



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



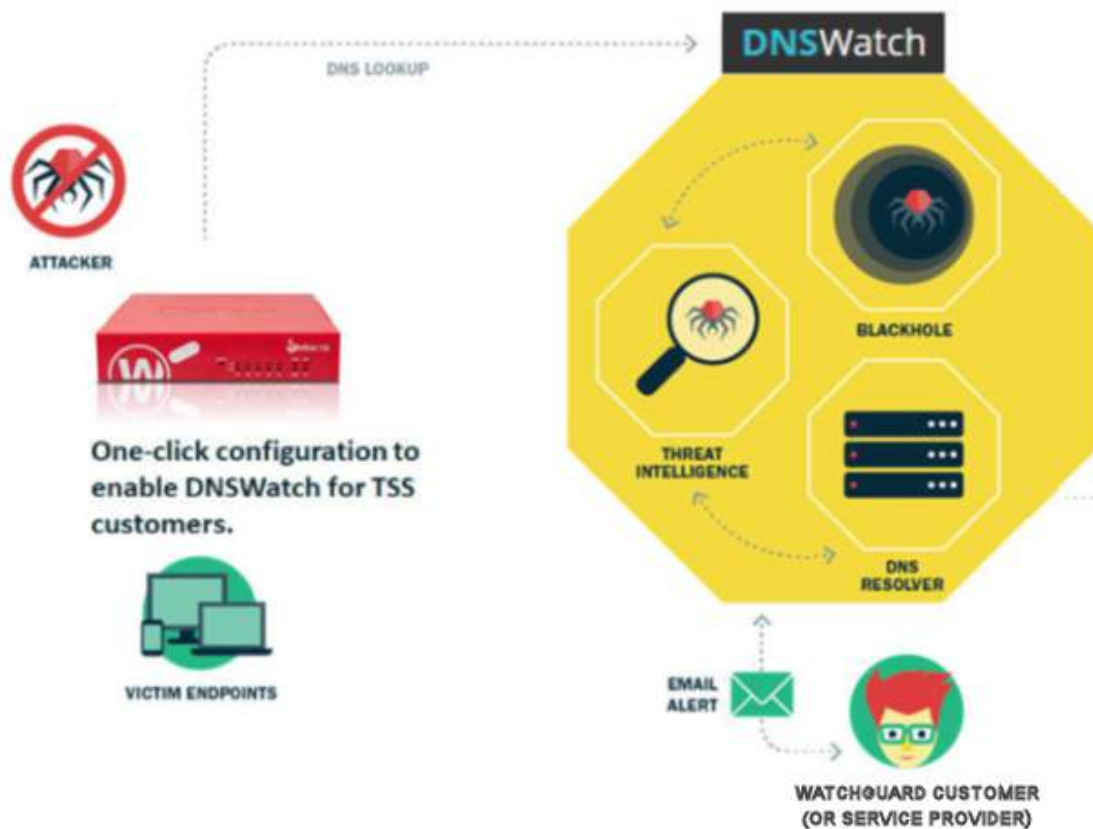
Spearphishing



CEO
Fraud

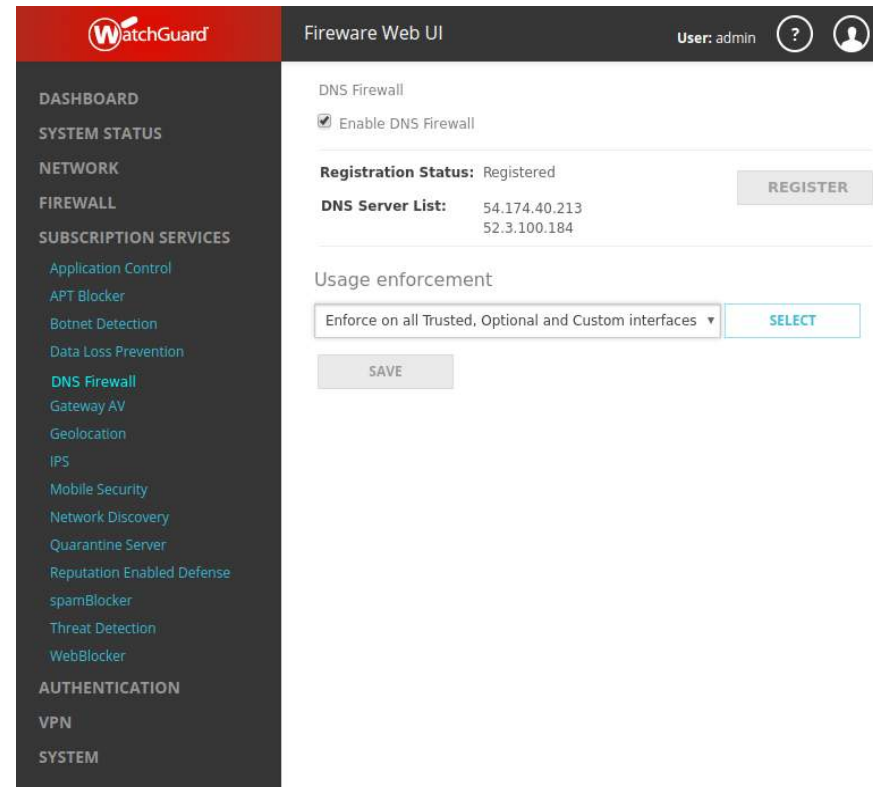
DNSWatch schützt wirkungsvoll vor Phishing

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




The screenshot displays the WatchGuard Fireware Web UI interface. The top navigation bar includes the WatchGuard logo, the title "Fireware Web UI", and the user "User: admin". The left sidebar menu lists various system services, with "DNS Firewall" highlighted in blue. The main content area is titled "DNS Firewall" and features a checked checkbox for "Enable DNS Firewall". Below this, the "Registration Status" is shown as "Registered" with a "REGISTER" button. The "DNS Server List" includes the IP addresses "54.174.40.213" and "52.3.100.184". The "Usage enforcement" section has a dropdown menu set to "Enforce on all Trusted, Optional and Custom interfaces" and a "SELECT" button. A "SAVE" button is located at the bottom of the configuration area.

Phishing Education

STRONGARM WEBSITE BLOCKED

