SonicWall キャプチャ脅威評価

レポート先:
SonicWall

レポート元ファイアウォール:
18B16920****

ファイアウォール モデル:
SONICWALL TZ300W Japan

SonicOS バージョン:
6.5.1.1-42n.jpn

収集期間:
Jul 09 2018 21:16:49 +0900 to
Jul 10 2018 12:26:23 +0900

※レポート抜粋版

キャプチャ脅威評価

SonicWall キャプチャ脅威評価レポートは、SonicWall 次世代ファイアウォール装置によって検知および遮断された異なる脅威が起こった時点でのスナップショットです。また、ネットワーク上の様々なトラフィックを洞察するために、このレポートは上位アプリケーション トラフィック、上位ユーザ、上位 URL 種別およびセッション数を含むアプリケーションとユーザ基準のデータを提供します。

お客様の現環境を簡単に診断！

脅威指標

1	2	3	4
低	中	高	深刻
ネットワークに起こる識別可能な活動も悪意のあるコード活動もありません。	違法となり得るアプリケーションまたは脅威がネットワーク上に確認されました。	ネットワーク上のいくつかのアプリケーションが、性能に影響を及ぼしているか、ポリシーを回避するサービスを提供している	いくつかのアプリケーションが、ネットワークの性能に影響を及ぼしており、悪意のある活動することで知られるアプリケーショ

この格付けは、ネットワーク上に確認されたすべてのアプリケーションのリスク レベルの平均点であり、ネットワークにもたらす脅威の指標となります。

脅威 防御

0	ボットネット
2	ウイルス
0	スパイウェア
110	IPS

エンドポイント

5 上位イベント 143 IPs

上位トラフィック (国別)

1. United States
2. Japan
3. Russian Federation

組織名
SonicWall

SonicWall 装置
SONICWALL TZ300W Japan

SonicOS バージョン
6.5.1.1-42n.jpn

購読サービス
App Control, GAV, IPS, SPY, CFS, GeoIP, Botnet

収集期間
1 Day(s)

上位悪用回数

「上位悪用回数」セクションは、SonicWall 次世代ファイアウォールによって遮断された上位の悪用を提供します。レポートには、イベント種別、名前、およびシグネチャ毎に遮断された企ての合計数が含まれます。ファイアウォールによって遮断されたその他の悪用の可能性については、SonicWall セキュリティ SonicAlerts ページをご参照ください。

イベント種別	名前	遮断 ⇅
GAV	Eicar-Test-Signature	2
IDP	NetBIOS Name Request Probe	78
IDP	EICAR TEST FILE	23
IDP	Obfuscated JavaScript Code 27	5
IDP	Echo Reply	4

リスク通信の発生を確認

次のステップ

上位悪用回数の情報を使用することによって、ネットワーク上のシステムがこれらの種別のマルウェア攻撃または脆弱性に対して対策がされているかどうかを判断することができます。未対策のほとんどは、パッチが当てられていないソフトウェア、またはエンドポイントで使用される脆弱性のあるバージョンのソフトウェアが原因です。

⇅ = sorted by

上位アプリケーション（種別別）

「上位アプリケーション（種別別）」セクションは、上位のアプリケーション、種別、リスク レベル、トラフィック量、およびセッション数の情報を提供します。この情報は、ネットワーク上で使用されているそれらのアプリケーションのリスク スコアと共に、アプリケーション帯域幅の使用量を知覚的に提供します。

アプリケーション	種別 ⇅	リスク	トラフィック	セッション
Apple Updates	APP-UPDATE	2 Elevated	1.14 KB	3
VK	APP-UPDATE	1 Low	46.71 KB	3
Apple iMessage	APP-UPDATE	1 Low	10.48 KB	1
Microsoft Windows Updates				
Microsoft Office 365	BUSINESS-APPS	1 Low	56.03 MB	721
Salesforce CRM	BUSINESS-APPS	2 Elevated	10.55 MB	123
Dropbox	BACKUP-APPS	2 Elevated	90.83 MB	152
Microsoft OneDrive	BACKUP-APPS	2 Elevated	72.05 MB	138
Evernote	BACKUP-APPS	2 Elevated	80.61 KB	10
Audio Video Stream				
Image	FILETYPE-DETECTION	1 Low	2.72 MB	69
Archive	FILETYPE-DETECTION	1 Low	3.86 KB	1
General DNS	General	2 Elevated	87.23 MB	10,840
General URL	General	2 Elevated	13.30 MB	1,102
Service SMB	General	2 Elevated	4.12 MB	353
General NETBIOS	General	2 Elevated	2.02 MB	420
General UDP	General	2 Elevated	182.62 KB	7
General TCP	General	2 Elevated	110.45 KB	4
General DHCP	General	2 Elevated	90.54 KB	612
Google Talk	IM	2 Elevated	44.15 KB	199

