

# THE HACKER NEWS

## Mal•ware/'mæl,we(ə)r/



# *Editorial*

Welcome readers, techies working in the darkness of night and any other internet security minded folk. June finds us exploring the new "F" word: malware.

You will learn lots from our regular author, Perluigi Paganini as he takes you through the history of malware and its consequences. We introduce two new authors, Charlie Indigo who will get your mind to thinking about the future of internet security and just what kind of world we will be living in. Gerald Matthews gives us an overview of malware and how the FBI, of all people, helped us out.

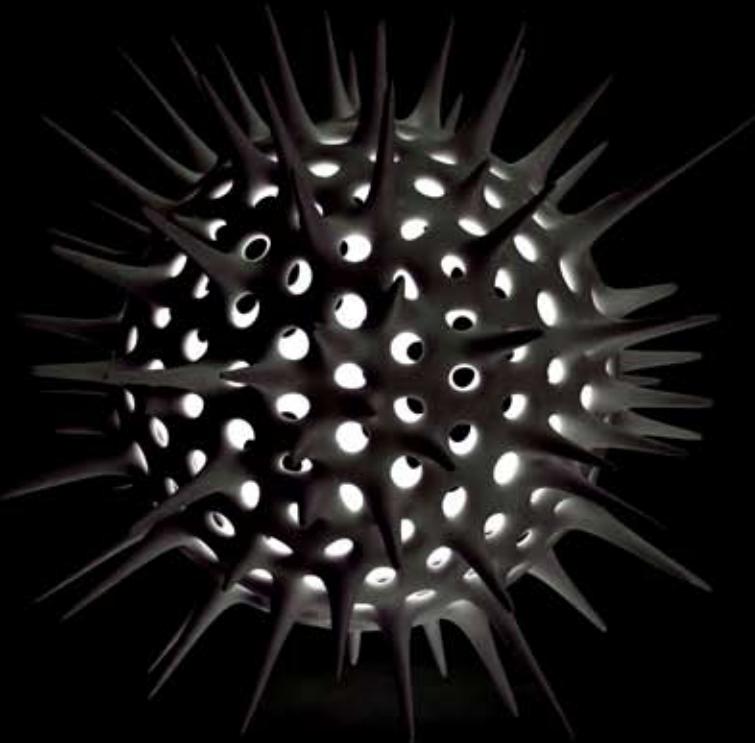
Our founder, Mohit Kumar writes about the topic in general and Ann Smith ,Our Executive Editor, of course, will wow you with a thorough provoking editorial.

Thanks again for your readership.....we hope to hear from you soon.

**Mohit Kumar,  
Editor-in-chief,  
The Hacker News**

# Malware /'mæl,we(ə)r/

*Author : Mohit Kumar, founder THN*



**Software that is intended to damage or disable computers and computer systems.**

Today the Internet is an indispensable component of contemporary life but unfortunately the internet is also a haven for Malware “malicious software” created and frequently controlled by, cybercriminals. Unreservedly it is clear malware is intended to manipulate and control your computer. In the very beginning or birth of, the incentive for Malware was probably nothing more than the power of seeing if it could be done. Nowadays, the incentive is predominantly a financial one.

Dealing effectively with the intricate labyrinth of viruses, Trojan Horses, Worms, and Rootkits that plague today's IT environment is certainly far from an uncomplicated chore. And not surprisingly so, the threats continue to grow evermore sophisticated on a daily basis. To begin to comprehend the development and expansion of Malware “Malicious Software” it is sensible to define the trend, by looking into the history of malware and understanding the many divergent types of malware. While there is no intrinsic basis for a virus to be malevolent, and reportedly the first viruses weren't, it was unquestionably simple enough to write viruses that could do some serious damage and wipe out hard drives.

Previous to the early 1970s, the use of Malware would have been unlikely to have evolved much simply because there were very few computers, and they were by in large not connected to each other. With the scarceness of connections, there would be no way a virus could spread, therefore, making it unlikely for any Malware to proliferate from one computer to another.

A number of the first known computer viruses could infuse or affix themselves to an already existing program therefore proliferate by executing and infecting other programs when the valid but infected program was fired up. Viruses such as these types would characteristically search the computer's disk, locating each application program then rewriting or adding code to the application programs making them adept at infecting whichever computer they came in contact with. This category of virus infection proliferated by sharing a program on a floppy disk. As the development and use of computers became more prevalent, Malware rapidly evolved from just a nuisance to real threats; with the UNIX computers being Malwares first targeted marks.

By the 70s and 80s, programs identified as Rootkits were extensively developed and hackers with criminal intent, "Black Hats" utilized these applications to conceal their existence, therefore, giving them the ability to do as they so pleased with any unwary user's infrastructure. Viruses were the very first personal computer malware type to surface and around 1982 Rich Skrenta, a 15-year-old high school student, wrote "Elk Cloner" for Apple II computers therefore initiating the very first Virus targeting an Apple computer. Consequently, "Elk Cloner" became the first virus to be widely spread.

See the Wikipedia Timeline of Notable Computer Viruses and Worms  
[http://en.wikipedia.org/wiki/Timeline\\_of\\_notable\\_computer\\_viruses\\_and\\_worms](http://en.wikipedia.org/wiki/Timeline_of_notable_computer_viruses_and_worms)

Viruses, like any malware program, are written to carry out some act on your computer that you would reasonably not allow ~ such as, and not limited to; erasing files, crashing of your system, pilfering your personal identity information, pilfering intellectual property, and taking your computer hostage until you pay a rate or fee. While countless people have brand all Malware as viruses, the idiom "Virus" has a very specific meaning. A virus is malware that cannot promulgate from computer to computer without some form of assistance. Early on viruses were spread as floppy disks were passed from one computer to another. Or, viruses were often spread as users shared files over

a network or by emailing infected files to others. Worms were birthed because viruses just didn't get around fast enough and what makes Worms even more insidious is that they can move between networks and computers without assistance from anyone. Once a worm infects a network, in all likelihood, it will spread to all connected computers within minutes or hours. Worms can spread exceedingly quickly and were specifically written to exploit vulnerabilities and as long as the vulnerabilities can be seen by the worm the worm will do their job extremely well. Spyware are devious programs that report and track your computing movements exclusive of your consent. Although Spyware it isn't intended to inflict damage, Spyware can adversely affect the functioning performance of your computer over a period of time.

Spyware generally comes packaged together with free software and will automatically install itself with the program you innocently intended to download. Some indications that your computer is infected by Spyware may consist of sudden adjustment to your web browser, redirections of your search engine efforts and repeated displaying of pop-ups. Spyware can also be characterized as adware which is fundamentally add-supported software that has the capacity to track your every computer activity. Trojans, Keyloggers and Rootkits are all interrelated and they usually have a tendency to support each other.

