Threat Intelligence Report

Widespread Exploitation of VPNs lacking MFA

Issue #401

Executive Summary: Virtual Private Networks (VPNs) are an extremely popular tool among small businesses and enterprises alike to allow employees to remotely access company data and applications.

To log in to the VPN, a username and password must be entered – however security experts from the private sector and government alike warn this is not sufficient to protect sensitive data and applications from intruding criminal/hacking enterprises. Multi-Factor Authentication (MFA) is recommended to ensure that username and password alone don't grant access.

The Big Deal: VPNs are internet-exposed devices.

That means even if a criminal/hacker was not directly aware of your company, they can find you using tools that scan the internet for VPNs to target. The Shodan Search Engine, https://www.shodan.io, is a popular legal platform that researchers – and criminals/hackers unfortunately – use to perform searches for internet-connected devices such as VPNs.

Famous Last Words: "We're a small company"… just small enough to suffer in silence.

While the constant intrusions into hospitals, cities like Dallas and Oakland, big casinos, and health insurers are going to grab the headlines, for every one of them, there are thousands of small and mid-size businesses being victimized. To the point above, you can be targeted by your internet-exposed device before a threat actor even knows your company's name.

Why are Attackers succeeding:

- Humans like to re-use passwords.
- So many data breaches have occurred that there is a surplus of exposed credentials.
- Sometimes very easy-to-guess or default passwords are created or left on mission-critical infrastructure (username: "Admin" password: "Admin" is a common one).
- Attacks are automated.

The Bottom Line: Whether you consider yourself a small, mid-size, or large company, recognize that a username and password alone on a VPN are not enough to secure your business data. Implement MFA.

If This Sounds Familiar: Back in 2021 a cyber event that gained widespread US attention was the hack of the Colonial Pipeline which sent gas prices soaring along the East Coast. Digital Forensics showed that this hack occurred due to a VPN account that didn't use MFA.[1] Fast forward three years to 2024, and these attacks are still happening at scale.

Most Prolific Threat Actor Currently Known for This Attack: Akira Ransomware[2]

Mini-Profile: Akira Ransomware[3] *(screenshot from threat actor dark webpage below)*

- Akira surfaced in mid-2023, but analysis of the cryptocurrency wallets that receive payments from victims suggest these are long-time criminals associated with Conti – the most prolific ransomware threat of 2022 until disbanding and re-branding.[4]
- Extortion demands often surpass $1,000,000.[5]
- Out of the different extortion types (data theft with blackmail; encryption to block access to systems; denial of service attacks on website/e-commerce platforms; harassment), they are most known for data theft with blackmail and encryption to block access to systems.

Just a little bit technical: Attacks automated by software trend in two directions: trying many usernames/passwords against one device/website/application is known as brute-forcing. Alternatively, taking one set of username/password that was found or purchased illicitly and trying that out against many devices/websites/applications is known as credential stuffing. Both types of attacks are highly effective and damaging when MFA is not in place.

1, Colonial Pipeline Hacked Via Inactive Account Without MFA - https://www.crn.com/news/security/colonial-pipeline-hacked-via-inactive-account-without-mfa

2. Akira Ransomware Targeting VPNs without Multi-Factor Authentication - https://www.helpnetsecurity.com/2023/08/31/ransomware-cisco-vpn/

3. Akira Ransomware is "bringin' 1988 back" - https://news.sophos.com/en-us/2023/05/09/akira-ransomware-is-bringin-88-back/

4. Blockchain data shows Conti gang tied to Akira and spate of ransomware attacks - https://www.scmagazine.com/news/blockchain-conti-akira-ransomware

5. Ransomware Spotlight Akira - https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-akira