BLUE SHIELD UMBRELLA

EUROPEAN THREAT INTELLIGENCE

NO MORE THREATS OUT OF THE BLUE

CLOSING THE GAP BETWEEN 0-DAYS AND SIGNATURES

BlueShield

Probleme in der IT-Security: BLUE SHIELD UMBRELLA

BlueShield

- Es gibt keine 100%ige Prävention in der Cyber-Security
- Der Cyber-Security-Markt hat keine Antworten auf
  - Phishing oder zielgerichtete Phishing Angriffe
  - Schadsoftware-Infektionen (z.B. Ransomware, C&C Malware oder 0-days)
  - Missbrauch von kompromittierten Webseiten um deren Anwender zu infizieren
- Es werden jeden Tag 200k neue Domänen registriert – 70% davon werden als gefährlich eingestuft!
- Blacklist-basierte Ansätze sind reaktiv – und die Hersteller kommen nicht hinterher

BLUE SHIELD UMBRELLA

ist der erste KI-basierte Whitelist-DNS-Filter der Welt

Die Lösung:
BLUE SHIELD UMBRELLA

- Pro-aktiver Echtzeit Whitelist-DNS-Filter auf Basis von Big Data und künstlicher Intelligenz sowie aktive Forschung und kontinuierliche Weiterentwicklung in Österreich
- Alle unbekannten oder nicht geprüften Domänen werden erst gar nicht aufgelöst und sofort geblockt – permanente dynamische Analyse und Re-Checks aufgelöster Domänen
- Nahtlose Integration aller mobilen Geräte
- Einfache, zentrale Inbetriebnahme ohne zusätzliche Software-Installation
- Visibilität über alle infizierten Computer in der Infrastruktur

Blacklist vs. Whitelist

- x Reaktiv
- x Hersteller kommen nicht mehr nach
- x Erzeugt gefährlichen GAP!

- ✓ Pro-Aktiv
- ✓ Domänen müssen sich permanent „qualifizieren“
- ✓ Alles was nicht auf der Whitelist ist, wird geblockt

Wie kommt man auf die „Gästeliste“?

- Machine-Learning aus historischen Daten (passive DNS/ IP-Database mit weltweitem Sensor-Netzwerk)
- Weltweite NOC- (Network Operation Center) Kooperationen für Echtzeit-Netflow-Daten aller Zielsysteme
- Domain Sandboxing
- Threat Intelligence Feeds für Supervised Learning

„Erzähle mir die Vergangenheit, und ich werde die Zukunft erkennen“ – Konfuzius

Die Bedeutung:
BLUE SHIELD UMBRELLA

- Alle Arten von Phishingversuchen schlagen fehl
- Internettraffic von Schadsoftware oder anderen Infektionen wird sofort geblockt und protokolliert (30 Tage)
- Driveby-Infektionen von Webseiten werden praktisch auf Null reduziert bzw. in der Folge blockiert und reportet
- Sofortige Statistiken für das Unternehmen

- Mehrwehrt von Blue Shield Umbrella bereits in unter 24 Stunden erkennbar – und dies zu einem fairen Preis!

Schnittstellen:
BLUE SHIELD UMBRELLA

Blue Shield bietet folgende Schnittstellen:

- “klassische“ Implementierung mittels DNS Forwarder (statische IP des Internet Breakouts vorausgesetzt)
- DNS-over-https-/ DoH-Agents für alle gängigen mobilen Plattformen (Windows, Mac, iOS und Android)
- Generische DoH-Konfiguration für alternative Implementierung (z.B. Zero-Trust-Agents, Router/ Firewall – wenn dynamische IP-Adresse vorhanden)
- Rest-API Schnittstellen für Integration in andere Lösungen (z.B. SIEM, NAC/NAP, …)

Weitere Vorteile:
BLUE SHIELD UMBRELLA

- IP Feed für alle gängigen Next Generation Firewall zur Erweiterung der IPS Systeme (alle 15 Min. aktualisiert in verschiedenen Formaten für den regelmäßigen Import/ Aktualisierung)
- Looks-Alike-Domain Protection auf ML Basis und proaktive Überwachung bei Registrierung von ähnlichen Domains inklusive Benachrichtigung
- Forensik Agent für tiefere Analysen
- Windows Mobile Agent kann neben reinen DoH auch für IP-Filtering erweitert werden

