**Th3j35t3r**

theJester // Jester

**Criminal History:**

* **Targeting Ecuadorian stock market**
* **DDoS’ing jihadist, Westboro, Wikileaks, and other websites**
* **Phishing/watering hole attack with some collateral damage**

**Jester is an unidentified, patriotic hacktivist known to be based in the US, with a large social media presence. He is known for his token “TANGO DOWN” tweets upon DDoS’ing or otherwise taking down his targets, which range anywhere from 4chan to Islamist news outlets to the president of Iran. Jester has admitted to being a veteran that served in Afghanistan and elsewhere as a part of “four operational tours”. A defense contractor said that Jester was a former coworker of his and worked for US Special Operations Command.**

**Jester is known for developing Xerxes, a tool he once used to stress-test servers and now uses to take down jihadist propaganda sites. He used this tool first in 2010 to take down the Taliban’s propaganda site, and continued to use it against the WikiLeaks site, 4chan, and Wesboro’s websites. The WikiLeaks attacks came around the same time as Operation Mastercard and Operation PayPal, two infamous attacks by Anonymous in retaliation to the two companies dropping support to the site. He said that Wikileaks was endangering the safety of troops overseas. The alleged operation against 4chan was retaliation for some of the users’ attempts at revealing Jester’s identity. The attacks against Westboro were retaliation for their celebration of the deaths of homosexual US troops.**

**Later, Jester changed tactics. He used a cross-site-scripting vulnerability to post links to falsified articles on Jihadist pages. This was a psyops campaign to lessen the moral of Jihadist troops by posting articles insinuating their failures in the Middle East.**

**The Jester moved on to target LulzSec, vowing to out the identity of the “childish” group. After several failed attempts at revealing the identity of Sabu, he later hit pay-dirt, followed by the arrest of Hector Monsegur.**

**The Jester continued to target WikiLeaks related targets, including the Ecuadorian stock exchange (while Snowden was staying in Ecuador) and the site itself. He expressed contempt towards Snowden and Assange for WikiLeaks.**

**The Jester also launched a watering-hole attack, changing his Twitter avatar to a scannable QR code. Allegedly, the QR brought the users to a site with an embedded code that checked the device to see if the Twitter account on the device was a known Jihadist account. Allegedly, if the device was in control of a registered Jihadi account, the account was taken over and the device was hacked.**

**One of Jester’s more famous attacks possibly lead to the arrest of several Anonymous members. This completely broke protocol from his normal attacks, showing a more technical and operationally brilliant side to Jester’s attacks. According to a SANS report from 2012, in the middle of his operations against Wikileaks, Jester began performing reconnaissance against several members of Anonymous. Jester advertised a much more powerful replacement for Anonymous’ Low Orbit Ion Cannon (LOIC) tool, one that promised anonymity and added power for the attacker. On the surface, the tool was very stealthy, evading AV and offering a very powerful attack vector. On the surface, the tool was exactly as advertised.**

**The reality was, Jester was advertising a backdoored version of the tool that allowed investigators to identify the attack. Jester did all of this without the source code of the attack tool, changing the functionality and anonymity capabilities without changing the source code and recompiling.**

**Not only did this possibly result in the detainment of several Anonymous members, but it also derailed their confidence in their own tools. Anonymous was already rife with infighting, but their lack of trust in their own tools and other members distributing the tools created even more issues within the group.**

**In another lone wolf covert disinformation campaign, Jester used a PHP vulnerability in a Libyan news site to post injected articles that insinuated the Libyan government was losing the war against the rebels. This was a brilliant technical psyops campaign that could have caused many people to join the rebels, or at least to abstain from joining the government. It also would have demoralized the government soldiers, who weren’t likely to have perfect intelligence that would have denied those allegations.**

**Jester carried out attacks against 200 different targets in two years, appearing to be doing so with a part time job. This is an incredible pace, especially for a part time hacker doing all of his work alone. Nothing indicates that Jester is working with anyone else, and he himself has indicated that he prefers working alone. In the grand scheme of things, Jester’s mistakes have been minor. His fluid investigative and offensive techniques indicate that he is well trained and an extremely adept researcher.**

**It is of the researcher’s opinion that Jester is at least tacitly working with federal investigative agencies. The researcher came to this opinion because of a few points made in the SANS paper about Jester. The SANS paper, as well as several others, indicated that Jester’s DDoS attacks could potentially be pushing Jihadists to more covert means of recruiting and communication. If they aren’t able to speak on the Clearnet, or on Twitter, or through normal Email, they will move on to the Darknet, Jabber, and IRC channels. DDoS attacks, even when carried out via custom made tools, are low-expertise attacks. Jester has indicated a much higher level of skill than just DDoS attacks.**

**Jester also seems to have a much higher level knowledge about intelligence gathering than the average hacker. He knows that his attacks may be compromising ongoing law enforcement investigations. Jester, in the researcher’s opinion, is launching overt attacks via DDoS in his public facing life, but he is also passing information on to LE or federal investigators in order to assist in their much more powerful infiltrations.**

**The SANS report also indicates Jester could only be working a part time job, unless it is pure coincidence that he is only launching attacks in the afternoon. He didn’t likely work in the US military long enough to draw any sort of retirement, so to assume that his only income is from a part time job, and that he carries out his attacks, develops his tools, and performs reconnaissance in the afternoon and on weekends with no pay… that is very hard to believe, in the author’s opinion.**

**It would also fit in the standard procedures of the federal government. Foreign officers in the CIA commonly work a cover job in their station to provide a reason for being in the country. It would make sense for the US government to recruit someone with a cover job, one that offered them plausible deniability and offered Jester a cover as well. Jester could be taking recruitment pages offline while passing intelligence about users and administrators to intelligence officials. This would offer the best of both worlds, letting investigators gather intelligence as well as taking their recruitment portals offline.**

**Just about every single target on the US government’s list is an enemy of the United States in some form. Ghadafi’s regime in Libya was one the US had wanted to overthrow before. He was no friend of the United States. Anonymous and Lulzsec, both anarchist groups who had taken aim at the United States and their intelligence services in the past. The Jihadists are an obvious target, as are Wikileaks and Assange.**

**Westboro Baptist is the only target that doesn’t fit the bill, but it would make sense that Jester would want to target them because of their anti-millitary beliefs, and the Intelligence Community would benefit from turning a blind eye. Targeting Westboro also furthers Jester’s cover as a patriotic lone wolf hacker.**

**It is not necessarily of the author’s opinion that Jester is directly working as a US Intelligence operator. This evidence is entirely circumstantial, and in the grand scheme of things it doesn’t matter that much. Jester is a highly intelligent operator who has taken aim at several high value targets who are enemies of the US and the international community. I am, however, of the opinion that at some point in his operational history, Jester has either approached or been approached by US intelligence officials to pursue a joint effort.**

**Targets:**

**Jihadis**

**Snowden**

**Assange**

**Wikileaks**

**LulzSec**

**4chan**

**Westboro**

**Connections:**

* US Government
* US Military
* Anonymous
* Saladin
* Xerxes
* Leonidis
* US Special Forces