Generated on: Mon Feb 4 00:02:36 2013

Generated by: FMG-VM

Report Name: S-schedule-utm-reports t1-2013-02-04-0000

Data Range: 2013-01-01 00:00 - 2013-02-04 00:00 PST (FAZ local)

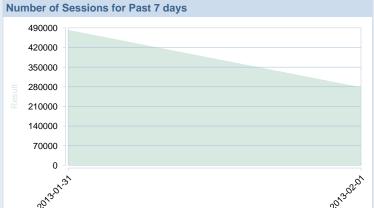
Devices: 11 (See Appendix A)

Date : Mon Feb 4 00:02:36 2013 Date Range : 2013-01-01 00:00-2013-02-04 00:00 PST (FAZ local) FortiAnalyzer Host Name : FMG-VM



Bandwidth and Applications

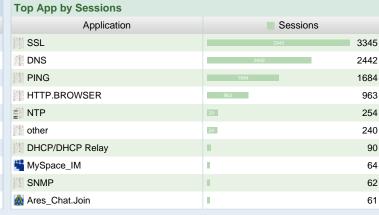


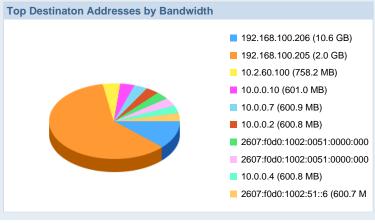


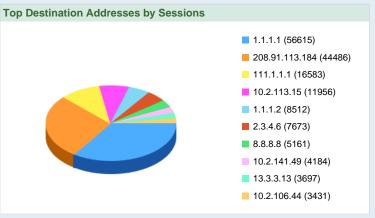
Top Users by	Bandwidth		
User	IP	Bandwidth Traffic Out Traffic	: In
! 10.2.60.105	10.2.60.105	11520483048 11.6 (GB
1 0.2.1.114	10.2.1.114	1.20	GВ
1 0.2.106.101	10.2.106.101	622.1	ИΒ
Meggie	10.0.0.7	600.1	ИΒ
Kirk	10.0.0.10	600.1	ИΒ
Alan	2607:f0d0:1002:51::6	600.1	ИΒ
Lauren	2607:f0d0:1002:0051:0000:	600.1	ИΒ
Luiz	10.0.0.4	600.1	ИΒ
Tom	10.0.0.2	600.1	ИΒ
R mike	2607:f0d0:1002:0051:0000:	600.0	ИΒ

Top User by Sessions			
User	IP	Sessions	
! 10.2.141.99	10.2.141.99	25804	25804
1 0.2.121.25	10.2.121.25	17709	17709
! 10.2.66.1	10.2.66.1	16007	16007
1 0.2.141.98	10.2.141.98	15873	15873
! 10.2.141.94	10.2.141.94	13578	13578
1 0.2.1.105	10.2.1.105	13042	13042
! 10.2.66.2	10.2.66.2	10968	10968
1 0.2.66.49	10.2.66.49	10427	10427
! 10.2.101.31	10.2.101.31	9424	9424
! 10.2.66.30	10.2.66.30	9079	9079

Top App by Bandwidth			
Application	Bandwidth	Traffic Out	Traffic In
	2400118000	2400118000	4.8 GB
MS.Windows.Update	1900796950	1900758036	3.8 GB
SSL	613539		636.5 MB
HTTP.BROWSER	1		18.9 MB
other			7.6 MB
DNS	I		1.1 MB
MySpace_IM			679.4 KB
Google.Talk	1		678.1 KB
Stream.Media			668.5 KB
Ares_Chat.Join			660.7 KB

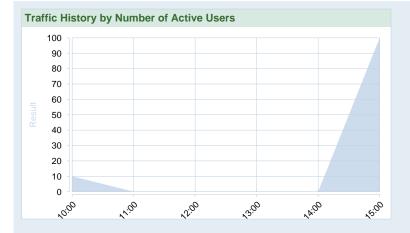








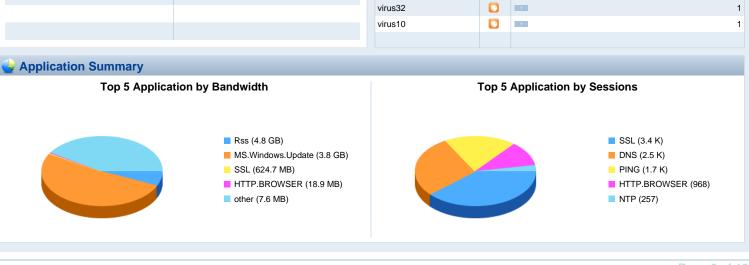


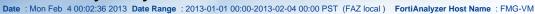




User Activity Summary (10.2.60.105)

