Best Practices
Mit DNSWatch Phishingversuche wirksam verhindern

Thomas Fleischmann
Senior Sales Engineer

Thomas.Fleischmann@watchguard.com

Die Herausforderung

Cyber-Angriffe finden häufig sehr gezielt statt.

Der Mensch ist im Fokus!

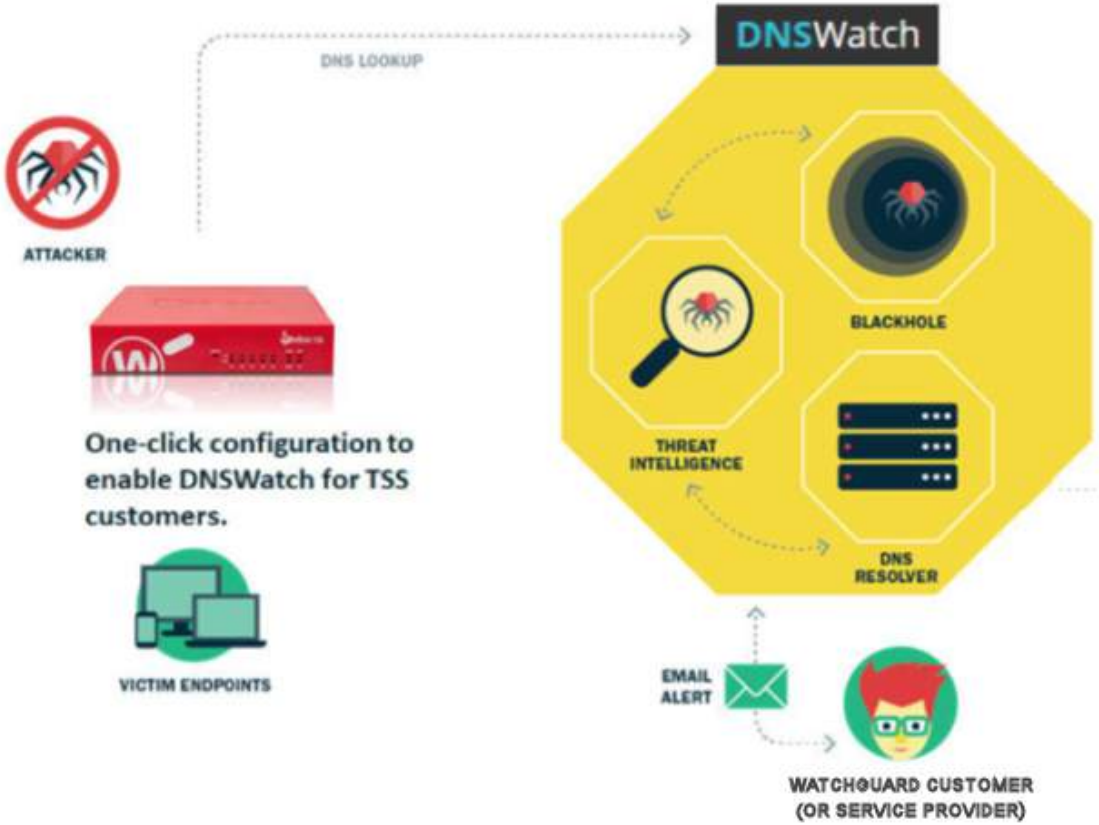
Happy Clickers

Spearphishing

CEO Fraud

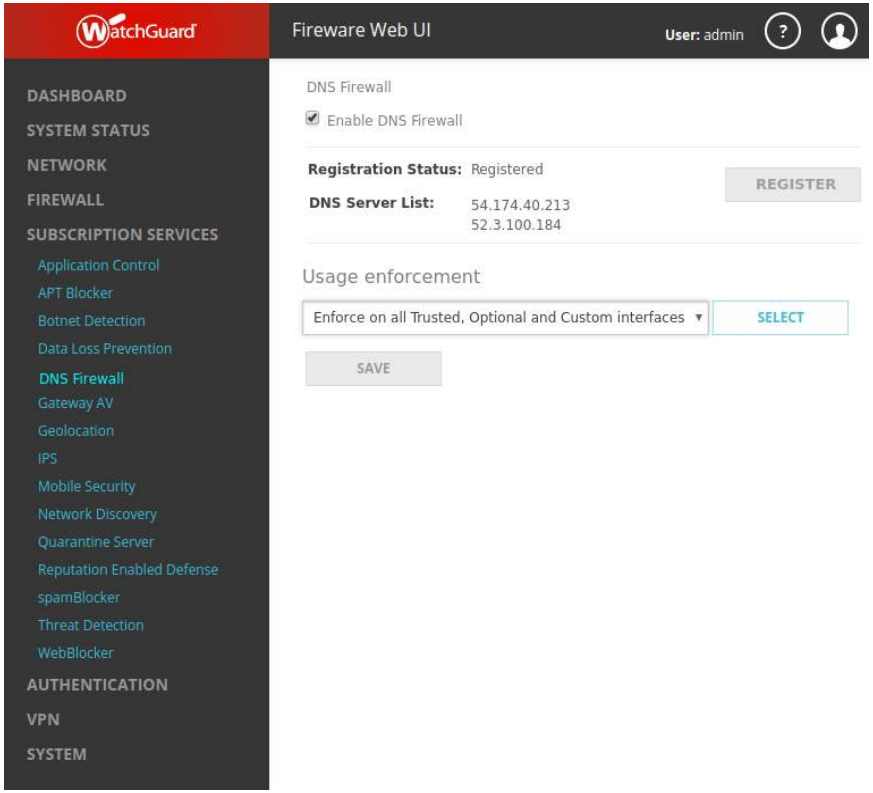
DNSWatch schützt wirkungsvoll vor Phishing