“Black Hats” often use Rootkits technology to conceal their programs. Trojans are malware set up when a user downloads software from a Web site, characteristically by merely and innocently clicking a link. However, hidden within it is a disreputable program. On the other hand, Keyloggers can capture all your keystrokes. Your passwords, pins and other private and strategic information can be seized systematically and rapidly sent to the “Black Hats’ server; all captured without you even being aware and often used in a criminal manner.

It is good to remember, that Malware is not simply a virus but in fact consists of specific Viruses, Worms, Trojans, Adware, Rootkits and Spyware and many, many other very malevolent contaminations. It can be said that a small number of these programs are nothing more than an irritation, while a large majority poses a very grave threat to your computer. In spite of all the types of Malware, each offers their own unique security threat, and they should definitely be avoided at all costs. The more that computer users become educated about malicious software, all the better because initially the Internet was fabricated on trust.

Researchers that contributed to the design and construction of the net had the vision of a network built on the principle that each and every network computer could trust the other computers it was connected to. Today, the internet is considered a very crucial part of our global society's central nervous system; and if we allow the internet to remain vulnerable, Malware attacks could threaten our whole world's economic balance.

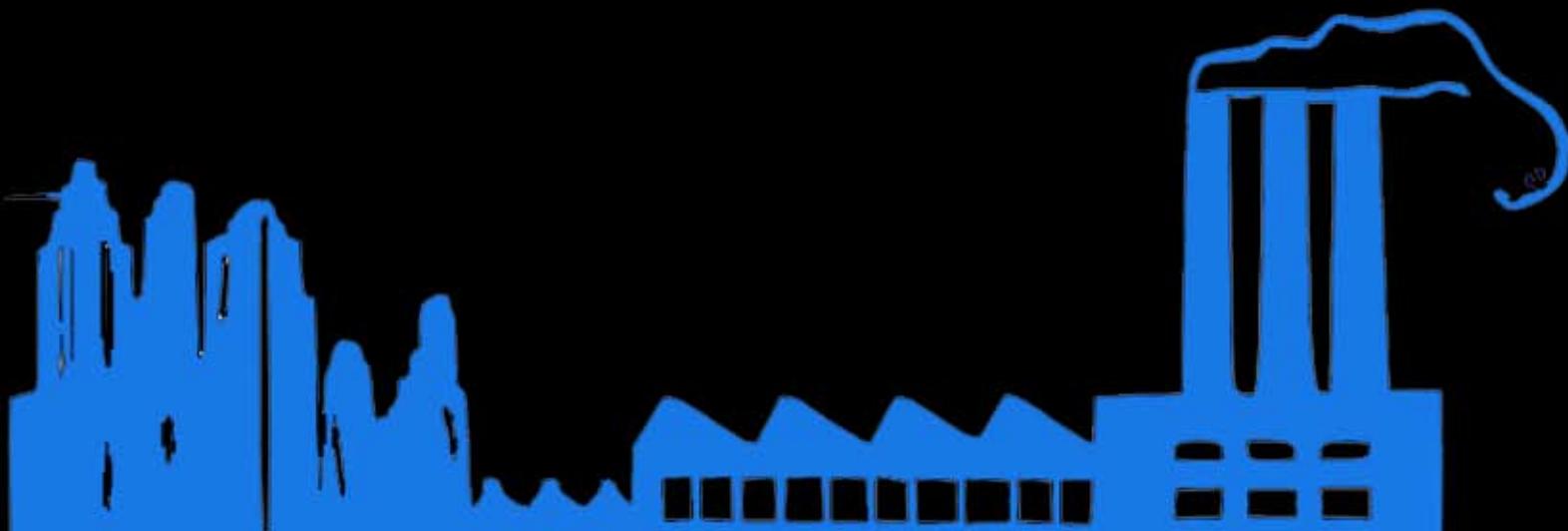
# The Malware Factory

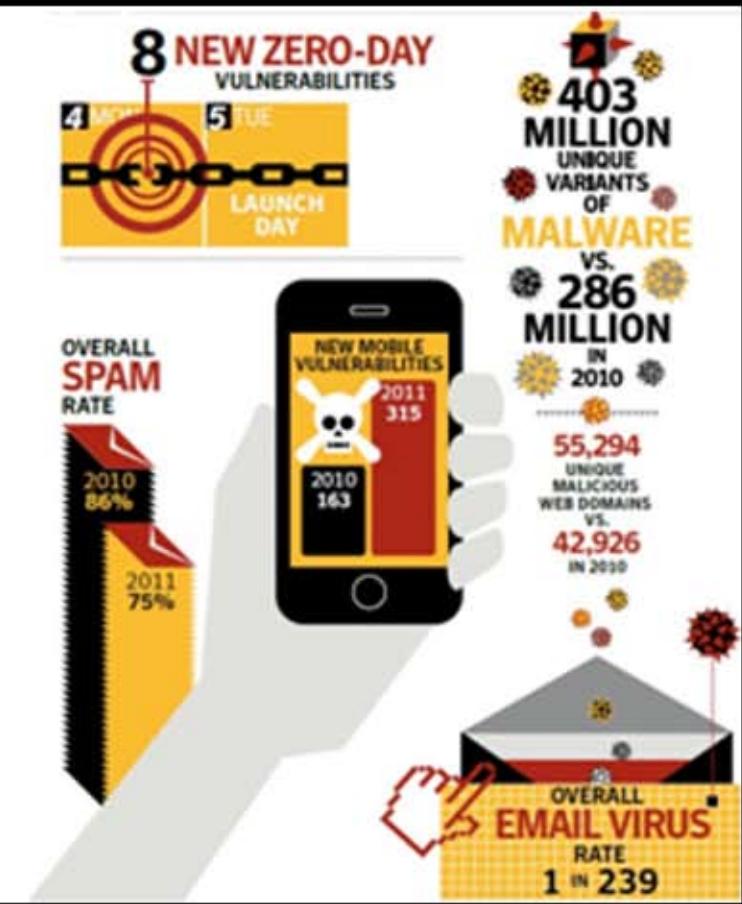
Author : Pierluigi Paganini

With the term malware we refer a heterogeneous family of malicious software designed with the purpose to disrupt computer operation, gather sensitive information, or gain unauthorized access to victims systems. With the term we indicate, in fact, several types of malicious code such as computer viruses, worms, trojan, spyware, ramsonware, adware, rootkits, and other applications.

In recent years we have witnessed an unprecedented growth in the development of malware linked to the rapid change of the technological context supported by the increased use of internet and the explosion of mobile services. The Internet has condensed billions of entities into a single virtual marketplace in which the spread of pathogens is to be considered natural as would happen in real life between individuals.

To give an idea of what we have observed in the recent years consider that in the last couple of years the release rate of malicious code and other unwanted programs was greater than the one related to the previous 20 years. To monitor the diffusion of the cyber threats major security firms have deployed specific networks all over the world capturing spam, phishing and malware data through a variety of sources, such as decoy accounts and network probes. Billions of email messages and Web requests are processed daily in dedicated data centers, and gathered information is put in relation with data acquired through an antifraud community of enterprises, law enforcement advisors and consumers feedback.





