Threat Activity Report

Time

11/20 09:45:00-11/21 09:44:59

Virtual System

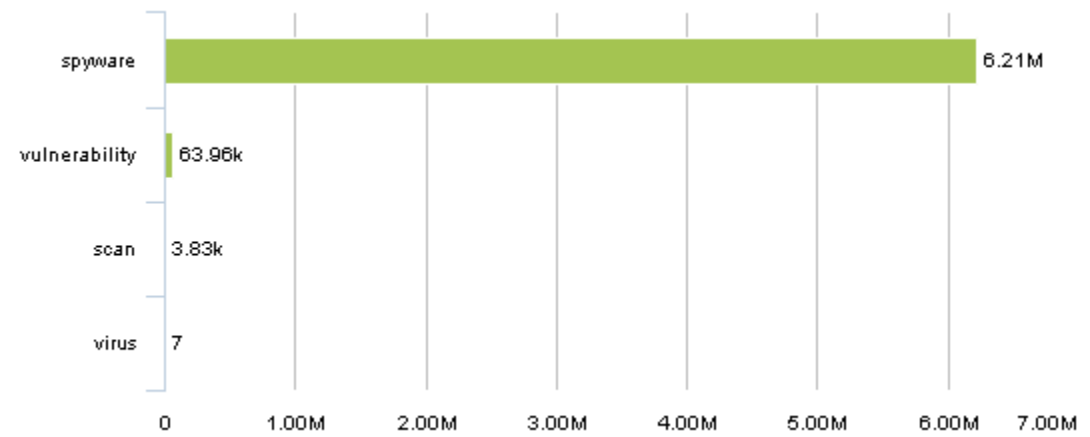
vsys1

ACC Risk Factor

Threat Activity

threats

Home



Threat Name	ID	Severity	Threat	Threat Ca	Count
Suspicious TLS Evasion Found	14978	informat	spyware	spyware	6.2M
Microsoft RPC Endpoint Mapper Detection	30845	informat	vulnerabi	info-leak	35.3k
Suspicious HTTP Evasion Found	14984	informat	spyware	spyware	29.2k
HTTP OPTIONS Method	30520	informat	vulnerabi	info-leak	9.9k
Microsoft Windows WinReg Access Attempt	33865	low	vulnerabi	code-execu	9.6k
SCAN: Host Sweep	8002	medium	scan	scan	3.8k
Microsoft Windows Registry Read Attempt	34940	low	vulnerabi	info-leak	2.8k
Suspicious HTTP Response Found	39825	informat	vulnerabi	protocol-ar	1.4k
NetBIOS nbtstat query	31707	informat	vulnerabi	info-leak	1.2k
Microsoft Windows Server Service NetrServerGetInfo Opr	30861	informat	vulnerabi	info-leak	1.1k
others	others	others	others		3.1k