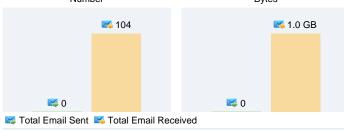










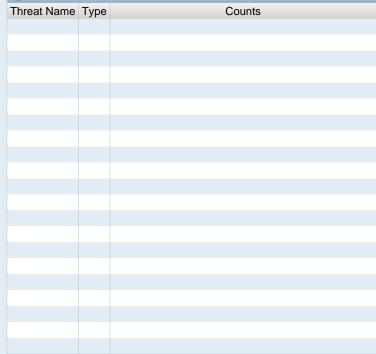


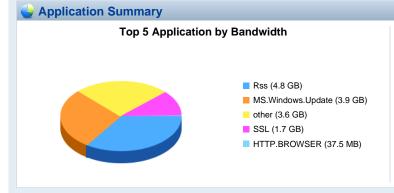
Top 5 Email Recipients

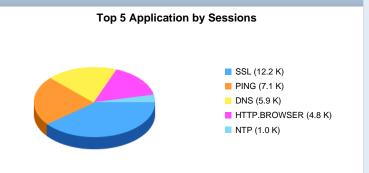
Recipient	Bandwidth
recipient37	200.4 MB
recipient39	200.4 MB
recipient24	200358051 200.4 MB
recipient36	200357590 200.4 MB
recipient34	200.4 MB

Sender	Bandwidth
sender33	200301406 200.3 MB
sender3	200291419 200.3 MB
sender23	200290735 200.3 MB
sender11	200289152 200.3 MB
sender2	200285529 200.3 MB









76

Total Email Sent K Total Email Received

🔀 53.2 KB



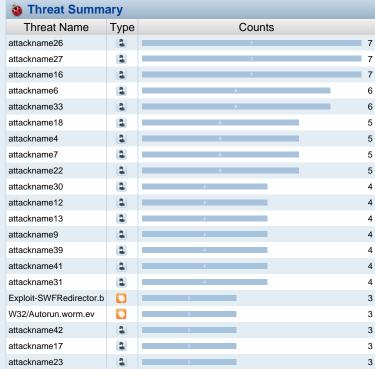


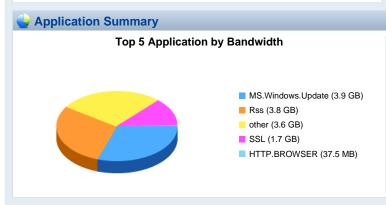
Top 5 Email Recipients

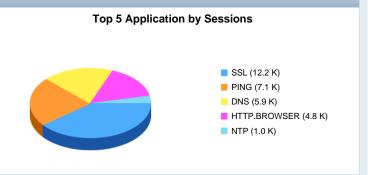
Recipient	Bandwidth
recipient37	200.4 MB
recipient36	200.3 MB
recipient27	200.3 MB
recipient14	200330434 200.3 MB
recipient8	200323485 200.3 MB

Sender	Bandwidth
sender33	200271112 200.3 MB
sender12	200259549 200.3 MB
sender21	200252300 200.3 MB
sender2	200249377 200.2 MB
sender13	200246701 200.2 MB











User Activity Summary (Tom)