Let's look at the case of Symantec that used a similar model of analysis and provides periodical reports and bulletins on the evolution of malware and of cyber threats. Giving a look to the last issue of "Internet Security Threat Report" we can get an idea of the trends related to malware evolution and the sector mainly impacted.

There has been reported an increase respect of last year, of a surge in polymorphic malware attacks, particularly from those found in Web attack kits and socially engineered attacks using email-borne malware. Particularly dangerous is malware that exploits

zero-day vulnerabilities, which is almost impossible to know when they attack a target, because they are developed to operate in stealth mode to evade detection systems. According the reports there has been an increase of unique variants of malware 140% respect of 2010, passing from 286 million of variants to 403 million.

The trend has also confirmed looking at data related to new zero-Day vulnerabilities showing 8 new vulnerabilities per day.

## THE PRINCIPAL CHANNELS FOR PROPAGATION OF MALWARE

The spread of malware in recent years has been made possible by following various schemes for which we try to provide a quick overview below.

One of the main channels exploited for Malware is the internet and in particular the possibility to host the malicious agent on compromised websites. The categories of web sites mainly impacted by this type of attack are Blogs & Web communications, Hosting/Personal hosted sites, Business/Economy, Shopping and Education & Reference. The malware diffusion during the last year is rapidly increased due to the growth of "Drive-by attacks" against internet users. The figures are amazing with hundreds of millions of system infected every year. The infection process is subtle but effective, it is sufficient that -

users visit a compromised website. The redirection of the users navigation on the site follows different schemes, for example it is necessary a click on a link contained in an email or on a link published on social network, in this way the victim is hijacked on infected websites. Very common are attack techniques such as ‘clickjacking’ or ‘likejacking’ that deceives the users attracting him to watch a video or simply expressing its pleasure regarding a specific topic using “I like” function.

Another factor that has dramatically impacted on the malware diffusion is the availability in internet of exploit toolkits which allows creation of new malware requesting few capabilities. This peculiarity has facilitated the rapid adoption and diffusion of the attack kits in the criminal world that have intercepted the growing demand in a millionaire businesses, a phenomenon that continues in its inexorable rise. Let also consider how quickly these kit are updated with new exploits, in some cases new developments are committed to add new features to an existent malware, causing the malware factory. If you are scared of the price of these toolkit, don't worry, usually they are really cheap with prices ranging from a few dollars to a few thousand.

Another preferred channel used to spread malware is of course the email. During the last year the number of malicious email has increased targeting mainly large companies. Usually malicious emails contain infected files as attachments that exploit vulnerabilities in the target system. It's clear that to circumvent the user the content of the mail appears legitimate and tries to catch the attention of the victim.

Similar attacks are used by cybercriminals but also by governments like what happened in Syria where the regime, in order to persecute opponents has used malicious email containing malware to trace them. This is not the only schema for malware diffusion, as we have already discussed malicious emails could also contain links to infected web sites.

I have left for last the discussion of another method of malware diffusion that is seriously impacting user's digital life, the social networks. During the last year with the impressive growth of social networks we have also observed the increase of the number of malware propagated using the popular social platforms.

Millions of users always connected and with low awareness on the cyber threats are ideal victims for cybercrime that once again uses malware to exploit user's vulnerabilities. In the social networking the fundamental factor is the use of social engineering techniques to circumvent users which most often are redirected on compromised web sites through the sharing of "malicious hyperlinks".

The most important social networks are always under attacks, cyber criminals and hackers daily address social network's users with any kind of malware variant, as is the case of the last discovered related to Zeus Trojan.

The experts of Trusteer firm have discovered a new variant Zeus malware responsible for a series of attacks against principal internet service providers. The variant carried out attacks using the P2P network architecture targeting users of Facebook, Hotmail and Yahoo and Google Mail. The malware is really appreciated by cyber criminals that have improved its feature over the months. Zeus Trojan was born as an agent able to steal banking information by logging keystrokes and form grabbing, it is spread mainly through phishing and drive-by downloads schemes.

The malware variant that hit Facebook uses a web injection mechanism to propose to the victims a special price reduction of 20% for purchases made with Visa or MasterCard debit card using their Facebook account. The scam promises in fact that after registering debit card information, the victim will earn cash back when they purchase Facebook points. Of course, the user is proposed a form for the registration of their debit card info that is equivalent to a legitimate one also in terms of proposed layout.

## **What are the main motivations behind the design of a malware?**

Threat that makes fruitful the use of malicious programs in several areas. The areas where the malware have found major use are:

- Cybercrime
- Warfare
- Hacktivism
- Governments monitoring

The criminal organizations are the most active in the development and diffusion of malware, malicious programs that could be developed to realize complex frauds with reduced risks. Criminal gangs have discovered how much more lucrative cybercrime is and how reduced are the possibilities to be legally pursued. Computer crime by its nature has placed in cyberspace direct effects on the real world, but due this characteristic, its persecution is virtually impossible for the absence of globally shared regulations against this type of illicit activity.

Malware can be used in different fraud patterns, mainly to steal users sensible information like banking credentials. The diffusion could happen through several channels like social networking, mail spamming, visiting infecting host or hijacking web navigation. The common factor is the identity theft of the user for fraudulent activity. During the last weeks we have watched the rapid diffusion of new generations of Ransomware demonstrating that the use of malware could be adapted for different models of cybercrimes.

Ransomware is a type of malware which restricts access of the computer resources of the victim demanding the payment of a ransom for the removal of the restrictions. To prevent the access to the resources the malware encrypts files of the infected machine.

Cybercrime is not only the sector that adopts malware for its criminal purposes but one of the most interesting usages is related to cyber warfare. Borrowing definition of “cyber weapon” provided by security experts Thomas Rid and Peter McBurney :

***“A computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings”***

We can immediately think to the effect of a computer malware targeted against a strategic objective such as a critical infrastructure.

Over the years many cyber weapons have been identified and without a doubt the most famous of which is the virus Stuxnet. For its development there is a common opinion that US and Israel Governments, a pool of high specialists are involved.

Stuxnet is not the unique example of usage of malware as a cyber weapon, Duqu malware in fact is a similar agent that has been deployed with the purpose of information gathering, ideal for espionage operations. The reality is more complex, the future for malware in cyber warfare scenario is made of dedicated platforms used to create multiform and modular agents that could target specific objectives simply including new components.