通信負荷の増え続けるクラウドアプリケーション

機密情報漏洩リスクのあるオンラインストレージサービス

⇅ = sorted by

上位アプリケーション（種別別） （続き）

「上位アプリケーション（種別別）」セクションは、上位のアプリケーション、種別、リスク レベル、トラフィック量、およびセッション数の情報を提供します。この情報は、ネットワーク上で使用されているそれらのアプリケーションのリスク スコアと共に、アプリケーション帯域幅の使用量を知覚的に提供します。

アプリケーション	種別 ⇅	リスク	トラフィック	セッション
Google QUIC	INFRASTRUCTURE	2 Elevated	40.09 KB	101
Akamai CDN	INFRASTRUCTURE	1 Low	26.37 KB	176
Amazon CloudFront	INFRASTRUCTURE	1 Low	26.16 KB	136
Google	MISC-APPS	1 Low	20.53 KB	3
Google API	MISC-APPS	1 Low	15.09 KB	102
Microsoft CryptAPI				
Uber				
Netflix	MULTIMEDIA	1 Low	209.60 MB	220
Youtube	MULTIMEDIA	1 Low	201.34 MB	71
Google Play				
Apple Bonjour				
Freegate	PROXY-ACCESS	3 High	2.00 MB	79
Twitter	SOCIAL-NETWORKING	2 Elevated	20.67 MB	307
Facebook	SOCIAL-NETWORKING	1 Low	18.89 MB	225
LinkdIn	SOCIAL-NETWORKING	1 Low	288.02 KB	16
LINE	VoIP-APPS	2 Elevated	22.90 MB	40
Microsoft Internet Explorer	WEB-BROWSER	2 Elevated	114.63 KB	10
Google Chrome				
Microsoft Outlook.com (Hotmail)	WEBMAIL	1 Low	3.99 MB	80
Mail.ru	WEBMAIL	1 Low	255.91 KB	28

企業回線を圧迫するストリーミングメディア

通信を迂回させるプロキシアプリケーション

情報漏えいに繋がる SNS やウェブメールアプリケーション

⇅ = sorted by

上位アプリケーション（帯域幅別）

過度の需要、特に大きいダウンロードやビデオ ストリーミングは、ネットワーク インフラストラクチャ上に容認できない負担をかけます。

これらのアプリケーションは、ネットワーク帯域幅を一番多く消費する代表です。

アプリケーション	リスク	トラフィック ⇅	セッション
SSL	1 Low	1.06 GB	2,122
Netflix	1 Low	209.60 MB	220
YouTube	1 Low	201.34 MB	71
Facebook	1 Low	18.89 MB	225
Twitter	2 Elevated	13.30 MB	1,102
Encrypted Key Exchange	4 Severe	10.68 MB	66
MPEG	1 Low	10.03 MB	4
Google QUIC	2 Elevated	8.89 MB	225
Google Chrome Data Compression Proxy	1 Low	8.28 MB	48
Amazon.co.jp	1 Low	5.68 MB	32
LINE	2 Elevated	4.12 MB	353
Google	1 Low	3.99 MB	80
Microsoft Internet Explorer	2 Elevated	3.73 MB	110
Image	1 Low	2.72 MB	69
Microsoft Outlook.com (Hotmail)	1 Low	2.58 MB	104