Cloud-based DNS filtering solution

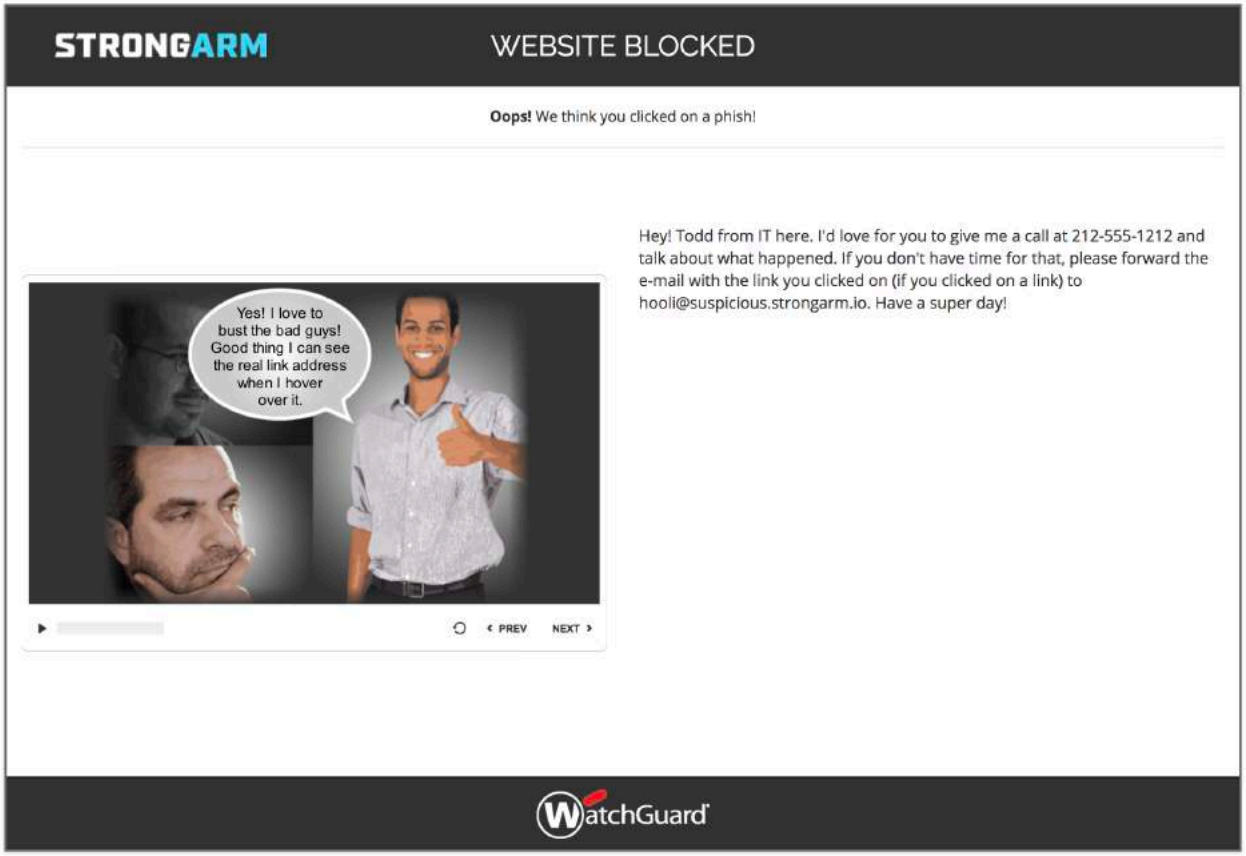


Zusätzliches Security-Layer

- Einfach implementiert
- Verhindert Angriffe auf Domain-Name Basis
- Wirkungsvoll für alle Protokolle und Ports
- Schützt auch ohne Einsatz von Proxies



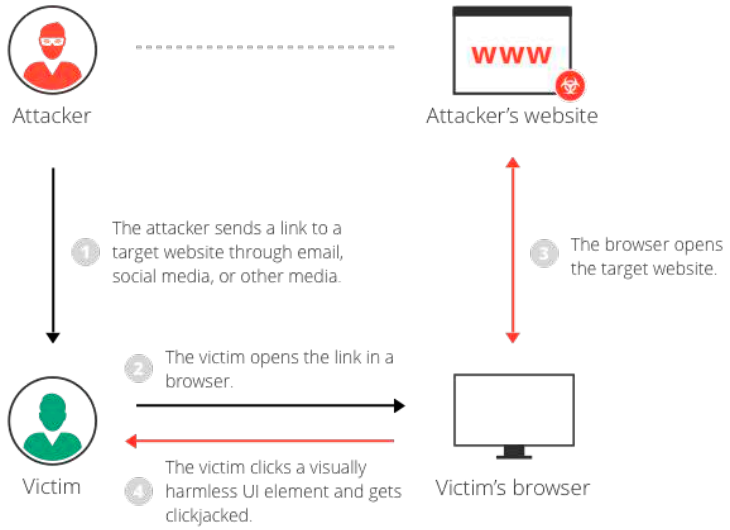
Phishing Education



DNSWatch Overview

- DNSWatch ist ein neuer Service für Firebox-Appliances, der DNS Anfragen überwacht, um Verbindungen zu schädlichen Domains zu verhindern.

