アプリケーションおよびリスク分析レポート

Customer ABC 様向け

作成者: Palo Alto Networks

Tuesday, January 22, 2013

Palo Alto Networks
3300 Olcott St
Santa Clara, CA 95054
Sales 866.207.0077
www.paloaltonetworks.com

Palo Alto Networks の強み

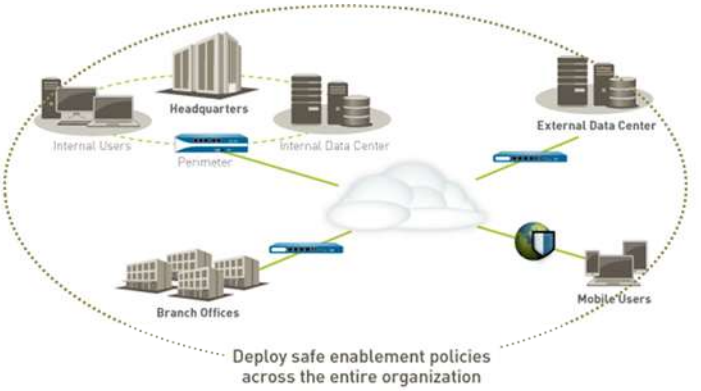
アプリケーションや脅威をめぐる状況、ユーザの行動、ネットワーク インフラストラクチャの根本的な変化によって、従来のポートベースのファイア ウォールが提供していたセキュリティの効果は徐々に失われつつあります。ユーザは様々な種類のデバイスを使用してあらゆるタイプのアプリケーションにアクセスしており、その多くは業務のために使用しています。データセンタの拡張、仮想化、モバイル、クラウド中心の取り組みの結果、組織はアプリケーションへのアクセスを可能にしながら同時にネットワークを保護するための方法について、再考を余儀なくされています。Palo Alto Networks の次世代ファイアウォールにより、組織はすべてのユーザが場所に関係なく、安全にアプリケーションを利用できるようにして、関連するビジネスやセキュリティ リスクを軽減することができます

すべてのアプリケーションをすべてのポートで常時識別　App-ID は、トラフィックがファイアウォールに到達するとすぐに複数の識別メカニズムをトラフィック ストリームに適用することで、使用されているポートや暗号化（SSL または SSH）、回避技術に関係なく、ネットワークを通過するアプリケーションを正確に識別します。ポートとプロトコルだけでなく、どのようなアプリケーションがネットワークを通過しているかについての正確な情報は、セキュリティ ポリシーの決定すべてにとっての基礎となります。不明なアプリケーションは通常トラフィックの中でわずかな割合しか占めていませんがリスクの可能性は高く、自動的に分類して組織的な管理を行います。これにはポリシー コントロール、調査、脅威のフォレンジック、カスタム App-ID の作成、または Palo Alto Networks App-ID 作成用のパケット キャプチャが含まれます。

IP アドレスだけでなくユーザとデバイスをポリシーに関連付け　デバイスや場所に関係ないアプリケーションとユーザ識別に基づくセキュリティ ポリシーは、ポートと IP アドレスだけに依存したものよりも効果的にネットワークが保護できます。幅広いエンタープライズ向け ディレクトリサービスとの統合によって、アプリケーションにアクセスする Microsoft Windows、Mac OS X、Linux、Android、または iOS ユーザの識別が提供されます。出張中のユーザやリモートで作業するユーザは、ローカルまたは企業ネットワークで使用されているポリシーと同じ一貫したポリシーでシームレスに保護されます。ユーザのアプリケーション アクティビティに対する可視化と制御を組み合わせることで、組織はアクセスしている場所や方法に関係なく、Oracle や BitTorrent、Gmail またはネットワークを通過するその他のアプリケーションを安全に使用することができます。

既知および未知のあらゆる脅威から防御 - 既知のマルウェア
サイトに組織的な脅威防止策を講じることで、脆弱性攻撃、ウイルス、スパイウェアや悪質な DNS クエリを単一のパスでブロックします。一方、バーチャルサンドボックス環境で未知のファイルを実行し、100 を超える悪意のある動作を直接監視することで、カスタムまたはその他未知のマルウェアを積極的に分析し識別します。新しいマルウェアが検出されると、感染ファイルと関連するマルウェア トラフィックに対するシグネチャが自動的に生成され配信されます。すべての脅威防御分析でアプリケーションとプロトコルの詳細なコンテキストを使用し、たとえ脅威がトンネルや圧縮コンテンツ、ハイポートなどでセキュリティの回避を試みたとしても検出できるようにします。

安全なアプリケーション利用ポリシーは、次の方法で組織のセキュリティを向上します。インターネットの境界では不要なアプリケーションをブロックし、許可されたアプリケーションについては既知と未知のいずれのアプリケーションも脅威がないか調査することで、脅威の及ぶ範囲を狭めることができます。従来型または仮想型のデータセンタでは、許可されたユーザによってのみデータセンタ アプリケーションが使用されるようにすることで、コンテンツを脅威から保護し、バーチャル インフラストラクチャの動的な性質がもたらすセキュリティ上の問題に対応します。エンタープライズの支社やリモート ユーザは、本社で導入されているものと同じポリシーの拡張によりセキュリティが実現できるため、ポリシーの一貫性が確保できます。



サマリと主な結果

今回PAN Japan様向けに、Palo Alto Networks の次世代ファイアウォールを使用してアプリケーションとリスクの分析を実施いたしました。このレポートはこの分析結果を総括したもので、最初に主な結果と全般的なビジネス リスク評価について説明します。次に、特定のアプリケーション、テクノロジ リスクと脅威に基づいて PAN Japan 様のトラフィックを分析し、ネットワークの使用方法に関する概要を示します。そして最後にまとめと推奨策について説明いたします。

Customer ABC 様による対応が必要と思われる主な内容:

ネットワーク上に個人用のアプリケーションがインストールされ、使用されています
エンドユーザは業務に関係なく各種のアプリケーションをインストールおよび使用しており、ビジネスやセキュリティ上のリスクにつながる可能性があります。

アクティビティを隠ぺいするためのアプリケーションが検出されました -
ITに精通した社員がアクティビティを隠ぺいするアプリケーションを使用しています。この種のアプリケーションの例としては、外部プロキシ、リモート デスクトップ アクセス、非 VPN 関連の暗号化トンネルが挙げられます。誰がどのような目的でこれらのアプリケーションを使用しているのかを調査する必要があります。

情報漏洩につながる可能性があるアプリケーションが検出されました -
ファイル転送アプリケーション(P2Pまたはブラウザ ベース、あるいはその両方)が使用されており、セキュリティ、情報漏洩、コンプライアンス違反、および著作権侵害の可能性といった深刻なリスクが様に及んでいます。

通信アプリケーションの個人使用が検出されました -
社員が個人用の各種通信アプリケーションを使用しています。この例としては、インスタント メッセージング、Web メール、VoIP/ビデオ会議などがあります。この種のアプリケーションにより、生産性の低下、コンプライアンス違反、および事業継続性のリスクが発生します。

帯域幅と労働時間を浪費するアプリケーションが使用されています -
メディアアプリケーションおよびソーシャル ネットワーキング アプリケーションが検出されました。この 2 つのアプリケーションはいずれも、企業の帯域幅と社員の時間を消費することで知られています。

ハイ リスク アプリケーションによってもたらされるビジネス上のリスク

ネットワークを通過するアプリケーションによってもたらされるビジネスリスクの可能性は、ハイリスクなアプリケーション（1 ～ 5 段階で レベル4 と 5 のリスクが潜むもの）の特徴を分析することで確認できます。これらの動作特性がビジネス上でのリスクを誘発する可能性があります。たとえば、アプリケーションのファイル転送がデータの漏洩につながったり、検出を回避する機能やその他のアプリケーションをすり抜ける機能がコンプライアンス違反リスクにつながったり、帯域幅の大量消費が運用コストを増加させ、悪意のあるソフトウェアの攻撃を受けやすいアプリケーションや脆弱性のあるソフトウェアが事業継続性のリスクをもたらす可能性があります。関連するビジネス リスクを効果的に管理する上で最初の手順は、アプリケーションが運ぶと思われるリスクを識別することです。