Kaspersky's director of global research & analysis, Costin Raiu, discovered with his team the existence of a common platform to build the malwares Duqu and Stuxnet, that they named "Tilded platform" because many of the files of the agents have names beginning with the tilde symbol "~" and the letter "d.". What is really interesting is that the researcher is convinced that the same framework has been also used to create at least three other pieces of malware confirming the existence of a "factory" platform that Costin Raiu defined using the following statement:

***"It's like a Lego set. You can assemble the components into anything: a robot or a house or a tank,"***

But malware could be also the next option of a group of hacktivists such as Anonymous. During the last couple of years we have witnessed the escalation of operations conducted by the Anonymous group, the hacker group that is expressing a social dissent through cyber attacks. It is common conviction that the group uses only DDoS attacks for its operations, but the collective is changing and some security experts believe that they are also exploring other options such as malware deployment. The purposes of malware usage maybe different, malicious software could be used to attack strategic objectives with targeted campaigns and also to conduct cyber espionage operations. Also DDoS attacks could be automated infecting machines of the victims or simply hosting a malware on a website that redirect the attacks against the chosen targets.

Another regrettable usage of malware is monitoring and controlling, typically implemented by governments and intelligence agencies. In most cases virus and trojan have been used to infect computers used to attack dissident, opponents and political oppositions. The purpose is to track their operation on the web, gather sensible information and localize them. In many cases the use of malware has made possible the capture of the victims and their ruthless suppression.

During the Syrian repression the government has discovered that dissidents were using a program such as Skype to communicate, so it has used the same channel to spread the backdoor “Xtreme RAT”. The schema of the targeted attacks was simple, after the arrest of some dissidents, the government has used their Skype accounts to spread a malware hidden in a file called MACAddressChanger.exe that was accepted by others activists. The dissidents were confident in the MACAddressChanger usage that they have used in the past to elude the monitoring system of the government. Xtreme Rat is a malware that belongs to the Remote Access Tool category simply to retrieve online at a low price (Full version Price: €100 EUR). To confirm that backdoor has been installed by the Syrian Government is the IP address of the command server that belongs to Syrian Arab Republic – STE (Syrian Telecommunications Establishment).

The sample reported is not the only one, the experts of the Trend Micro firm have in fact discovered the usage of the malware DarkComet to infect the computers of the opposition movement. The malware is used to steal documents from the victims and it appears to have been spread through Skype chats. Once in execution the malware tries to contact the command and control (C&C) server to receive instruction and also to transfer the stolen information. It has been observed that the C&C server is a resident of Syria, the range of the IP addresses is under the control of the government of Damascus.

## **What is the future of Malware?**

The scenarios reported share the same trend in the malware growth, more complex agents are daily developed and are able to exploit well known vulnerabilities including 0-days ones. Millions of PC are infected with new variants of malware composing scary botnets that are used for several purposes, the major concerns come from mobile technologies and cloud computing paradigm, in particular the mobile world has registered the major number of malwares that have targeted its platforms and operating systems.

To give an idea on how attractive is the mobile technology for malware developers let's give a look to the Mobile Threat Report released by security firm F-Secure that warns of a dramatic increase in malware targeting mobile devices, especially Androind OS based. The following table reports interesting statistics on mobile threats discovered between 2004 and 2011, showing an impressive growth grouped by malware type.

TABLE 2: MOBILE THREAT STATISTICS BY TYPE, 2004-2011

	2004	2005	2006	2007	2008	2009	2010	2011	TOTAL
Adware									-
Application								5	5
Backdoor							3		3
Garbage				8					8
Hack-Tool							4	8	12
Monitoring-Tool							1	15	16
Riskware				1		1	8	1	10
Spyware				5	15	6		2	33
Trojan	11	105	160	23	13	24	47	141	524
Trojan-Downloader								1	1
Virus	14	19	17	6					56
Worm				2	8	6	22		38
	25	124	191	46	28	38	80	185	717

According to the report “In Q1 2011, 10 new families and variants were discovered. A year later, this number has nearly quadrupled with 37 new families and variants discovered in Q1 2012 alone,” the report states.”

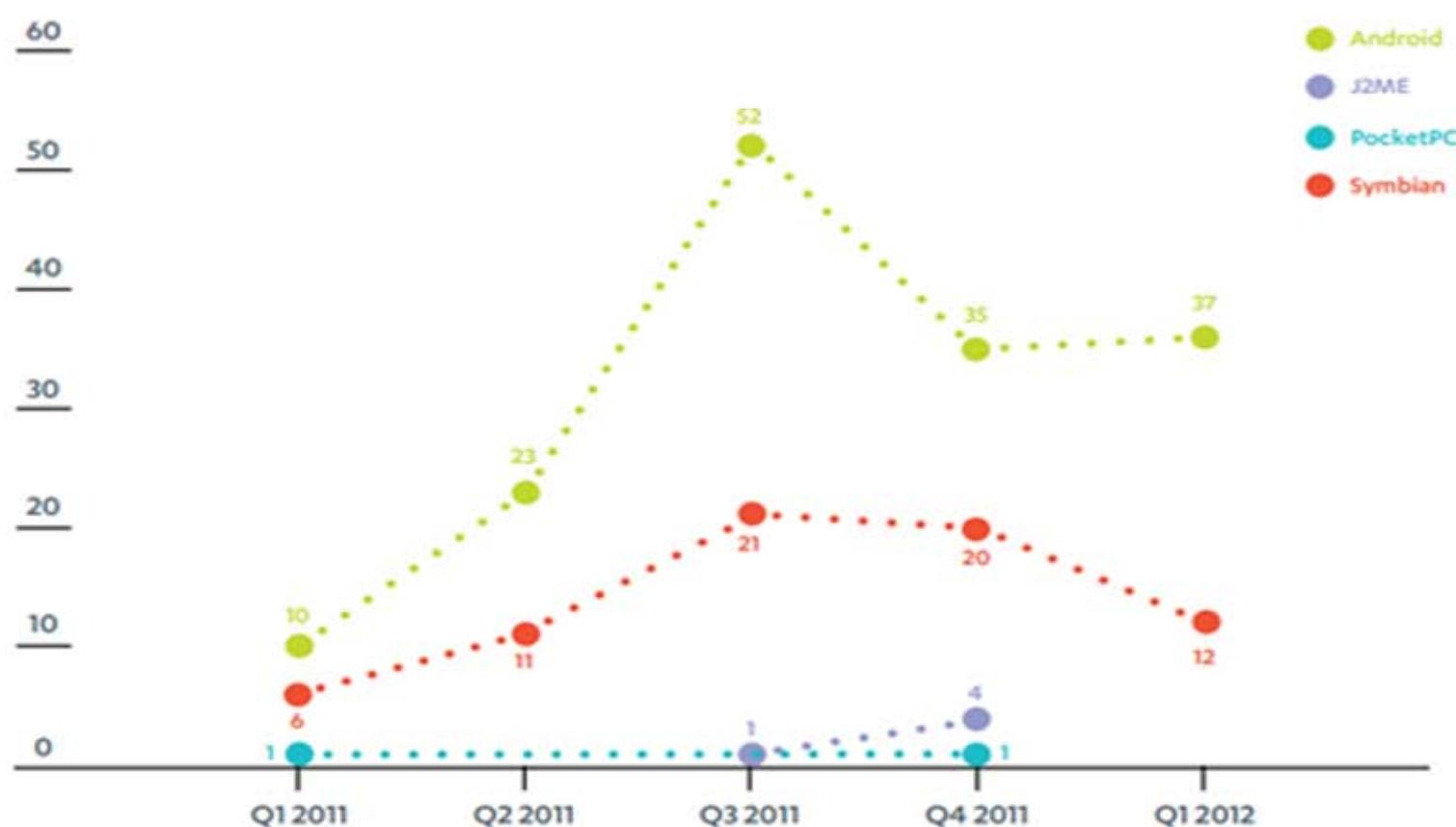


FIGURE 4: NEW FAMILY OR VARIANT RECEIVED PER QUARTER, 2011-2012

The experts of F-Secure attributes the growth to the increasing number of variants designed to evade antivirus protections by utilizing a greater number of signatures.