Compromised Hosts

Home

No data to display

WildFire Activity By File Type

malicious grayware benign

Home

No data to display

No data to display

WildFire Activity By Application

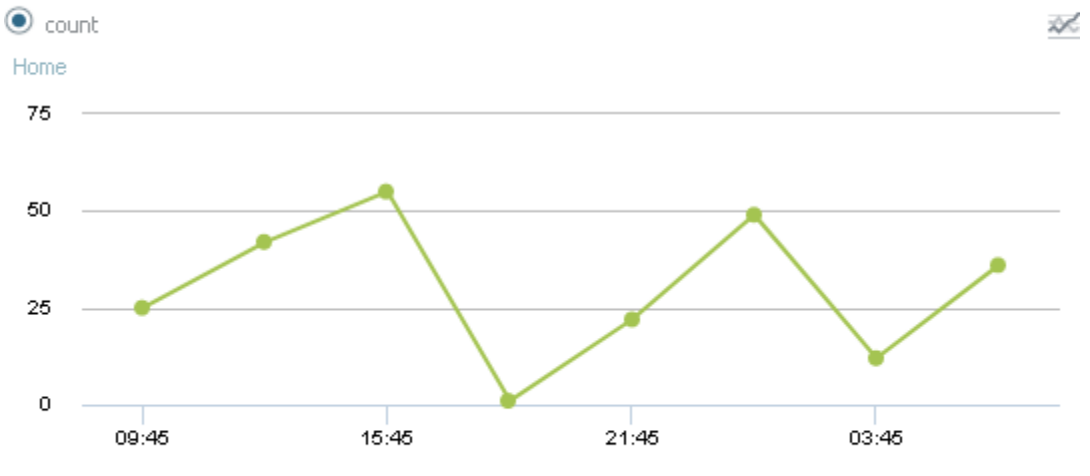
malicious grayware benign

Home

No data to display

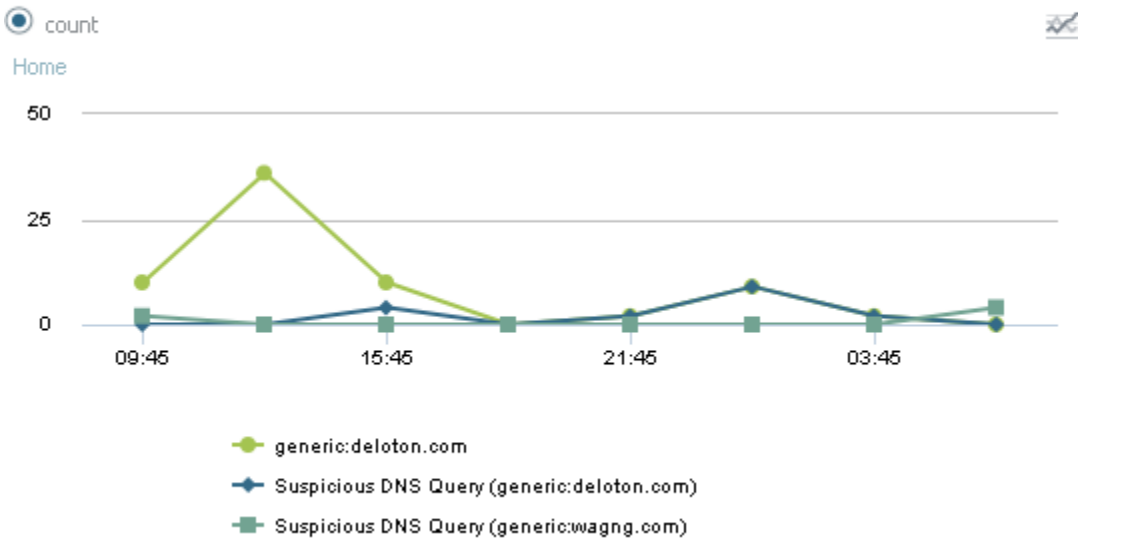
No data to display

Hosts Visiting Malicious URLs



Source Address	Source User	Count
CPRAMPROXY02	None	94
cprll_sal1707.cpram.cp.co.th	None	34
cprlk_end1614.cpram.cp.co.th	None	27
cprlk_add1610.cpram.cp.co.th	None	13
cprllprod8.cpram.cp.co.th	None	12
cpramlk_379.cpram.cp.co.th	None	9
192.168.24.103	None	8
cprlk_iso1404.cpram.cp.co.th	None	4
cprllchon15.cpram.cp.co.th	None	4
cpramlk-56_047.cpram.cp.co.th	None	4
others	others	33

Hosts Resolving Malicious Domains

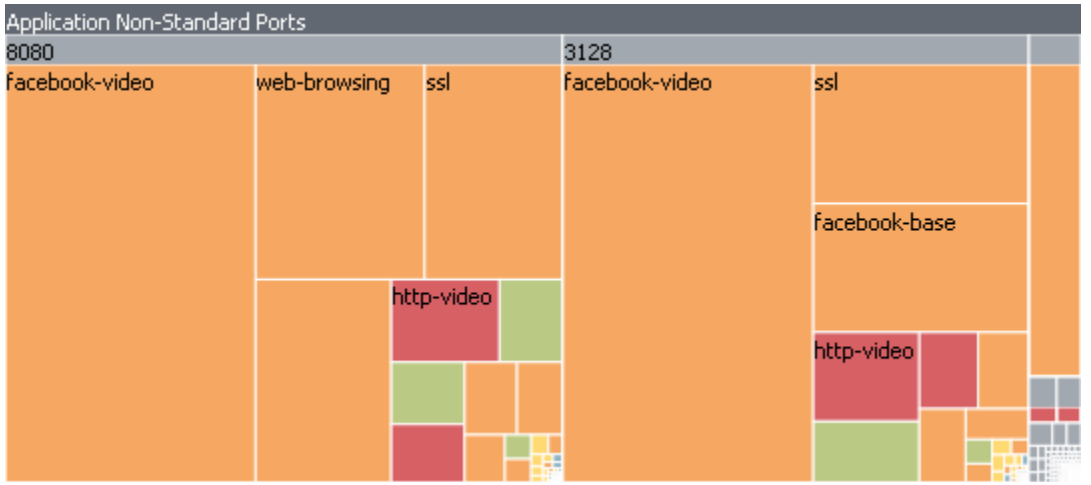


Attacker	Attacker Name	Count
CPRAMPROXY03	None	36
CRLLCPRAMAD01	None	19
cprll_sal1707.cpram.cp.co.th	None	11
CRLLCPRAMAD02	None	9
cprll_eng1406.cpram.cp.co.th	None	6
cprll_tpc41501.cpram.cp.co.th	None	2
cprllprod8.cpram.cp.co.th	None	2
cprll_eng1404.cpram.cp.co.th	None	2
cprll_whc1211.cpram.cp.co.th	None	2
cprll_cic1301.cpram.cp.co.th	None	1
others	others	2

