**Chinese Red Hacker Army**

Chinese Red Hacker Army // Red Hacker Alliance // Honkers // Honker’s Union // 中国红客队 // 红客

**Criminal History:**

* Hacking and DDoS’ing US government and military networks
* Organizing to distribute and dump US data, or pass it on to Chinese government agencies
* Protesting in the streets, resulting in minor damages to the US embassy in China

**The Chinese Honker’s, a play on words with the Chinese word for hacker (hei ke – 黑客), is a particularly patriotic group of hackers that rose after particularly tumultuous times between the US and the People’s Republic. Incidents such as the Belgrade Bombing and the Hainan Island Incident, as well the disputes over the South China Sea. The best way to think about the Honkers, known as the Red Hacker Army or the Honker’s Union, is a patriotic Anonymous: there is no formal membership, nor are they a standing group. They appear and reappear at will, launch disjointed, only vaguely organized attacks, and organize over Darkweb forums.**

**The Honkers emerged in May 1999 after the Belgrade bombing incident. On May 7th, 1999, during the height of the Kosovo War, US forces dropped 5 JDAM bombs on the Chinese embassy in Belgrade, killing 3 and wounding 20 Chinese citizens. There was immediate outrage from China, who insisted that the attack was intentional, while the US said that it was a result of faulty intelligence and outdated maps.**

**The Guardian, ever the bastion for anti-US sentiment, summarized a report put out by the Sunday Observer and a Danish paper (Politiken) stating that the attack was not accidental, and was a result of intelligence that the Chinese were aiding in rebroadcasting communications for the Slavs. The Chinese also were rumored to be electronically monitoring missiles launched from US and NATO ships offshore, passing on the information to Yugoslavian forces. They carried parts from a crashed US F-117 stealth jet, and may have been planning to use the parts to develop countermeasures.**

**The resulting protests lead to a huge PR win for the CPC, enraging the populous, who had begun embracing Western culture. The Chinese seemed to be fanning the flames, bussing protestors to demonstrations outside of the US embassy and delaying news of the Clinton apology for the bombing. This could have been one large reason behind the rise of the Honker Union, and gives a good look at what is meant by the indirect government support from the US government.**

**The Honkers formalized in 2001 after the Hainan Island incident. On April 1, 2001, a US spy plane collided with a Chinese fighter jet in the disputed South China Sea, killing the pilot. Much like the Belgrade bombing incident, there was immediate outrage from the Chinese mainland. There were protests, even as the Chinese imprisoned the 24 man crew of the US spy plane. The US insisted that the Chinese jet, which was far more maneuverable and was operating in (debatably) international sky, was hotdogging around the plane, resulting in the accident. Indeed, seeing the size discrepancy and the price of the US spy plane, it’s extremely unlikely that the US pilot would have even been able to intentionally ram the Chinese jet. The years leading up to the accident saw many occurrences of near misses between US and Chinese jets because of hotdogging. Regardless, the US paid almost 35,000 USD in reparations and apologized as well. This played very well into the CPC’s hands, again fanning anti-Western sentiment and patriotism.**

**The Honkers attract controversy based upon whether or not they are supported or sponsored by the PRC’s government. As a patriotic, often anti-Western group that derives their name from the color of the Communist Party, it wouldn’t be a huge surprise. The government didn’t exactly condemn the attacks after the Hainan Island incident, slapping them on the wrist before condemning, in much stronger terms, the Americans who they viewed as the real cause of the attacks.**

**The risk now is in ad-hoc attacks. There is a risk that many of the old Honker actors who received more acclaim for their technical skills were picked up by formal government agencies. The Honkers themselves are a risk any time the political tensions between the two superstars rise. As the dispute in the South China Sea rises, the US should expect patriotic hacking attacks to become increasingly common. The Honkers are a very disjointed, disorganized group. What they lack in technical expertise, they gain in numbers. They’re difficult to trace because and their lack of central control, and don’t have a set list of IOCs (Indicators of Compromise) because of the varying styles of attack. They organize on Darkweb Chinese language forums, which lack the law enforcement penetration that Western forums have.**

**The lack of IOC’s, government penetration in online forums, and overall knowledge of the Honker operating procedures means they could be a legitimate threat in the future, despite their general lack of technical ability. They can be unpredictable, and because they’re a foreign actor and political tensions between the nations are so high, prosecuting any individual in the group can be extremely difficult. This can lead the actors to be even more brazen, knowing at the very most that the government is throwing a blind eye their way.**