図 1 は、ビジネス リスク算出のサマリを示しています。 付録 A では、ビジネス リスクの詳細を説明しています。

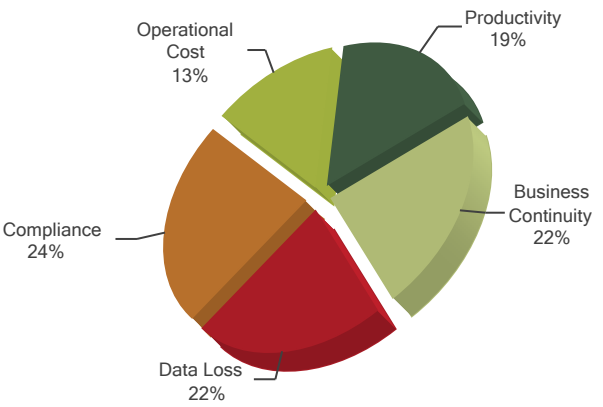


図 1: ハイ リスク アプリケーション が誘発 するビジネス リスクの詳細

確認されたハイ リスク アプリケーション

ハイ リスク アプリケーション（リスクレベル 4 または 5）をカテゴリ、サブカテゴリ、および使用バイト数ごとに分類して以下に示します。アプリケーション カテゴリ、サブカテゴリ、およびテクノロジが確認できれば、ビジネス グループとの間で、事業上の価値とアプリケーションのリスクを話し合う場合に役立ちます。

149 ハイ リスク アプリケーションに関する主な結果:

アクティビティの隠ぺい:
(8)種類のプロキシアプリケーションおよび (4) 種類のリモートアプリケーションが検出されま した。さらに、VPNではない暗号トンネルアプリケーションも検知されました。IT テクノロジに精通した社員がネットワーク上のアクティビティを隠蔽するためにこれらの アプリケーションを使用する頻度が高まっており、Customer ABC様の環境におけるコンプライアンス違反と情報漏洩のリスクが 発生する可能性があります。

ファイル転送/データ漏洩/著作権違反:
(16)種類のP2P アプリケーションと (20)種類のブラウザベースのファイル共有アプリケーションが検出されました。これらのアプリケーションにより、Customer ABC様環境ではデータ消失に 加え、著作権侵害の可能性、コンプライアンス違反のリスクが高まり、脅威の媒介手段となる可能性があります。

通信アプリケーションの個人使用:
(10)種類のインスタント メッセージング、(16)種類のWebメール、(4)種類のVoIP/ ビデオ会議などのさまざまな通信アプリケーションが個人使用の目的でよく使用されていることが確認されました。この種のアプリケーションは、生産性の低下、コンプライアンス違反、および Customer ABC様における事業継続性のリスクを引き起こす可能性があります。

帯域幅の大量消費:
(25)種類の写真/ビデオアプリケーション、(2)種類のオーディオアプリケーション、(15)種類のソーシャル ネットワーキングアプリケーションなど、帯域幅を大量に消費することが判明しているアプリケーションが検出されました。この種のアプリケーションは社員の生産性の低下を表しており、帯域幅を大量消費すると共に、脅威を媒介する手段となる可能性があります。

Risk	Application	Category	Sub-Category	Technology	Bytes	Sessions
4	concur	business-systems	general-business	browser-based	25,510,321	651
5	google-docs-base	business-systems	office-programs	browser-based	41,633,763,580	14,895
4	ms-groove	business-systems	office-programs	peer-to-peer	8,694,941	55
5	google-docs-enterprise	business-systems	office-programs	browser-based	32,856	4
4	ms-update	business-systems	software-update	client-server	24,395,025,867	85,182
4	egnyte	business-systems	storage-backup	browser-based	30,215,234	465
4	sosbackup	business-systems	storage-backup	client-server	115,240	2
4	ms-exchange	collaboration	email	client-server	90,489,681,905	838,610
5	smtp	collaboration	email	client-server	52,324,415,049	229,232
4	gmail-base	collaboration	email	browser-based	19,770,419,222	266,309
4	hotmail	collaboration	email	browser-based	6,866,089,186	219,156
4	lotus-notes-base	collaboration	email	client-server	3,790,633,781	91,208
4	aim-mail	collaboration	email	browser-based	2,491,264,136	43,312
4	daum-mail	collaboration	email	browser-based	489,740,012	98
5	horde	collaboration	email	browser-based	169,785,104	5,701
4	netease-mail	collaboration	email	browser-based	153,522,284	3,922
4	squirrelmail	collaboration	email	browser-based	151,349,028	4,311
4	qq-mail	collaboration	email	browser-based	25,783,996	1,420
4	gmail-enterprise	collaboration	email	browser-based	7,152,024	61
4	outlook-web	collaboration	email	browser-based	4,528,330	196
4	mail.ru-mail	collaboration	email	browser-based	2,024,370	108
4	yandex-mail	collaboration	email	browser-based	1,846,624	19
4	blackberry	collaboration	email	client-server	1,286,040	415
4	imap	collaboration	email	client-server	1,190,047	943
4	roundcube	collaboration	email	browser-based	1,134,478	74
4	telenet-webmail	collaboration	email	browser-based	509,056	40
4	gmx-mail	collaboration	email	browser-based	489,832	96
4	pop3	collaboration	email	client-server	58,248	28
4	web-de-mail	collaboration	email	browser-based	44,616	5
4	yahoo-im-base	collaboration	instant-messaging	client-server	874,050,333	100,797
4	imo	collaboration	instant-messaging	browser-based	547,815,233	31,610
4	google-talk-base	collaboration	instant-messaging	client-server	13,515,765	1,211
5	ebuddy	collaboration	instant-messaging	browser-based	11,074,451	584
4	aim-express-base	collaboration	instant-messaging	browser-based	10,097,763	1,181
4	qq-base	collaboration	instant-messaging	client-server	4,804,698	430
5	jabber	collaboration	instant-messaging	client-server	466,698	3
4	gadu-gadu	collaboration	instant-messaging	client-server	136,596	12
4	msn-base	collaboration	instant-messaging	client-server	65,323	47
4	mibbit	collaboration	instant-messaging	browser-based	19,242	6
4	live-meeting	collaboration	internet-conferencing	client-server	2,317,397,820	13,829
4	genesys-base	collaboration	internet-conferencing	client-server	260,804,441	4,902
4	att-connect	collaboration	internet-conferencing	client-server	136,964,816	4,220
4	facebook-base	collaboration	social-networking	browser-based	13,506,875,716	959,886
5	netlog	collaboration	social-networking	browser-based	636,715,936	8,801
4	sina-weibo-base	collaboration	social-networking	browser-based	397,538,146	27,239
4	orkut	collaboration	social-networking	browser-based	45,790,011	229
4	facebook-posting	collaboration	social-networking	browser-based	33,596,924	319
4	odnoklassniki-base	collaboration	social-networking	browser-based	32,705,456	1,526
4	vkontakte-base	collaboration	social-networking	browser-based	24,921,858	763
5	stumbleupon	collaboration	social-networking	browser-based	23,888,840	7,939
4	plaxo	collaboration	social-networking	browser-based	20,220,672	1,899
4	myspace-base	collaboration	social-networking	browser-based	5,410,291	220
4	facebook-apps	collaboration	social-networking	browser-based	3,977,542	100
4	cyworld	collaboration	social-networking	browser-based	2,896,214	191