Applications Using Non Standard Ports

bytes sessions threats content URLs

Home

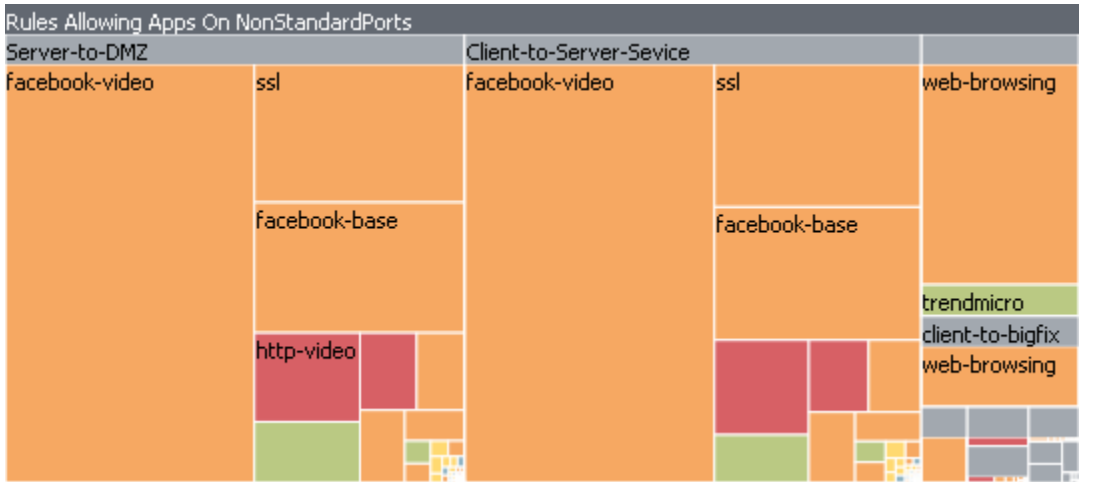


Port	Application	Risk	Bytes	Sessions	Threats	Content	URLs
3128	facebook-video	4	253.5G	56.1k	57.2k	0	41.2k
8080	facebook-video	4	253.1G	55.6k	51.8k	0	30.4k
8080	web-browsing	4	87.7G	75.0k	0	400.3k	24.7k
3128	ssl	4	72.5G	453.0k	2.2M	0	1.8M
8080	ssl	4	71.4G	438.6k	2.1M	0	1.4M
3128	facebook-base	4	66.9G	197.1k	174.3k	0	179.9k
8080	facebook-base	4	66.5G	197.1k	170.5k	0	173.2k
52311	web-browsing	4	40.1G	56.4k	7	3.9k	27.6k
3128	http-video	5	22.8G	14.2k	0	807	0
8080	http-video	5	21.6G	14.2k	0	810	0
others	others	others	48.5G	5.1M	1.1M	84.0k	1.5M

Rules Allowing Apps On Non Standard Ports

bytes sessions threats content URLs

Home



Rule	Application	Risk	Bytes	Session	Threats	Content	URLs
Client-to-Server-Sevice	facebook-video	4	253.1G	55.6k	51.8k	0	30.4k
Server-to-DMZ	facebook-video	4	252.4G	55.2k	56.3k	0	40.5k
Client-to-OfficeScan	web-browsing	4	87.7G	74.5k	0	400.3k	24.2k
Client-to-Server-Sevice	ssl	4	71.4G	438.7k	2.1M	0	1.4M
Server-to-DMZ	ssl	4	70.1G	425.2k	2.1M	0	1.7M
Client-to-Server-Sevice	facebook-base	4	66.5G	197.1k	170.5k	0	173.2k
Server-to-DMZ	facebook-base	4	66.1G	191.1k	170.1k	0	174.4k
client-to-bigfix	web-browsing	4	32.2G	40.2k	1	3.3k	22.3k
Server-to-DMZ	http-video	5	22.7G	14.2k	0	787	0
Client-to-Server-Sevice	http-video	5	21.6G	14.2k	0	810	0
others	others	others	54.3G	5.1M	1.1M	84.6k	1.5M