Initiales Setup – 15 Minuten: BLUE SHIELD UMBRELLA

- Freischaltung der Internet IP-Adresse(n) der Organisation
- Ändern des DNS-Resolver der Organisation auf die BSU-Adresse
- (optional: AD-Agent am DNS-Server installieren, um betroffene Benutzer/Hosts zu sehen)
- (optional: blocken/ weiterleiten von anderem DNS-Verkehr via Firewall zu BSU)
- (optional: Integration in das Log-Management/ SIEM)
- Login in das Management Interface

Technischer Instant Support: technik@blue-shield.at

Optionale Features:
BLUE SHIELD UMBRELLA

- Automatisches Reporting via eMail (*pdf, csv, …*)
- Automatischer Export der Logs via SFTP
- Zugriff auf alle Funktionalitäten mittels Rest-API
- Optionaler Schutz für mobile Endgeräte (*via Agents, mittels DoH*)
- DNS-Server Agent für Host-Orchestration („AD-Agent“)
- Erweiterte Integrationsmöglichkeiten für Kritische Infrastrukturen

Technischer Instant Support: technik@blue-shield.at


BlueShield
Domain: block.blue-shield.at
Cause: PHISHING
BLOCKED by
BLUE SHIELD
UMBRELLA
BLUESHIELD
OVERVIEW
TOP USER CALCULATED FROM AD AGENT (AFFECTED)
TOP HOSTS CALCULATED FROM AD AGENT (AFFECTED)
CATEGORIES
12569
10

BlueShield

INSIGHTS

Thema Malvertising

Definition Malvertising (Kofferwort aus Malware und Advertising):

- Malvertising (böswillige Werbung) nutzt Online-Werbung, um Malware auf Benutzercomputer zu verbreiten.

  Es kann auch als Angriffsvektor für Drive-by-Download-Angriffe dienen.

Warum gefährlich?

- Hochwirksam:

  Nutzer müssen nicht einmal auf die Anzeige klicken, um infiziert zu werden.
- Weite Verbreitung:

  Malvertising kann auf jeder Webseite erscheinen, die Online-Werbung nutzt.
- Schwierig zu erkennen:

  Malware kann so getarnt sein, dass sie wie reguläre Werbung aussieht. Webseitenbetreiber haben wenig bis keinen Einfluss darauf!
- Erschwertes Aufspüren:

  Täter nutzen oft Ad-Networks, was das Aufspüren des Ursprungs erschwert.

Beispiel: orf.at (01.06.2023)

BlueShield

- Statistik für orf.at:

```
sdk.privacy-center.org: 2
script-at.iocnt.net: 1
cdn.adnz.co: 1
at.iocnt.net: 1
imagesrv.adition.com: 2
```

Insgesamt 5 externe Domains nachgeladen, davon 0 geblockt.

Gesamtanzahl der Requests: 7

Beispiel: krone.at (01.06.2023)

BlueShield

```
static.criteo.net: 1
buy-eu.piano.io: 1
gum.criteo.com: 1
cdn.taboola.com: 3
nr-events.taboola.com: 1
www.google-analytics.com: 3
www.googletagmanager.com: 3
securepubads.g.doubleclick.net: 2
static.scarabresearch.com: 2
p1cluster.cxense.com: 1
cdn-eu.piano.io: 3
experience-eu.piano.io: 3
c2.taboola.com: 1
cdn.onthe.io: 1
cdn.scarabresearch.com: 1
```

```
cdn.onesignal.com: 2
c.amazon-adsystem.com: 2
ads.pubmatic.com: 1
cdn.cxense.com: 2
id-eu.piano.io: 1
connect.facebook.net: 1
script-at.iocnt.net: 2
at.iocnt.net: 2
sdk.privacy-center.org: 2
secure.cdn.fastclick.net: 1
apv-launcher.minute.ly: 1
snippet.minute.ly: 1
ca.openxcdn.net: 1 (BLOCKED)
invstatic101.creativecdn.com: 1
cdn.prod.uidapi.com: 1 (BLOCKED)
```

```
tags.crwdcntrl.net: 1
adservice.google.at: 2
adservice.google.com: 2
apps.apple.com: 1
play.google.com: 1
api.cxense.com: 1
www.dibeo.at: 1
www.kronehilft.at: 1
pubads.g.doubleclick.net: 1
jackpot.onelink.me: 1
cdn.vergleich.org: 10
www.facebook.com: 1
www.twitter.com: 1
www.youtube.com: 1
www.instagram.com: 1
```