Oops! We think you clicked on a phish!

Hey! Todd from IT here. I'd love for you to give me a call at 212-555-1212 and talk about what happened. If you don't have time for that, please forward the e-mail with the link you clicked on (if you clicked on a link) to hooli@suspicious.strongarm.io. Have a super day!

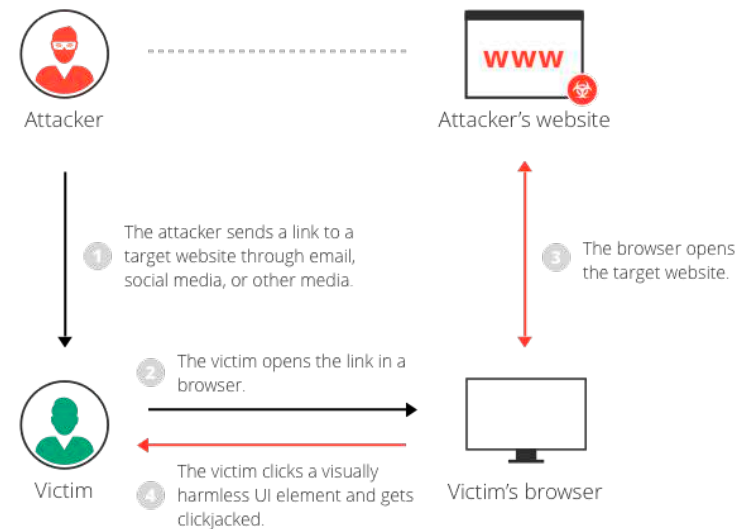


▶ ◁ PREV NEXT ▷

WatchGuard

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**

The screenshot displays the WatchGuard Fireware Web UI interface. The top navigation bar includes the WatchGuard logo, the title 'Fireware Web UI', and the user 'User: admin'. The left sidebar lists various subscription services, with 'DNSWatch' selected. The main content area shows the DNSWatch configuration page. A red box highlights the 'Registration Status' (Registered) and 'DNS Servers' (54.174.40.213 and 52.3.100.184). Below this, the 'Usage Enforcement' section has a dropdown menu set to 'Enforce on all Trusted, Optional, and Custom interfaces' and a 'SELECT' button. A 'SAVE' button is located at the bottom of the configuration area.

