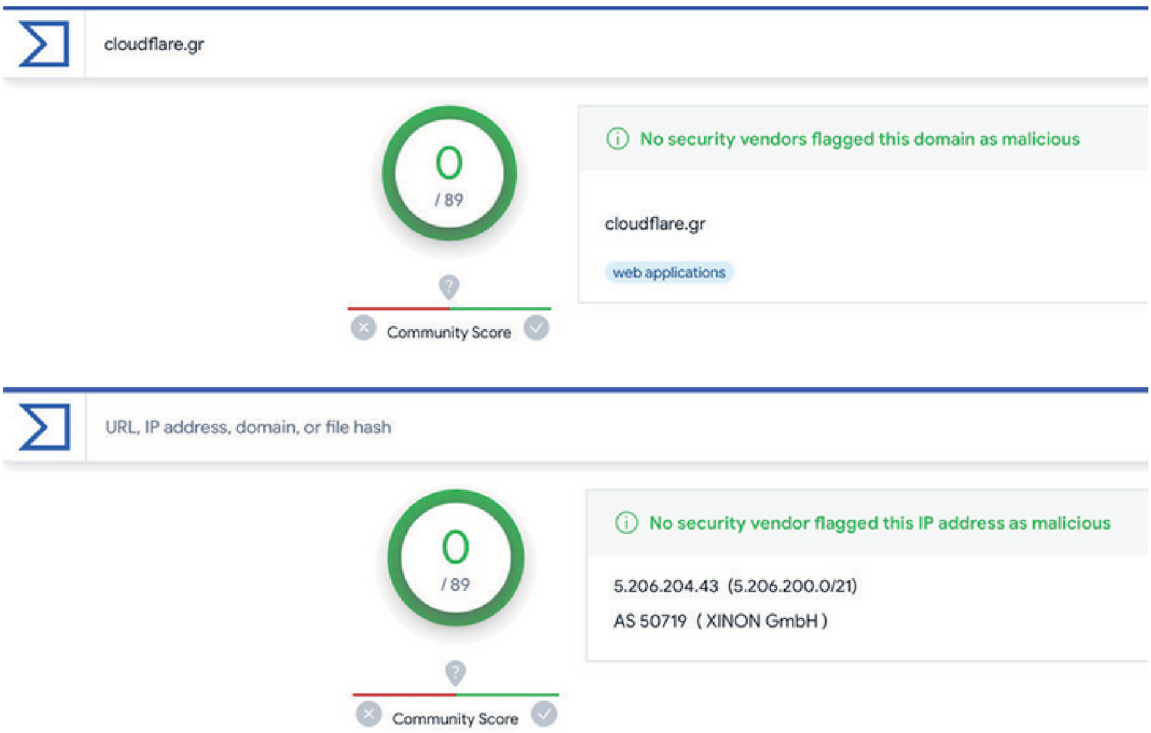
# Warum Domain-basierte Blacklists im Jahr 2024 versagen werden

BlueShield

In der sich ständig im Wandel befindlichen Landschaft der Cybersecurity sind Domain-basierte Blacklists ein weitverbreitetes Werkzeug, um Nutzer vor gefährlichen Inhalten zu schützen. Allerdings zeigen die Cyberangriffe der letzten Jahre den auf Blacklists basierenden Methoden eindeutig ihre Grenzen auf. Ein aktuelles Beispiel hierfür ist die Domain *cloudflare.gr,* die mit der IP-Adresse *5.206.204.43* verbunden ist – eine Adresse, die auch von der Domain *webex.ws* genutzt wird.

Besonders hervorzuheben ist hierbei: Während **Cloudflare-Domains** für gewöhnlich auf Cloudflare-eigenen Nameservern gehostet werden, verweisen die Nameserver von *cloudflare.gr* ungewöhnlicherweise auf *ns3.kasserver.com sowie ns4.kasserver.com.* Es existieren tausende maschinengenerierte Subdomains, hinter denen sich der C&C-Kanal von Malware vermuten lässt.

105947b6.service.protection.cloudflare.gr (Check)
105947b6.session.protection.cloudflare.gr (C&C Session)



Die **Solarwinds Malware** zeigte ein ähnliches Verhalten auf ihren Domains. Trotz dieser Ungewöhnlichkeiten hat eine Überprüfung durch **VirusTotal** gezeigt, dass sowohl *cloudflare.gr* als auch ihre IP-Adresse(n) als sicher eingestuft werden. Dies wiederum bedeutet, dass andere Sicherheitsanbieter ihre Nutzer NICHT vor dieser potenziellen Bedrohung schützen!

## Die Whitelist-Strategie von Blue Shield Umbrella

An diesem Punkt kommt die **Whitelist-Strategie** von Blue Shield Umbrella ins Spiel, welche sich als einzige effektive Lösung für dieses Problem herausstellt. Im Gegensatz zu herkömmlichen Blacklist-basierten Methoden, bei denen Domains und IP-Adressen erst nach Bekanntwerden von Missbrauch gesperrt werden, wird Blue Shield solche verdächtigen Domains oder IP-Adressen **nie** auf Ihre Whitelist setzen. Dadurch bietet Blue Shield Umbrella einen **proaktiven Schutz,** der seine Nutzer wirksam vor solchen Gefahren bewahrt.

Dieses aktuelle Problem mit *cloudflare.gr* ist allerdings nur die Spitze des Eisbergs. Um sich ausreichend für die Zukunft vorzubereiten und in einem anhaltenden Internet-Cyberkrieg vor Datenverlust und unbefugten Zugriffen sicher zu sein, erweist sich Blue Shield als unverzichtbar und alternativlos.

Mit seinem fortschrittlichen, auf Whitelist-basierenden Ansatz schützt Blue Shield seine Nutzer effektiv gegen die vielfältigen und sich ständig weiterentwickelnden Bedrohungen im Internet. In einer Zeit, in der herkömmliche Sicherheitsmaßnahmen nicht mehr greifen, ist Blue Shield die entscheidende Verteidigungslinie im Kampf um Sicherheit und Authentizität im Internet.

Dank seiner innovativen Technologie und der kontinuierlichen Überwachung von Netzwerkaktivitäten ist Blue Shield in der Lage, verdächtige Aktivitäten in Echtzeit zu erkennen und zu blockieren. Die Whitelist-Technologie ermöglicht es, nur vertrauenswürdige Anwendungen und Websites zuzulassen, während potenziell gefährliche oder unsichere Inhalte blockiert werden. Das sorgt für ein höheres Maß an Sicherheit und Schutz vor Malware, Phishing-Angriffen und anderen Bedrohungen.



BlueShield