CASE STUDY: GLOBAL SECURITY AWARENESS THROUGH PHISHING

Situation

Phishing is one of the easiest ways for an attacker to gain a foothold in an organization’s network. In 2017, 59 percent of RSM’s successful external network penetrations resulted from phishing, by far the largest attack vector. Recognizing the risk posed by phishing, a large manufacturing organization with a global reach contacted RSM to test its employees’ security awareness. This organization’s challenge was unique in that it required the phishing emails to be sent in English, Mandarin Chinese, German and Dutch.

Solution

After receiving a list of users to target, we conducted open source intelligence gathering on the organization to determine the best phishing pretext. Intelligence included public information from company websites, networking site profiles, open source information gathering tools and internet searches. For this particular assessment, we were tasked with sending phishing awareness emails globally. This required careful consideration of the laws and regulations of the in-scope countries. For example, both usernames and passwords are typically collected under a credential gathering pretext. However, due to Safe Harbor laws in Europe, we only collected usernames and had to assume the users also submitted their passwords.

On the following page is an example of the English version of the pretext. First the users received an email from the IT support team requesting users to verify that they could log into a new Outlook 365 portal and report any issues. This pretext was then translated into the required languages.

Once the target clicked the link, the user was directed to a RSM-owned website, which was a cloned version of the Office365 portal. After credentials were submitted, the user was taken to a training page where they were informed that they’ve just failed the assessment and what they should have seen in the email.
Results

We sent out 2,908 emails and tracked whether recipients visited the malicious site included in the phishing email, as well as whether they submitted their credentials. Those who visited the site were considered to have failed the phishing campaign, and those who submitted credentials were considered to have been compromised by the campaign. 1,026 visits were made to the malicious website and a total of 640 usernames were gathered. This represented a failure rate of 35 percent and a compromise rate of 22 percent.

Interestingly, results differed across the four in-scope countries, with Belgium surpassing the other countries in compromise and failure rates. Although the organization performed poorly globally, the results indicated that security awareness training was likely inconsistent across the enterprise.

We successfully leveraged credentials acquired via phishing to successfully compromise the organization during a concurrent external penetration assessment. Even though only one user provided credentials during penetration testing, we were able to log into the VPN with the compromised account and pivot to multiple systems, ultimately compromising a domain administrator’s account. This provided full access to the targeted domain and system access on other machines connected to the network.

The results show that phishing is a particularly serious issue for organizations with a global footprint. Organizations should take a top-down approach to security awareness. This means that an overarching policy, consistent training tools and executive buy-in should be present at an enterprise level. Department-, site- and region-specific training and procedures should be tailored to unique requirements and build on the higher-level policy.