"Wicked Rose" and the NCPH Hacking Group

by Ken Dunham & Jim Melnick

Zero-day attacks, where an attack occurs before public knowledge of a vulnerability is known, is a growing cause of concern for security professionals in the 21st century. An unprecedented number of zero-day attacks took place in 2006, largely involving Microsoft Office Files. Ken Dunham, Director of the Rapid Response Team, and Jim Melnick, Director of Threat Operations, led the VeriSign iDefense intelligence team to track down Chinese hackers for hire out of China, responsible for many of the attacks in 2006. Wicked Rose is the ring-leader of the NCPH hacking group and this is the story of their maturation into significant global threat by 2006.

1 Introduction to N.C.P.H.

N.C.P.H. (Network Crack Program Hacker) has about ten members or associates. Four core members exist as of 2006:

- (Wicked) Rose
- KuNgBiM
- Rodag
- Charles

There are also some six other associates within NCPH and two other positions (possibly unfilled positions) whose purpose is unclear. However, "Rose" or "Wicked Rose" seems to be the primary leader. Membership rules, recruiting goals and standards are unknown. However, some members appear to be current or former students of Sichuan University of Science and Engineering.[1]

The group is responsible for development and deployment of exploit codes related vulnerabilities in Microsoft Word Malformed OLE Structure Code Execution and Microsoft Excel Malformed BIFF Structure Code Execution.

2 Public Knowledge of a Zero-Day Word Exploit

The story of NCPH zero-day attacks begins publicly on May 18, 2006. On this day the Internet Storm Center reports a new possible zero-day attack. iDefense worked closely with SANS and other organizations to analyze the threat landscape as it related to exploitation of this vulnerability. Within the next 36 hours, iDefense gained access to multiple codes and extracted a new rootkit called GinWui. Independent research proved the following:

- Exploitation targeted a new vulnerability that allowed attackers to successfully exploit computers running fully patched versions of Microsoft Word 2002 and others.
- Exploitation dated to May 12, 2006 and involved at least six unique hostile exploit files. iDefense confirmed that attacks targeted two organizations, one in the United States and one in Japan.
- Chinese-authored rootkits GinWui.A and GinWui.B exist in several attacks. iDefense identified the rootkits' source and authors as Chinese actor "Wicked Rose" and others profiled later in this report.

[1] www.suse.edu.cn & http://www.study-in-china.org/school/Sichuan/suse/

- Successful installation of the rootkit requires Administrator or Debugger rights. Initial exploitation, however, does not require Administrator rights.
- iDefense identified unique malicious code attacks pointing to nease.net and authored several Snort signatures for this traffic. iDefense continues to monitor other domains related to the attack.

