# Global Information Assurance Certification Paper

# The Jester Dynamic: A Lesson in Asymmetric Unmanaged Cyber Warfare

*GIAC (GCPM) Gold Certification*

Author: TJ OConnor, tj_oconnor@me.com
Advisor: David Shinberg

Accepted: December 30, 2011

Abstract

Sophisticated and complex to implement, long-term cyber attacks are often considered the work of intelligence agencies and crime syndicates. However, the oversight and bureaucracy that comes from such management often hinders the ultimate lethality of the attack. In this paper, we will examine the significant impact a lone-wolf patriot hacker has had over the course of the last two years, and what important lessons we can learn from him on how to wage a successful fight in this domain. We will highlight the relatively successful patriot hacking campaign of The Jester.

# 1. Introduction

We live in an era where a single soldier can digitally leak thousands of classified documents (possibly changing the course of war), attackers can compromise unmanned drone control software and intercept unencrypted video feeds, and recreational hackers can steal and release personal information from members of cyber think-tanks. (McCullagh, 2009) (Finkle, 2011) Our inability to defend ourselves against the onslaught of such attacks constantly reminds us of the bureaucracy that comes with large organizations tasked with defending and launching such attacks. As a nation, we still do not understand cyber. An asymmetric platform, cyber favors the individual. This could not be more evident than when analyzing the capabilities of a single lone-wolf patriot hacker. In this paper, we will discuss the actions of a cyber minuteman known as The Jester (aka th3j35t3r) and assess his ability to successfully conduct asymmetric unmanaged cyber warfare.

# 2. Background

On December 30, 2010, a patriot hacker posted a message to an Internet Chat Relay (IRC) Server. Quoting Steve Jobs, the hacker typed: "*A small team of A players can run circles round a giant team of B and C players*" (Th3j35t3r, 2010). Known as Th3j35ter, the hacker claimed to have just successfully compromised members of a powerful hacker group known as Anonymous. By back-dooring the Anonymous group's Low Orbit Ion Canon toolkit, the hacker had removed the anonymous functionality from a toolkit of the members of the rival hacker group and planned to expose them. Most in the intelligence and cyber-security communities would consider this feat alone a cyber-war grand slam. However, this attack happened halfway into a two-year campaign of over two hundred successful attacks, with targets ranging from militant jihadists, ministers of hate, WikiLeaks to rival hacker groups. Before we discuss the tools, campaign, and effectiveness of this hacker, let us begin with some general background information about the patriot lone-wolf hacker known as The Jester.

TJ OConnor, toconnor@mastersprogram.sans.edu

## 2.1. Military Service Background

As The Jester's cyber-attack campaign began with militant jihadists, it does not seem a far stretch that he would have a US military background. In an interview with the website threatchaos.com, The Jester claimed to have served as a former soldier in support of Special Forces deployed to Afghanistan. "*I am an ex-soldier with a rather famous unit…. I was involved with supporting Special Forces, I have served in (and around) Afghanistan amongst other places*" (Greene, 2010).

Often confused with Special Operations Forces, the US Special Forces Command contains five active component and two National Guard component groups with specific regional orientations. Members of each group are subject matter experts in their specific regional area of operation and conduct seven doctrinal missions: Unconventional Warfare, Foreign Internal Defense, Special Reconnaissance, Direct Action, Combatting Terrorism, Counter-proliferation, and Information Operations (Special, 2012). Since 9/11, thousands of soldiers have deployed with Special Forces Groups to Afghanistan. In Afghanistan, Special Forces Operation Detachments proved instrumental in establishing the Northern Alliance that ousted the Taliban Government. It is highly likely that in the course of conducting or supporting Special Forces missions, The Jester could have gained the technical skillsets necessary to perform his current cyber attacks.