- DNSWatch schützt vor schädlichem “Clickjacking” und ”Phishing” – unabhängig von verwendetem Protokoll, Port und der Art des Endgeräts.



DNSWatch Overview

- DNSWatch steht ab Fireware v12.1.1 zur Verfügung.
- DNSWatch ist als Funktion in WatchGuard's Total Security Suite integriert.
- Unterstützt von: Firebox T Series, M Series, XTMv, FireboxV und Firebox Cloud.
  - Firebox im Bridge-Mode unterstützt DNSWatch nicht.

DNSWatch Übersicht

- DNSWatch Komponenten:
  - Threat Intelligence — beständig aktualisierte Feeds über schädliche Domains.
  - DNS Resolver — Löst DNS Anfragen auf
  - Blackhole — Ziel der Anfragen zu schädlichen und geblockten Domains
  - Dashboard — cloud-based management
  - Firebox — leitet DNS Anfragen an DNSWatch weiter.

DNSWatch und Firebox

- DNSWatch kann Verbindungen zu schädlichen Domains früh und vor anderen Sicherheitsfunktionen stoppen.

- Ein neues zusätzliches Security Layer für Datenverkehr über Proxy- und Packetfilter Regeln.

- DNSWatch schützt Nutzer, deren DNS anfragen über die Firebox geleitet werden.

DNSWatch und Firebox

- DNS Anfragen von Systemen, welche durch eine Firebox geschützt sind, werden an DNSWatch weitergeleitet.
- DNSWatch prüft, ob diese Domain eine Gefahr darstellt.
  - *Ist die Domain keine Gefahr*:
    - DNSWatch löst die DNS Anfrage regulär auf
  - *Stellt die Domain eine Gefahr dar*:
    - DNSWatch beantwortet die DNS Anfrage mit der IP-Adresse des DNSWatch Blackhole Systems.
    - DNSWatch sammelt weitere Informationen über die gefährliche Anfrage des zugreifenden Clients.
    - Bei HTTP und HTTPS Anfragen, DNSWatch leitet den Zugriff auf eine flexible anpassbare Deny-Page um.

DNSWatch Threat Intelligence

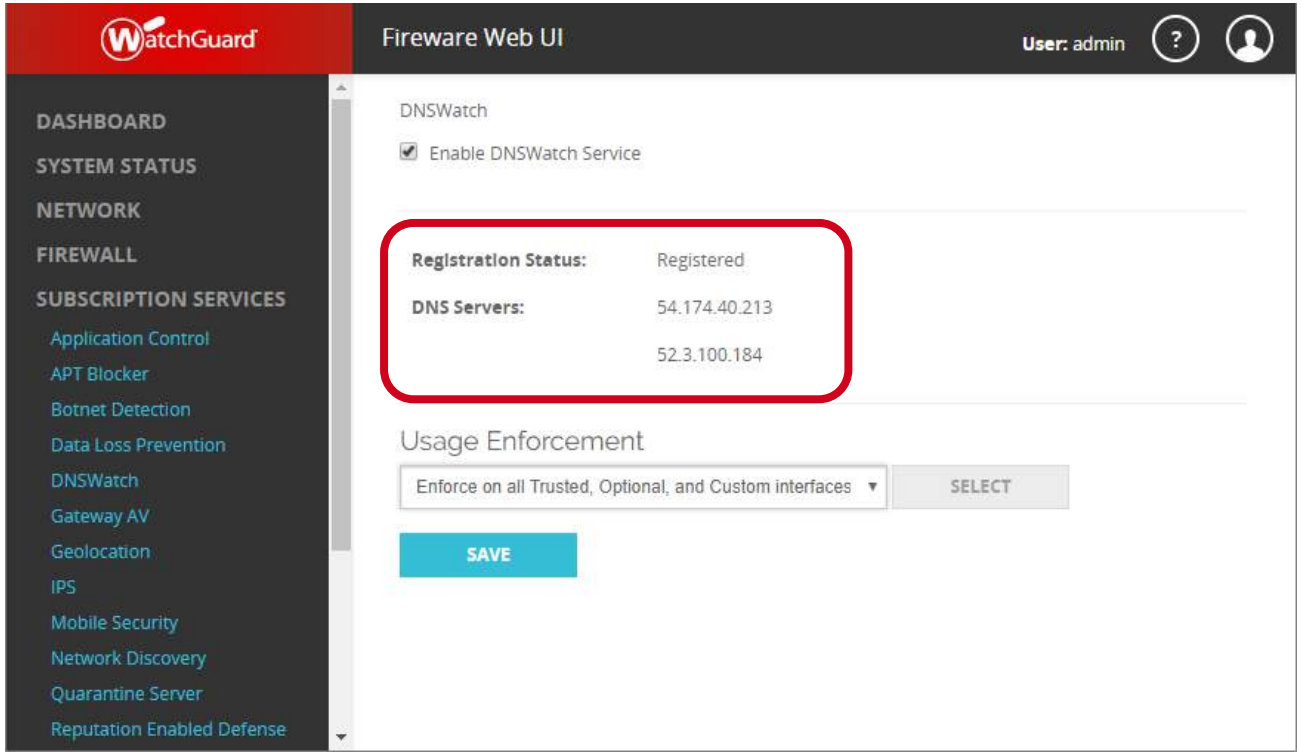
- WatchGuard verwendet Heuristik und weitere Analysemethoden, um schädliche Websites und Zertifikate zu erkennen.