4	me2day	collaboration	social-networking	browser-based	1,401,729	222
4	ameba-now-base	collaboration	social-networking	browser-based	916,096	27
4	twitter-posting	collaboration	social-networking	browser-based	144,134	28
5	skype	collaboration	voip-video	peer-to-peer	3,211,862,084	67,576
4	sip	collaboration	voip-video	peer-to-peer	975,071	6,703
4	msn-voice	collaboration	voip-video	peer-to-peer	382,664	268
4	yahoo-voice	collaboration	voip-video	peer-to-peer	10,479	2
4	blog-posting	collaboration	web-posting	browser-based	24,221,436	1,265
4	dropbox	general-internet	file-sharing	client-server	71,306,108,068	49,057
4	sharefile	general-internet	file-sharing	browser-based	28,965,723,195	329
4	skydrive-base	general-internet	file-sharing	browser-based	12,051,827,913	42,611
4	yousendit-base	general-internet	file-sharing	browser-based	3,169,186,574	3,309
5	ftp	general-internet	file-sharing	client-server	2,972,890,312	159,576
5	webdav	general-internet	file-sharing	browser-based	2,374,813,805	743,167
4	rapidshare	general-internet	file-sharing	browser-based	2,229,394,510	4,674
4	4shared	general-internet	file-sharing	browser-based	895,149,103	3,335
5	dl-free	general-internet	file-sharing	browser-based	314,531,348	16
4	sendspace	general-internet	file-sharing	browser-based	196,068,719	39
4	google-drive-web	general-internet	file-sharing	browser-based	179,280,129	3,064
5	bittorrent	general-internet	file-sharing	peer-to-peer	141,849,043	2,919
4	docstoc-base	general-internet	file-sharing	browser-based	107,144,990	1,245
4	live-mesh-base	general-internet	file-sharing	client-server	64,812,019	3,652
4	mediafire	general-internet	file-sharing	browser-based	27,960,135	544
5	xunlei	general-internet	file-sharing	peer-to-peer	9,447,431	237
4	tftp	general-internet	file-sharing	client-server	6,378,966	124
4	leapfile	general-internet	file-sharing	browser-based	1,866,442	60
4	office-live	general-internet	file-sharing	client-server	1,764,052	486
5	fileserve	general-internet	file-sharing	browser-based	1,758,672	121
4	putlocker	general-internet	file-sharing	browser-based	911,649	49
4	divshare	general-internet	file-sharing	browser-based	806,216	34
4	megaupload	general-internet	file-sharing	browser-based	655,720	40
4	file-host	general-internet	file-sharing	browser-based	279,684	12
5	emule	general-internet	file-sharing	peer-to-peer	146,246	12,291
4	qq-download	general-internet	file-sharing	peer-to-peer	139,589	13
4	fs2you	general-internet	file-sharing	browser-based	26,550	146
5	imesh	general-internet	file-sharing	peer-to-peer	20,396	6
5	flashget	general-internet	file-sharing	peer-to-peer	17,496	8
5	ares	general-internet	file-sharing	peer-to-peer	6,456	5
4	sugarsync	general-internet	file-sharing	client-server	2,466	3
5	hotfile	general-internet	file-sharing	browser-based	1,728	2
4	ifolder	general-internet	file-sharing	client-server	860	1
5	filesonic	general-internet	file-sharing	browser-based	290	2
4	web-browsing	general-internet	internet-utility	browser-based	1,022,566,846,826	22,179,799
4	flash	general-internet	internet-utility	browser-based	158,436,800,881	156,867
5	rss	general-internet	internet-utility	client-server	4,848,499,935	48,434
4	web-crawler	general-internet	internet-utility	browser-based	305,837,941	1,446
4	google-desktop	general-internet	internet-utility	client-server	17,393,181	1,744
4	mobile-me	general-internet	internet-utility	browser-based	2,827,976	22
4	zamzar	general-internet	internet-utility	browser-based	1,896,535	87
4	apple-appstore	general-internet	internet-utility	client-server	5,196	1
5	http-audio	media	audio-streaming	browser-based	30,632,503,680	5,861
4	pandora-tv	media	audio-streaming	browser-based	85,676	8
5	youtube-base	media	photo-video	browser-based	794,438,117,672	64,230
4	rtmpt	media	photo-video	browser-based	143,575,265,482	467,568
5	http-video	media	photo-video	browser-based	74,698,881,187	15,479
5	asf-streaming	media	photo-video	browser-based	20,214,822,137	625

4	dailymotion	media	photo-video	browser-based	4,294,514,400	3,018
5	vimeo	media	photo-video	browser-based	4,097,890,325	3,983
4	justin.tv	media	photo-video	browser-based	1,334,745,030	144
5	tudou	media	photo-video	browser-based	898,937,697	479
4	rtmp	media	photo-video	browser-based	726,458,006	716
5	youku	media	photo-video	browser-based	543,126,119	231
4	limelight	media	photo-video	browser-based	286,203,546	1,064
4	rtmpe	media	photo-video	browser-based	283,322,921	323
4	ppstream	media	photo-video	peer-to-peer	140,748,509	4,627
4	youtube-safety-mode	media	photo-video	browser-based	140,135,860	16
4	yahoo-douga	media	photo-video	browser-based	133,573,064	788
4	youtube-uploading	media	photo-video	browser-based	84,975,512	20
4	sky-player	media	photo-video	client-server	66,149,998	44
5	brightcove	media	photo-video	browser-based	33,028,117	275
4	mogulus	media	photo-video	browser-based	23,090,336	198
5	funshion	media	photo-video	client-server	16,255,497	786
4	pplive	media	photo-video	peer-to-peer	3,178,580	250
4	metacafe	media	photo-video	browser-based	1,628,462	128
5	sopcast	media	photo-video	peer-to-peer	16,360	13
4	veetle	media	photo-video	browser-based	10,148	2
4	socialtv	media	photo-video	browser-based	1,643	1
4	ssl	networking	encrypted-tunnel	browser-based	480,191,784,585	13,850,959
4	ssh	networking	encrypted-tunnel	client-server	4,764,041,770	65,330
5	hamachi	networking	encrypted-tunnel	peer-to-peer	603,545,587	28,287
4	tor	networking	encrypted-tunnel	client-server	280,314,014	4,542
4	dns	networking	infrastructure	network-protocol	7,823,820,284	131,889,828
4	icmp	networking	ip-protocol	network-protocol	2,687,618,962	12,414,893
5	http-proxy	networking	proxy	browser-based	203,458,544,016	27,556,042
5	cgiproxy	networking	proxy	browser-based	972,202,458	14,073
5	glype-proxy	networking	proxy	browser-based	142,123,159	2,782
5	kproxy	networking	proxy	browser-based	4,902,156	282
5	phproxy	networking	proxy	browser-based	1,950,120	44
4	labnol-proxy	networking	proxy	browser-based	561,837	16
5	coralcdn-user	networking	proxy	browser-based	316,520	17
5	guardster	networking	proxy	browser-based	4,986	2
4	ms-rdp	networking	remote-access	client-server	854,849,154	353
5	logmein	networking	remote-access	client-server	461,110,419	2,238
5	x11	networking	remote-access	client-server	182,507,954	55
5	vnc-base	networking	remote-access	client-server	165,937,418	18

図 2: ネットワークを通過するハイリスクアプリケーション(レベル 4 または 5)

リスクを判定するためのアプリケーションの特性

Palo Alto Networks の調査研究チームは、アプリケーションの動作特性に基づいてリスクレベル 1 ～ 5 を判定しています。これらのアプリケーション特性はアプリケーションの可視化に不可欠な要素で、管理者はこれらの特性を使用してネットワークで見られる新しいアプリケーションを分析し、これらのアプリケーションを安全に実行できるようにします。

アプリケーションの動作特性の定義

乱用されやすい: 不正目的のための使用、または意図した以上のことを行うように簡単に設定できるもの。この例として、SOCKS だけでなく、DropBoks、AppleJuice、NEOnet などの比較的最近登場したアプリケーションが挙げられます。

他のアプリケーションをすり抜けさせる: 他のアプリケーションをトランスポートすることが可能なもの。この例として SSH と SSL に加え、Hopster、TOR と RTSP、RTMPT が挙げられます。