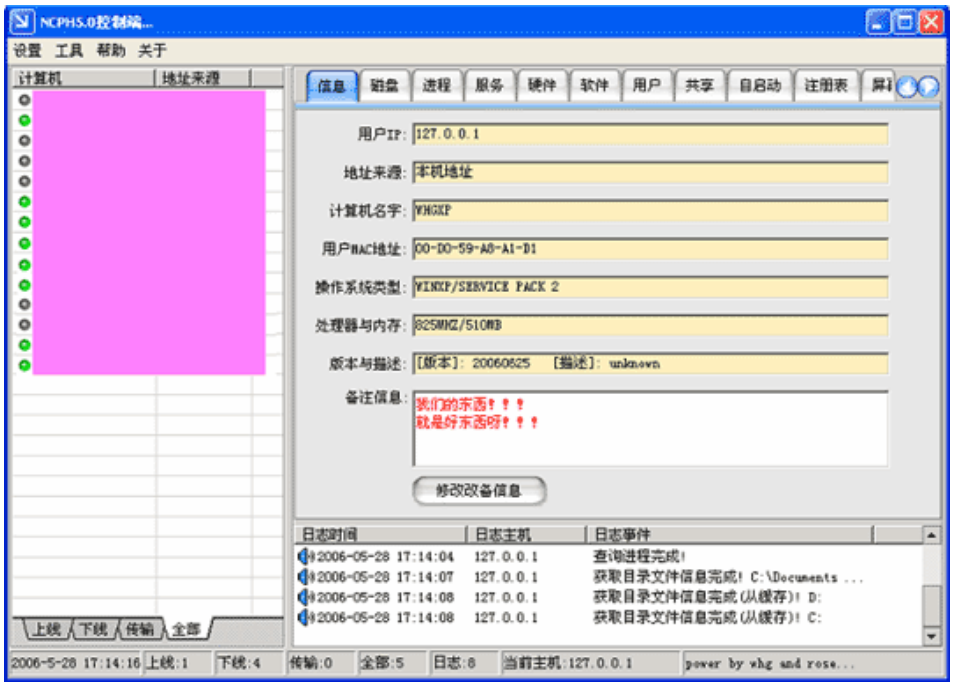
The original attack upon a large DoD entity within the USA began on May 12, 2006. Targets of the attacker were apparently "Googled" by the attacker. Three variations of a Microsoft Word zero-day attack are involved in the attack. A few dozen attack files are first distributed to less than a dozen targets to identify which version works within the organization.

Once attackers identify the vulnerable version of Microsoft Word used within the organization close to 200 messages sent out to multiple targets within the organization within 24 hours. This second wave of attack is distributed as "Planning document 5-16-2006.doc". This code is improved beyond the first variant sent out earlier to identify the vulnerable version of Word within the targeted network.

A third attack commences on May 17, 2006. During this period, the Internet Storm Center and others get involved and the case becomes public. In the end, iDefense identified six unique samples, of which three are more prevalent than other variants.

3 The GinWui Backdoor Rootkit Payload

Zero day attacks commenced in May 2006 attempted to install a GinWui backdoor Trojan horse and Windows rootkit. A DLL file called winguis.dll and several SYS files install themselves when a computer is successfully attacked through an exploit. Two versions of the GinWui rootkit are installed during several attacks in May and June 2006.



NCHP 5.0 Screenshot (GinWui Rootkit)

Wicked Rose is the author of the GinWui malicious code. His code and support posts related to GinWui distributions exist on the Chinese NCPH and Evil Octal forums. Wicked Rose associates with WHG and others on this form. WHT hosted version "3.0beta.3" of the "NCPH

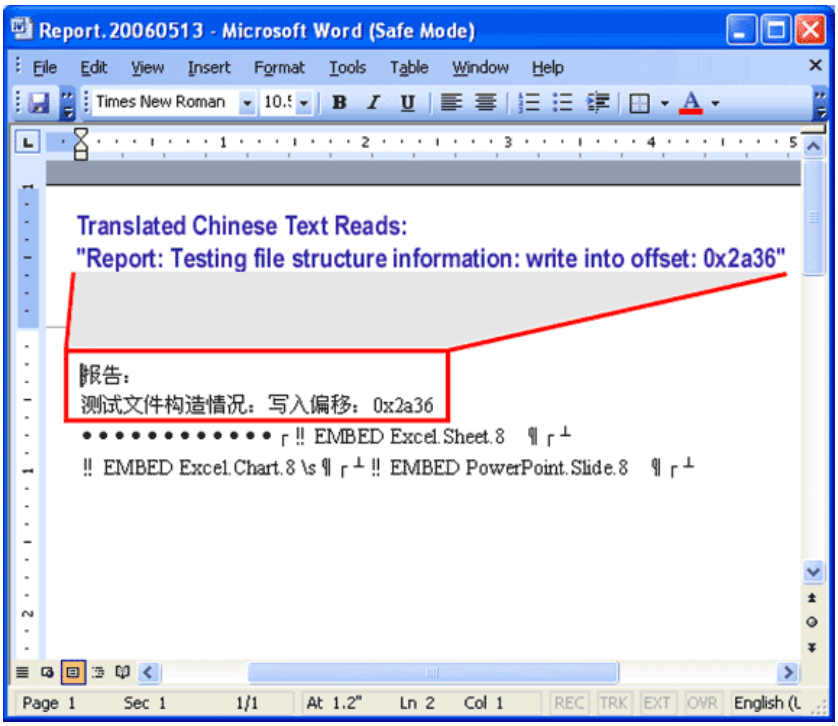
remote control" rootkit code on May 2, 2006. This distribution of GinWui was largely unknown and undetected by anti-virus companies at the time of release.