- DNSWatch ruft täglich zusätzliche “Threat-Feeds” ab, um neueste Informationen zu schädlichen Domains zu integrieren.

- DNSWatch Nutzer können auch manuell geblockte Domains mit WatchGuard teilen, um dadurch den Dienst DNSWatch zu unterstützen.

Enable DNSWatch on the Firebox

- Nach Aktivierung kann der Status der Registrierung mit den DNSWatch Systemen in der Fireware Web UI eingesehen werden.
- Select **Subscription Services > DNSWatch**

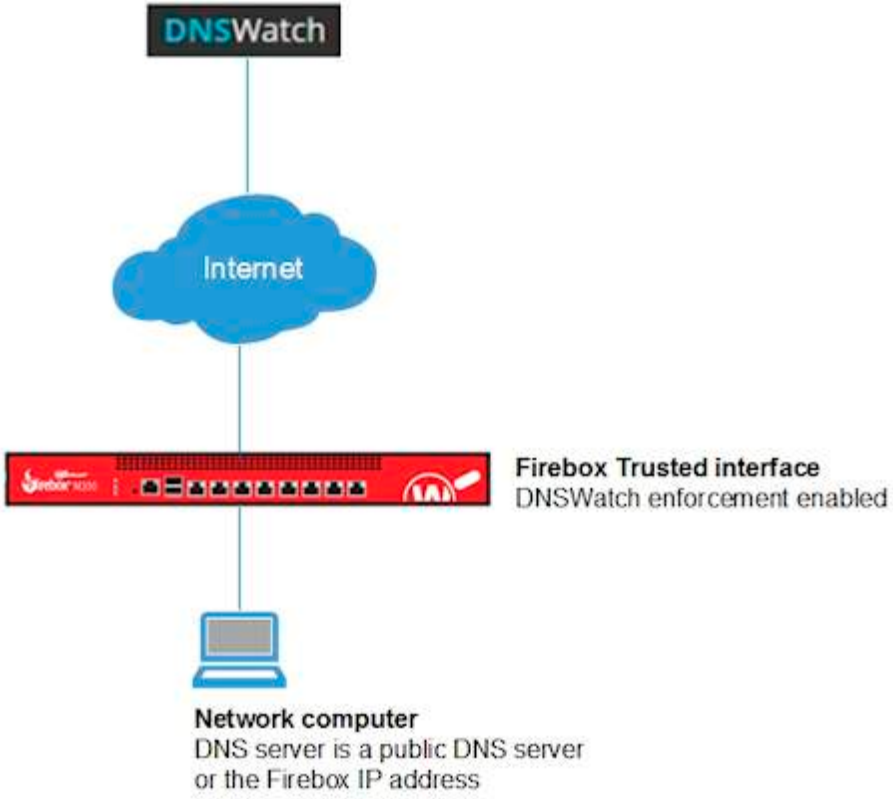


DNSWatch Usage Enforcement

- Die Option **Usage Enforcement**
  - Nutzen Sie *Usage Enforcement*, wenn in der Firebox Konfiguration keine **internen/lokalen** WINS/DNS Server eingetragen sind
    - Durch *usage enforcement* werden alle ausgehenden DNS Anfragen an DNSWatch geleitet, auch wenn ein Client oder Server einen spezifischen DNS Server nutzt.
  - *Disable enforcement* sollte genutzt werden, wenn ein lokaler DNS Server in der Firebox WINS/DNS Konfiguration verwendet wird.
    - Ist *usage enforcement* deaktiviert, werden ausgehende DNSWatch weiterhin an die in Clients/Servern konfigurierten DNS Server geleitet.

DNSWatch Netzwerkintegration

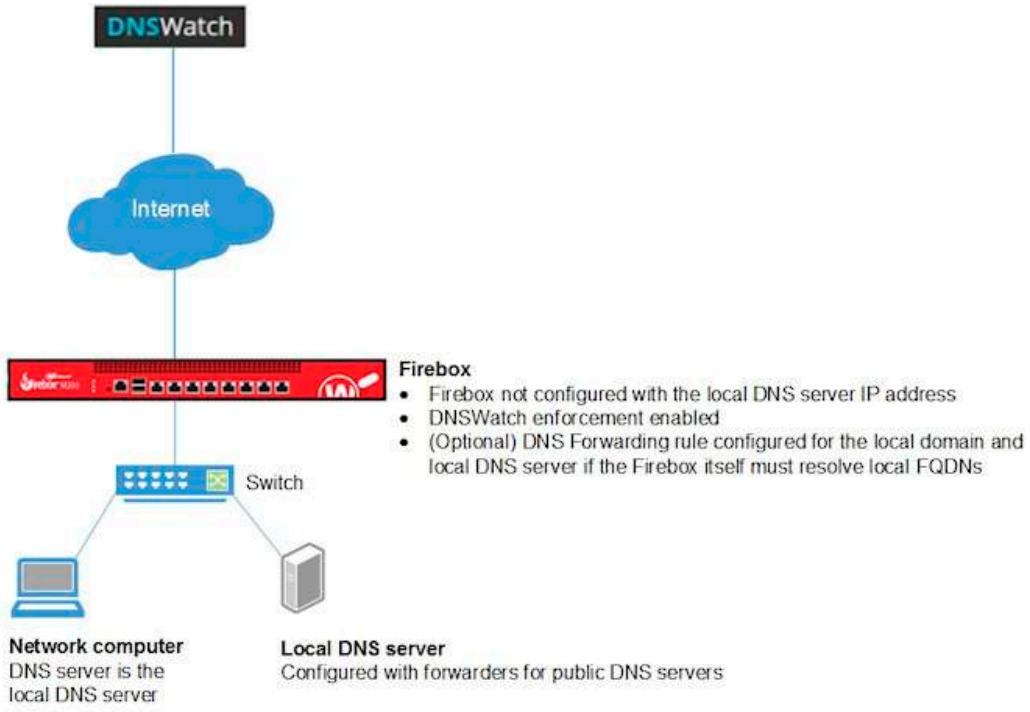
- Beispiel 1 — Netzwerk ohne lokalen DNS Server