*"A comparison between the number of malicious Android application package files (APKs) received in Q1 2011 and in Q1 2012 reveals a more staggering find – an increase from 139 to 3063 counts. This growth in number can be attributed to malware authors crafting their infected or trojanized applications to defeat anti-virus signature detection, distributing their malware in different application names, and trojanizing widely popular applications,"* the report notes.

The situation can only worsen in the near future, and cause more than worry about the evolution of malware in the mobile landscape. I'm worried by the impressive increase of polymorphic malware that are able to provide different signatures to evade security systems making difficult pattern-matching detection implemented by major antimalware software.

The battle against these powerful cyber threats must move on two parallel tracks, prevention and response. The first aspect requires a high level of awareness of the related risks that can be obtained through well-designed information campaigns and through the establishment of a greater number of control centers and monitoring institutions. Regarding the second aspect it is desirable that computer crimes can be prosecuted with a globally recognized law that provides stiff penalties for criminals.

# *A quick guide to "THE FLAME"*

*Author : Nidhi Rastogi*



**Introduction** - The bar has been raised, YET AGAIN. The recently discovered worm referred as “The Flame,” has snatched the title for the most sophisticated cyber weapon to date since Stuxnet and Duqu. It was brought to public’s attention by the UN’s International Telecommunication Union when they contacted a Russian Security Firm, Kaspersky Lab, to find an unknown piece of malware that was deleting sensitive information across the Middle East.

**What it does –** On an infected system, among many other things, Flame can sniff network traffic, take screenshots, and capture keystrokes. The most intriguing of them all is its ability to record audio conversations and Bluetooth usage on top of what it already does. It’s the size of the worm, an unusually large 20Mb and the complexity of the code that has made it hard for security professionals to get their heads around its complete capability. All this data is periodically available, even after the detection of the worm, to a handful of command-and-control servers through a covert SSL channel. The latest known number of these CnC’s was 11.

**How it enters the system and what it does? –** The Flame worm was signed by a forged Microsoft certificate. When an infected machine ran a Microsoft’s Windows Update, the worm enabled the connection to get redirected through an infected machine which sent a fake, malicious Windows update to client, using a server.

Microsoft further elaborated this on their MSRC website and issued a Security Advisory (2718704). The advisory stated that the creators of the virus obtained that certificate by manipulating a component of the Windows OS known as terminal services licensing. A bug in TS licensing allowed the hackers to use it to create fake certificates that identified Flame as being from Microsoft.

**Who is behind it?** - A statement was issued by a senior administration source from the hacktivist group, “Anonymous” in the New York Times that President Barack Obama sped up the initiative launched by his predecessor, George W Bush aiming to use computer viruses to attack Tehran's uranium-enrichment program. Other reports point fingers at rival countries like Iraq. At this point in time, nothing can be said with certainty.

**Likeness to Stuxnet and Duqu** - From the initial analysis by Kaspersky Lab, it can be safely assumed that the creators of Stuxnet, Duqu and Flame are powerful forces, such as Nation States, who have the ability to support the manpower and resources to back these projects. However, Stuxnet and Duqu attacked specific infrastructures and looked for focused information unlike Flame that is simply looking for any kind of intelligence. While the Tilded platform was used for Duqu and Stuxnet, Flame does not.

**Should we fear our Flame?** Majority of the people are not entirely at risk since Flame has been aimed at highly specific and targeted attacks. Even geographically, the attack has been confined to middle-east nations.

**Steps taken to prevent further attacks** - Researchers at Kaspersky lab have found that Flame has been maintaining a log of information on server connections and have taken steps to cut off Internet access for machines infected with the Flame worm. Microsoft too has issued a Security Advisory to alert people of the forged certificate and has released a path to counter its impact. Several Antivirus firms have updated their antivirus to enable detecting this worm.

**About the Author** - Nidhi Rastogi is a Cyber security professional based in New York. She has over 7 years of experience in a variety of roles including wireless security, mobile devices, and application development at companies like Verizon Wireless, GE Energy, and LTI. Nidhi is a Masters graduate in Computer Science from University of Cincinnati and can be contacted at [nidhi.gupta@gmail.com](mailto:nidhi.gupta@gmail.com)

# HELP, I'M LOST IN ANONYMOUS AND I CAN'T GET OUT!!

*Author : Ann Smith, Executive Editor, Thn*



Oh, fuck a duck. I am lost. Every time I try to navigate my way around Anonymous, I get lost in a maze of posters that say “WE ARE LEGION, WE ARE COMING, WE ARE THERE, WE ARE GOING THERE, WE ARE GOING TO GO THERE, WE’VE BEEN THERE, WE WENT AND CAME BACK.”

I can’t figure out if they are coming or going. What I can figure out is that minus a few good hacks for some peripheral causes (not to say they aren’t important) for the at least minimum of 100 posts a day on my Facebook page of the claim that Anonymous is taking down corruption, greed, dishonest government, and a plethora of other causes, I see nothing.

What I do see is my grammar school playground and the day a kid brought a Yo-Yo. It started a stampede to the Woolworths because every kid in the school just had to have a Yo-Yo. It didn’t matter if you could “walk the dog,” “rock the cradle,” or just clumsily roll it out and pray for a return, you were just fine cause you “had” one.

Since Anonymous came on the scene in 2003, I have seen the very same phenomenon. Everyone wants to be and claims to be an Anon. I must get 4-5 messages a day from kids that say they are Anons and have great monikers like, ANON HACKER GENIUS, I AM A BAD ASS HACKER, HACKER EVIL, EVIL HACKER WILL TAKE YOU OUT, but want to know if I can tell them how to hack a Facebook page.

To complicate being lost in space, on July 7, 2011 Anonymous officially shutdown and became three separate groups. Anononops, Anonnet, and Anonplus. Holy crap and wtf! Even a compass won't tell me which way I am standing.

The truth is that as a people we are either utterly obsessed or totally uninterested. As fads go, we are utterly obsessed with the mystic of Anonymous and all it stands for but frankly, just like the Yo-Yo I feel people will eventually become disinterested as you get only so much "playtime" off any given thing.