Versions of GinWui used in targeted attacks of May and June 2006 are private versions, not released to the public. This proves that Wicked Rose either constructed the zero day attacks or sold private code to users that performed the attack.

Wicked Rose later documents additional updates to his rootkit code, version .50, at http://rodag.blogbus.com/index.html. By this time Wicked Rose was performing full-time development of this malicious code as a hacker for hire.

4 June 21, 2007 – Continued US Targeted Attacks

Just over a month later, following initial GinWui based targeted attacks, another Microsoft Word exploit occurs on June 21, 2006. A spoofed e-mail is sent to a target containing a hostile Microsoft Word document. Analysis of the attack reveals that it's likely a test file used to identify what version of Word may be running within the targeted organization, rather than a refined targeted attack upon a known version of Microsoft Word. Chinese text within the Word document reveal Chinese characters discussing a systematic evaluation of offsets for Microsoft Word exploitation:



RipGof attacks reveal a Chinese string related to systematic testing of offsets for exploitation.

5 Backtracking Targeted Attacks: RipGof

In June 2006 another targeted attack emerges, but it's not GinWui this time but a new code, RipGof.B. The attack attempts to exploit MS06-027 to install RipGof.B, a Trojan horse. This is the same exploit code used in the former Zero-Day attacks linked to Wicked Rose and the NCPH hacking group. The exploit code is still private at this time, proving that the author of both GinWui and RipGof attacks are the same individual or group or affiliated through underground criminal operations.

RipGof.B is an improvement of the former exploit used in GinWui attacks. RipGof.B attacks included improvements to shellcode that attempts to fork to different locations based upon the address value of the stack to exploit multiple versions of Microsoft Word. Once installed, RipGof.B attempts to connect to enjoy.irdet.com and enjoy.bmwsee.com over TCP port 80. It runs as a rootkit and backdoor Trojan horse and phones home to a Chinese server with stolen data.

RipGof malicious code does not exist as a distribution in the underground, leading investigators to look into the original RipGof.A malicious code. Over a year prior to the 2006 targeted attacks RipGof.A emerges in the wild. RipGof.A attempted to exploit the Jet Engine Database exploit in March 2005. This proves attempted exploitation and installation of code through RipGof for a year prior to more sophisticated codes and attacks.

In summary, RipGof and GinWui attacks both use the same private exploit code against Microsoft Word and both install rootkit based codes to steal and send information back to Chinese sources. This circumstantial evidence reveals that Wicked Rose and the NCPH group likely began their exploitation efforts at least a year and a half to two years prior to sophisticated attacks that commenced in 2006. Once the group found a vulnerability within Microsoft Word they were able to improve upon it and their targeted attack techniques to distribute multiple targeted attacks and malicious codes for criminal gain as hackers for hire.