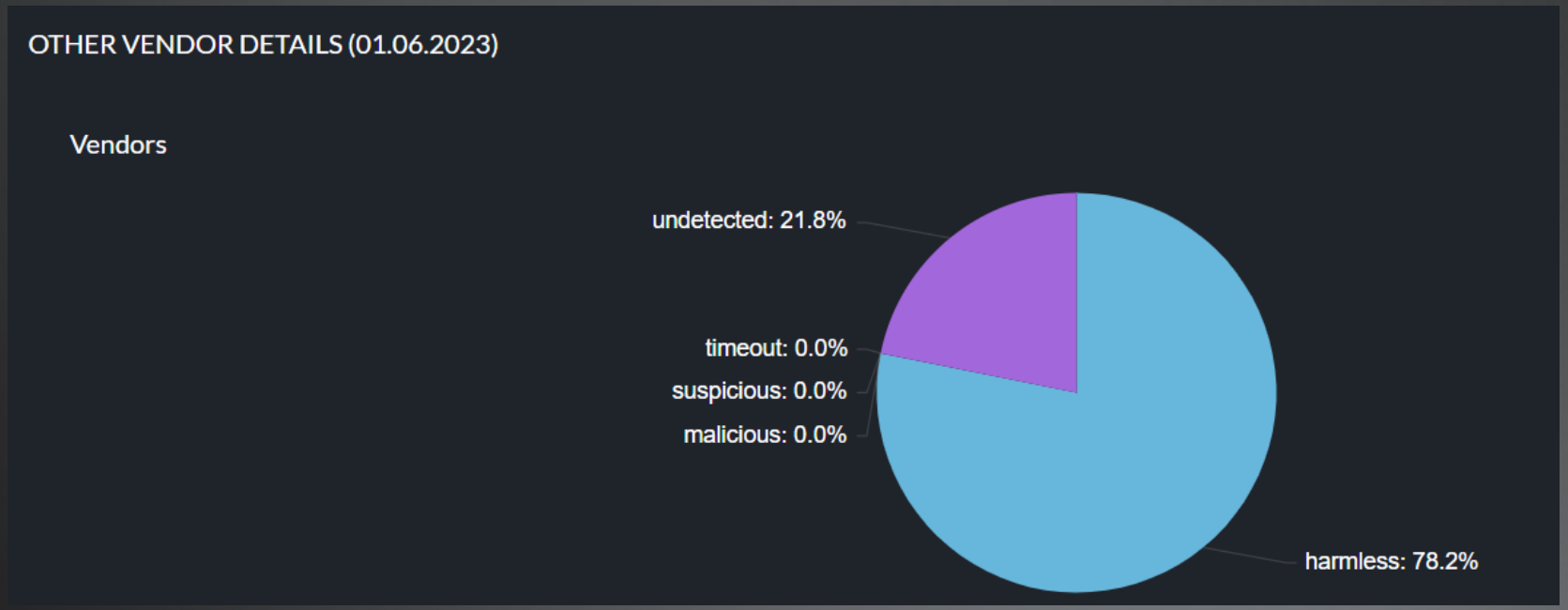
Insgesamt 45 externe Domains nachgeladen, davon 2 geblockt.

