Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:26:03 UTC

Description(IBM) Though well-known and familiar from previous online fraud attacks, QakBot continually evolves. This is the first time IBM X-Force has seen the malware cause AD lockouts in affected organizational networks.

Although part of QakBot is known to be a worm, it is a banking Trojan in every other sense. QakBot is modular, multithread malware whose various components implement online banking credential theft, a backdoor feature, SOCKS proxy, extensive anti-research capabilities and the ability to subvert antivirus (AV) tools. Aside from its evasion techniques, given admin privileges, QakBot’s current variant can disable security software running on the endpoint.