Registration Status:	Registered
DNS Servers:	54.174.40.213
	52.3.100.184

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.



Usage Enforcement

Disable enforcement ▾

Enforce on all Trusted, Optional, and Custom interfaces

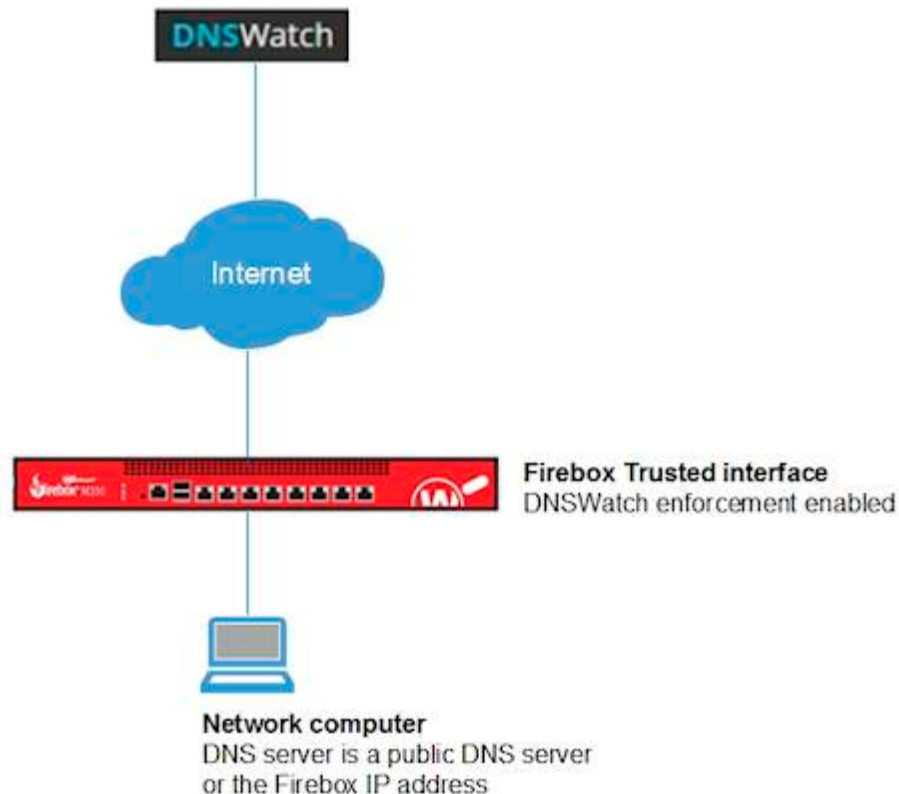
Enforce on selected interfaces

Disable enforcement

SELECT

DNSWatch Netzwerkintegration

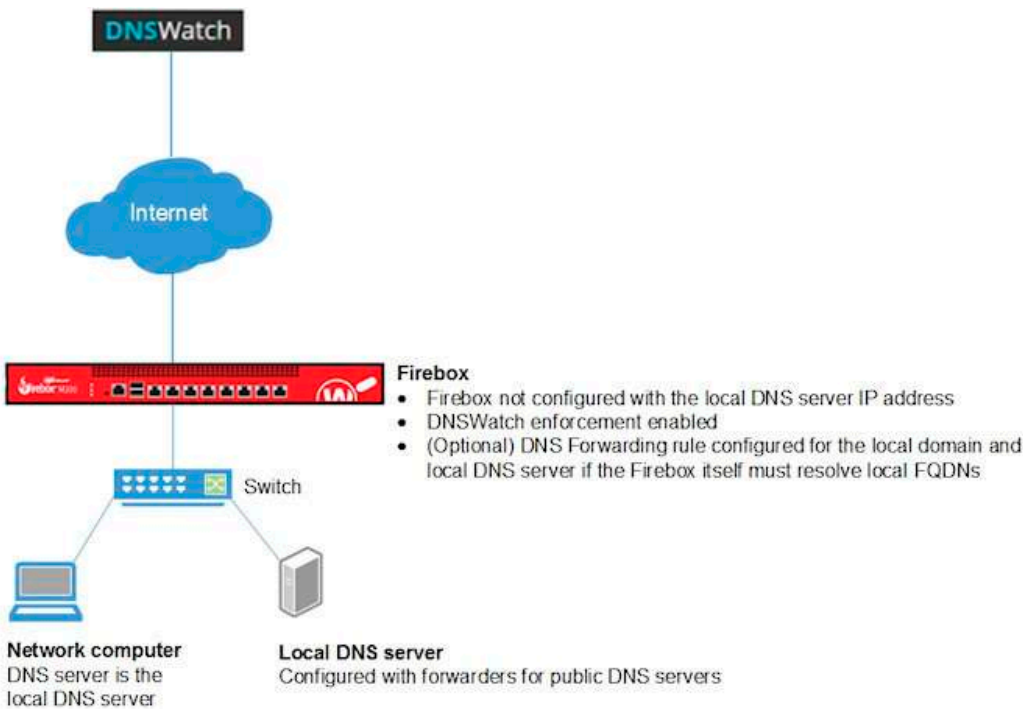
