

A User With Security Awareness Training Gets Phished

Cybercriminals disguise phishing emails to look so legitimate that even cybersecurity-educated users click on them from time to time.

THE CHALLENGE

A sizable medical organization with dozens of locations placed an ad with Indeed as it normally does when looking to hire new team members. This organization had recently become a security monitoring client of ours.

The HR department that used Indeed quite often never thought twice about opening an email from the job site as it had been a trusted source for a very long time.

On a Tuesday afternoon, our Security Operations Center (SOC) had an alert pop up on the board that a specific user at this medical organization had malicious activity spinning up on their PC.




Our security analysts began their investigation. They determined that user X received an email with a malicious link that went out to a site and downloaded a malicious file. During our investigation, we also determined that a second user received this malicious email. The email appeared to have come from a legitimate business contact at Indeed.

The file was downloaded and extracted and ran a .vbs script, which automatically called out to several suspicious IP addresses and downloaded a second executable. This malicious executable then called an outdated, and corrupted, version of a Windows process called Mobsync.exe, which beamed out to further malicious IP addresses, and created multiple scheduled tasks on the host to automatically redownload and run the malicious files if deleted.

Once downloaded and run, the process then beamed out across the network and attempted to move laterally and infect other machines. Three other hosts were infected by this activity.



FACTS OF THE CASE

-  **TYPE OF ATTACK**
Malware
-  **METHOD**
Phishing email
-  **TARGET**
Medical organization

OUR SOLUTION

The SOC proactively isolated the three infected machines from the network, banned all the hashes of the associated malicious executables to prevent execution, and halted the malicious processes. However, because of the scheduled tasks, the processes were still attempting to run. The hosts were kept in network isolation until they were remediated or reimaged.

When we pulled up the initial phishing email, it looked exactly like the typical emails Indeed would send them, and the attached resume appeared legitimate. What the user didn't know, is they got phished and the resume they opened had malware embedded in it that ultimately ran a malicious script.

ASSESSMENT & RESULTS

If the client did not have our endpoint security monitoring, this malicious file would have never been detected, and these bad actors would have most likely been able to move laterally across the customer's network, infecting them with malware. Due to the sophistication of this attack, this particular user fell victim to the phishing attack even though they had received security awareness training. Although security awareness training is one component of an overall security program, it's important that organizations take a continuous security monitoring approach that provides visibility, detection, response, and containment capabilities. Early detection is key to mitigating the damage and impact of a breach.