I still fly my green and black Anonymous flag proudly next to my Italian flag and my American flag and when I take out my handy dandy secret decoder ring it tells me that there is a hive of Anons that are working buzzingly to centralize, organize and take some action.

Still, as a former not so good Yo-Yo performer, I worry. I think the people who are stepping up to a movement of hope.....hope for change...need to know that their efforts at being a part of a dream, are not forsaken.

Anonymous or whatever it has evolved to is really the last hope for people to believe they can make a difference against tyranny and injustice. Even if they call themselves Anons and can't hack their way out of a paper bag, they still want to be associated with an organization that will work to give people back their power, restore economic disorder, return homes and livability to families, and most importantly, take down corrupt institutions like Bank of America, Goldman Sachs, the Koch Brothers, and a litany of others like them.

I'm still lost but maybe Anonymous will soon provide a working map of what we are and where we are going. In the meantime, which way is West?

Ann Smith is the Executive Editor of The Hacker News and can be found at <http://www.facebook.com/ann.smith.92102>

# WHAT IS MALWARE

*Author : Gerald Mathews*

What is Malware? Malware are tools and programs that one sets up to infect another's system and directs them somewhere else. Before I begin talking about what malware is I would like to talk about the latest malware exploit that was created back in November 2011.

In November 2011, a nasty exploit to computers that redirected DNS Servers was created and used. This nasty virus was soon diverted by the FBI, in possibly the most friendly and fair way our government has ever done. For months now the FBI has homed servers to divert and fix what this malware program caused, but on July 9th 2012 the FBI announced ending their operation and shut down these servers. The effects have been estimated to great measures, to the fears that millions of Americans will lose connection to the internet, and the world going up in flames due to lack of communication. Since the Feds announcement corporations like Google have announced programs that have been running now since the 23rd of May. These programs scan your computer for this DNS switcher program "aka the nasty malware program".

Now, it is true most virus databases are able to track down and delete malware programs on your system, but in the new world with our new internet based technology, that may not be the case anymore. So what does this program do? What has been leaked out of the feds about it? Well you can rest assured our brother was arrested in November shortly after the release of his program. Due to this fact they are assured that they have fixed the problem, due to higher thinking we can only think they have over looked something.

The only thing we can hope for is that this will only affect a small handful of systems. Common users mostly. So what is malware? Malware are programs that force you to do what someone else wants. Malware programs create bot nets, using innocent peoples computers/common user systems as weapons without there knowledge. For the longest time apple users were told they wouldn't have to worry about this issue. Late April, early May this was proven false which also made all systems at risk now.

So you're probably wondering how one would download one of these programs, which is a really good question. Back in the dark ages, they had to

be installed through third party programs from the downloads you got for games software from untrusted sources. Today, in the modern age of technology, these programs, like all viruses, can be automatically uploaded to your system through cookies and random file downloads websites through the many games we play online. Many of you readers are also at risk due to the fact IRC servers send data packets that may contain such files.

The only luck is that certain ISPs change up there DNS servers monthly, corporations like Comcast, while they do this they also release and renew IP address granting you probably the most open and free way to have anonymous web browsing at least for the first 20 minutes from the renewal.

If your reading this, your probably intelligent enough to avoid unwanted downloads. Hopefully you are, malware has been around for generations and will be around for generations more. So there's no need to worry we're all at risk.

During the course of the computers life so far, a lot of different things have plagued computers, from threats to actual harm. Where do I see malware going? Well to be honest with how all things, programs and ect have gone, I see infecting a system with malware getting easier. Due to the nature of computers and people everything gets easier. I see this being done with much of the programs that left the 90s in pieces becoming easier.

From beast 2.0 to HOIC everything has gotten simple.

Gerald W. Mathews , a young political and world affairs journalist with a background in networking and security. Goes by multiple alias, spends most of this time running security test and a minecraft server. Also, can be found in the multiple IRC channels of Anonymous, EFNET and many more. He doesn't side with any political party nor Anonymous but views them all for an unbiased result, making him able to write political and world affairs with out worry.

# Malware on the go... Now on your favourite Mobile Platform!

*Author : Shashwat Pradhan*

**Introduction:** Malware is going places. With the flashfake trojan hitting macs, the super virus flame for windows and of course the exponential increase (in the past year) in malware for our favourite mobile platform android! I admit the last one is pretty surprising but true. It won't be uncommon to see your latest, top of the line phone with a gigahertz processor getting infected like a PC or maybe not! The latest trend shows that android malware has been acting discreetly. Smart phones are getting more advanced and are being considered as a PC replacement. As they store all important data, contacts in addition to mobile banking, they are a good target for malware authors. The majority of existing Android malware is very obvious in its intention to provide some kind of benefit, usually financial, to the attacker. The best examples of this are the SMS Trojans that send SMS messages to premium rate service numbers. Even symbian is quite susceptible to malware attacks whereas iOS devices only attract malware when jail broken. Windows Phone 7 seems safe so far (Not the previous versions of Windows CE). We will be mostly focusing on android malware in this article as it is the new black.

## What is mobile malware?

Mobile malware gains access to a device for the purpose of stealing data, damaging the device, or annoying the user, etc. The attacker defrauds the user into installing the malicious application or gains unauthorized remote access by taking advantage of the devices vulnerability.

## History of mobile malware

The first instance of a mobile virus occurred in June 2004 when it was discovered that a company called Ojam had engineered an anti-piracy Trojan virus in older versions of their mobile phone game Mosquito. This virus sent SMS text messages to the company without the user's knowledge. This virus was removed from more recent versions of the game; however it still exists on older, unlicensed versions.

In July 2004, computer hobbyists released a proof-of-concept mobile malware named Cabir. The worm then attempts to spread to other phones in the area using wireless Bluetooth signals.

In March 2005 it was reported that a computer worm called Commwarrior-A had been infecting Symbian series 60 mobile phones. This worm replicates itself through the phone's Multimedia Messaging System (MMS). It sends copies of itself to other phone owners listed in the phone user's address book. In August 2010, the first malicious program named Trojan-SMS.AndroidOS.FakePlayer.a classified as a Trojan-SMS was detected on the Android platform. It has already infected a number of mobile devices. It sends SMS messages to premium rate numbers without the owner's consent which can rake up huge bills.

Since then, there has been no stopping the growth rate of malware for mobiles. By the beginning of 2005, the main types of mobile malware had evolved:

1. Worms that spread via smartphone protocols and services
2. Vandal Trojans that install themselves to the system by exploiting Symbian design faults
3. Trojans designed for financial gain

## Why attack Android?

1. Popularity of the platform: Android has about 300 million users (40-50% market share) with 85,000 activations per day, providing a great market size for the malware. It accounts for 65% of the total mobile malware. Initially malware mostly targeted symbian due to its popularity but it is now declining.