However, at least one defense official offers a contradicting viewpoint. An unnamed former defense operative argued in a *New York Times* interview that The Jester was a "former military contractor involved in US Special Operations Command projects" (Vance, 2010). Three command levels above the Special Forces, USSOCOM mission is to support the geographic combatant commanders, ambassadors and their country teams, and other government agencies by preparing Special Operations Forces to successfully conduct special operations, including civil affairs and psychological operations. With an annual budget of $4.9 billion, USSOCOM employs several subject matter expert contractors, including those with specific technical skillsets (Global Security, 2012). It is equally likely that The Jester served in the capacity of a contractor to support a USSOCOM mission. Finally, it is also possible that The Jester transitioned to a role as a USSOCOM contractor after leaving his support role in the US Special Forces.

Additionally, The Jester also claimed to have served twice as an "*airborne frontline combat trooper*" (h3r0d07u5, 2011). Considered the home of the Airborne, and also host to US Army Special Operations Command and formerly two Special Forces Groups, Fort Bragg may be a former post if The Jester did serve in the military. Regardless of the exact specifics, it does appear that his prior service fundamentally motivates The Jester to carry out cyber attacks. In the next section, we will examine some of these specific motivations.

## 2.2. The Motivations and Philosophy of Utilitarianism

Largely motivated by his prior military service, The Jester appears focused on denying safe haven to terrorists and ministers of hate that use the Internet as their platform. In an early 2010 interview, The Jester discussed "*the horror of watching his friends and fellow soldiers be murdered by Jihadi operatives who have long been exploiting the Internet*" (Freed, 2010). During the Hacker Halted security conference, The Jester spoke with conference attendees via Internet Relay Chat. Figure 1 shows a partial transcript from this discussion. He argued that the omnipotence and growth of the Internet has granted terrorists a safe haven, and stated his intentions to prevent such action. Furthermore, The Jester claims to have discovered caches of Jihadi information planted on legitimate US sites by Jihadi hackers (Freed, 2010).

```
18:28] <@th3j35t3r> I am motivated by the fact that previously...
[18:28] <@th3j35t3r> for a bad person to recruit a potential bad person....
 [18:28] <@th3j35t3r> teach them to make IEDs...
[18:29] <@th3j35t3r> or vests
[18:29] <@th3j35t3r> they had to meet
[18:29] <@th3j35t3r> which was great
[18:29] <@th3j35t3r> made them easier to spot
[18:29] <@th3j35t3r> now
[18:29] <@th3j35t3r> there is no need for a physical meeting
 [18:30] <@th3j35t3r> I am here to say - no guys - you aint gonna use the web to blow
my buds up.
```

**Figure 1:** Partial Th3J35t3r Transcript From Hacker Halted

This internal desire to deny Internet sanctuary to Jihadists appears to stem from his military service. His service also appears to push his desire to protect both current and fallen American soldiers. After attacking the Westboro Baptist Church for protesting at the funerals of fallen US soldiers, The Jester posted: "*There is an unequal amount of*

*good and bad in most things. The trick is to work out the ratio and act accordingly*" (Th3J35t3r, 2010). This quote closely resembles the fundamentals behind the ethical theory of utilitarianism, best described by Jeremy Bentham as the greatest happiness principle. Bentham asserts that an individual can only weigh the ethical considerations of an action by knowing and calculating the consequences and outcomes (Bentham, 1948). This philosophy accurately describes The Jester's actions. In a 2010 interview, The Jester explained his ethical concerns about his attacks: "*I do wrestle with whether what I am doing is right, but figure if I can make their communications unreliable for them, all the better*" (Freed, 2010).

Over a two-year period, The Jester has successfully attacked over two hundred targets. One could argue that The Jester almost feels compelled to prevent his adversaries from succeeding in their message of hate. Considering the sheer enormity of targets The Jester has successfully attacked over a prolonged period of time, this endeavor has most likely become a lifestyle and mission for The Jester. In section four, we will closely study specific targets. However, let us outline a broad overview of the timeline of activities in the next section.