- Beispiel 1 — Netzwerk ohne lokalen DNS Server



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



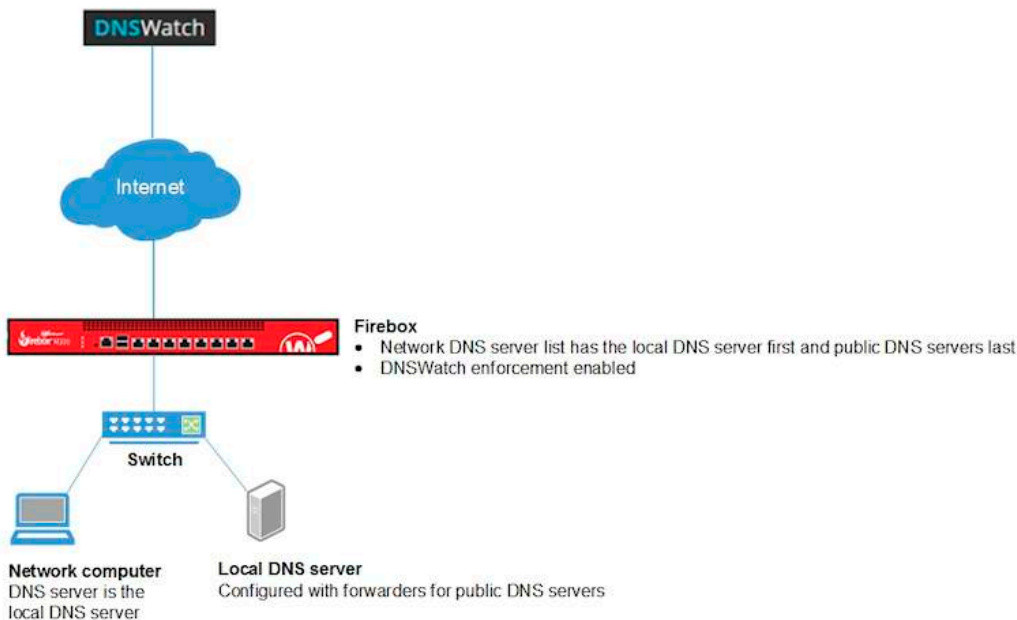
DNS-Anforderungen für interne Ressourcen
 Wenn ein Host in Ihrem Netzwerk eine DNS-Anforderung für eine interne Ressource in Ihrem Netzwerk sendet, löst der lokale DNS-Server die Anfrage auf.

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.

