**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China, who insisted that the attack was intentional, while the US said that it was a result of faulty intelligence and outdated maps.**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.**

**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**