"This Phishing Email Is Pushing Password-Stealing Malware to Windows PCs"

Submitted by grigby1 on Mon, 06/07/2021 - 2:43pm

Researchers at Fortinet have released details about a phishing campaign that delivers a new variant of Agent Tesla, which is one of the oldest forms of Remote Access Trojan (RAT) malware. The new Agent Tesla campaign aims to steal usernames, passwords, and other sensitive information, in addition to cryptocurrency, from victims. Agent Tesla focuses on stealing sensitive information from compromised Windows machines through the use of keyloggers that send what the victim is typing to the attacker, thus allowing them to see usernames, passwords, and more. According to the researchers, the new Agent Tesla campaign distributes an updated version of the malware via phishing emails designed to look like business emails. One email asks the user to open a Microsoft Excel attachment titled "Order Requirements and Specs." The attachment has a macro that initiates a process, which downloads and launches Agent Tesla. This is done through various stages, including downloading PowerShell files, running VBScript, and more, to help conceal the installation of Agent Tesla and allow the attacker to monitor activity on the infected machine. The researchers found that this new version of Agent Tesla pings the operator every 20 minutes, sending any newly detected input. The attack also hijacks any Bitcoin wallet on the victim's machine. The attacker can find a valid Bitcoin address by monitoring activity on the infected machine and abusing the PowerShell code. Once the attacker spots the valid Bitcoin address, the code modifies the address and changes it to the one owned by the attacker. This article continues to discuss the new Agent Tesla phishing campaign and why this RAT malware remains popular among cybercriminals.

ZDNet reports "This Phishing Email Is Pushing Password-Stealing Malware to Windows PCs"