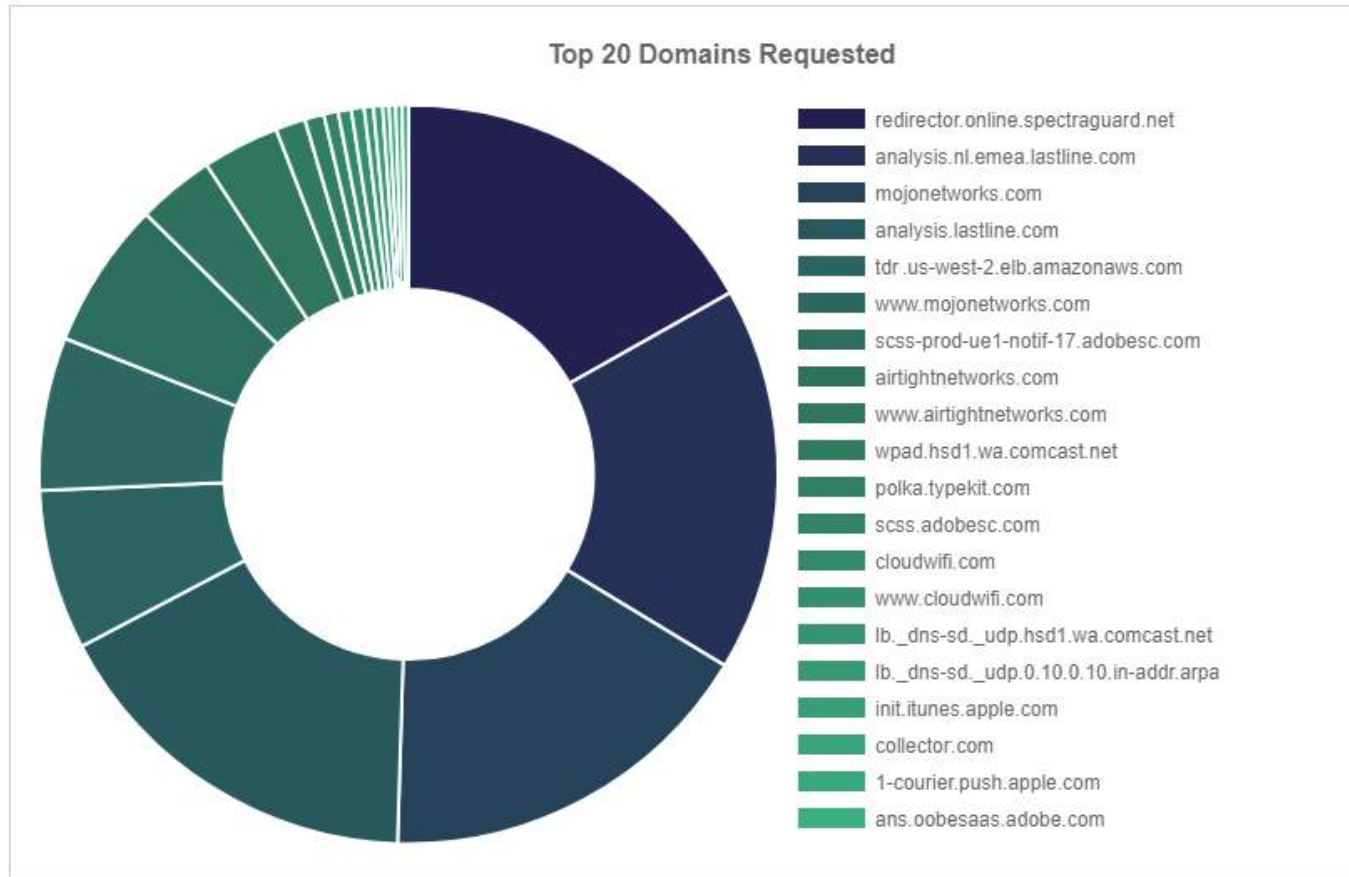
DNS-Anforderungen für externe Ressourcen
Wenn ein Host in Ihrem Netzwerk eine DNS-Anforderung für eine externe Ressource sendet, leitet der lokale DNS-Server die Anforderung an die öffentlichen IP-Adressweiterleitungen weiter, die auf dem Server konfiguriert sind. Da jedoch die DNSWatch *Usage Enforcement* 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.

