730 アプライアンス レポート

レポートのデモ | 2013 年 **4 月 6 日** 04:24am / 2013 年 **4 月 17 日** 06:11pm

アンチボット
283 個のマルウェア

アンチウイルス
364 個のマルウェア

IPS
3 件のインシデント

Threat Emulation
0 個の悪質なファイル
1000 ファイルをスキャン

帯域消費の上位ランク

High Bandwidth | 上位ランク カテゴリ
45.6GB(26.8%) 帯域幅

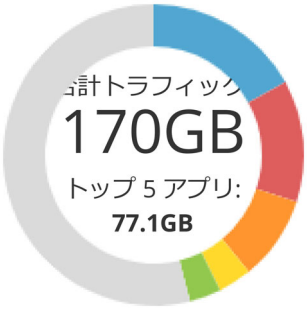
youtube.com | 上位ランク サイト
31.1GB(18.3%) 帯域幅

John A | 上位ランク ユーザ
25GB(14.7%) 帯域幅

130GB
受信の合計

40GB
送信の合計

アプリケーション別の帯域消費



- **17%** YouTube
- **13%** Gmail
- **9.1%** SSL Protocol
- **3.6%** Wikipedia
- **3.4%** Facebook
- **53.9%** その他

7 台の感染ホスト

- **5** 台のホストが高/深刻な感染
- **4** 台の感染疑いのあるサーバ
- **7** 台の最近アクティブな感染ホスト

15 個の高リスク アプリケーション

- **最も使用している高リスク アプリケーション:**
  WinMX World, eMule, 3proxy.com, DroidVPN, その他...
- **高リスク アプリケーションの上位ユーザ:**
  John A, Tim R, Dan B, Jill F, Beth D, Jeffie M, その他...

名前: **Gateway-ID-7F21D278** | バージョン: **R77.20.00-devel** | MAC: **00:1C:7F:21:D2:78**