**Now, certain members of various Chinese patriotic and otherwise affiliated hacker groups are being all but directly employed by the CPC. Topsec, a cyber security company in Beijing, at one point employed Lion, the founder of HUC, and employs several other members and former members of other Chinese threat groups. The chairman at the head of Topsec stated in an interview that the CPC contributed half of the 440M USD company’s startup funding, and they do receive and act on directives from the PLA. This means that, at one point, the head of the HUC was essentially a government contracted network operator.**

**Lion is also known for developing the Lion worm, a worm that automatically propagated to Redhat Linux machines using a BIND 0-day, and for writing HTran, a proxy software used in a lot of the APT1 attacks. Though this was before he was employed by Topsec, this means the Chinese government is indirectly employing the author of a widespread worm, and uses the tools developed by this author.**

**On the Honker website (cnhonkerarmy.com) you can find a wide variety of topics, including discussion on mobile security （手机安全）, general tech discussion (技术讨论区), and discussion on patriotism (爱国交流). The topics are targeted at users with a base understanding of computer science (计算机基础) to more specific communication about scripting languages (脚本技术). There is even a discussion portion about Red Hacker culture (红客文化区) where users trade wallpapers (post: 做了一张红客壁纸，大神无进！ -- I made a Honker wallpaper, even god won’t enter!) and discuss the history, culture, and attitude of the Honker community.**

**An interesting linguistic piece I noticed: at least a few users on the forum use Honker the same way most use the word Hacker. This is an excerpt from a post titled “What is a honker?”**

**什么事红客**

长久以来，存在一个专家级程序员和网络高手的共享文化社群，其历史可以追溯到几十年前第一台分时共享的小型机和最早的ARPAnet实验时期。 这个文化的参与者们创造了“网络红客”这个词。 网络红客们建起了Internet。网络红客们使Unix操作系统成为今天这个样子。网络红客们搭起了Usenet。网络红客们让WWW.正常运转。如果你是这个文化的一部分，如果你已经为它作了些贡献，而且圈内的其他人也知道你是谁并称你为一个网络红客，那么你就是一名网络红客。

**Translation:**

**What is a honker?**

**A long time ago, there was a professional programming and networking sharing community, whose history can be translated back to a few decades ago that time shared the first microcomputers and ARPAnet experiment. The participants of this culture created the term [Honker]. Honkers created the internet. Honker’s created what became today’s Unix systems. Network honkers created Usenet. Network honkers created the www (internet) operations. If you are part of this culture, if you were a part of these contributions, and others in this circle know who you are and know you’re a honker, then you’re a honker.**

**This is an interesting linguistic phenomenon, because it means the Chinese either a, hold some kind of conspiracy theory that the Chinese patriotic hackers created ARPAnet, or b, they use honker interchangeably with hacker. This means that the word honker in some cases is not used patriotically, and instead is merely used as a slang word for hacker.**

**Here is why that is important: through my studies of the Chinese language and Chinese hacking community, the Chinese language is often leveraged to avoid censorship. For example: the word for harmony and the word for crab are both the same in pronunciation but are written entirely differently. In the years past, Chinese netizens have used the characters for river crab (河蟹 – hexie) instead of the word for censorship (和谐 – hexie) to discuss censorship while circumventing keyword based censorship mechanisms. This could be another reason behind the prevalence of the honker term, that it’s not necessarily in reference to patriotic hackers but could possibly be a method of circumventing censorship, or simply be another internet slang term.**

**Infiltrating the Red Hacker Army (cnhonkerarmy.com)**

**Today, 28 June 2017, I signed up for an account on the HUC website with the username 无黑无白都灰（there is no black or white, everything is gray）. My purpose for this is to get a bit more intelligence on what it is the Honkers are talking about. Several of their posts contain attachments which can only be accessed by verified users.**

**A full stop for irony here, I authenticated with a gmail address, in a patriotic site dedicated to cyber excellence in China, a country where Google is banned… Throughout my studies, I’ve also noticed that many Chinese sites also use Google analytics and other such Google software, showing that while the company is formally banned and their site blocked, they are still okay with taking advantage of Google products.**

**Anyhow, I’m going to use this section to detail my findings on the site and create another section for any other findings in my research of the Honker’s Union.**