Alerts 6 FILTER ▶

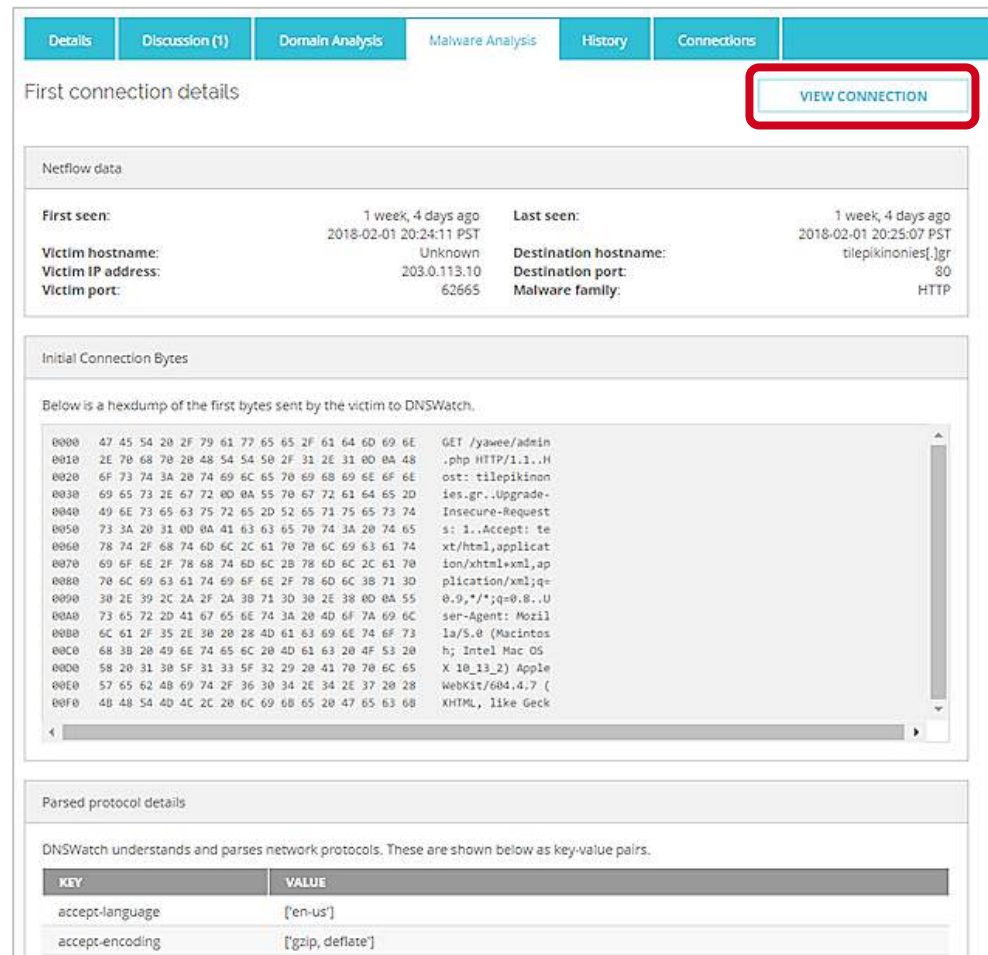
An alert summarizes a group of connections that DNSWatch has blocked from reaching a potentially malicious domain. Below is a full list of alerts for your team. You can also view a full list of [connections](#) that DNSWatch has blocked if you need more details.

