INFOSTEALERS – PREDECESSOR TO RANSOMWARE ATTACKS

BY JAY BORDEN

What is an infostealer? It is malware designed to gather private information from any device and send it to cybercriminals.

Why are infostealers so dangerous? The information captured and sent is usernames, passwords, customer files, bank accounts, and everything else you consider private and want to protect.

That information provides access to the accounts and applications. It provides access to the company or organization network where the malware can spread laterally, to everyone else on the network, where more information is stolen, and malware is spread. That malware may be ransomware.

Infostealers are typically installed by an Initial Access Broker, IAB. These are individuals or groups that make the first penetrations into a company or organization and then sell or rent the access they gained to other criminal groups who then install other malware including ransomware. Each group does what they do best.

Infostealers preceded ransomware in about one-third of reported ransomware attacks. This is significant. If you know the infostealer is there, passwords can be changed along with other specific actions rendering the stolen information useless. That can protect against malware and ransomware infections.

Ransomware, to be effective, has to operate behind the scenes until activated. That is how it is spread to so many devices and servers on the network. Ransomware encrypting information on one or two devices won't accomplish the purpose. It must spread as far and wide as possible before springing. The further it spreads the more devices are encrypted and the better the leverage the attackers have in convincing you to pay the ransom.

INFOSTEALERS – PREDECESSOR TO RANSOMWARE ATTACKS

CONTINUED

How to stay safer?
The first step is knowing infostealers are there. Then change passwords and disable session cookies. Be sure to have up-to-date, immutable backups. In the event of a successful ransomware attack that allows everything to be restored without paying the ransom. What is an immutable backup? It is one that cannot be changed or edited. This prevents ransomware from encrypting it. Backups are a prime target for ransomware attackers because without a secure, up to date backup that has not been encrypted by the attackers you have little choice but to pay the ransom.

Changing passwords and backing everything up only works if you know the attack may be coming. Time is your friend.

Even if the attack is not ransomware, the infostealer and the access it provides will not result in anything good for a company. The Initial Access Broker will sell the access afforded by the infostealer to any other attacker that pays their price. The result will be other types of malware, viruses, Remote Access Trojan, RAT, and others. Whichever the attack type, if successful, it will cause damage.

Many companies looked at by One Brightly Cyber have multiple instances and multiple types of infostealers on their devices. Having one infostealer is bad enough; more are worse. Knowing it is there is the first step in defusing it.

One Brightly Cyber can find the infostealers and compromised passwords and Personally Identifiable Information, PII, typically months or more before other services. Don't know what to do next? OBC gives the steps to take. We also have real US-based people with extensive experience available for guidance and to help in case of a successful cyberattack.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.