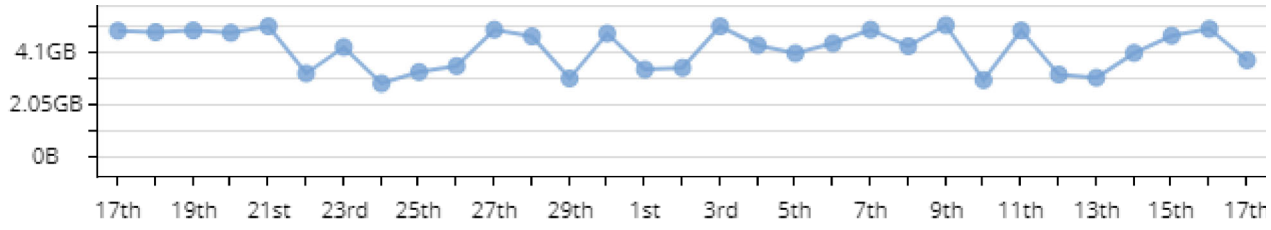
目次

レポートのデモ: 2013 年 4 月 6 日 04:24am / 2013 年 4 月 17 日 06:11pm

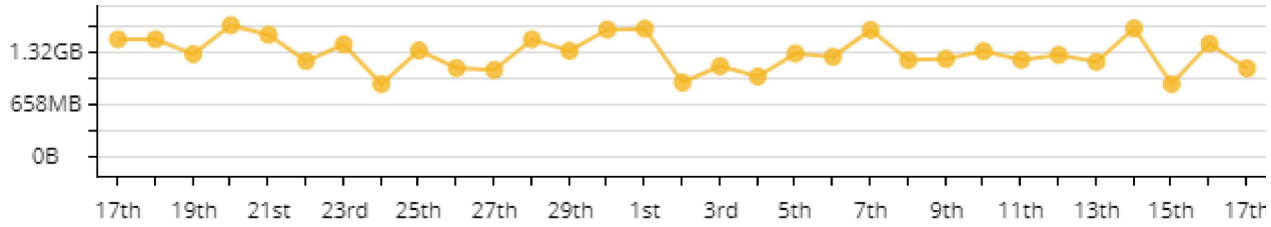
ネットワーク使用量

レポートのデモ: 2013 年 4 月 6 日 04:24am / 2013 年 4 月 17 日 06:11pm

受信トラフィック



送信トラフィック



帯域幅の使用量

日付	帯域幅	受信	送信
9 17th	6.38GB	4.91GB	1.47GB
9 18th	6.32GB	4.85GB	1.47GB
9 19th	6.21GB	4.92GB	1.28GB
9 20th	6.48GB	4.83GB	1.64GB
9 21st	6.61GB	5.09GB	1.53GB
9 22nd	4.43GB	3.24GB	1.19GB
9 23rd	5.67GB	4.27GB	1.4GB
9 24th	3.75GB	2.84GB	905MB
9 25th	4.62GB	3.29GB	1.33GB
9 26th	4.63GB	3.53GB	1.11GB
9 27th	6.04GB	4.95GB	1.08GB
9 28th	6.16GB	4.69GB	1.47GB
9 29th	4.36GB	3.04GB	1.32GB
9 30th	6.4GB	4.8GB	1.59GB
10 1st	4.99GB	3.39GB	1.6GB
10 2nd	4.38GB	3.46GB	923MB
10 3rd	6.21GB	5.08GB	1.13GB
10 4th	5.34GB	4.34GB	999MB
10 5th	5.31GB	4.02GB	1.29GB
10 6th	5.66GB	4.42GB	1.25GB
10 7th	6.54GB	4.96GB	1.59GB
10 8th	5.51GB	4.31GB	1.21GB
10 9th	6.35GB	5.13GB	1.22GB
10 10th	4.29GB	2.97GB	1.32GB
10 11th	6.13GB	4.92GB	1.21GB
10 12th	4.46GB	3.19GB	1.27GB
10 13th	4.25GB	3.07GB	1.18GB
10 14th	5.65GB	4.04GB	1.61GB
10 15th	5.62GB	4.72GB	904MB
10 16th	6.4GB	4.98GB	1.41GB
10 17th	4.86GB	3.75GB	1.1GB
サマリ	**170GB**	**130GB**	**40GB**

上位アプリケーション

レポートのデモ: 2013 年 4 月 6 日 04:24am / 2013 年 4 月 17 日 06:11pm

帯域幅別の上位アプリケーション

アプリケーション	リスク	帯域幅	受信	送信
YouTube		28.3GB(17%)	26.7GB	1.62GB
Gmail		21.4GB(13%)	14.8GB	6.62GB
SSL Protocol		15.5GB(9.1%)	12.4GB	3.12GB
Wikipedia		6.09GB(3.6%)	5.09GB	1GB
Facebook		5.81GB(3.4%)	2.53GB	3.28GB
Check Point Endpoint Security		5.77GB(3.4%)	5.56GB	209MB
Kerberos Protocol		5.5GB(3.2%)	4.2GB	1.3GB
uTorrent		5.48GB(3.2%)	5.07GB	415MB
DNS Protocol		4.34GB(2.6%)	3.18GB	1.15GB
WinMX World		3.49GB(2.1%)	1.95GB	1.54GB
上位ランク アプリケーション...		**102GB(60%)**	**81.4GB**	**20.3GB**

セッション別の上位アプリケーション

アプリケーション	リスク	セッシ...
SSL Protocol		2.1G
DNS Protocol		1.9G
Facebook		1.8G
YouTube		1.5G
Gmail		1.1G
Wikipedia		799M
AppWiki		799M
Check Point Endpoint Security		569M
Kerberos Protocol		379M
Feedburner		243M
上位ランク アプリケーション...		**11G**

上位サイト

レポートのデモ: 2013 年 4 月 6 日 04:24am / 2013 年 4 月 17 日 06:11pm

帯域幅別の上位サイト

サイト	帯域幅	受信	送信
youtube.com	31.1GB(18%)	29.1GB	1.98GB
mail.google.com	23.5GB(14%)	14.8GB	8.74GB
linkedin.com	10.8GB(6.3%)	7.28GB	3.48GB
cnn.com	10.7GB(6.3%)	6.67GB	4.02GB
Wikipedia.org	9.37GB(5.5%)	8.18GB	1.19GB
facebook.com	5.49GB(3.2%)	2.26GB	3.24GB
Amazon.com	3.75GB(2.2%)	2.55GB	1.2GB
Ebay.com	1.11GB(0.7%)	757MB	355MB
Ask.com	328MB(0.2%)	218MB	109MB
上位ランク サイト合計	**96.1GB(57%)**	**71.8GB**	**24.3GB**

セッション別の上位サイト

サイト	セッシ...
mail.google.com	4.4G
cnn.com	2G
linkedin.com	1.7G
facebook.com	1.6G
youtube.com	990M
Amazon.com	600M
Wikipedia.org	594M
Ebay.com	178M
Ask.com	55M
上位ランク サイト合計	**12G**

上位カテゴリ

レポートのデモ: 2013 年 4 月 6 日 04:24am / 2013 年 4 月 17 日 06:11pm

帯域幅別の上位カテゴリ

カテゴリ	帯域幅	受信	送信
High Bandwidth	45.6GB(27%)	35.6GB	10GB
Email	17GB(10%)	12.6GB	4.42GB
Supports File Transfer	15.6GB(9.2%)	13.3GB	2.3GB
Social Networking	14.2GB(8.3%)	11.2GB	2.94GB
SSL Protocol	12.4GB(7.3%)	12.1GB	312MB
Share links	10.5GB(6.2%)	8.55GB	1.94GB
Transmits Information	9.07GB(5.3%)	7.98GB	1.09GB
VoIP	8.94GB(5.3%)	6.83GB	2.11GB
Low Risk	2.47GB(1.5%)	1.9GB	568MB
上位ランク カテゴリの合計	**136GB(80%)**	**110GB**	**25.7GB**