6 Timeline of Events

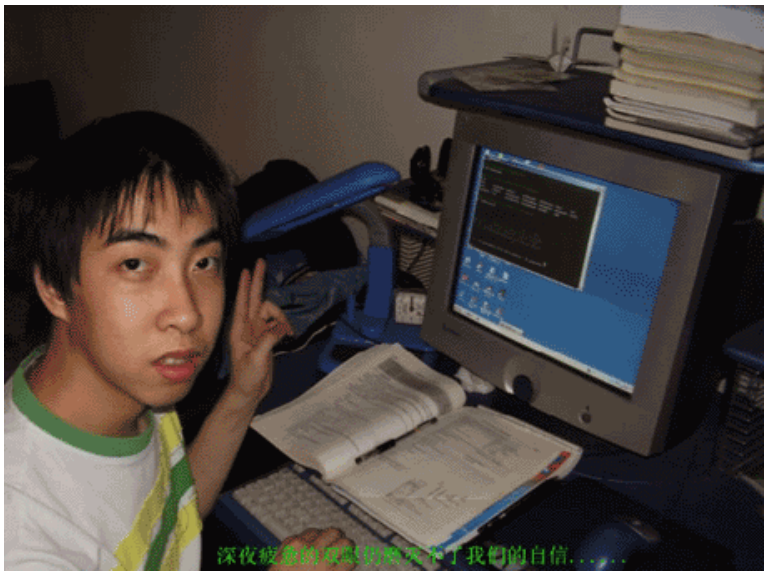
Wicked Rose and the NCPH hacking group are implicated in multiple Office based attacks over a two year period. An attack in 2006 used RipGof.B in the attack. RipGof.A first emerged a year earlier using an exploit that is relatively unsophisticated. Over the next year the Evil Security Team, also out of China, creates the Dasher worm and uses the PcShares Trojan in an attack. Wicked Rose gives a recommendation on the Trojan the day it is updated in the spring of 2006, showing a close affiliation between Wicked Rose and the Evil Security Team actors. Multiple attacks that take place in May and June and later 2006 are related to privately held exploit code for both Microsoft Word and Excel, proven to be developed by Wicked Rose. A timeline of proven associated events related to Wicked Rose attacks is below:

April 22, 2005 - RipGof.A JetEngine DB Attack
Dec. 19, 2005 – Dasher worm and PcShare Trojan attack by Evil Security Team
April 27, 2006 Update to windowsupdates.net attack site
April 30, 2006 - Wicked Rose Drops out of School
May 2, 2006 – 3.0beta3 NCPH remote control (GinWui) public release
May 12, 2006 - Initial probing and GinWui.A exploitation attempts against US target
May 15, 2006 - PcShare Trojan update recommended by Wicked Rose on day of new release
May 16, 2006 - Update to windowsupdates.net attack site
May 16, 2006 - Multiple GinWui.A attacks against US target
May 18, 2006 - SANS reports zero-day attack
May 19, 2006 Update to windowsupdates.net attack site
May 20, 2006 - GinWui.B Attack
May 20, 2006 - WZT Kicked out of NCPH
May 29, 2006 - GinWui.C Attack
June 1, 2006 Update to windowsupdates.net attack site
June 9, 2006 – Mdropper.F Attack
June 14, 2006 – Daserf.A Attack
June 15, 2006 – Mdropper.G Attack

June 15, 2006 – Booli.A Trojan Attack
June 16, 2006 - Flux.E Attack
June 18, 2006 - RipGof.B Attack
June 23, 2006 – PPDropper.A
June 23, 2006 – Booli.B Trojan attack
June 25, 2006 - GinWui.D Attack
June 26, 2006 - GinWui.E Attack
Sept. 27, 2006 – PPDropper.F Attack
Sept. 30, 2006 – GinWui.G Attack
Oct. 9, 2006 – Wicked Rose reports pay increase; likely in September