脆弱性が判明している: 脆弱性の悪用が判明しているアプリケーション。

• **ファイルの転送:** 1 つのネットワークから別のネットワークにファイルを転送することが可能なもの。この例として FTP と TFTP に加え、Web メール、MegaUpload や YouSendIt などのオンライン ファイル共有アプリケーションが挙げられます。

マルウェアでの使用: マルウェアの伝播、攻撃の開始、またはデータの盗難に悪用されたことがあるもの。マルウェアに使用されるアプリケーションには、コラボレーション（電子メール、IM など）および一般的なインターネット カテゴリ（ファイル共有、インターネット ユーティリティ）が含まれます。

帯域幅の大量消費: 通常使用で一般的に 1 Mbps 以上を消費するアプリケーション。この例として、BitTorrent、Xunlei、DirectConnect などの P2P アプリケーションに加え、メディア アプリケーション、ソフトウェア更新、およびその他の業務アプリケーションが挙げられます。

セキュリティを回避する: インストール作業自体が簡略化していて、既存のセキュリティ インフラストラクチャからすり抜けるために、意図された目的以外でポートまたはプロトコルを使用するもの。

Customer ABC様においては、ネットワークを通過するアプリケーション、その個別特性、およびそれを使用する社員を認識することで、関連するセキュリティ ポリシーによりアプリケーション トラフィックをどのように処理するかを効果的に決定できるようになります。多くのアプリケーションには、複数の動作特性があることに注意してください。

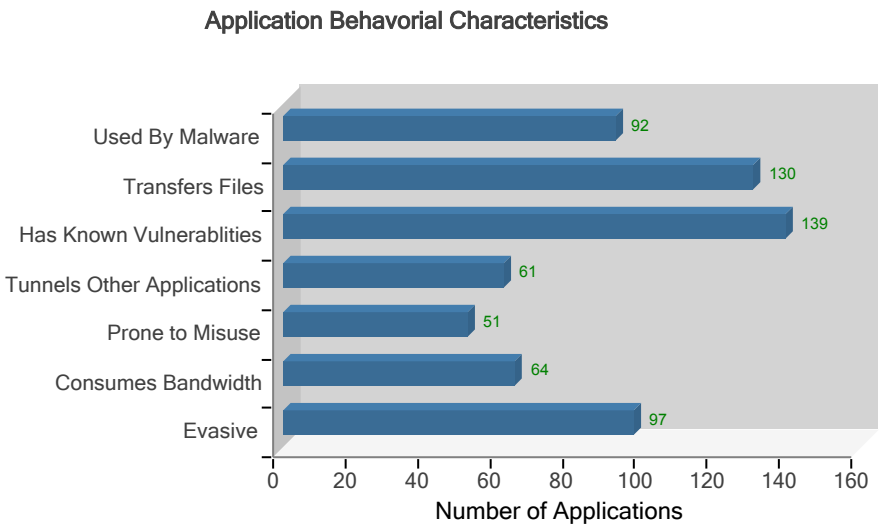


図 3: 検出 された ハイリスク アプリケーション の動作特性

ネットワークを通過する上位のアプリケーション

上位 35 のアプリケーション（帯域幅の消費量に基づく）をカテゴリおよびサブカテゴリごとに分類して以下に示します。アプリケーションのカテゴリ、サブカテゴリ、およびテクノロジに加えて、その動作特性（前ページに示す）を確認することにより、アプリケーションがもたらす事業上の利点を全般的に把握することができます。

Risk	Application	Category	Sub-Category	Technology	Bytes	Sessions
2	ldap	business-systems	auth-service	client-server	18,911,214,404	4,629,859
2	mssql-db	business-systems	database	client-server	26,556,867,539	115,329
3	hp-jetdirect	business-systems	management	client-server	20,233,231,770	143,910
5	google-docs-base	business-systems	office-programs	browser-based	41,633,763,580	14,895
4	ms-update	business-systems	software-update	client-server	24,395,025,867	85,182
3	symantec-av-update	business-systems	software-update	client-server	17,971,076,742	180,476
3	ms-ds-smb	business-systems	storage-backup	client-server	113,310,728,947	2,158,072
3	nfs	business-systems	storage-backup	client-server	10,565,321,342	4
4	ms-exchange	collaboration	email	client-server	90,489,681,905	838,610
5	smtp	collaboration	email	client-server	52,324,415,049	229,232
4	gmail-base	collaboration	email	browser-based	19,770,419,222	266,309
3	yahoo-mail	collaboration	email	browser-based	13,463,765,796	526,681
3	gotomeeting	collaboration	internet-conferencing	client-server	22,024,086,711	2,774
3	webex-base	collaboration	internet-conferencing	client-server	8,157,947,397	34,883
3	sharepoint-base	collaboration	social-business	browser-based	14,007,827,774	61,172
4	facebook-base	collaboration	social-networking	browser-based	13,506,875,716	959,886
2	twitter-base	collaboration	social-networking	browser-based	8,968,282,256	744,608
4	dropbox	general-internet	file-sharing	client-server	71,306,108,068	49,057
4	sharefile	general-internet	file-sharing	browser-based	28,965,723,195	329
4	skydrive-base	general-internet	file-sharing	browser-based	12,051,827,913	42,611
4	web-browsing	general-internet	internet-utility	browser-based	1,022,566,846,826	22,179,799
4	flash	general-internet	internet-utility	browser-based	158,436,800,881	156,867
3	grooveshark	media	audio-streaming	browser-based	47,864,197,745	82,467
5	http-audio	media	audio-streaming	browser-based	30,632,503,680	5,861
1	shoutcast	media	audio-streaming	client-server	12,657,703,648	288
5	youtube-base	media	photo-video	browser-based	794,438,117,672	64,230
4	rtmpt	media	photo-video	browser-based	143,575,265,482	467,568
5	http-video	media	photo-video	browser-based	74,698,881,187	15,479
5	asf-streaming	media	photo-video	browser-based	20,214,822,137	625
4	ssl	networking	encrypted-tunnel	browser-based	480,191,784,585	13,850,959
2	netbios-ns	networking	infrastructure	network-protocol	34,010,505,778	8,273,281
2	snmp-base	networking	infrastructure	client-server	30,583,933,520	56,569,462
2	msrpc	networking	infrastructure	network-protocol	15,624,336,434	3,124,147
1	ipv6	networking	ip-protocol	network-protocol	10,469,696,734	286,249
5	http-proxy	networking	proxy	browser-based	203,458,544,016	27,556,042

図 4: カテゴリ、サブカテゴリ、およびテクノロジ別に分類した帯域幅消費量が多い上位のアプリケーション

上位 35（464 中）のアプリケーションに関するに関する主な結果:

最も一般的なタイプのアプリケーションは、photo-videoとemailでした。

アプリケーションのサブカテゴリ

検出されたすべてのアプリケーションのサブカテゴリ分類を、帯域幅の消費量順に以下に示します。この表から、最も使用量の多いアプリケーションの概要を把握することができます。IT 組織では、これらのデータを基に効果的にアプリケーション イネーブルメント活動の優先度を決定することができます。

Sub-Category	Number of Applications	Bytes Consumed	Sessions Consumed
internet-utility	32	1,214,020,285,176	50,783,569
photo-video	55	1,064,866,249,610	818,925
encrypted-tunnel	8	485,985,389,405	13,956,761
proxy	8	204,580,605,252	27,573,258
email	33	197,573,744,831	2,306,786
file-sharing	45	128,550,470,645	1,063,902
storage-backup	5	123,907,863,739	2,158,567
infrastructure	31	102,264,936,924	211,047,826
audio-streaming	17	101,939,088,942	126,605
software-update	16	55,866,996,572	410,090
office-programs	10	41,945,426,587	31,522
social-networking	46	41,494,440,221	2,292,090
management	22	37,477,819,872	1,377,680
internet-conferencing	10	33,503,329,599	60,988
database	7	30,945,587,431	257,733
auth-service	7	27,243,155,418	8,383,479
remote-access	20	15,382,254,514	74,363
social-business	4	14,187,963,286	64,630
ip-protocol	4	13,157,321,440	12,701,148
general-business	17	10,713,525,925	218,821
erp-crm	4	5,331,079,488	32,679
instant-messaging	27	4,777,865,450	432,037
voip-video	14	3,650,853,188	108,526
web-posting	9	1,587,988,567	5,558
gaming	9	222,273,053	5,243
routing	4	7,350,363	7,772
Grand Total	464	3,961,183,865,498	336,300,558