Cabir's author states, "Symbian could be a very extended operating system used in mobile phones in the future. Today it is more extended and in my opinion it could be more yet M\$ is fighting also for being in this market."

2. There must be well-documented development tools for the platform. In the case of android which uses java in its apps it has one of the best developer guides and documentation. Cabir's author states, "Caribe was written in c++. Symbian/nokia is giving us a complete sdk for developing applications for symbian operating system."

3. The presence of vulnerabilities or coding errors. Android based on linux kernel is an open source and also gives great flexibility in programming with its APIs thus favourable to malware authors.

## **So what does mobile malware do?**

Malicious programs available on the official Android Market (now google play) became yet another headache in 2011. The first such incident was recorded in early March 2011, after which threats began to appear on the Android Market on a regular basis. Because apps are self-signed, there is no good way to verify that an application is coming from a trusted source. Theft of intellectual property is common, as rogue developers are repackaging versions of legitimate applications and selling them under their own names.

The most common malware are SMS Trojans that send SMS messages to premium rate service numbers as was demonstrated in a fake 'instagram' & fake 'cut the rope' app mostly found outside Google Play.

Plankton is a malware that exploits the Dalvik class loading capacity to remain hidden and dynamically extend its own functionality. Thus it can easily evade static analysis. Dalvik is an integral part of the OS. Android apps are converted into the Dalvik Executable format before execution. Plankton can further act by collecting the bookmark information on the infected device, installing or removing home screen shortcuts, stealing browser history information and collecting runtime log information.

Android malware authors have seized an opportunity to infect unsuspecting smartphone users with the launch of the latest addition to the immensely popular "Angry Birds Space." (Uploaded on unofficial android markets) The Trojan horse, Andr/KongFu-L, appears to be a fully-functional version of the popular smartphone game, but uses the GingerBreak exploit to gain root access to the device, and install malicious code. The Trojan communicates with a remote website in an attempt to download and install further malware onto the compromised Android smartphone. With the malware in place, cybercriminals can now send compromised Android devices instructions to download further code or push URLs to be displayed in the smartphone's browser. Effectively, your Android phone is now part of a botnet, under the control of hackers.

Backdoor Trojans on Androids have gotten a bit more sophisticated: instead of performing just one action, they use root exploits and launch additional malware. Perhaps the best (and most serious in terms of functions) example of a backdoor was detected at the very start of 2012 on the RIC bot: Backdoor.Linux.Foncy.

This backdoor was in APK Dropper (Trojan-Dropper.AndroidOS.Foncy), which in addition to the backdoor also had an exploit (Exploit.Linux.Lotoor.ac) in order to gain root rights on the smartphone and an SMS Trojan (Trojan-SMS.AndroidOS.Foncy).

Links to mobile malware apps have also been found on mobile Facebook recently. The malware package was called any\_name.apk. Once installed it appears to have been designed to earn money for fraudsters through premium rate phone services.

Keyloggers have also been spotted on Android. They capture all the data you enter in the keyboard. These can easily steal any data you type like passwords, banking data, etc.

Since mobile apps can use Web View they can navigate to websites without even a browser bar thus making phishing pages even more successful thus making your passwords very vulnerable.

We have also seen rare instances of QR codes being used to guide users to malicious websites.

The first attack using Man-in-the-Mobile technology took place in 2010. Perhaps among the most critical events of the past year was the confirmation of the existence of ZitMo for Blackberry and the emergence of a ZitMo and SpitMo version for Android. The appearance of ZitMo and SpitMo for Android is especially interesting as they have the ability to spread very rapidly.

RIM's Blackberry also has documentation admitting "Potentially malicious users might create malware that is designed to steal personal data or your organization's data, create a denial-of-service attack to make your organization's network unusable, or access your organization's network using a device."

## Notable mobile malware:

**1. Cabir:** Infects mobile phones running on Symbian OS. When a phone is infected, the message 'Caribe' is displayed on the phone's display and is displayed every time the phone is turned on. The worm then attempts to spread to other phones in the area using wireless Bluetooth signals.

**2. Duts:** A parasitic file infector virus and is the first known virus for the PocketPC platform. It attempts to infect all EXE files in the current directory (infests files that are bigger than 4096 bytes).

**3. Skulls:** A trojan horse piece of code. Once downloaded, the virus, called Skulls, replaces all phone desktop icons with images of a skull. It also will render all phone applications, including SMSes and MMSes useless.

**4. Commwarrior:** First worm to use MMS messages in order to spread to other devices. It can spread through Bluetooth as well. It infects devices running under OS Symbian Series 60. The executable worm file, once launched, hunts for accessible Bluetooth devices and sends the infected files under a random name to various devices.

**5. DroidDream (aka Android.Rootcager):** DroidDream infected at least 60 legitimate applications in the Android Market and attacked hundreds of thousands of users in the first quarter of 2011. It changes the victim into a botnet, penetrates the security system Android and steals the victim's data.

**6. GGTracker:** This threat was born in June by displaying the page the mobile web version of Android Market. The victims are asked to download a battery-saving applications. Once installed, the rogue application that will send a premium SMS at the rate of U.S. \$ 40 per SMS.

**7. Net-Worm Iphone:** the worm stole user data and let malicious users remotely control infected smartphones. This variant also attacked users of jailbroken iPhones and iPod Touches where the default SSH password was not changed.

## How can you protect yourself?

1. Try downloading apps from reliable sources like google play. Google also has secretly had a system in place named "Bouncer" to scan apps for malicious code.
2. Carefully check permissions of applications before installing them. A flashlight app, for instance, probably shouldn't need to send SMS Messages or your location. The general rule of thumb: If an app is asking for more than what it needs to do its job, you should skip it.

3. Avoid sideloading : Avoid directly installing Android Package files (APKs). They are a common path for virus infections.
4. Install an anti-virus on your mobile. It is getting increasingly necessary to do so with the growth of mobile malware.

## Conclusion

Undoubtedly the past year has been most critical in the rise of mobile malware and we expect the trend to continue. Also smartphones and tablets are using the same OS but are not interchangeable for one simple reason — tablets do not function as telephones. That means that most people who own tablets will also own a smartphone, driving up the number of potential victims and an increasing the number of threats targeting them.

We have also seen the beginning of mobile hacktivism with Trojan-SMS.AndroidOS.Arspam. Hacktivism includes malicious programs that are designed with a clear political motive. This type of malware has emerged in the mobile world as a means of protest to promote political ends by malware authors.

We can safely assume that 2012 will not only have more malware but also more harmful malware. Statistics say that around 4% of android users will encounter malware on there smartphones in 2012.

Thus we can say that malware will continue to grow on mobile platforms but will not completely be mitigated from PCs, however, we must keep our guard up because we can't predict what will come next.

# **How Secured Computers Can Still Be Infected With Drive By Malware**

*Author : Lee Munson*



These days we hear a lot of messages that tell us to try and be safe on our computers. And it has not even stretched to our mobile phone use. While some of us might be tired of hearing the same messages over and over again we still will take heed of them. Because we know that if we do not then we will end up in a world of trouble when it comes to whatever electronic device that we were being lazy with at the time. The computer security problems of the world are serious and are not something that you can take lightly.

