Summary: Emily Williams wasn't real, but the two hackers who created her from social media profiles got her a government job, a company laptop, VPN credentials - and compromised a government network.

Using social media profiles and a photo of a real (and consenting) woman, two hackers fooled a government employer into believing she was an employee, conning them out of a company laptop, network credentials, and more.

They used "her" Facebook and LinkedIn connections to send out holiday cards linked to an attack site, which the government employees visited, and scammed one employee into sending her a work laptop - as well as network access credentials and more, such as SalesForce logins.

The researchers used the imaginary pretty girl's poisoned holiday e-cards to gain administrative rights, obtain passwords, install applications and stole documents with sensitive information - some of which, according to the hackers, included information about state-sponsored attacks and country leaders. Miss Emily Williams - run by puppetmasters security researchers Aamir Lakhani and Joseph Muniz - even convinced a security team executive to click a javascript exploit masquerading as a birthday card, thus compromising his laptop. Lakhani told an audience at RSA Europe 2013 on Wednesday, October 30, "This guy had access to everything. He had the crown jewels in the system."

Mr. Lakhani presented the team's research findings at RSA Europe in a talk titled Social Media Deception, the results of his team's sanctioned 90-day "Emily Williams" penetration test experiment on a US government agency, conducted at the end of 2012.

Lakhani declined to state which U.S. government agency was infiltrated and compromised by the fictitious Miss Williams. He told the RSA audience that his team's pre-Snowden attack was performed on a very secure agency that specializes in offensive cybersecurity and protecting secrets, one where previously only zero-day attacks had been successful in pentests leveraged against the unnamed agency.

Mr. Lakhani explained that his team had tried the attack with fictitious male characters, but as men they were not successful. He said that in actuality, through the Emily Williams platform, the team had achieved their objective within a week of deployment but that they ran their experiment for its full 90 days to see how far it could go. And it went pretty far.

Emily Williams - the attack - was based on Robin Sage, another fictitious person created in 2009 as a demonstration in the ease of obtaining information from intelligence on US military personnel via social networks; the successful Robin Sage findings were presented at Black Hat 2010 ("Getting in bed with Robin Sage"), to the anger and embarrasment of many.

Miss Williams first came into being on Facebook and LinkedIn sometime during 2011. The waitress who volunteered the fictitious character's photos worked at an establishment frequented by the target company's employees - the nearby Hooters - yet no employee recognized her in person at any time during the experiment. We found a non technical female employee from the restaurant industry (that happened to be a few blocks from our target) to volunteer pictures for Emily's appearance.

We developed a fake social security number, residence and other areas that may be searched to make Emily seem real. We gave Emily an IT background from the University of Texas and updated her profile with a matching employment background. Before zeroing in on the government target's employees, Lakhani and Muniz built up Miss Williams' presence on social media, netting her hundreds of connections, with only one man flagging her as suspicious.

Another man asked how Emily might know him, and when the researchers answered with information they obtained in the man's profile, he said he did indeed remember the imaginary girl. Once Wiliams had friends, the hackers updated her Facebook and LinkedIn profiles with just-hired status at the government target, and gave her an engineering title. The attractive, imaginary young woman connected with the target's employees via social media and connected with Human Resources, IT Support, Engineering and those in executive leadership roles.

The congratulations for "her" new job rolled in.

As our target audience friend number grew, we started moving up the rank eventually capturing people from Human Resources and Engineering who would be responsible for hiring Emily if she existed.

We moved all the way up to executive leadership...

As it was near the holidays, no one questioned when Miss Williams posted seasonal cards to Facebook directed at specific targets among her coworkers - which they clicked, and then were seamlessly, unknowingly owned. The cards, of course, were part of the hackers' deception.

The security researchers said that they were intent on doing no harm to their targets.

They had many options for obtaining network access to host systems through social media. One popular one they declined to use is Blackhole, which delivers a malicious payload - but the researchers pointed out they "felt [Blackhole] wasn't safe for our target's systems."

Instead they used The Browser Exploitation Framework (BeEF), they said, "based on our feeling that compromising browsers was not as evil as using malware." Via the holiday card ruse, targets clicked to execute a signed Java applet that opened a reverse shell back to Lakhani and Muniz via an SSL connection.

Stage 3 focused on obtaining access to host systems through social media. There are many options to do this such as the very popular Blackhole exploit kit however we did not want to use any method that could potentially harm our target's system based on personal ethics. Blackhole is the most prevalent web threat seen today leveraging a malicious payload that we felt wasn't safe for our target's systems. We chose to use The Browser Exploitation Framework (BeEF) based on our feeling that compromising browsers was not as evil as using malware.

BeEF leverages browser vulnerabilities to assess the security posture of a target. BeEF "hooks" targets as beachheads for launching direct command modules. Different browsers have various vulnerabilities, which means the more vulnerable a browser is, the more unique attack vectors become available to the hacker. We installed Backtrack 5R3 on a server and developed a BeEF hooking server that was public facing. We tested systems by accessing our BeEF server, hooking systems and launched commands such as taking a screen shot capture. More on building a BeEF system can be found HERE.

The next step was luring employees of the target to our BeEF system. There are many methods hackers accomplish this such as offering free media sites (IE download music, movies, etc. … see more on why this is risky behavior HERE), phishing emails and fake URLs designed to look and feel like something else. We decided to post virtual holiday cards on Emily William's social media pages and direct invites to specific targets. The goal was having a user click the holiday card, wait for the card to pop up and have our system probe the browser for vulnerabilities during the waiting period. Once we hooked the target, we would look for passwords and insider information to gain access to the target agency. We launched three campaigns targeting systems during Thanksgiving, Christmas and New Years. We were able to figure out domain credentials to create an inside email address for Emily Williams, VPN passwords to gain internal access and other methods to compromise our target.

Once we hooked the target, we would look for passwords and insider information to gain access to the target agency. We launched three campaigns targeting systems during Thanksgiving, Christmas and New Years. We were able to figure out domain credentials to create an inside email address for Emily Williams, VPN passwords to gain internal access and other methods to compromise our target. Lakhani told the RSA audience that government contractors also fell for their creation's tainted holiday treats, including employees for antivirus companies.

All the while, the team's social engineering continued. Men working for the government agency gave the pretty girl special treatment. Some men offered to help Miss Williams at her new job by doing her a few favors; namely circumventing usual channels to get her a work laptop, and access to the organization's network.

Lakhani told RSA attendees that the level of access their Pygmalion obtained was higher than what a new hire would have gotten if "she" had gone through the proper channels.

Lakhani and Muniz may have angered a number of government employees, but the pair had so much success they began to receive requests from other companies and organizations to try the same test. In the RSA Deception talk this week Lakhani said, "So we also did the same type of penetration test for very large financial institutions like banks and credit card companies, healthcare organizations and other firms, and the results were almost exactly the same."

Lakhani cautioned RSA Europe attendees, "Every time we include social engineering in our penetration tests we have a hundred percent success rate."

The talk concluded with a number of recommendations for companies to follow if they want to avoid falling victim to an Emily Williams attack. Some of these are detailed in the team's post, How To Educate Your Employees About Social Engineering.

But, he opined, social engineering trainings aren't ever going to be enough if employees don't have an understanding of constant situational awareness.