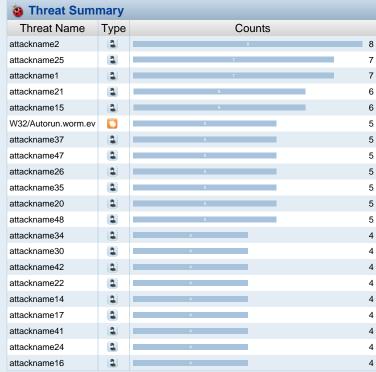


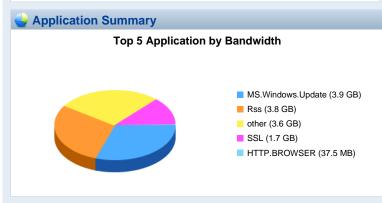
Top 5 Email Recipients

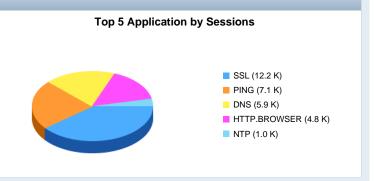
Recipient	Bandwidth
recipient39	200368254 200.4 MB
recipient37	200362701 200.4 MB
recipient29	200351845 200.4 MB
recipient27	200342008 200.3 MB
recipient24	200334253 200.3 MB

Sender	Bandwidth
sender33	200288425 200.3 MB
sender3	200284393 200.3 MB
sender23	200278612 200.3 MB
sender12	200270581 200.3 MB
sender22	200256129 200.3 MB



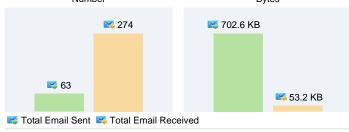












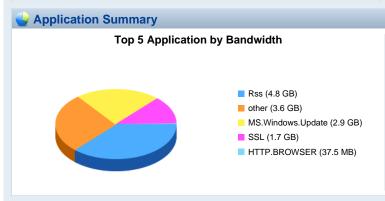
Top 5 Email Recipients

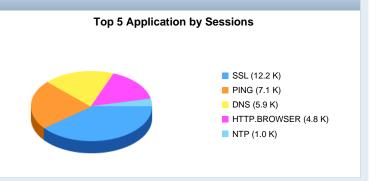
Recipient	Bandwidth
recipient39	200354122 200.4 MB
recipient37	200.4 MB
recipient34	200.3 MB
recipient24	200331092 200.3 MB
recipient27	200328113 200.3 MB

Sender	Bandwidth
sender3	200277315 200.3 MB
sender33	200270905 200.3 MB
sender21	200269491 200.3 MB
sender23	200255135 200.3 MB
sender11	200253256 200.3 MB



Threat Summa	ary		
Threat Name	Туре	Counts	
attackname31	2	6	6
attackname10	2	6	6
attackname16	2	6	6
attackname36	2	5	5
attackname25	2	5	5
attackname3	2	5	5
attackname18	2	5	5
attackname27	2	5	5
attackname45	2	5	5
attackname13	2	4	4
attackname26	2	4	4
attackname38	2	4	4
attackname19	2	4	4
attackname37	2	4	4
attackname47	2	4	4
attackname7	2	4	4
attackname0	2	4	4
Exploit-SWFRedirector.b	*	3	3
attackname6	2	3	3
attackname17	2	3	3
attackname32	2	3	3