**The general layout of the site is a cringeworthy red front page that starts playing “intense background music” right off the bat. American security researchers beware, these guys mean business. In the forum section of the page, there is a section for announcements (官方公告区), a section for noobs (新手交流区), one for technology discussion (技术讨论区)， a section for the sharing of materials (资源共享区)，a section for Honker culture (红客文化区)，and a section to discuss administrators (讨论管理区).**

**I’m going to start from the noob section. In this section, there are subforums for general discussion, foundations of programming, instant messaging, and noob education. The posts in the general discussion board were very similar to something you would think to find in the noob section of the forum: “I downloaded a pirated version of QQ and now have been blacklisted, how do I fix this?” Or “Why do I have to test software from the forum in a VM?”**

**An interesting problem I’ve run in to is what I would suppose is some form of security mechanism. You can’t post or reply to other’s until you have at least one friend on the forum. I’ve sent several requests in hopes that one of them blindly accepts the request, but because of the timezone difference it may be a while until I get a reply.**

**Something interesting I’ve found is that it seems like there may be some animosity on the forum towards authority. It’s less so in the noob sections of the forum, but on several others there are comments here and there that are speaking out against posts being deleted and rules being enforced. I don’t know if the authority in question is the Admins or if it is towards the government.**

**The rules section of the forum prohibits any talk that might be against party policy, which would include dissenting opinion or speech critical of the party. The rules are very ambiguously worded in a seemingly intentional way. This would allow the administrators to remove just about whatever they want.**

**Infiltrating the Red Hacker Army (cnhonkerarmy.com) – 6/29/2017**

**I did some more looking through a couple of the threads on several forums… It’s painful to read. There are tutorials for download, in which the poster is admitting that the tutorial download is an executable… There are people asking for how to circumvent the authentication mechanisms on WeiBo, the Chinese Facebook/Twitter ripoff, and there are those of them that brag about knowing C, while other users call them God.**

**One of the more interesting points I found was when I saw a posting that listed “common hacking tools and technology”. In it, the users listed Java, notepad++, and Python. Users continued their worship of C code as god-level hacking skill. Not a one of them, out of almost 200 posts, listed Metasploit, sqlmap, or anything remotely connected to the Linux OS. It was shocking to see how low the general skill level is on the forum, even after combing Hack Forums.**

**I’m going to continue posting on the site. Hopefully, I can sift out the majority of the garbage skids and find a couple that have a little more skill. They’re all braggarts, which makes them pretty easy targets to gather information.**

**Some of the only technical posts I saw were tutorials on how to crack WEP/WPA wifi networks. In one particular post, the author made a huge deal about being able to crack WPA by brute force, exhaustive dictionary methods. There was another post that bragged about finding a 4 year old redirection attack against Struts on Apache. There are very few technical posts, and most of them are about this quality.**

**I did find a thread that looked like some sort of HF style beef. Two hackers apparently had gone back and forth hacking each other’s website, and one of them posted a CSRF vulnerability in the other’s site. I tried to visit the site, and it was entirely down.**

**The majority of my research today thus far has been on the vulnerability research section (漏洞研究, for those of you following along at home), and what I’ve found is… underwhelming. The majority of the vulnerabilities that I’ve found are dated back to 2012, and are now very much well-known vulns. There were a few posts discussing IIS vulnerabilities, one about a 2012 JRuby vulnerability, and a few more scattered “how can I hack this, it has SQL…” type posts.**

**One thing I did notice, however, is that the primary reason behind the lack of vulnerability research on the forum is due to the lack of an English translation. In English-speaking countries, there are a multitude of websites one can go to in search of CVE information or exploit source code and proof of concept. This isn’t the case for the average Chinese hacker, as detailed in a post asking for sources of vulnerability updates. There were no answers on that post, except one citing the lack of Chinese language vulnerability research sites.**

**As shown by the multitude of attacks in the past few years that involved ancient, legacy exploits, this is still a threat. If at some point in the future the Chinese tech community moves to publishing Chinese language vulnerabilities, the threat may become more serious. As of right now, though, it means that if the systems are patched, you are likely safe from the script kiddies of China’s Hack Forums.**

**Targets:**

**US Government Networks**

**US Media Corporations**

**US Military Networks**

**Japanese, Vietnamese, Iran, Filipino, and Tibetan sites and networks**

**Connections:**

**CPC / PLA**

**Chinese Red Hacker Alliance**

**SQLSlammer**

**Lion (site administrator)**

**HTran**

**APT1**

**Topsec**