## 2.3. Timeline of Activities

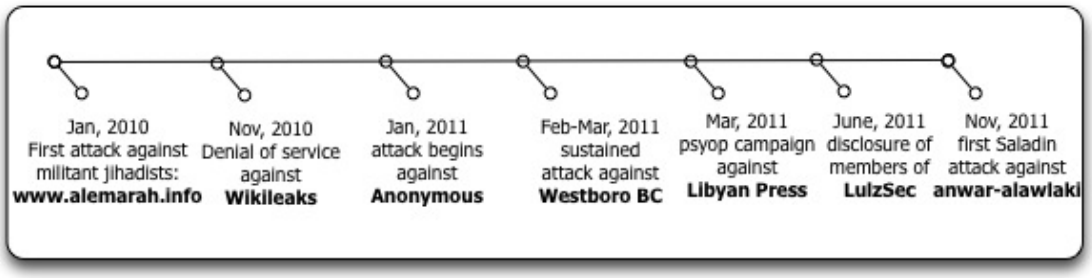



**Figure 2:** Timeline of The Jester's Significant Activities

We can best split The Jester's attacks into six separate campaigns that we will expand in section 4. The Jester launched the first campaign on January 1, 2010. On this day, he began a series of attacks against militant Jihadists websites with an attack on www.alemarah.info. During his militant Jihadists attacks, The Jester primarily used his homebrew tool, XerXes, to deny service to these particular websites. This attack

continues to date, with the latest attack occurring on December 4, 2011, against http://www.majahden.com/, with a new tool aptly named Saladin.

Nearly a year into his disruption of militant Jihadists websites, The Jester attacked the WikiLeaks Web site on November 28, 2010. While still a denial of service attack, this attack differed from previous attacks. Previous attacks lasted for only short periods of time. In the attack on WikiLeaks, The Jester tweeted "*TANGO DOWN - INDEFINITLEY - for threatening the lives of our troops and 'other assets'.*" This attack also lead The Jester into his next campaign to attack those who supported WikiLeak's defense, primarily the hacker group Anonymous.

The campaign against Anonymous began on January 24, 2011. During this phase, The Jester showed an entirely new skillset by performing reconnaissance against the members of the hacker group and then exposing them through a back-doored executable provided to the members of the group. Although The Jester and Anonymous appeared to work together during his next campaign, The Jester did appear to gloat when fifteen members of Anonymous were arrested in June 2011: "*15 more 'Anonymous' arrested (again). Legion didn't 'expect' that huh - Tick Tock Toldya.*"

Regardless of their differences, it appears The Jester and Anonymous worked together to attack The Westboro Baptist Church. The longest-running individual attack, The Jester shut down the website run by the controversial Westboro Baptist Church from late February 2011 to March 2011. Almost a week into the attack, The Jester bragged that his attack platform was a single 3G phone that shut down the website of The Westboro Baptist Church.

After attacking The Westboro Baptist Church, The Jester moved onto a more international target, where he changed tactics again. With rebel uprisings and internal turmoil happening in Libya, The Jester hatched a plan to disrupt online media with false news stories. This psychological operations campaign culminated with the successful injection of stories into popular news media like the *Tripoli Post* in March 2011.

As The Jester successfully attacked Libyan online media, a new and dangerous splinter cell of Anonymous formed. This elite crew, known as LulzSec, attacked significant targets, including the Central Intelligence Agency of the United States. By

June of 2011, it appeared as if nobody could stop "The Lulz." Teaming with an independent group of security professionals, The Jester uncovered the true identity of the group's leader in the summer of 2011. A successful arrest of the group's key members ended The Jester's campaign against LulzSec by fall 2011.

## 2.4. False Identities, Sympathizers and Supporters

Arguably, The Jester has many sympathizers, with over 28,000 Twitter followers. Let us assume that some of these provide limited intelligence support to The Jester in identifying malicious activities and nominating potential targets. However, based on his ability to remain anonymous, it is generally assumed that The Jester does not receive any material support from his sympathizers. A note on his official blog further indicates that The Jester would prefer his sympathizers contribute to the Wounded Warrior Project, an organization that provides support to disabled veterans returning from war.

