CRITICAL FINDINGS: VPN CYBER POSTURE

A glance into the cyber hygiene of VPN's while remote working tools are on the rise

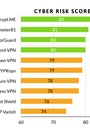
BLACK KITE

OVERVIEW

As the COVID-19 pandemic spreads worldwide, more workplaces are embracing remote working options. This model increases attention to ***third-party*** *SAAS, in which businesses leverage to keep operations up and running in this unanticipated climate.*

Here, Black Kite identifies select company's digital footprint based on their commercially facing domain and revealing the associated vulnerabilities, as the use of remote working tools ramps up with the outbreak of COVID-19.

Cyber Scores of Top Ten VPNs



We made a list of Top Ten business VPN solutions based on the CNET, PCMag and Tech Radar. Taking this list, we assessed the external security health of each company's digital footprint based on their commercially exposed domain.

METHOD

PROCESS

We started the process by entering the domain names for each VPN. Based on that domain name, we are/were able to derive a comprehensive digital footprint of the company including all the related domains, subdomains, IP addresses , services, emails, etc..

PLATFORM

Black Kite's platform aims to provide full visibility into a cyber ecosystem. It enables enterprises to continuously assess third-party risks, assigns a letter grade to each vendor, correlates findings with industry standards to inform compliance requirements, and determines probable financial impact if a third-party experiences a breach.

REASONING

Relying on VPN for company security is a common mistake among employees. Human element is still the weakest link and thus the first line of defense in cyber security. With an increased number of phishing attacks targeting credentials these days, employees should be vigilant about their sensitive information when accessing company's resources remotely.

CATEGORY AVERAGES

Lowest Category Scores

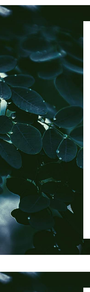
Of 19 categories analyzed, **Patch Management (72.4) and Website Security (74.8)** were the lowest scored categories on average. Not far behind were **Fraudulent Domains & Apps**.

For **Patch Management**, Black Kite's risk scoring engine collects details related to the version number of the systems and software from internet-wide scanners like Censys, Shodan, Zoomeye etc. Out-of-date systems accessible from the Internet may have vulnerabilities, either related to the application servers or the application framework. The vulnerabilities can be design flaws or implementation bugs, which enable attackers to compromise applications or potentially the entire system. Hackers particularly look for weak links in company cyber defenses, including one of the easiest targets - obsolete systems. Successful exploitation may result in loss of data, reputation, credibility, or cause financial problems.

Website Security is a special analysis of the company's main website. The findings in this category are collated from the SSL/TLS Strength, Patch Management, Application Security, Web Ranking, and Brand Monitoring findings and blended together to give an overall score for the website related digital assets.

Fraudulent, private mobile, or desktop applications are used to hack or phish employee or customer data. This category searches for possible fraudulent or pirate mobile or desktop apps on Google Play, App Store and pirate app stores.

CATEGORY AVERAGES



Black Kite's **3D Vendor Risk @ Scale ™** platform provides easy-to-understand letter grades in each risk category. Here, we see the average weighted cyber score of our Top Ten VPN list is "C+".

Of the ten VPNs, six received "C" grades, while the remaining four received a grade of "B". The Black Kite platform delivers the distribution of vendors according to their grades, which provides insight into the security posture.

Most Common Issues

CRITICAL FINDINGS

DNS Amplification

As the most extensive vulnerability, DNS amplification attacks are orchestrated when the attacker instructs bots or a botnet to send DNS queries with a forged source address to a legitimate server. This type of attack results in a large response sent back to the attacker's victim, the real owner of the forged address. The process typically involves an attacker sending a DNS name search request to a public DNS server, spoofing the source IP address of the targeted victim.

Remediation: Common ways to prevent or mitigate the impact of DNS amplification attacks include tightening DNS server security, blocking specific DNS servers or all open recursive relay servers, and rate limiting.

CRITICAL FINDINGS

Invalid, Incorrect, Expired or Self-Signed SSL Certificates

Although 2nd in our list, SSL Certificates are by far the most frequent and critical issue we discovered on the digital assets of VPNs. SSL protocol makes sure information travels safely through the Internet in a secure manner if the certificate is trusted. This process helps prevent an ill-intentioned individual from sniffing the network to steal confidential information, such as users' credentials. Especially in a cloud VPN architecture, lacking SSL controls on servers puts a company's assets such as corporate data, employee credentials, and other sensitive information at risk.

Remediation: There are many reasons for an SSL certificate to become invalid: (1) It is revoked (2) It is self-signed (3) Certificate chain is broken (4) The domain specified in the certificate does not match the website (4) Certificate time violation. Mitigate the reason(s) those apply to the system.

CRITICAL FINDINGS

Publicly Available SMB Service

SMB port (Port 445) related vulnerabilities are one of the most frequently found security issues on networks around the world. Over the years, there have been many security vulnerabilities in Microsoft's implementation of the protocol or components on which it directly relies. Real-time attack tracking shows SMB as one of the primary attack vectors for intrusion attempts, such as the 2014 Sony Pictures attack and the WannaCry ransomware attack of 2017.

Remediation:
(1) Blocking 445 at the external firewall is relatively easy and solves many problems.
(2) Disable SMBv1
(3) If possible, block all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all external boundary devices.

The Black Kite (formerly known as NormShield) platform's intuitive interface compiles reports and communicates risks in qualitative, quantitative, and easy to understand business terms for executives. The interface also allows IT-security teams to drill down to the technical details in each risk category.

With the alerting mechanism, the users of the platform become aware of the security vulnerabilities within a cyber ecosystem promptly and can take immediate actions.

WWW.BLACKKITETECH.COM