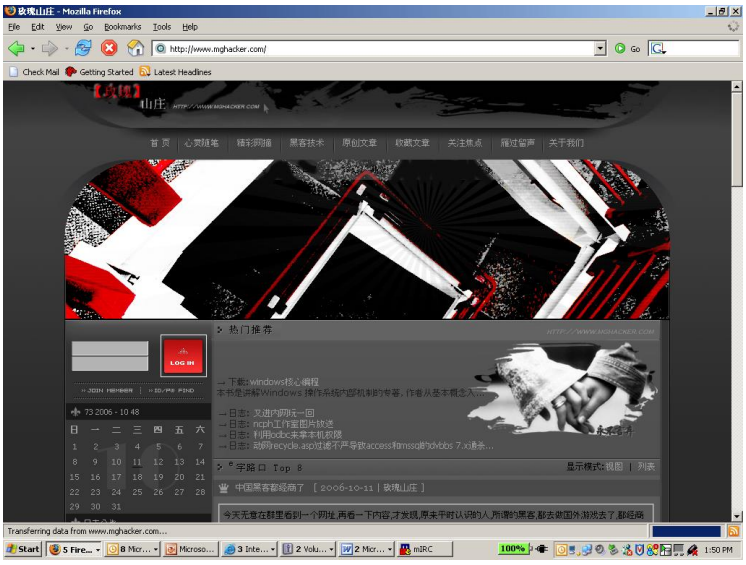
7 A Pictorial Introduction to Wicked Rose and NCPH

Just who are Wicked Rose and the NCPH hacker group? As it turns out, a collection of college students in China who likely room with one another and regularly support their hacking interests. In-depth research implicates Wicked Rose as the ring-leader of the group, responsible for managing hacker for hire relationships and paying group members for their work as hackers. During the time of targeted attacks in 2006 their income increased significantly, to full-time wages for part time hacking. Wicked Rose, leader of the group, is pictured below:



玫瑰 黑客 (MeiGui HeiKe) **"Rose Hacker"**
QQ number is 5372453 ***www.mghacker.com***

Wicked Rose maintains a personal site at www.mghacker.com.



Wicked Rose's Website: www.mghacker.com

Rose is an approximate 20-year-old (2006) student at the Sichuan University of Science & Engineering. In the spring of 2006 Wicked Rose claims to have dropped out of school for full time hacking opportunities. Specifically, on April 30, 2006 his blog entry claims he did not register for his university exam. He performed significant updates to his rootkit code from March through June 2006. He later returned to school by September 2006.

Wicked Rose claims responsibility on his blog for targeted e-mail based attacks containing Microsoft Word and CHM exploits from the spring of 2006.

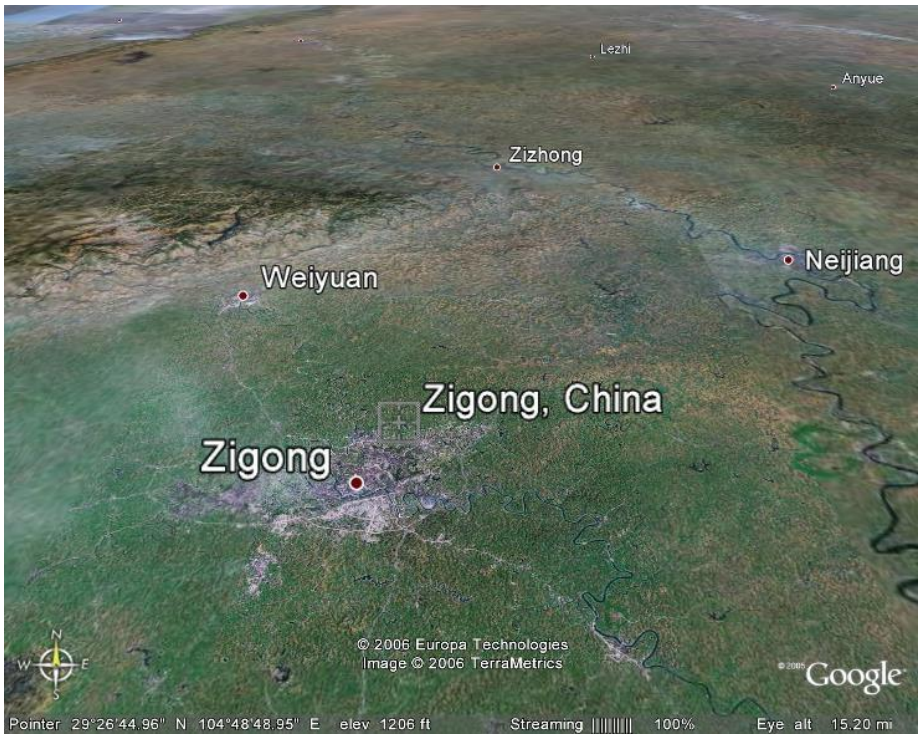
Other NCPH-member websites include: http://rodag.blogbus.com, http://www.cppblog.com/charles and http://kungbim.blogbus.com. The main NCPH website is www.ncph.net:

NCPH Studio website www.ncph.net

Registration information for ncph.net reveals a Chinese registrant:

Registrant Contact: ncph studio (ncph2005@126.com) si chuan li gong xue yuan zigong, Sichuan, cn 643000 P: +86.13154663992 F: +86.13154663992

The main location of the NCPH group is in Zigong, Sichuan Province, in south-central China.

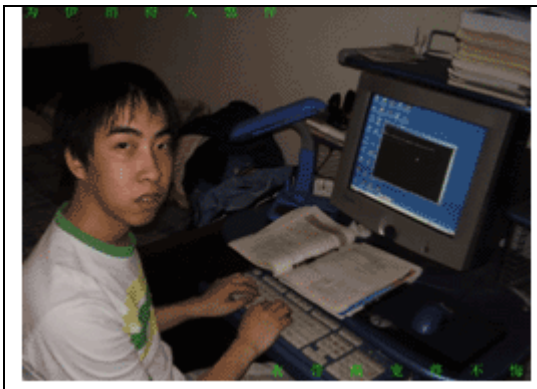


Zigong, Sichuan Province, in south-central China

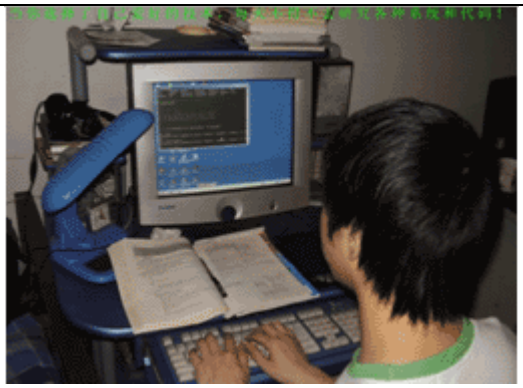
The NCPH group (NCPH Studio) in Zigong, China, is shown here:

NCPH hackers at work in the "ncph studio"
Left to right: "Wicked Rose," KuNgBiM, Charles and Rodag

Additional photos featuring Wicked Rose and NCPH hackers are below, captured from their various websites and blog entries in 2006. Chinese translation for each photo are below:



"Wicked Rose"
From an ancient Chinese poem, expressing the devotion of his heart for hacking.

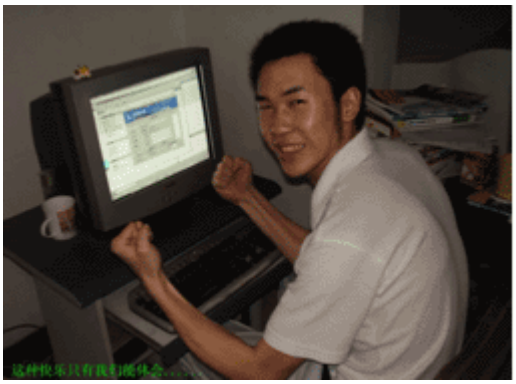


"After you choose the technology you love, you have to research every system and code everyday!"

Charles: "Silence belongs to our world..."

Charles
"Charles always laughs so brightly when searching for program problems!"

Ronag
"Behind every successful design, he always has a slight smile…"



KuNgBiM
"Only we can feel this kind of happy..."