Aktivieren Sie in den DNSWatch-Einstellungen die *Usage Enforcement*. Wenn *Usage Enforcement* aktiviert ist, überwacht die Firebox den Verkehr von Port 53 in Ihrem Netzwerk. Die Firebox leitet alle ausgehenden DNS-Anforderungen von Ihrem Netzwerk an DNSWatch weiter, auch wenn Hosts in Ihrem Netzwerk manuell mit verschiedenen DNS-Servern konfiguriert sind.

DNSWatch Netzwerkintegration

- Beispiel 2 — Netzwerk mit einem lokalen DNS Server
  - DNS Server der Firebox sind **nicht** die lokalen DNS Server

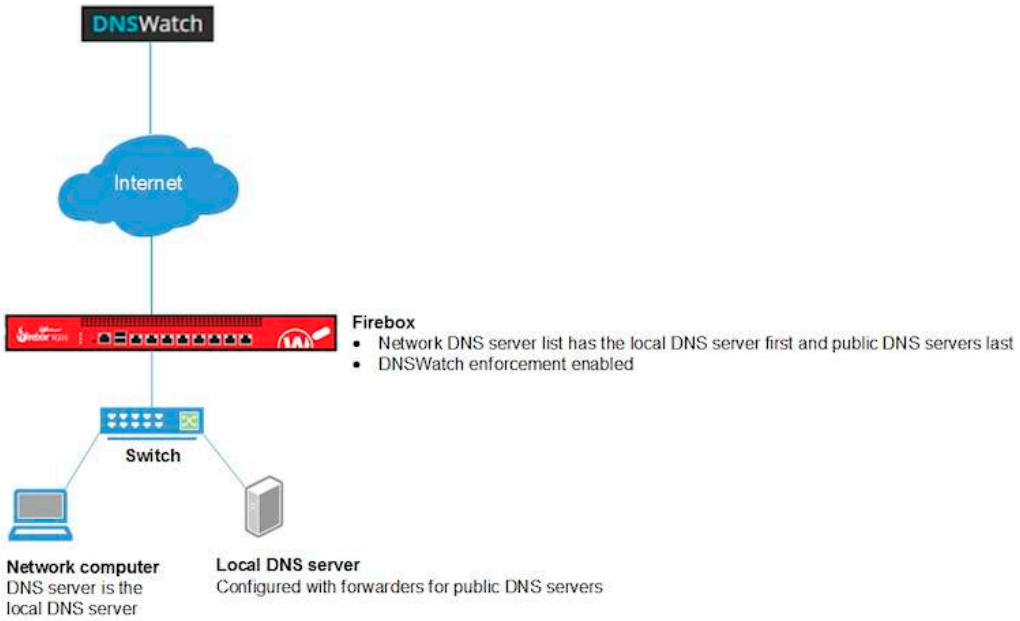


DNS-Anforderungen für interne Ressourcen
Wenn ein Host in Ihrem Netzwerk eine DNS-Anforderung für eine interne Ressource in Ihrem Netzwerk sendet, löst der lokale DNS-Server die Anfrage auf.
Wenn die Firebox selbst eine Anforderung für eine lokale Ressource im Netzwerk von beispiel.com generiert, verwendet die Firebox die von Ihnen für beispiel.com konfigurierte DNS-Weiterleitungsregel, um die Anforderung an den lokalen DNS-Server weiterzuleiten.

DNS-Anforderungen für externe Ressourcen
Wenn ein Host in Ihrem Netzwerk eine DNS-Anforderung für eine externe Ressource sendet, leitet der lokale DNS-Server die Anforderung an die öffentlichen IP-Adressweiterleitungen weiter, die auf dem Server konfiguriert sind. Da jedoch die DNSWatch *Usage Enforcement* aktiviert ist, wird die Anfrage von der Firebox durch zwischengespeicherte Informationen aufgelöst oder an DNSWatch weitergeleitet.

DNSWatch Netzwerkintegration

- Beispiel 3 — Netzwerk mit lokalem DNS Server
  - DNS Server der Firebox sind die lokalen DNS Server



DNS-Anforderungen für interne Ressourcen
Wenn ein Host in Ihrem Netzwerk eine DNS-Anforderung für eine interne Ressource in Ihrem Netzwerk sendet, löst der lokale DNS-Server die Anfrage auf.