次のステップ

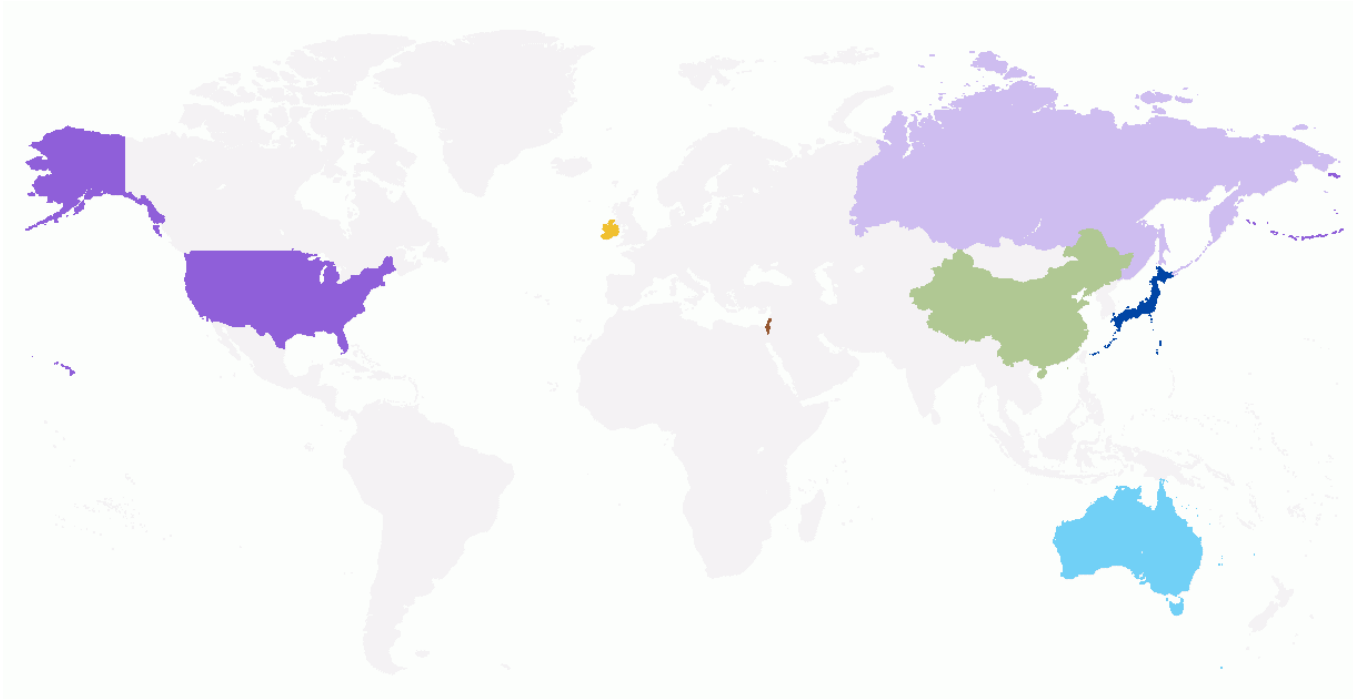
非生産的かつネットワーク帯域幅の多くを使用するアプリケーションを発見した場合は、SonicWall ファイアウォールのアプリケーション制御を使用して、それらのアプリケーションに対する帯域幅制限またはアクセス遮断を行うポリシーを作成することができます。

⇅ = sorted by

上位国（トラフィック別）

「上位国（トラフィック別）」セクションは、ファイアウォール背後のデバイスまたは特定の国に送信されるトラフィックの概要を提供します。このデータは、トラフィックが特定の場所に送信されているのか、また、それらの企てに対して地域 IP またはボットネット ポリシーを作成するべきなのかを判断するために使用されます。

監査期間中において検知された送信元による上位 10 ヶ国が以下に示されます。



国	トラフィック	セッション ⇅	遮断
United States	2.13 GB	15,570	no
Japan	907.39 MB	5680	no
Russian Federation	141.86 MB	357	no
Australia	1.97 MB	31	no
Ireland	230.09 KB	27	no
China	698.00 KB	21	no
Israel	56.19 MB	14	no

通信発生を認識していない国との多量のトラフィックやりとり

⇅ = sorted by

レポートの設定

レポートの完全な一式を提供するために、SonicWall 次世代ファイアウォールの管理 GUI で次のオプションを有効にしてください。オプションが設定されていない場合、最終的なキャプチャ脅威評価レポートには全データの内の部分集合のみが含まれます。

ページ	状況	
Aggregate Reporting	✓	Enabled. Reporting for aggregate data logs enabled.
App Reporting	✓	Enabled. Reporting for aggregate application data logs enabled.
URL Reporting	✓	Enabled. Reporting for aggregate URL data logs enabled.
URL Category Reporting	✓	Enabled. Reporting for URL category data logs enabled.
GAV Reporting	✓	Enabled. GAV is licensed and GAV status is enabled.
Spyware Reporting	✓	Enabled. Spyware is licensed and Spyware status is enabled.
IPS Reporting	✓	Enabled. IPS is licensed and IPS status is enabled.
Geo IP Reporting	✓	Enabled. Reporting for aggregate geo IP data logs enabled.
App IP Reporting	✓	Enabled. Reporting for aggregate app IP data logs enabled.
User IP Reporting	✓	Enabled. Reporting for aggregate user IP data logs enabled.