Gesamtanzahl der Requests: 74

Beispiel: krone.at (01.06.2023)

BlueShield

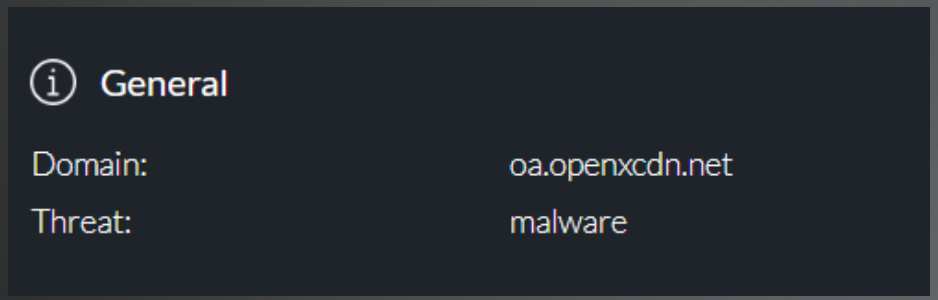
Andere Hersteller:



Beispiel: krone.at (01.06.2023)

BlueShield

Blue Shield:



VT-Datenbank:

(Payload, die mit dieser Domäne interagieren)

https://www.virustotal.com/gui/file/6167572d3633074f0864fd9b38660a2538860fe6a39b75d6cab2c2f5bc7442d8/detection

https://www.virustotal.com/gui/file/431ed7acad476fbd31abb136fa6b1022b597b4de179d456e680879303b3b575b/detection

https://www.virustotal.com/gui/file/9dcace1e1c5492d0b187a834ef81e9edf0d5c86771449a30bb8622eb53d2e4d7/detection

VirusTotal Hashes

Search Term: oa.openxcdn.net

source of data: VirusTotal

TStamp	Detection	SHA256 Hash
2023-05-29 09:19:54	1 of 75	9dcace1e1c5492d0b187a834ef81e9edf0d5c86771449a30bb8622eb53d2e4d7
2023-05-29 09:18:38	1 of 75	431ed7acad476fbd31abb136fa6b1022b597b4de179d456e680879303b3b575b
2023-05-28 10:36:01	1 of 75	98d203cf47c472db249df5230e8e0769b1e1fb1415528d5513026d25ad3b5356
2023-05-27 13:00:14	48 of 75	6167572d3633074f0864fd9b38660a2538860fe6a39b75d6cab2c2f5bc7442d8
2023-05-25 09:29:44	2 of 75	c30eb248125e1ca379268dd03382de01a45fa392a048dd2b71be75dc06a9c9c7

Beispiel: golem.de (12.06.2023)

https://www.golem.de/news/polymorphe-malware-ki-stellt-it-sicherheitsloesungen-vor-neue-herausforderungen-2306-174818.html

Auch dieses Beispiel bestätigt, wie wichtig der Einsatz von Blue Shield Umbrella ist!

Beispiel: golem.de (12.06.2023)

BlueShield

Supply Chain z.B SolarWinds – BSU hat diese Domain niemals erlaubt.

