Does Crime Pay?

Amateur Attack Group Offers $1M to Entice Employees

Cybercriminals try to trick employees into clinking links to infiltrate and exploit system weaknesses via phishing emails. Additionally, a new approach by a Nigerian criminal enterprise takes a more direct approach. If they cannot trick employees into clicking on links in phishing email, perhaps they can be upfront, and invite them to orchestrate the breach. This group is offering employees a cut of the ransom, initially offering as much as $1M, if employees help sabotage their employer by installing DemonWare on their network. They identify prospective employee targets using LinkedIn.

Researchers at Abnormal Security posed as prospective willing accomplice employees. The criminal group promised the prospective accomplices they would not be caught by their employer because the ransomware would encrypt everything on the system. They instructed them to launch the ransomware physically or remotely and provide two links for an executable file that could be downloaded on WeTransfer or Mega.nz. The criminal group also provided an Outlook email account and Telegram username for the employee to contact them as needed. The researchers determined, “Based on the actor’s responses, it seems clear that he 1) expects an employee to have physical access to a server, and 2) he’s not very familiar with digital forensics or incident response investigations.”

The criminal group claims to have coded the ransomware themselves but DemonWare is freely available from GitHub, placed there by its original author to demonstrate how easy ransomware is to make and use, and is considered one of the least sophisticated forms of ransomware. DemonWare has been around for a few years and was tied to the groups that attacked Microsoft Exchange’s ProxyLogon set of vulnerabilities, CV#-2021-27065, discovered in March.

There are five fundamental types of insider threats:

1. Non-responders to awareness training;
2. Inadvertent insiders;
3. Insider collusion such as with vendor partners;
4. Persistent malicious insiders; and
5. Disgruntled employees.

And, now add 6. Accomplice employees – cash strapped employees and/or employees looking for a quick buck.