**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.**

**Targets:**

**Jihadis**

**Snowden**

**Assange**

**Wikileaks**

**LulzSec**

**4chan**

**Westboro**

**4chan**

**Connections:**

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