Escrow Assistant Falls Victim to Watering Hole Attack

WEST, a company committed to protecting title agents, real estate professionals and lenders from cyber fraud, issued an alert for industry members to be on the lookout for watering hole attacks after an escrow assistant became the victim of one.

The escrow assistant was searching online for a subordination agreement and thought they had found a link to the needed file type. The link took them to another site at a university, where they found the zip file. The escrow assistant then downloaded the file.

"Unfortunately, the content of the zip file was not a PDF document; it was a script that attempted to contact a command-and-control server controlled by an attacker," the alert stated. "The attacker's intent was to infiltrate the network, steal information, and start a ransomware attack."

A watering hole attack tricks users within a specific industry by infecting websites they typically visit or find in industry-related searches. The websites are infected with malicious files which are commonly associated files used by the targeted industry.

Unlike other forms of escrow or real property fraud, these attackers are not targeting a specific victim. Instead, they use the watering hole to set their traps and then wait for any unsuspecting user to fall victim by opening one of these malicious files.

"Watering hole attacks have not targeted real estate and settlement services in the past, but it seems they may now be on the attackers' radar," the alert continued. "Doing random searches for business-specific templates and then clicking a link to download them is an unnecessary risk and one that could affect not just you but your entire company as well. Follow procedures, use company documentation, and be alert and aware when doing searches online. Pay attention to where you're going, what you may be clicking on, and where any links may take you."

When in doubt, one should not click on files from untrusted sources. Take the extra time to check, and then double-check, that the file is being provided by a trusted source.