Wenn die Firebox selbst eine Anforderung für eine lokale Ressource generiert, leitet der Firebox-Resolver die Anforderung an den lokalen DNS-Server weiter.

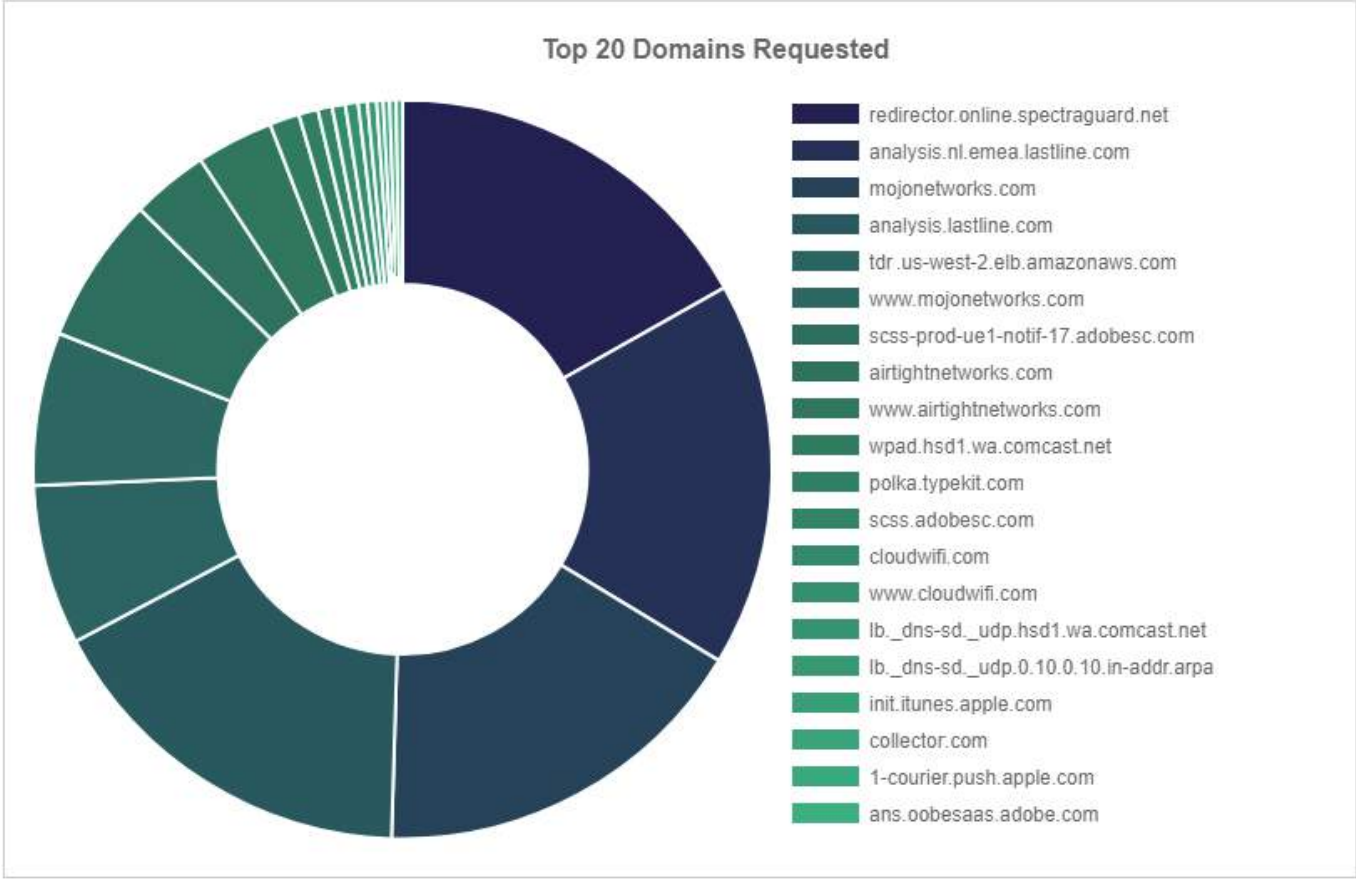
DNS-Anforderungen für externe Ressourcen
Wenn ein Host in Ihrem Netzwerk eine DNS-Anforderung für eine externe Ressource sendet, leitet der lokale DNS-Server die Anforderung an die öffentlichen IP-Adressweiterleitungen weiter, die auf dem Server konfiguriert sind. Da jedoch die DNSWatch *Usage Enforcement* aktiviert ist, wird die Anfrage von der Firebox durch zwischengespeicherte Informationen aufgelöst oder an DNSWatch weitergeleitet.