図 5: 消費バイト数順に示したすべての検出アプリケーションのサブカテゴリ

アプリケーションのサブカテゴリに関する主な結果:

帯域幅の消費量が最も多いアプリケーションのサブカテゴリは、internet-utility, photo-video, encrypted-tunnel でした。

HTTP を使用するアプリケーション

何らかの方法、形式、形態で HTTP を使用する（ただしポート 80 は使用しない場合もある）上位 25 のアプリケーション（帯域幅の消費量に基づく）を以下に示します。多くのアプリケーションは、一早い導入とアクセス簡略化を実現するために HTTP を使用しますが、非業務アプリケーションではセキュリティをバイパスするために HTTP を使用しますが、非業務アプリケーションではセキュリティをバイパスするために HTTP を使用することがあります。アプリケーション ポリシーを設定する際に、どのアプリケーションが HTTP を使用するかを把握することが重要になります。

Risk	HTTP Application	Technology	Bytes	Sessions
4	web-browsing	browser-based	1,022,566,846,826	22,179,799
5	youtube-base	browser-based	794,438,117,672	64,230
5	http-proxy	browser-based	203,458,544,016	27,556,042
4	flash	browser-based	158,436,800,881	156,867
4	rtmpt	browser-based	143,575,265,482	467,568
4	ms-exchange	client-server	90,489,681,905	838,610
5	http-video	browser-based	74,698,881,187	15,479
4	dropbox	client-server	71,306,108,068	49,057
3	grooveshark	browser-based	47,864,197,745	82,467
5	google-docs-base	browser-based	41,633,763,580	14,895
5	http-audio	browser-based	30,632,503,680	5,861
4	sharefile	browser-based	28,965,723,195	329
4	ms-update	client-server	24,395,025,867	85,182
3	gotomeeting	client-server	22,024,086,711	2,774
5	asf-streaming	browser-based	20,214,822,137	625
4	gmail-base	browser-based	19,770,419,222	266,309
3	symantec-av-update	client-server	17,971,076,742	180,476
2	msrpc	network-protocol	15,624,336,434	3,124,147
3	sharepoint-base	browser-based	14,007,827,774	61,172
4	facebook-base	browser-based	13,506,875,716	959,886
3	yahoo-mail	browser-based	13,463,765,796	526,681
1	shoutcast	client-server	12,657,703,648	288
4	skydrive-base	browser-based	12,051,827,913	42,611
2	twitter-base	browser-based	8,968,282,256	744,608
3	webex-base	client-server	8,157,947,397	34,883

図 6: 消費バイト数順に示した上位の HTTP アプリケーション

上位 25（349 中）の HTTP アプリケーションに関するに関する主な結果:

ネットワークを通過し、何らかの方法で HTTP を使用するアプリケーションには、業務関連と非業務関連のアプリケーションがあります。

上位の URL カテゴリ

アプリケーション トラフィックの可視性に関して検討すべき別の側面として、ユーザが使用する Web サイトの識別と制御があります。URL フィルタ制御にアプリケーション制御と脅威防御を組み合わせることで、ネットワーク セキュリティを大幅に向上させることができます。以下の表に最も頻繁にアクセスされている URL カテゴリを示します。

URL Category	Count
business-and-economy	12,324,042
search-engines	4,176,341
content-delivery-networks	3,347,768
unknown	3,288,567
web-advertisements	3,036,954
news-and-media	3,034,400
computer-and-internet-info	3,011,787
private-ip-addresses	1,944,833
shopping	1,888,818
streaming-media	1,626,144
internet-portals	1,549,721
social-networking	1,207,404
web-based-email	962,672
financial-services	703,414
sports	699,224
travel	571,212
society	562,097
auctions	493,282
shareware-and-freeware	430,405
reference-and-research	379,204
entertainment-and-arts	353,828
personal-sites-and-blogs	341,728
motor-vehicles	251,791
dynamically-generated-content	233,509
computer-and-internet-security	206,833

図 7: 上位の URL カテゴリ

上位25 の URL に関する主な結果:

URL カテゴリのレポートには、業務関連と非業務関連の Web アクティビティが示されています。

アプリケーションの脆弱性を検出

使用するポート ホッピング、トンネリング、その他の回避手法に関係なく、ネットワーク上のアプリケーションの可視性増加を脆弱性攻撃に対する防御にも拡大することで、脅威の検出とブロックが確実に行えるようにします。ネットワーク上で検出されたアプリケーションの脆弱性の数を、重要度ごとにランキングしたものを以下の表にまとめました。

Threat Name	Application	Category	Severity	Count
Microsoft SQL Server Stack Overflow Vulnerability	mssql-mon	code-execution	Critical	964
Microsoft ASP.Net Information Leak brute force Attempt	web-browsing	brute-force	Critical	781
Microsoft ASP.Net Information Leak brute force Attempt	flash	brute-force	Critical	25
Microsoft IIS ASP.NET NULL Byte Injection Information Disclosure Vulnerability	hotmail	info-leak	Critical	10
Microsoft ASP.Net Information Leak brute force Attempt	silverlight	brute-force	Critical	9
Microsoft Windows Print Spooler Service Format String Vulnerability	netbios-dg	code-execution	Critical	5
Oracle Java SE Remote Java Runtime Environment Remote Code Execution Vulnerability	web-browsing	code-execution	Critical	4
OpenSSL SSLv2 Malformed Client Key Parsing Buffer Overflow Vulnerability	ssl	code-execution	Critical	2
Blackhole Exploit Kit	web-browsing	code-execution	Critical	2
Microsoft Internet Information Server ISAPI Extension Buffer Overflow Vulnerability	http-proxy	code-execution	Critical	1
SIP Max-Forwards Header Field Overflow	sip	overflow	High	93,177
HTTP NTLM Authentication Brute Force Attack	http-proxy	brute-force	High	83,858
MIT Kerberos kadmind RPC Library Unix Authentication Stack Overflow Vulnerability	rpc	code-execution	High	7,309
HTTP NTLM Authentication Brute Force Attack	apple-update	brute-force	High	3,627
HTTP Forbidden Brute Force Attack	http-proxy	brute-force	High	1,696
Fragroute Evasion Attack For Unknown-tcp Traffic	unknown-tcp	code-execution	High	1,043
HTTP: User Authentication Brute-force Attempt	sharepoint-base	brute-force	High	743
HTTP Forbidden Brute Force Attack	sharepoint-base	brute-force	High	742
HTTP Forbidden Brute Force Attack	web-browsing	brute-force	High	636
HTTP NTLM Authentication Brute Force Attack	facebook-base	brute-force	High	556
FTP: login brute force attempt	ftp	brute-force	High	520
HTTP NTLM Authentication Brute Force Attack	twitter-base	brute-force	High	501
HTTP NTLM Authentication Brute Force Attack	hotmail	brute-force	High	359
HTTP NTLM Authentication Brute Force Attack	rtmpt	brute-force	High	341
HTTP: User Authentication Brute-force Attempt	sharepoint-documents	brute-force	High	304

図 8: 重要度と件数順に示した上位の脅威

最も多く検出された 25（537中）の攻撃に関する主な結果:

Palo Alto Networks の次世代ファイアウォールは、ポートやプロトコルに関係なく、ネットワークを通過する脆弱性攻撃の可視化を実現します。

検出された537脆弱性の中で、4%件が Critical レベル、25%件が High レベル、4%件が Medium レベルでした。残りは、Low または Informational でした。

