoing online profile and exposure points.
- Understand how your online presence has a clear and present correlation to your physical safety and security.
- Have a plan for how to deal with unwanted data exposure.
- Have an ongoing strategy for how to maintain knowledge and the growing volumes of online data that is publicly available about you and your family.
- For those vendors who work closely with the family or at your residence(s), have a service contract that explicitly defines and/or restricts certain types of social media use as it relates to your family, property, assets, and schedules.

Al-Qaida's Edict to Target HNW Persons by Using Social Media

Al-Qaida's main publication, INSPIRE Magazine in September 2015, has put out a call to lone wolf attackers in the United States to target high net worth businessmen. While the article did specify certain individuals by name, the terrorist operatives were urged to target anyone of prominence.

The Al-Qaida instructions provide a guide on how to collect information on the targets and using social media to gain intelligence is one of the tactics included.

Mindstar Security & Profiling specializes in security solutions for family offices, high profile/high net worth executives, and their families. Our customized focus includes the security trifecta of Internet/Social Media Safety, Physical Security and IT Security.

1001 Sycolin Rd SE, Suite 1A
Leesburg, VA 20175

Phone: 703-404-1100
Fax: 703-404-5549
www.mindstarsecurity.com
E-mail: info@mindstarsecurity.com

MINDSTAR
SECURITY & PROFILING