DNSWatch Configuration Examples

- Networks with a local DNS server
- Networks without a local DNS server
- Mobile VPN configurations
- Multiple internal networks
- BOVPN configurations

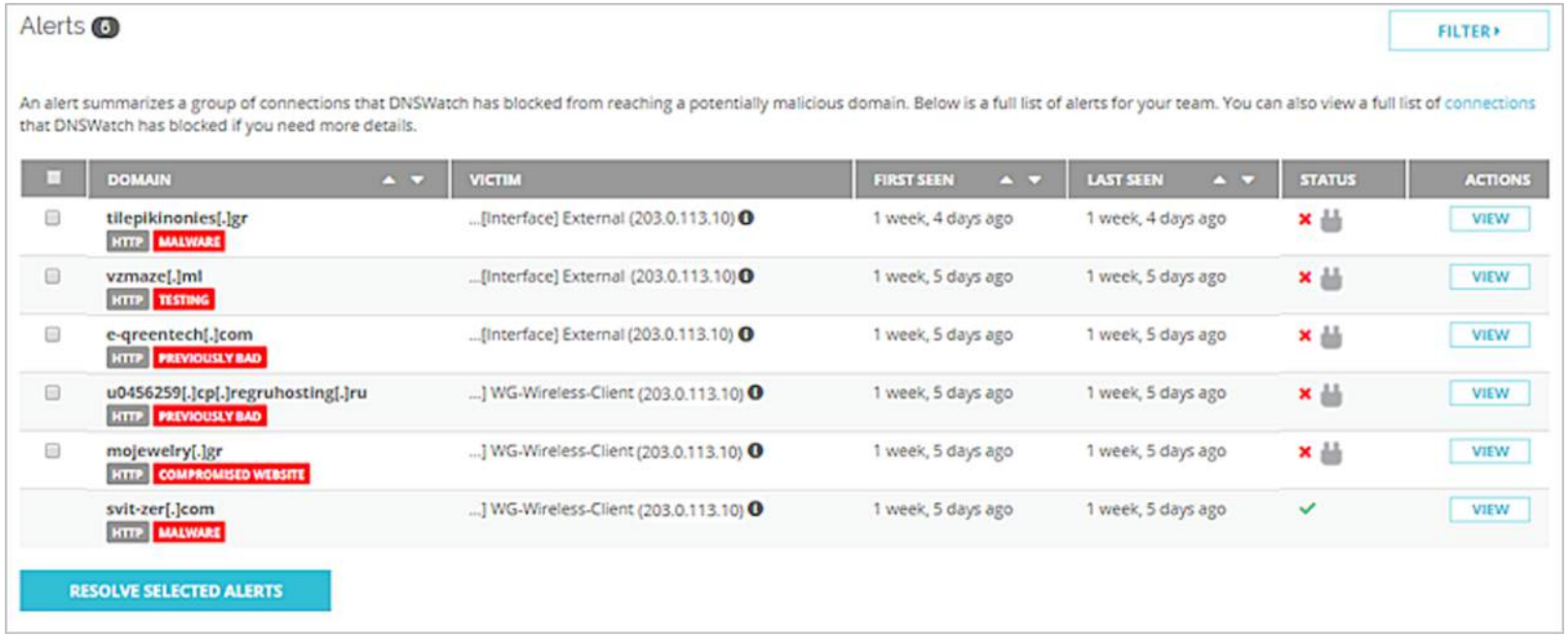
https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/services/dnswatch/dnswatch_config_examples_c.html

DNSWatch Reporting



DNSWatch Alerts

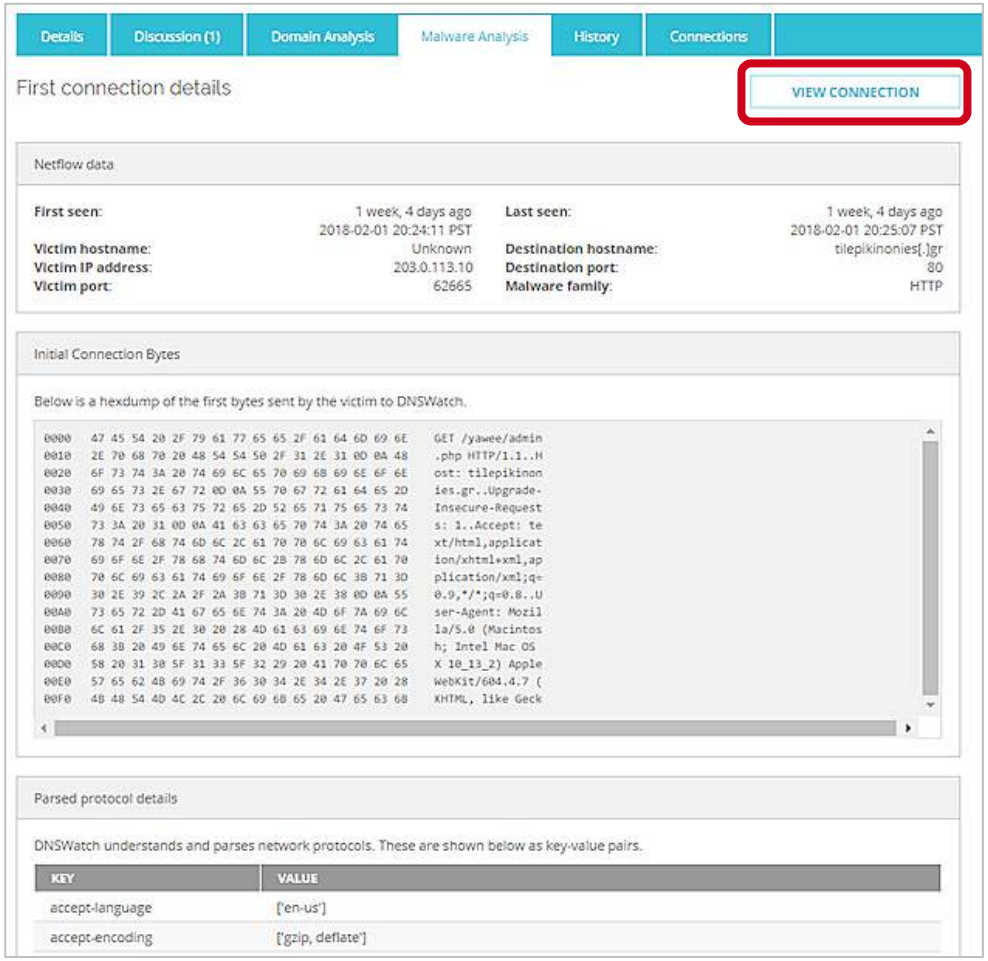
- Alerts stellen die festgestellten Zugriffsversuche auf schädliche Domains dar, die DNSWatch verhindert hat.