セッション別の上位カテゴリ

カテゴリ	セッシ...
SSL Protocol	2.7G
Low Risk	1.9G
High Bandwidth	1.8G
Social Networking	1G
Transmits Information	810M
Email	584M
Supports File Transfer	420M
Share links	324M
VoIP	292M
上位ランク カテゴリの合計	**10G**

上位ユーザ

レポートのデモ: 2013 年 4 月 6 日 04:24am / 2013 年 4 月 17 日 06:11pm

帯域幅別の上位ユーザ

ユーザ	帯域幅	受信	送信
John A	25GB(15%)	19.2GB	5.8GB
Beth D	24GB(14%)	19.1GB	4.93GB
Tim R	19.1GB(11%)	15.6GB	3.5GB
Dan B	18.3GB(11%)	15.3GB	3.06GB
Jill F	16GB(9.4%)	10GB	6GB
Lorrie B	6.62GB(3.9%)	5.1GB	1.52GB
Jeffie M	6.52GB(3.8%)	4.06GB	2.46GB
Elvis L	5.08GB(3%)	3.63GB	1.45GB
Nicola H	1.7GB(1%)	949MB	748MB
Lena H	1.25GB(0.7%)	611MB	635MB
上位ランク ユーザ合計	**124GB(73%)**	**93.6GB**	**30.1GB**

セッション別の上位ユーザ

ユーザ	セッシ...
Jill F	3G
John A	2.9G
Beth D	2.5G
Tim R	1.8G
Dan B	1.5G
Jeffie M	1.2G
Lorrie B	760M
Elvis L	725M
Nicola H	374M
Lena H	317M
上位ランク ユーザ合計	**15G**

セキュリティ イベント

レポートのデモ: 2013 年 4 月 6 日 04:24am / 2013 年 4 月 17 日 06:11pm

セッション別の上位の潜在的な高リスク アプリケーション

アプリケーション	リスク	セッシ...	帯域幅
WinMX World		46M	3.49GB
eMule		40M	357MB
3proxy.com		35M	1.23GB
DroidVPN		14M	846MB
Proxy based anonymizers		4.9M	1.58GB
uTorrent		1.5M	5.48GB

セッション別の上位の潜在的な高リスク アプリケーション ユーザ

ユーザ	セッシ...
John A	1G
Tim R	800M
Dan B	800M
Jill F	400M
Beth D	140M
Jeffie M	80M
Lorrie B	62M
Elvis L	54M
Nicola H	14M
Lena H	10M

侵入 & 攻撃イベント

レポートのデモ: 2013 年 4 月 6 日 04:24am / 2013 年 4 月 17 日 06:11pm

セッション別の上位保護

保護	セッシ...	帯域幅
Cross-site Scripting	4244T	N/A
Xerver HTTP CRLF Injection Response Splitting	2538T	N/A
ASCII Only Request	904T	N/A

上位マルウェア

名前	深刻度	インシ...
Possible bot tunneling through SMT...		31
Trojan-Clicker.Win32.Refpron.oc		20
Trojan.Win32.SurfSidekick.B		14
Trojan.Win32.VBKrypt.eqap		5
Scar		4
Worm.Win32.FFAuto.ey		4
JiFake		3
Cutwail		2
Trojan-Downloader.Win32.CodecPac...		2
Virut		1

感染したホスト

レポートのデモ: 2013 年 4 月 6 日 04:24am / 2013 年 4 月 17 日 06:11pm

感染したホストの一覧

ホスト	深刻度	保護の名前	最後のインシデ...	インシ...
192.168.0.2 (host2)		Bot.b	14 10, 2019	54
192.168.0.4		Bot.b	10 10, 2019	6
192.168.0.5 (host5)		Bot.b	14 10, 2019	35
192.168.0.1 (host1)		Bot.c	11 10, 2019	6
192.168.0.3 (host3)		Bot.c	9 10, 2019	1
192.168.0.6 (host6)		Bot.c	17 10, 2019	77
192.168.0.7 (host7)		Bot.c	17 10, 2019	8
192.168.0.9		Bot.c	10 10, 2019	53
192.168.0.1 (host1)		Bot.a	16 10, 2019	12
192.168.0.8		Bot.a	13 10, 2019	29
192.168.0.10 (host10)		Bot.a	8 10, 2019	2

感染の疑いがあるホストの一覧

ホスト	深刻度	保護の名前	最後のインシデ...	インシ...
192.168.0.11 (host11)		Virus.a	10 10, 2019	47
192.168.0.12 (host12)		Virus.a	15 10, 2019	25

インシデント数別の上位感染ホストおよび感染疑いのあるホスト

ホスト	インシ...
192.168.0.6	273
192.168.0.9	177
192.168.0.7	155
192.168.0.2	135
192.168.0.12	118
192.168.0.11	91
192.168.0.5	89
192.168.0.1	87
192.168.0.8	81
192.168.0.10	78