Wicked Rose and NCPH hacking photos

WHG ("Fig")

WHG is not a core member of NCPH but a close affiliate of Wicked Rose. WHG appears to be central to development of the NCPH rootkit, aka GinWui. WHG is credited by Wicked Rose as one of the authors of this malicious code. WHG is an experienced malicious code author with the following contact information:

- E-mail address: whg@163.com
- QQ Number: 312016
- Website: http://cnasm.com
- Real Name: May be "Zhao Jibing",赵纪斌.
- Location: Believed to be employed in the Sichuan province of China.

WZT

WZT is a former member of the NCPH group who was kicked out during the time of zero-day attacks in May 2006. WZT was removed on May 20, 2006. During this time period the zero-day attacks became publicly disclosed, increasing pressure upon the hacking group. It is feasible that WZT may have offended the group in some way related to zero-day attack techniques, strife over hacker for hire deals, or competition for hacker for hire deals.

WZT is a former coding expert within the NCPH group and many years experience in hacking. He is responsible for creating multiple tools and regularly giving credit to the infamous Li0n Chinese hacker (founder of Honker Union (HUC) Chinese group. WZT maintains a website at tthacker.cublog.cn.

The Jiangsu Connection?

WHOIS registrant data for related domains used within attacks and hacker sites reveals a connection with the Jiangsu province of China. One domain, windowsupdates.net, is used in attacks and revolves to an IP address in the Sichuan province. Meanwhile, the registrant "zhaofeng network" is reportedly based out of Jiangsu, not Sichuan. Some of the WHOIS information clearly contains fraudulent information to presumably direct researchers away from the true identity and location of the attacker responsible for registering the hostile domain. The connection to the Jiangsu and Sichuan provinces remains unclear.

8 Concluding Comments

Prior to Wicked Rose and NCPH hacker for hire attacks in 2006, Chinese hackers are only known for their patriotic hacking. This disturbing development reveals two critical threats: 1) motives of Chinese hackers are changing 2) Chinese hackers are regularly associated with sophisticated attacks as of 2006.

Wicked Rose implicates himself in his early blog entries and website posts in 2006 and prior. An unknown company or entity reportedly paid Wicked Rose for hacking at the rate of 2,000 RMB a month, about $250 USD. At this time Wicked Rose gave 200 RMB to NCPH hackers and kept the rest for himself. Once targeted attacks took place the payment increased five-fold to 5,000 RMB monthly with $1,000 a month going to NCPH hackers. This is a significant amount of money in China, effectively paying hackers a full-time wage for part-time hacking.

Throughout the summer of 2006, while Wicked Rose was not in school, over 35 zero-day attacks, proof-of-concept codes, and attacks against un-patched Microsoft Office vulnerabilities are discovered in the wild. With Wicked Rose claiming responsibility for early attacks and the lead author of both GinWui and the NCPH hacking group, there is little doubt left as to his involvement in attacks to date.

By the end of 2006 attacks become increasingly sophisticated. In one instance a popular PowerPoint file distributed during the Christmas holiday season for the last two years prior is used within a socially engineered attack upon one individual within an energy sector US based company. The PowerPoint file is modified to include an exploit that silently installs malicious code. This same individual receives another e-mail containing a Microsoft Word exploit. In this case only one individual within the company is targeted, and with just two messages socially engineered for maximum success. This is a much more targeted and stealthy approach for attacks compared to the earlier attacks performed by the group in the late spring of 2006.

NCPH continues to be a significant threat going forth for several reasons.

1. Attacks continue to take place in the wild and are very difficult to identify on a targeted basis. Only the most sophisticated networks and system administrators are able to properly protect and capture hostile targeted attack files before an attack takes place.
2. NCPH is a serious dedicated hacking group that is methodical and disciplined in their development of new exploits and attacks.
3. NCPH is motivated by both the thrill and challenge of hacking and money as a motive.
4. Attacks by the group are highly targeted and stealthy, very difficult to detect and remove.