

NewNet 66 wants you to be aware of the exploits we block from entering our educational network on a daily basis. The sheer quantities are staggering but offer a glimpse of what we are up against. The threat landscape is changing. Hackers are more determined than ever to steal valuable data, credit card and banking account credentials and much more. Computer hackers, much like the gold diggers of the Wild West of yester-year, are determined to hit the mother lode of sellable business and personal information.

NewNet 66 is determined to provide the most secure educational network possible for our school districts knowing that many do not have the resources or technical skill sets to fully protect their networks. Traditional port based firewalls have been the main stay for the last decade but today they do not provide adequate protection. Next generation firewalls are necessary in providing visibility into networks so that steps can be taken to stop the sophisticated attempts by the bad guys.

*It's all about the money.
Big bucks are made
daily selling confidential
information.*



In this report we show many types of exploits NewNet 66 blocks from entering our educational network each day. The report data represents a **24 hour period for November 22, 2010**. Most of the data in this report comes from one of two PaloAlto Next Generation firewalls which reside at the head end of our network providing us the visibility required to protect our schools.

This report breaks the threat landscape down into the following categories.

- Vulnerabilities
- Spyware
- Viruses
- URL Filtering Categories
- Spam

Having visibility into the network is critical in determining what threats are present. If you can't identify the threats then you can not stop them from occurring.



Vulnerabilities

By simple definition a computer vulnerability is a weakness allowing an attacker to reduce the ability for that system to perform it's task.

Below is a screen capture of the top 10 vulnerabilities seen in the 24 hour period. It is very important to note the Microsoft SQL Server Stack Overflow which tops the list. SQL is an application that exists on almost every financial and student information server used in K12.

Top 10 Vulnerabilities we Blocked 24 hour period 11-22-10

	Threat/Content Name	ID	Count
1	Microsoft SQL Server Stack Overflow	30009	39,430 
2	Over Long HTTP Host Header	32148	14,249 
3	HTTP JavaScript Obfuscation Detected	31825	3,676 
4	Microsoft IIS ASP.NET NULL Byte Injection Information Disclosure Vulnerability	32735	3,316 
5	ISC BIND 9 Dynamic Update Request Denial of Service	32783	806 
6	Microsoft Works File Converter Section Header Index Table Remote Code Execution Vulnerability	30592	724 
7	Microsoft Windows win.ini access attempt	30851	386 
8	NetBIOS nbtstat query	31707	247 
9	HTTP JavaScript Obfuscation Detected	31826	230 
10	MAIL: User Login Brute-force Attempt	40007	229 

Total 63,293



Spyware

Spyware is software that obtains information from a users computer without the users knowledge or consent. For the purpose of this report Malware, Trojans, and Bots, are grouped in this category.

The number one event is Conficker which is trying to find it's "Command and Control" bad guy server. The "Phone Home" spywares listed below (#1,2,3, and 9) reside inside a NewNet 66 school district and are trying to phone home information to the bad guys. All of the phone home attempts are being blocked.

Top 10 Spyware Events we Blocked 24 hour period 11-22-10

	Threat/Content Name	ID	Count
→	1 Conficker DNS Request	20000	243,865 
→	2 Win32.Conficker.C p2p	12544	18,986 
→	3 Bot: Torpig Phone Home DNS request	12657	2,543
	4 Bot: Win32.Buzus.Spambot	13054	134
	5 MyWay_Speed_Bar Track activity 2	10731	132
	6 Spyware: Mal.Iframe-F	19897	60
	7 SCN_Toolbar Hijacks IE auto searches and error pages	11863	38
	8 MyWay_Speed_Bar Ads	10729	16
→	9 Bot: Win32.Bredolab.Botnet Phone Home	13053	11
	10 MyWebSearch_Toolbar mysaconfig request	10705	8

Total 265,793

Viruses

Traditional viruses are still part of the threat landscape but not nearly as prevalent as in past years.

The viruses listed at right were blocked from entering our network.




Top 10 Viruses we Blocked 24 hour period 11-22-10

	Threat/Content Name	ID	Count
1	AdWare/Win32.adinstaller.acf	2857684	21 
2	AdWare/Win32.adinstaller.um	2709378	12 
3	AdWare/Win32.funweb.nz	2176628	8 
4	JS/Worm.twitter.	253956	5 
5	AdWare/Win32.funweb.nx	2135920	5 
6	Trojan/Win32.lukicsel.fc	2133831	3 
7	TrojanDownloader/Win32.agent.arv	2449888	3 
8	Trojan-downloader/Html.Agent.nym	259379	3 
9	Virus/Win3551e69b47b5f972b8da0..	2280795	3 
10	WORM/Win32.prolaco.t	2722963	3 

Total 66

NewNet 66 firewall technologies allows us to block attempts by users at our schools from accessing web sites that present exploits that could put the school network at risk. Often times the users are not aware that their workstation is trying to access the bad sites.

URL Categories we Blocked 24 hour period 11-22-10











	Category	Repeat Count
1	phishing-and-other-frauds	310,972 
2	malware-sites	30,996 
3	proxy-avoidance-and-anonymizers	133 

Total 342,891

Known Bad Guys

Reviewing firewall logs is critical in determining "who" is trying to access the network. NewNet 66 reviews traffic logs daily and often we find bad guys. Below is a screen capture of the Top 10 IP addresses we block from entering our network.

Top 10 Source IP Addresses we Blocked 24 hour period 11-22-10

	Source address	Source Host Name	Source User	Bytes	Packets	Repeat Count
1	122.227.164.71	122.227.164.71 China		0	0	80,009 
2	61.163.164.183	hn.ly.kd.adsl China		0	0	72,390 
3	221.192.199.46	221.192.199.46 China		0	0	37,897 
4	221.192.199.48	221.192.199.48 China		0	0	37,029 
5	61.147.112.247	61.147.112.247 China		0	0	32,267 
6	61.114.231.235	ns.unique-cat01.net Japan		0	0	28,055 
7	61.164.116.52	61.164.116.52 China		0	0	23,924 
8	61.160.213.178	61.160.213.178 China		0	0	23,260 
9	172.16.1.244	172.16.1.244 Private IP not routable on Internet		0	0	23,165 
10	61.175.223.118	61.175.223.118 China		0	0	20,635 

Total 378,631

Spam

Email is the most abused technology in use today. Spam is a source of exploits that come in many forms and often target users with phishing attacks that coach the user into clicking on Internet links that are exploits. The amount of spam NewNet 66 blocks is staggering as noted in the screen capture below.

NewNet 66 utilizes two spam blocking servers.

Spam Statistics for October 2010 - One Month Overview

	Month	Domains	Total Messages	Allowed Messages	Allowed %	Blocked Messages	Blocked %
Server 1	<u>2010/10</u>	107	3,045,049	473,462	15.55 %	2,571,587	84.45 %
Server 2	<u>2010/10</u>	105	3,758,142	549,516	14.6220 %	3,208,626	85.3780

Conclusion

In this 24 hour period NewNet 66 blocked a total of 1,050,674 exploits.

Most of the exploits originated outside our network and some came from NewNet 66 school districts that have infected workstations or servers. Regardless of the source, NewNet 66 security technologies blocked the threats.

On average NewNet 66 blocks over 1,000,000 exploits per day keeping our school districts safe.