Public Exposure Checks Explained

When we say public exposure checks, what we mean is the process a threat intelligence analyst takes to determine what information is publicly available online about their organization, and if this can be exploited in any way to cause damage. This can range from employees posting pictures of them in the office on social media to employee credentials in data breach dumps for sale on the dark web. This work is important, and works to protect the organization more than you think.

SOCIAL MEDIA MONITORING

Image Metadata

Why do we care if people take selfies in the office? – We're not robots, and let's face it, we don't work 100% of the time we're at work. As long as we're not disruptive or unproductive it's usually fine. But taking photos at work can cause some serious issues. You'd be surprised at what information can be contained in a single photo. If you took a photo at work, depending on the device and settings, attackers could potentially discover the make and model of the device you took the photo on, the devices name (we typically name our devices after ourselves, such as "Josh's iPhone"), the date and time the photo was taken, and in some cases even direct GPS coordinates. If this photo gets posted to social media, attacker could immediately find the exact location of that office – super not good if it's a secure or covert site.

Leaked Information

Following on from the example above of taking photos or videos in an office, there's still more damage that can be done. Maybe the selfie looked really good and you're getting tons of likes on Instagram, but what about the computer screens in the background that are extremely clear, and show the operating system and programs your organization uses. What about the whiteboard on the far wall with confidential business diagrams and information all over it. And the sticky note on someone's screen with their login details. Even tiny details can help attackers in the long-run. An innocent photo could end up being a goldmine of information for attackers, so be careful what you post, and refer to the organization's social media policy!

Early Warnings Signs of Insider Threats

John posts on Twitter that he hates his job. Okay, maybe he's just had a bad day. John continues to tweet how he's had enough, he doesn't get any respect from his peers, and he's "going to do something about it". This Tweet could mean a lot of different things – maybe John is going to work extra hard, or just maybe he's going to become an insider threat, and intentionally cause damage to company assets. The security team can monitor the situation, and work to monitor this individual closer using forensic-grade tools such as DTEX. Whether the employee uses technical skills and access to damage IT equipment, steals confidential documents and gives them to competitors, or works with malicious actors to give them a foothold in the network, monitoring early-signs like this could turn out to be nothing, or it could save the organization a lot of money by stopping an attack before it happens.

Brand Abuse and Impersonation

Social media account hijacking requires access to legitimate login credentials. Impersonations do not, and therefore are much more dangerous. Impersonations can occur when a threat actor pretends to be individuals or organizations, often seeking to either tarnish a reputation, cause general chaos and confusion, or conduct a phishing campaign. With almost no effort, in the digital world nefarious actors can create digital footprints (websites, social media, e-commerce, apps, etc.) that look like your brand and execute a monetization strategy to target your customers. The immediate impact of brand infringement on your business is lost revenue and eroded customer trust.

DATA BREACH DUMPS

Data breaches happen all the time, and unfortunately sometimes employees get caught up in it. While it is not the job of the security team to alert employees if their personal email addresses have been included in data breaches, it is important when company email addresses are included, especially if passwords were leaked. Password reuse is common, and it won't go away – it's just too convenient, but it's very insecure. If James G was going on a work trip and stayed with The Blue and White Hotel, when he books it he'll probably use his work email, as it's a work trip, and he can get the expenses refunded by the company. If hotel gets hacked, and email addresses and passwords are leaked, it's only a matter of time before *someone* tries to use James' credentials elsewhere.

Acquiring Data Breach Lists

Sometimes these lists can be shared on the clear web, and threat intelligence analysts can acquire them for analysis, looking for any company-owned email addresses. Other times it can be a lot harder to get access, such as if the list is only being sold to trusted customers on the dark web. Threat intelligence companies around the world work hard to infiltrate dark web marketplaces, and will sometimes purchase data breach lists on behalf of all their clients, allowing them access to only the data related to their organization, reducing further exposure of credentials or private details.

< Previous Topic | Mark Complete ✓ | Next Topic >

Back to Lesson