ネットワーク上で検出されたスパイウェアとウイルス

使用するポート ホッピング、トンネリング、その他の回避手法に関係なく、ネットワーク上のアプリケーションの可視性増加により、スパイウェア、関連するコマンド、制御トラフィック、ウイルスの検出とブロックが行えます。 下の図 9 および 10 は、ネットワーク上で検出されたスパイウェアとウィルスの例です。

Threat Name	Application	Type	Severity	Count
ZeroAccess.Gen Command and Control Traffic	unknown-udp	spyware phone home	Critical	3,051,614
Bot: Mariposa Command and Control	unknown-udp	spyware phone home	Critical	105,675
TDL4 DNS Request Traffic	dns	spyware phone home	Critical	465
Alueron Command and Control Traffic	http-proxy	spyware phone home	Critical	292
Win32.Conficker.C p2p	unknown-udp	spyware phone home	Critical	190
ZeroAccess.Gen Command and Control Traffic	bittorrent	spyware phone home	Critical	14
Conficker DNS Request	dns	spyware download	High	200,277
Trojan.agent:orgnet.pl	dns	Suspicious DNS	Medium	33,348
Trojan.inject:comee.pl	dns	Suspicious DNS	Medium	1,974
generic:8jc3b0a2a97ftbll0cza.com	dns	Suspicious DNS	Medium	1,477
Suspicious user-agent strings	web-browsing	spyware phone home	Medium	1,304
Backdoor.bredolab:bhostdb.webtelmex.net.mx	dns	Suspicious DNS	Medium	1,066
Suspicious user-agent strings	http-proxy	spyware phone home	Medium	819
generic:spacingtheinsi.su	dns	Suspicious DNS	Medium	705
generic:logging.vitruvian.biz	dns	Suspicious DNS	Medium	544
generic:a.adtpix.com	dns	Suspicious DNS	Medium	543
generic:xxx.p54c9e.com	dns	Suspicious DNS	Medium	373
Virus.sality:s-188-64-85-58.atmcdn.pl	dns	Suspicious DNS	Medium	202
generic:woohoowoo.com	dns	Suspicious DNS	Medium	183
generic:rankey.nefficient.co.kr	dns	Suspicious DNS	Medium	174
Rogue DNS Servers Request	dns	spyware phone home	Medium	167
Trojan.vbkrypt:peasjv.com	dns	Suspicious DNS	Medium	164
Trojan.vbkrypt:gokrxn.com	dns	Suspicious DNS	Medium	151
generic:ws.smartiengine.com	dns	Suspicious DNS	Medium	105
Trojan.jorik:d0m78c.com	dns	Suspicious DNS	Medium	102

図 9: 重要度と件数順に示した上位のスパイウェア

最も多いウイルス

Threat Name	Application	Count
Virus/Win32.WGeneric.dghz	web-browsing	6
Virus/Win32.WGeneric.digl	flash	2
HTML/Trojan.redir.ej	web-browsing	2

図 10: 件数順に示した上位のウイルス

最も多く検出された(78中)スパイウェアとウイルスに関する主な結果:

Palo Alto Networks の次世代ファイアウォールは、ポートやプロトコルに関係なく、ネットワークを通過するウイルスとスパイウェアの可視化を実現します。

最も一般的なタイプのマルウェアは、spyware phone homeでした。

ネットワーク上で検出された最新のマルウェア

全30 個のファイル に対して、WildFire が 03 December 2012 以前の 7 日間に渡り分析した結果、2 個のマルウェアが検出されました。

最新のマルウェア アンチウイルス ベンダ対応内容のサマリ

VirusTotal（VT）の統計に基づき、WildFire が検出したマルウェアに対応しているアンチウイルス（AV）ベンダのサマリを以下に示します。

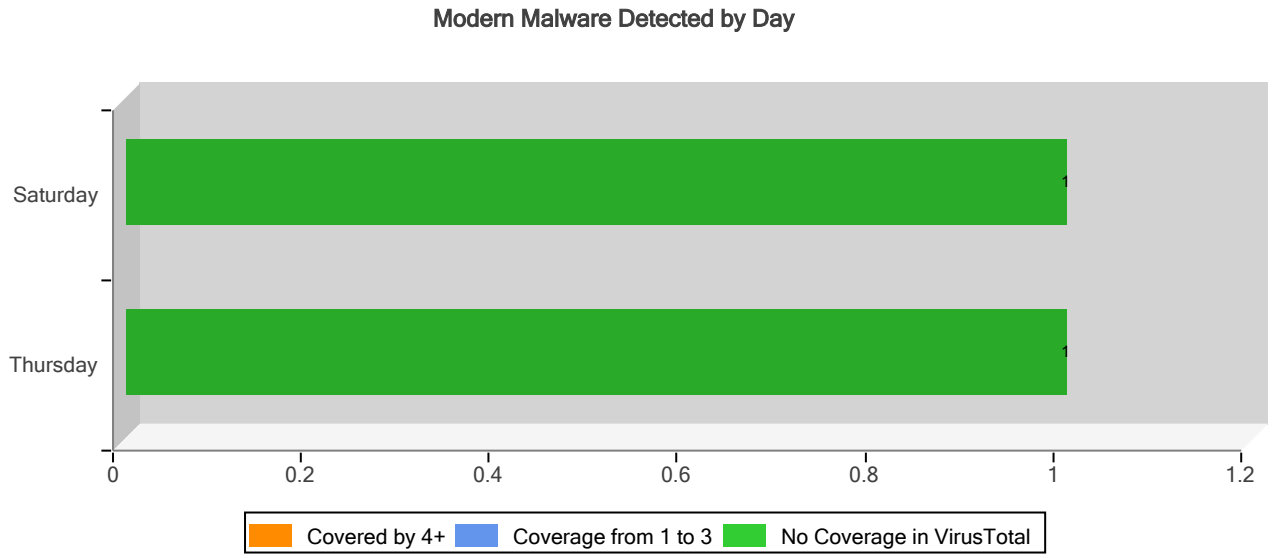


図 11: VirusTotal の統計に基づき WildFire が検出したマルウェア に対応している アンチウイルス ベンダ

WildFire が検出したマルウェアのサンプル

以下のリストは WildFire が検出したいくつかの悪意のあるファイルと、その VirusTotal ベンダ対応状況を示したものです。ファイル名の最初の 30 文字を MD5 チェックサムと一緒に示しており、WildFire コンソールでサンプルを詳細に調査できるようになっています。

Filename	MD5	Application	AV Vendor Coverage
about.exe	252cb0f4587c3bb60c9a5b2b50459f07	web-browsing	Unknown to VT
Launcher.exe.deploy	1b185788f9fbb9fe41e56c9e473e867e	web-browsing	Unknown to VT

図 12: WildFire が検出した悪意のあるファイルの例

WildFire が検出した最新のマルウェアに関する主な結果:

上記のデータは、2 種類の悪意のあるファイルがあったことを示しており、これらは WildFire がなければ検出されずにネットワークを通過していたことになります。この種の最新の脅威は高度な攻撃の最前線にあるもので、あらゆる階層のセキュリティ対策において検出と対応ができるようにしておく必要があります。

ネットワーク上を通過するファイルとファイル タイプ

ファイルを転送するアプリケーションは、今日のビジネス環境に不可欠なものです。ネットワーク上を通過しているファイルとコンテンツのタイプを把握することで、組織は各種のビジネスおよびセキュリティ上の脅威を回避できます。以下の表に、最も一般的なファイルとコンテンツのタイプ、関連するアプリケーションを示します。