DNSWatch Alert Details – Malware Analysis

- Details zu von DNSWatch festgestellten Gefahren werden dargestellt.

- weitere Details sind über “View Connection” sichtbar.



Direkte Kommunikation

Todd O'Boyle commented 12 months ago — Strongarm Support Team

Hey, this infection looks serious! We've got the malware contained so you don't have to worry about that.

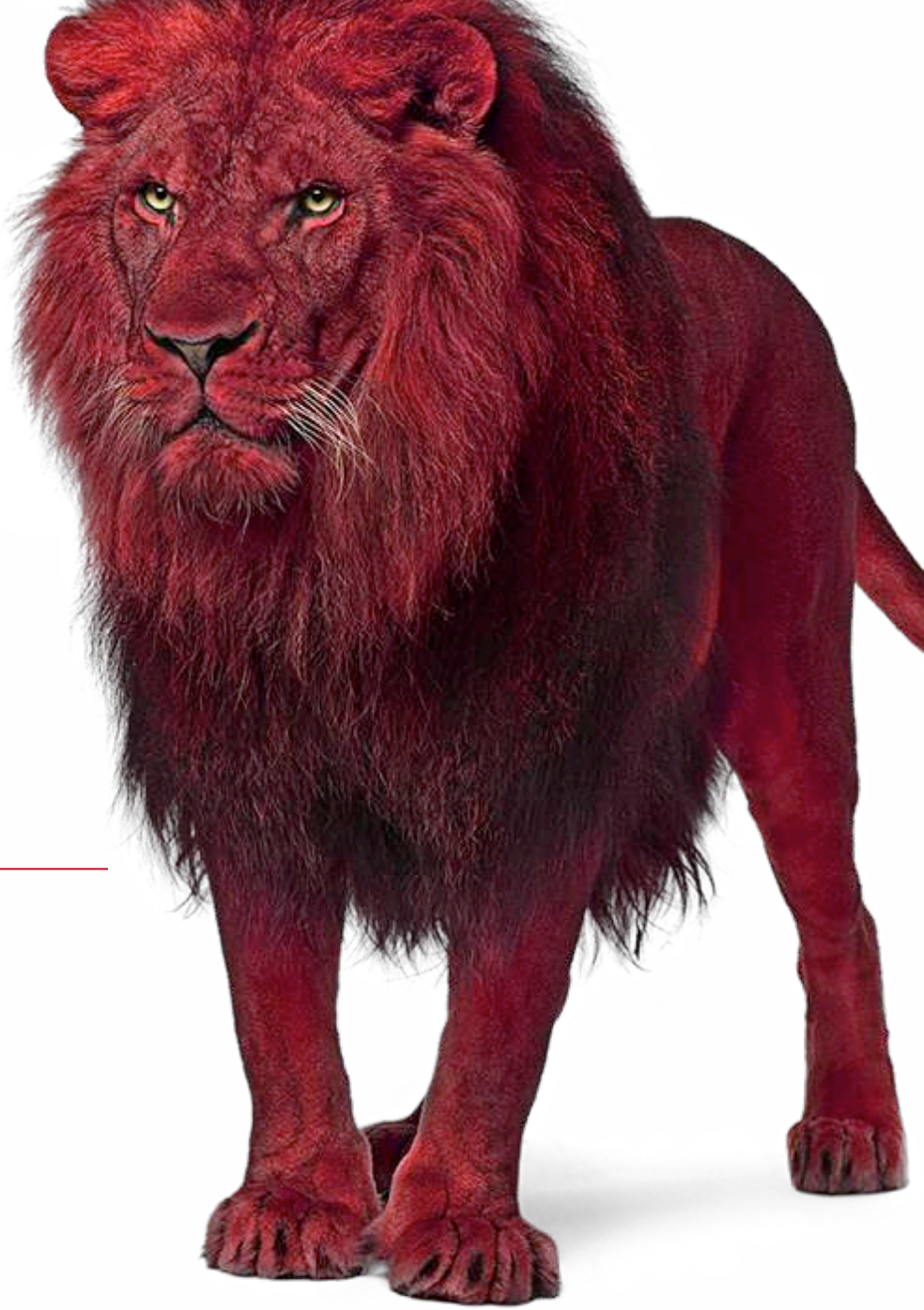
This looks like a real Poison Ivy RAT infection. All of the details of the victim are in the Details tab. You need to decide if you would like to use the Strongarm Remediation feature to remotely kill the malware or find the VICTIM system and re-image the system.

We're here for you if you'd like more analysis support! Good luck!

Sam the IT Manager commented 12 months ago

Thanks! I've made contact with TargetedUser and am going to send a tech to clean the workstation. I'll let you know if we need anything!

Live Demo



Vielen Dank