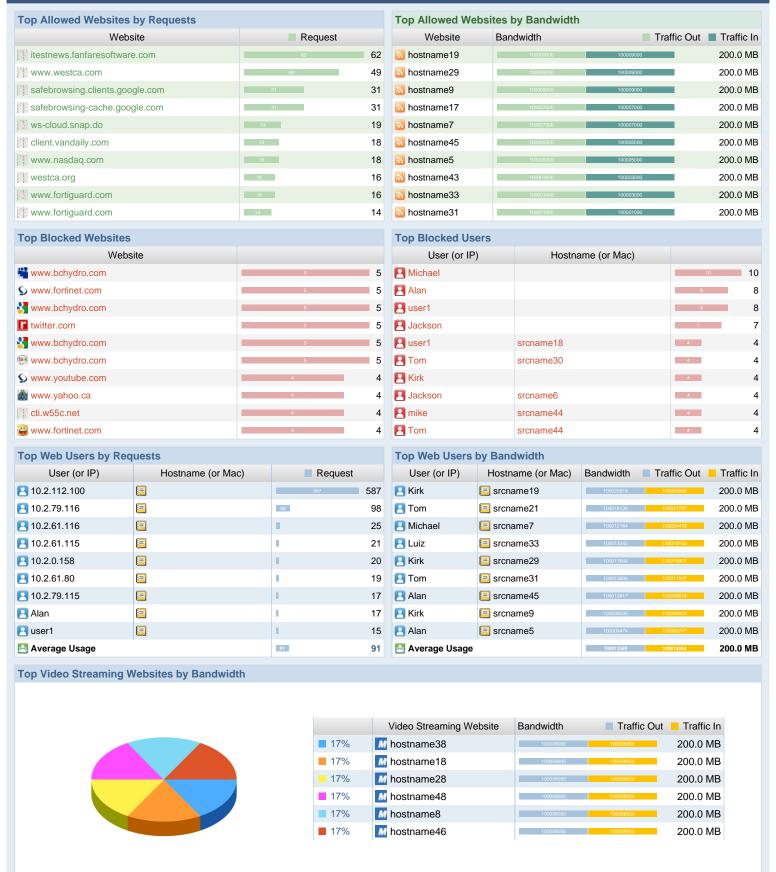








Web Usage







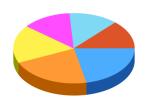
Emails

Top Senders by Number of Emails			Top Senders by Combine	ed Email Size
Sender	Number of Emails		Sender	Combined Email Size
Kirk	76	76	™ Tom	1000663348 1000.7 MB
	70	70	⋈ mike	1000.7 MB
i mike	66	66	k Luiz	1000.5 MB
™ Tom	65	65		1.7 MB
Meggie	63	63	Kirk	838.1 KB
Lauren	62	62	Meggie	702.6 KB
Michael	59	59		643.3 KB
Jackson	51	51	Michael	627.5 KB
⊯ Luiz	49	49		620.9 KB
K Alan	39	39	🔀 Alan	435.3 KB
Top Recipients by Number	er of Emails		Top Recipients by Comb	ined Email Size
Recipient	Number of Emails		Recipient	Combined Email Size
K Alan	104	104	K Alan	1001159377 1.0 GB
™ Tom	92	92	∠ Lauren	1001.0 MB
K Lauren	89	89	Kirk	1000975178 1001.0 MB
✓ Jackson	89	89	⋉ Meggie	1000922321 1000.9 MB
Kirk	88	88	∠ Jackson	800964279 801.0 MB
⋈ mike	87	87		800842522 800.8 MB
⋉ Luiz	85	85	⋉ Tom	1.0 MB
	80	80	⋉ Luiz	950.5 KB
Meggie	79	79	⋉ mike	901.5 KB

Threats

Top Viruses by Name			Top Virus Victims			
Virus Name	Occurrences		Virus Victims	Occurrences		
Exploit-SWFRedirector.b	16	16	Jackson	17	17	
W32/Autorun.worm.ev	15	15	₽ user1	16	16	
C Acid	14	14	₽ Tom	15	15	
Exploit-PDF.q.gen!stream	13	13	Lauren	15	15	
OAOL	12	12	! Kirk	14	14	
び W32/VBMania@MM	12	12	Meggie	14	14	
Acme	11	11	! mike	13	13	
○ FakeAlertAVSoft	10	10	Michael	11	11	
C Generic	10	10	Luiz Luiz	10	10	
Actifed	7	7	Alan	7	7	

Top Attack Source

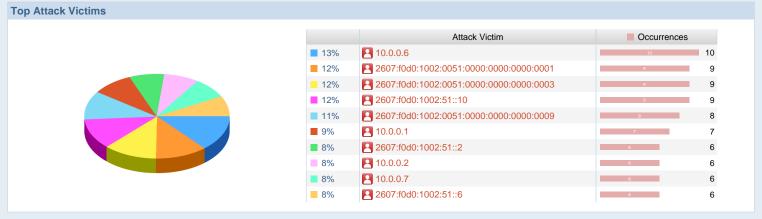


	Attack Source	Occurrences
22%	■ Alan	5 5
22%	₩ Kirk	5
17%	: ■ mike	4 4
13%	⊞ Jackson	3
13%	: ■ Jackson	3
13 %	: ■ Lauren	3





Threats







Appendix A

Devices: FG100D3G12800081[root],

FG200B000000001[root],

FG200B0000000002[root],

FG200B000000003[root],

FG200B0000000004[root],

FG200B0000000005[root],

T G200B000000000000[100t]

FG200B0000000006[root],

FG200B0000000007[root],

FG200B0000000008[root],

FG200B0000000009[root],

FG200B000000010[root]





Α	b	p	eı	nd	lix	В