File/Content Name	Data or File	Transfer Direction	Application Used	Count
ZIP	file	Download	web-browsing	22,538
ZIP	file	Download	google-earth	16,839
ZIP	file	Download	symantec-av-update	6,343
ZIP	file	Download	itunes-base	5,087
Microsoft Cabinet (CAB)	file	Download	ms-update	4,344
ZIP	file	Download	sharepoint-base	3,490
FLV File	file	Download	youtube-base	3,287
MP3 File	file	Upload	http-proxy	2,574
ZIP	file	Download	flash	2,414
MP3 File	file	Upload	web-browsing	2,360
Adobe Portable Document Format (PDF)	file	Download	web-browsing	2,329
FLV File	file	Download	flash	2,256
Microsoft PE File	file	Download	web-browsing	2,108
Microsoft PE File	file	Upload	ms-ds-smb	2,043
Quicktime MOV File	file	Download	http-video	1,896
ZIP	file	Upload	sharepoint-documents	1,851
Adobe Portable Document Format (PDF)	file	Upload	smtp	1,771
Windows Executable (EXE)	file	Download	web-browsing	1,459
Java Class File	file	Download	web-browsing	1,420
ZIP	file	Download	sharepoint-documents	1,389
Windows Dynamic Link Library (DLL)	file	Upload	ms-ds-smb	1,386
ZIP	file	Download	silverlight	1,276
MP4 Detected	file	Download	http-video	1,271
ZIP	file	Upload	web-browsing	1,239
ZIP	file	Download	http-proxy	1,174
MP3 File	file	Download	grooveshark	1,082
Windows Dynamic Link Library (DLL)	file	Download	silverlight	998
Microsoft PE File	file	Download	silverlight	998
Microsoft PE File	file	Download	ms-ds-smb	803
Windows Executable (EXE)	file	Download	ms-ds-smb	766

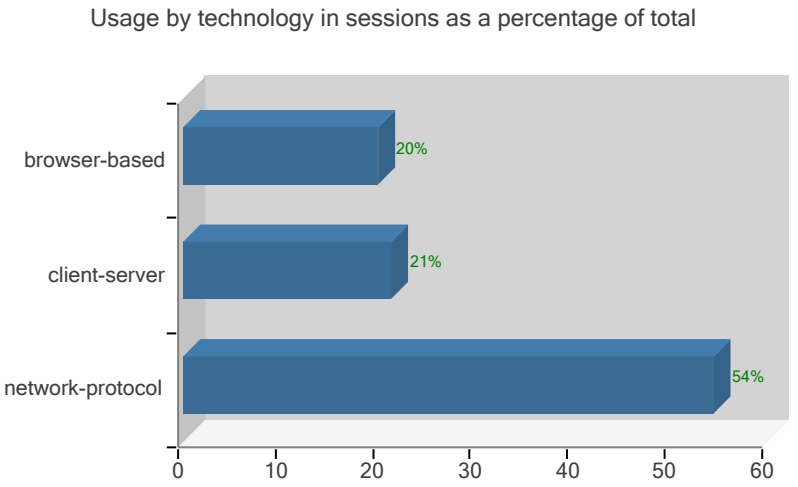
図 13: ネットワークを通過するファイルとコンテンツ タイプをタイプと数で分類

ネットワーク上を通過するファイルとコンテンツに関する主な結果:

評価では、タイプ(ファイルの拡張子だけを見るのではなく)と機密データ パターン(クレジット カードや社会保障番号)に基づき、ファイルを検出しました。

基礎になっているテクノロジとカテゴリ別のアプリケーション

基礎になっているアプリケーションとアプリケーション サブカテゴリに基づき、消費されているリソース（セッションとバイト）を確認することで、アプリケーションおよび脅威データを詳細に補足し、ネットワーク アクティビティの全貌が把握できます。以下の表は、アプリケーション サブカテゴリごとに、基礎になっているアプリケーションと消費されたバイト数に基づき、使用したセッション数を示します。



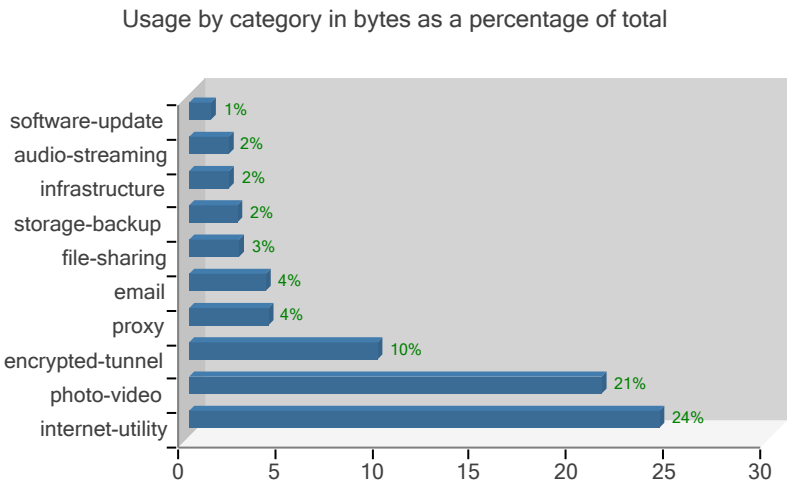


図 14: テクノロジ（セッション）とバイト数（カテゴリ）ごとのアプリケーション リソース消費量

カテゴリとテクノロジごとのアプリケーション使用状況の主な結果:

評価中、network-protocolがセッションの54%を消費しました。

カテゴリごとのアプリケーション使用状況では、internet-utility アプリケーションが全体帯域幅の 24% を消費しました。

調査結果:

調査分析の計画段階で、一般的な多くのネットワーク環境はオープンな状態であり、どのアプリケーションがネットワークを通過しているかを確認できないことから、Customer ABC様の環境においても、さまざまなビジネス リスクとセキュリティ リスクが考えられることを説明しました。今回の調査結果から以下の点が判明いたしました。

アクティビティを隠蔽するアプリケーションを検出: ネットワークでアクティビティを隠蔽するアプリケーションが確認されました。IT テクノロジに精通するユーザが、アクティビティを隠蔽し、セキュリティをバイパスするためにこれらのアプリケーションを使用しています。

P2P およびオンライン ファイル転送アプリケーションの使用: P2P およびオンライン ファイル転送/共有アプリケーションにより、Customer ABC様の環境においてセキュリティ、情報漏洩、および著作権侵害のリスクが及ぶ可能性があります。

メディア アプリケーションおよびソーシャル ネットワーキング アプリケーションの使用:
ネットワークでエンターテインメントや個人的な連絡方法として使用されるアプリケーション(メディア、オーディオ、ソーシャル ネットワーキング)が確認されました。これらのアプリケーションは、士気低下、人材流失、利用ユーザの満足度と生産性低下、脅威に対する露呈、コンプライアンス、および情報漏洩のリスクといった様々な点を考慮しながらバランスをどのように取るかという重要な IT 課題を提示しています。

Web メール、IM、および VoIP の使用:
ネットワークでこれらのアプリケーション例が確認されました。これらのアプリケーションの多くは、簡単にファイアウォールをバイパスし、脅威を運ぶ手段となるだけでなく、データの漏洩を招く可能性があります。

推奨される対策:

安全なアプリケーション利用ポリシーの実装:
多くの組織と同様、様の環境においてもこれまではアプリケーション使用を統括する細分化されたポリシーが存在しなかったものと推察いたします。ユーザが活用するアプリケーションが増え、ユーザがセキュリティ回避を行う傾向と、その弱点を利用する脅威が拡大していることから、アプリケーション単位またはアプリケーション カテゴリ単位で使用を制御するセキュリティ ポリシーの適用を推奨します。 現在では、このようなポリシーによる制御が必要でかつ、また技術的にも可能です。

P2P およびオンライン ファイル転送/共有などのハイリスクなアプリケーションに対応:
ユーザがこれらのアプリケーションを使用して既存のファイアウォールによる制御をバイパスしていることから、Customer ABC 様にとって、これらのアプリケーションに伴うリスクが問題になる可能性があります。これらのリスクの把握、分類、および低減を行わない場合、Customer ABC様の環境で不正なデータ転送が行われるだけでなく、それらに関連したウイルスなどの脅威が及ぶ可能性があります。