So to make sure that we do not take them lightly we will follow the suggestions that we are told to make sure that our devices are safe. We will install the proper security tools in them. These tools might include antivirus and a firewall. And we will make sure that we are careful which links that we click on. If we are not sure about the link or if we do not know the person then we will skip clicking on it and wait for a more trusted path. But sometimes even with all of this work that you do, it is not enough. What happens when you do follow the rules and you still become infected?

There are times when you can follow all of the rules and your computer will still become infected. It is known as a drive by download and it happens not quite as often as the other types of ways to spread malware but more often than you think.

When we say drive by download, what we mean is that you just visit a web page and become infected by it. You can have no interaction with the actual web page but by just visiting it your computer can pick up an infection. It is just that easy. We are starting to see more and more attacks happen in just that manner. The bad guys know that people are starting to become more educated in ways to protect themselves on the computer. So they are trying to find work arounds to get past that type of protection. They know that you will not click on just any link that is available to you anymore so they will try to just get you to a page that seems legitimate.

In the past you would have to visit the malware ridden page and then click on a piece of malware to become infected. But the bad guys use technology such as Flash and JavaScript to automate the download of the malware to your computer. When you visit the page, you trigger, for lack of a better word, “a sensor” and when that sensor is ignited then it delivers its payload.

Stopping attacks like this is a lot harder than stopping the normal type of attacks that happen on your computer. The reason why it is so much more difficult is because it can happen on any type of web page. You could click on the wrong link and end up on a bad page or you could be on a normal web page that you go to and one of the ads that are on the page causes the problem.

While most malware detectors and antivirus solutions will stop older attacks that work in this manner, you can still fall victim to newer attacks. That is why you want to keep your security tools updated as much as possible.

# RAZOR SHARP

*Author : Ann Smith, Executive Editor, Thn*



Anonymous, as we know it, may be birthing a new face and presence on the internet as we have never seen before. If my conversation with a young hacker calling himself "Razor" plays out as he has planned we may, for the first time in Anonymous history, see the leadership it has needed to settle into the job that millions of people worldwide have wanted.

Anonymous has brought to the political stage a single word that people all over the globe harbor.

Hope. People have turned to the moniker "Anonymous" because it symbolizes the hope that they can be a part of correcting global government corruption that like a disease has spread to the organs of every tax paying citizen who cherishes freedom.

Razor is using a somewhat unorthodox approach to his bid for reign over the internet that some may find offensive. Since 2004 he has been involved in the evolution of the Anonymous movement and seen the ugly side of growth. Anonymous by its creed shuns any real sense of administration and order causing what would be understandable mayhem. Rouge groups of hackers taking down internet sites, breaking servers, defacing websites, for the Lulz of it and hide and seek shots at various political and environmental issues.

Finally, after repeatedly warning his long time comrades that this wasn't the way to make an impression on the internet or run a movement of change, he'd had enough.

On May 31, 2012 he issued a press release stating that all hacking nonsense stop or he would take down the 4Chan website and turn long time operatives of the Anonymous movement into the FBI.

Unfortunately.....no one took him seriously and soon after the press release, seeing no respectable response to his warning he, in fact, did turn over the personal information of approximately 50 people to the FBI in what he calls, “Operation Cleanse.”

The repercussions of this action will be felt for years to come. Operation Cleanse is the vehicle to bring an opportunity of solid leadership and command to a movement fraught with infighting, disorganization and lack of purpose.

This action is obviously hard for many to understand but Razor feels confident that it was the only action left to take in a movement gone wild.

The future of Anonymous lies in their ability to address the political and economic structure of the world. This is a big job indeed and one that they have not been able to attend since their inception.

Is this a case of the end justifies the means? This is a question to ask as we watch the developments of a new generation of the army of Anonymous.

Razor invites anyone interested in working for the global common good of the people and to bring freedom back to the working people to join him. You can contact him at screwgod123@yahoo.com

# National Security.....What's Next ?

*Author : Charlie Indigo*



We're entering a new age of global interactive networks as predicted in the 20th Century by the masters of mass communication and social theory such as Marshall McLuhan and Alvin Toffler. Human enterprise today, and for the next few generations, is constructing a broadband, integrated, interactive global communication infrastructure that touches every point on Earth at the same time. We're witnessing a worldwide convergence of television, telephone and computer into one interactive ecosystem linking us together, forever altering all the ways we live, love, learn, work, play and vote.

Those who we now define as hackers, as in the group Anonymous, will be running the internet in the years 2016 and beyond. This is because the need for a physical police state will be diminishing with the advent of Internet 2.0, --- the police will be replaced with software, a super brain that will monitor citizens globally by scanning phrases, signs of bullying, and any threats out terrorism that threaten our nationalist societies. Now, with the internet, governments will have to develop either into true democracies, or nationalist socialist societies as seen in WW2 with Nazi Germany and Italy.

The policing, as done by the super brain, will be run by global citizens through feedback that will take defense to a highly personal level. The criminals of the future, instead of being locked up in state institutions, will be banished from the global network of communications and media. They will be outcast as untouchables, unable to purchase what other citizens have access to, such as food, entertainment, cars and internet access. Without being able to communicate in this global network, you will not be able to get a job. You will not be able to be a part of society as we now see it. Hackers that try to meander their way through the future system of Internet 2.0 will have their tools taken from them.

What would persuade education institutions, media companies and governments to get behind a public drive to promote a sensibility and system of defense that makes global sense? Now we realize the cure for our fear of the future is developing peace of mind that comes from a global sensibility. Our interactivity gives us power. As creative beings, we can see multiple options. We can apply our thoughts, words and deeds to solve problems and build that sustainable future we want for ourselves, our children and grandchildren."

Personally, I do support this form of government, because it is the way of the future. One can protest in the face of inevitability, though this is done in vain. I plan on moving out into the wilderness to gain a sense of privacy, though technology is the medium I work through. I am a patriot that loves my country, and I do what I can to uphold the U.S. Constitution. Terrorism will become domestic, as citizens will not want to surrender their rights. Because of this, FEMA camps have been built all over America to tame renegades who fail to comply with the future of the system. It is all a reality, waiting to happen. Are you prepared?

Charlie Indigo was born and raised in St. Louis, Missouri, where he studied social psychology and film production at Webster University. Founder of Indigo Inc., film studio, he produces and directs narrative films and documentaries. As a photo-journalist, he conducts sociological studies of how people behave online, and delves into the everyday world of what it means to be a hacker. Social activist, and supporter of the free exchange of ideas, Charlie writes to show that behind every ideological conflict there are multiple perspectives, all with a human heart. He now resides at the Cahokia Mounds in Illinois, where 800 years ago the native tribe mysteriously disappeared.