<input type="checkbox"/>	DOMAIN ▲ ▼	VICTIM	FIRST SEEN ▲ ▼	LAST SEEN ▲ ▼	STATUS	ACTIONS
<input type="checkbox"/>	tilepkinonies[.]gr HTTP: MALWARE	...[Interface] External (203.0.113.10) ⓘ	1 week, 4 days ago	1 week, 4 days ago	✗ 🛡️	VIEW
<input type="checkbox"/>	vzmaze[.]ml HTTP: TESTING	...[Interface] External (203.0.113.10) ⓘ	1 week, 5 days ago	1 week, 5 days ago	✗ 🛡️	VIEW
<input type="checkbox"/>	e-qreentech[.]com HTTP: PREVIOUSLY BAD	...[Interface] External (203.0.113.10) ⓘ	1 week, 5 days ago	1 week, 5 days ago	✗ 🛡️	VIEW
<input type="checkbox"/>	u0456259[.]cp[.]regruhosting[.]ru HTTP: PREVIOUSLY BAD	...] WG-Wireless-Client (203.0.113.10) ⓘ	1 week, 5 days ago	1 week, 5 days ago	✗ 🛡️	VIEW
<input type="checkbox"/>	mojewelry[.]gr HTTP: COMPROMISED WEBSITE	...] WG-Wireless-Client (203.0.113.10) ⓘ	1 week, 5 days ago	1 week, 5 days ago	✗ 🛡️	VIEW
<input type="checkbox"/>	svit-zer[.]com HTTP: MALWARE	...] WG-Wireless-Client (203.0.113.10) ⓘ	1 week, 5 days ago	1 week, 5 days ago	✓	VIEW

[RESOLVE SELECTED ALERTS](#)

DNSWatch Alert Details – Malware Analysis

- Details zu von DNSWatch festgestellten Gefahren werden dargestellt.
- weitere Details sind über “View Connection” sichtbar.



The screenshot displays the DNSWatch Malware Analysis interface. The top navigation bar includes tabs for Details, Discussion (1), Domain Analysis, Malware Analysis, History, and Connections. The 'Malware Analysis' tab is active, and a 'VIEW CONNECTION' button is highlighted with a red box.

First connection details

First seen:	1 week, 4 days ago 2018-02-01 20:24:11 PST	Last seen:	1 week, 4 days ago 2018-02-01 20:25:07 PST
Victim hostname:	Unknown	Destination hostname:	tilepikiniones[.]gr
Victim IP address:	203.0.113.10	Destination port:	80
Victim port:	62665	Malware family:	HTTP

Initial Connection Bytes

Below is a hexdump of the first bytes sent by the victim to DNSWatch.

```

0000  47 45 54 20 2F 79 61 77 65 65 2F 61 64 60 69 6E  GET /yawee/admin
0010  2E 70 68 70 20 48 54 50 2F 31 2E 31 00 0A 48    .php HTTP/1.1..H
0020  6F 73 74 3A 20 74 69 6C 65 70 69 68 69 6E 6F 6E  ost: tilepikinion
0030  69 65 73 2E 67 72 00 0A 55 70 67 72 61 64 65 2D  ies.gr..Upgrade-
0040  49 6E 73 65 63 75 72 65 2D 52 65 71 75 65 73 74  Insecure-Request
0050  73 3A 20 31 00 0A 41 63 63 65 70 74 3A 20 74 65  s: 1..Accept: te
0060  78 74 2F 68 74 6D 6C 2C 61 70 70 6C 69 63 61 74  xt/html,applicat
0070  69 6F 6E 2F 78 68 74 6D 6C 2B 78 6D 6C 2C 61 70  ion/xhtml+xml,ap
0080  70 6C 69 63 61 74 69 6F 6E 2F 78 6D 6C 3B 71 3D  plication/xml;q=
0090  30 2E 39 2C 2A 2F 2A 3B 71 3D 30 2E 38 0D 0A 55  0.9,*/*;q=0.8..U
00A0  73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C  ser-Agent: Mozil
00B0  6C 61 2F 35 2E 30 20 28 4D 61 63 69 6E 74 6F 73  la/5.0 (Macintos
00C0  68 3B 20 49 6E 74 65 6C 20 4D 61 63 20 4F 53 20  h; Intel Mac OS
00D0  58 20 31 38 5F 31 33 5F 32 29 20 41 70 70 6C 65  X 10_13_2) Apple
00E0  57 65 62 48 69 74 2F 36 30 34 2E 34 2E 37 20 28  WebKit/604.4.7 (
00F0  4B 48 54 4D 4C 2C 20 6C 69 68 65 20 47 65 63 68  XHTML, Like Geck
  
```

Parsed protocol details

DNSWatch understands and parses network protocols. These are shown below as key-value pairs.

KEY	VALUE
accept-language	[en-us]
accept-encoding	[gzip, deflate]

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