プロキシおよびリモート アクセス アプリケーションの使用を取り決めるポリシーを適用:
これらのアプリケーションは、自宅のコンピュータとアプリケーションにアクセスする社員によって使用されることがあります。これにはビジネスとセキュリティの両方のリスクがあります。Customer ABC様の環境でもこの種のアプリケーションの使用に関するポリシーを実装する必要があります。

メディア アプリケーションの制御:
Customer ABC様は、一般ユーザの反感を買うことなく、これらのアプリケーションの使用に関するポリシーとそれを適用する手段について検討する必要があります。考えられるオプションとして、時間帯による利用の可否制御、または QoS マーキングや帯域制御による使用量制限などがあります。

アプリケーションの可視化と制御を実現:
アプリケーション レベルのリスクを低減する唯一の手段は、最初にアプリケーション トラフィックを可視化し、理解して、それを統括するポリシーを作成および適用できるようにすることです。特定のアプリケーションのみ可視性を得るにはいくつかのテクノロジがありますが、組織で流れるすべてのアプリケーション トラフィックの可視化、理解、および制御を行い、企業に適したスケーラビリティを提供できるのは、次世代ファイアウォールのみです。したがって、当社では、Customer ABC 様のネットワークに Palo Alto Networks ファイアウォールを配備し、アプリケーションごとに細分化されたポリシーを作成することで、アプリケーション トラフィックを可視化し、組織の優先度に応じてネットワークを管理・運用されることを推奨します。

付録 A: ビジネス リスクの定義

本書のリスク分析を行う上で、企業とそのプロセスにアプリケーションが及ぼす可能性のある影響を検討しました。ビジネスに対するリスクは、次の 5 つのカテゴリに分類できます。

生産性:
生産性に対するリスクは次に挙げる 2 種類の乱用から引き起こされます。

-
- 社員が、本来の業務を行う代わりに、業務とは無関係のアプリケーション（Myspace、Facebook、個人電子メール、ブログなど）を
  - 業務とは無関係のアプリケーション（YouTube、ストリーミング/HTTP オーディオなど）が帯域幅を大量に消費し、本来のアプリケーションのパフォーマンスが低下する。

コンプライアンス:
ほとんどの組織では、一連の政府規制およびビジネス規制を順守する必要があります（米国の場合、GLBA、HIPAA、FD、SOX、FISMA、PCI など）。これらの規制のほとんどは、組織の営業、財務、顧客、または社員のデータを保護することを目的としています。特定のアプリケーションは、それ自体が問題となるか、データに対する脅威となることで、これらのデータに大きなリスクをもたらします（BitTorrent および MySpace など）。ファイルを転送できるあらゆるアプリケーション（Web メール、Skype、IM）は、深刻なコンプライアンス問題を引き起こす可能性があります。

運用コスト:
運用コストに対するリスクには 2 つの可能性があります。1 つは、アプリケーションおよびインフラストラクチャが過度に不正使用され、ビジネス プロセスの機能を保証するために追加で機器やサービスを購入する必要性が生じることで（ストリーミング ビデオにより WAN 回線をアップグレードするなど）、2 つ目は、インシデントや攻撃により IT 費用が発生することです（攻撃またはウイルスによるセキュリティ問題の後にサーバーまたはネットワークを再構築するなど）。

事業継続性:
事業継続性のリスクとは、特定のビジネス プロセスの重要なコンポーネントを停止させるか、使用不能にするようなアプリケーション（またはアプリケーションが持つ脅威）を指します。この例として、電子メール、トランザクション処理アプリケーション、脅威の影響を受ける一般向けのアプリケーション、非業務アプリケーションが大量のリソースを消費することによるサービス拒否が挙げられます。

情報漏洩:
情報漏洩のリスクは、データの盗難、漏洩、または破壊に関連する従来方式の情報セキュリティのリスクを指します。この例として、顧客データの盗難、知的財産の盗難または不注意による漏洩、またはセキュリティ脅威/違反によるデータの破壊が挙げられます。アプリケーション（Facebook、Kazaa、IM、Web メールなど）に起因する悪用、企業のリソースを使用して実行される非業務関連アプリケーション（BitTorrent、IM など）をはじめとするさまざまな脅威がこれらのリスクの原因となります。

付録 B: Palo Alto Networks の主要テクノロジとサービス

Palo Alto Networks の次世代ファイアウォールにより、組織全体で専用ハードウェア プラットフォームまたは仮想化されたフォーム ファクタで提供される各種のテクノロジやサービスを使用して、アプリケーション、ユーザ、コンテンツの安全性を確保することができます。

App-ID: アプリケーションが使用しているポートやその他の回避技法に関係なく、App-ID は複数のトラフィック識別メカニズムを使用して、ファイアウォールが検出するとすぐにアプリケーションを正確に識別します。アプリケーションの識別情報をすべてのセキュリティ ポリシーの判断基準とします。未知のアプリケーションは分類と体系的な管理のために分類されます。

User-ID: 組織は、使用しているプラットフォームに関係なく、ユーザベースのアプリケーション利用ポリシーをあらゆるユーザに展開することができます。User-ID は各種のエンタープライズ ディレクトリ（Microsoft Active Directory、eDirectory、Open LDAP）や端末さーサービス製品（Citrix および Microsoft Terminal Services）にシームレスに統合できます。Microsoft Exchange、Captive Portal、XML API との統合によって、組織は通常ドメイン外にいる Apple Mac OS X、Apple iOS、および UNIX ユーザにもポリシーを拡大できます。

グローバルな保護: 本社サイトで使用されている安全なアプリケーション利用ポリシーと同じものを、場所やデバイスに関係なく、すべてのユーザに提供します。リモート ユーザは強力な認証を使用して最寄りのゲートウェイに自動的に、そして安全に接続し、オンライン状態にある間は、コーポレート ネットワークに接続して、会社の構内にいるかのように保護されます。その結果、一貫したポリシー、強化されたセキュリティ体制、運用コストの削減が実現できます。

Content-ID: 統一されたシグネチャ フォーマットと、遅延を軽減するシングル パス スキャニング エンジンを使用して、脆弱性攻撃、マルウェア、関連するマルウェアで生成されたC&C 通信を防止します。脅威の防止は完全なアプリケーションとプロトコル コンテキストに適用され、使用されている回避技法に関係なく、脅威を検出およびブロックできるようにします。URL フィルタリングによって Web 閲覧に対するポリシー制御を行い、ファイルとデータのフィルタリングによって不正なデータ転送を防止します。

WildFire: クラウドベースのバーチャル サンドボックス環境で直接ファイルを実行して、従来のシグネチャでは制御できないカスタム マルウェアを検出します。WildFire は実行ファイルに対して 100 種類以上の悪意のある振る舞いを監視し、結果を管理者に提供します。ファイルに悪意がある場合、シグネチャを自動的に生成してすべてのユーザに配信します。

Panorama: 組織が Palo Alto Networks ファイアウォールを1か所から管理できるようにして、グローバルで一元化された制御と、テンプレートや共有ポリシーなどの機能によるローカル ポリシーの柔軟性の両方のバランスを取ります。Panorama では、管理対象のデバイスや仮想システムを一元化して制御できます。

専用のハードウェアまたはバーチャル プラットフォーム: エンタープライズのリモート オフィス向けの PA-200 から、高速データセンタ向けの PA-5060 まで、各種専用ハードウェア プラットフォーム上で安全なアプリケーション利用機能が豊富に提供されています。プラットフォーム アーキテクチャはシングル パス ソフトウェア エンジンに基づき、ネットワーキング、セキュリティ、脅威防御、管理といった特定機能に特化した処理プロセッサを使用して高いパフォーマンスを提供します。また、ハードウェア プラットフォームで提供されるものとまったく同じファイアウォール機能は、VM シリーズという仮想ファイアウォールでも利用できるため、組織は仮想化およびクラウドベースのコンピューティング環境を保護することができます。

Appendix C: Additional Information

[Insert additional info]