All unsere Kunden waren immer geschützt, da diese nie auf die Allowlist gelangte.

```
882  q1b91c4fdd7q4td56rswoiou0govirsv.appsync-api.us-east-1.avsvmcloud.com          servitia.intern
883  q3b8h3lm9q7eoqa56260kun0e6iuir0e.appsync-api.us-east-2.avsvmcloud.com          sos-ad.state.
884  q3vcrhhcmddh7rl5oi602ou6iuir0grn.appsync-api.us-east-2.avsvmcloud.com          its.iastate.ed
885  q80cgv4eolosbfo4tvef0t12eu1.appsync-api.us-east-1.avsvmcloud.com            gncu.local
886  q882csbrq5oa58d4r6eud0i2st.appsync-api.us-east-1.avsvmcloud.com          escap.org
887  q8bps26mocuq6re4dutru70ct2w.appsync-api.us-east-1.avsvmcloud.com            pageaz.gov
888  q8g11thobvg6d604tvef0b12eu1.appsync-api.us-east-1.avsvmcloud.com            gncu.local
889  sf0q84qdutb323q6eo6e202e2h.appsync-api.us-east-1.avsvmcloud.com          cisco.com
890  q8vmaei8n3dpeui5vr2d32i2voe60be2.appsync-api.us-east-1.avsvmcloud.com          neophotonics.co
891  qb9it88vftri6v84euheoip0e12eu1.appsync-api.us-west-2.avsvmcloud.com          camcity.local
892  qbj26i5jnkrqdac5wh602un0twusouv0.appsync-api.us-west-2.avsvmcloud.com          vms.ad.varian
893  1cmge6dsclrtfejc6e0gdohu0et2w.appsync-api.us-east-1.avsvmcloud.com            sc.pima.gov
894  qfnf6ab6u28je4d5un0b2dioho7r1p0b.appsync-api.us-east-2.avsvmcloud.com          ad.optimizely.
895  qfnf6ab6u28je4i5un0c2dioho7r1p0c.appsync-api.us-east-2.avsvmcloud.com          ad.optimizely.
896  qg1e4bctbk3gdkr4e2sd0bdieo0be2h.appsync-api.us-east-1.avsvmcloud.com          corp.ptci.com
897  qgc2gj97t3sop4i5uhs0be2sd0govir1.appsync-api.us-east-1.avsvmcloud.com          amr.corp.intel
898  qgdubroda1vph414srd6sw0oe2h.appsync-api.us-east-1.avsvmcloud.com            repsrv.com
899  qipotpf1jic4gav5oi60eou6iuir0grn.appsync-api.us-east-2.avsvmcloud.com          its.iastate.ed
900  qit94i5tqf2j9mq5wo11r02irssrc2vv.appsync-api.us-east-2.avsvmcloud.com          ville.terrebonn
901  qj1bggoa06prfj646d6n0g6j02eu.appsync-api.us-east-1.avsvmcloud.com            spsd.sk.ca
902  qj82njdvtfuoi455uhs0be2sd0govir1.appsync-api.us-east-1.avsvmcloud.com          amr.corp.intel
903  qo046rspifbl4k04e2mvri0ge2m0te2h.appsync-api.us-east-2.avsvmcloud.com          coxnet.cox.com
904  qrieo21mr659tfk5wh60iun0bwusouv0.appsync-api.us-west-2.avsvmcloud.com          vms.ad.varian
905  qrjtdj3alnlcj0k4urso2ve2sd0be2h.appsync-api.us-west-2.avsvmcloud.com          aerioncorp.com
906  qvot463cl5rcg5r4urso2ve2sd02e2h.appsync-api.us-west-2.avsvmcloud.com          aerioncorp.com
907  r14ptgkl7qacucu5chsv0ee2h.appsync-api.us-west-2.avsvmcloud.com          bmrn.com
908  r1q6arhpujcf6jb6ervisu10odohu0it.appsync-api.us-west-2.avsvmcloud.com          central.pima.g
909  r1qshoj05ji05ac6eoip02jovt6i2v0c.appsync-api.us-west-2.avsvmcloud.com          city.kingston.
910  r69ncekf56jlkkr6oi602ou6iuir02rn.appsync-api.us-east-2.avsvmcloud.com          its.iastate.ed
911  r6b5cj43deojp665u30c2st.appsync-api.us-east-2.avsvmcloud.com          ah.org
912  r74br8r0cce4m6r6oi60eou6iuir0trn.appsync-api.us-east-2.avsvmcloud.com          its.iastate.ed
913  r75n0q0557bl6nv6oi60cou6iuir0orn.appsync-api.us-east-2.avsvmcloud.com          its.iastate.ed
914  r7kqk893t5lu82j6uhs0ie2sd0iovir1.appsync-api.us-east-2.avsvmcloud.com          amr.corp.intel
```


BlueShield
Domain: block.blue-shield.at
Cause: PHISHING
BLOCKED by
BLUE SHIELD
UMBRELLA
BLUESHIELD
OVERVIEW
TOP USER CALCULATED FROM AD AGENT (AFFECTED)
TOP HOSTS CALCULATED FROM AD AGENT (AFFECTED)
CATEGORIES
12569
10

TRY & BUY

BLUE SHIELD UMBRELLA

POC | 30 Tage kostenloser und unverbindlicher Test der Demovollversion

BlueShield

Blue Shield Security GmbH

Kornstraße 7a, A-4060 Leonding

+43 732 211 922

office@blue-shield.at

www.blue-shield.at