During an operation to identify the personal identity of the hacker known as #anonymousSabu, The Jester confessed that at least fifteen individuals had been falsely identified as The Jester and "*have been doxed… always incorrectly*" (Th3J35t3r, 2010). In October 2011, The Jester tweeted that "*rjacksix was first of at least 15 folks incorrectly doxed as me over year ago."* As he was the first individual falsely identified, it proves important to dig deeper into Mr. Robin Jackson (aka rjacksix).

During the operation known as Operation Payback, the hacker group Anonymous targeted Mr. Jackson. It is unknown how Anonymous identified Mr. Jackson as The Jester. Mr. Anthony Freed, a reporter at InfoSec Island, scoured social networking media Web sites to discover that Mr. Jackson was the Chief of Management Services Bureau for the State of Montana (Freed, 2010). Furthermore, Mr. Jackson formally studied the Russian language for the military, learned to program at Fort Meade (home of the US Cyber Command), and worked in the SCADA industry for GE (Freed, 2010). Mr. Jackson's profile certainly appears as if he could be a possible candidate.

Another figure closely linked to The Jester is Dr. Sam Bowne. A professor at the City College San Francisco, Dr. Sam Bowne presented research about The Jester at DEFCON 2011. At DEFCON 2011, Dr. Bowne confessed that he had been in communication with The Jester throughout The Jester's initial attack on WikiLeaks. Mr.

Bowne claimed The Jester even paused his attack briefly to provide proof of the attack (Bowne, 2011). Dr. Bowne and The Jester publically argued on Twitter in August of 2011, as shown in Figure 3.

**Sun Aug 14 16:57:48** +0000 2011,*@sambowne if u don't want ur students to imitate me keep vilifying me. However they're far more likely to hook up with #anonymous than me.*

**Sun Aug 14 16:51:44** +0000 2011,*RT @sambowne: @th3j35t3r: You need to hide, and you hide well. But I don't want students imitating you. cc: @marcus_bp*

**Sun Aug 14 16:41:29** +0000 2011,*@Marcus_BP @sambowne I am incognito, unlike Mr Bowne, who has utmost respect, as I have a lot more to worry about than likes of Anon/Lulz.*

**Figure 3:** Twitter Traffic Between The Jester and Mr. Sam Bowne

In preparation for this article, we spoke with Dr. Browne. He referred us to blog, where he argued that The Jester's activities are illegal. (Bowne, 2011) Further, he wanted to make it clear that he did not condone The Jester's activities in any capacity. It is possible that The Jester is a former student of Mr. Bowne, or at least sat in on one of his lectures. However, The Jester and Mr. Sam Bowne may just share respect for each other's competency in understanding Layer 7 denial of service (DoS) attacks. Because The Jester used Layer 7 DoS as his original and primary, we will use the next section to discuss these attacks.

# 3. Attack Platforms

## 3.1. Understanding Layer 7 DoS

Layer 7 DoS attacks prove the majority of The Jester's over two hundred successful cyber attacks. As opposed to a distributed denial of service attack (DDoS), Layer 7 DoS attacks require only one attacker instead of many. The attacks can be routed over proxies and prove difficult for an administrator to distinguish from normal traffic. (Bowne, 2011)

Two different attack toolkits highlight the flaws used in executing a Layer 7 DoS attack. First, we will examine the toolkit slowloris, written by Rsnake (Rsnake, 2012). Rsnake's slowloris toolkit succeeds in crippling a web server with minimal bandwidth and minimal side effects on unrelated services and ports (Rsnake, 2012). It performs this

attack by splitting HTTP requests and sending only limited parts at a time. This maintains an open connection on the web server, which keeps sockets from closing. In doing so, the toolkit exhausts the available sockets from the target.

Instead of sending HTTP requests, a separate toolkit known as R-U-Dead-Yet (RUDY) consumes resources by abusing HTTP POSTS (Raviv, 2010). RUDY slowly trickles one-byte injections into a post field. The target webserver consumes endless threads waiting for slowly trickled posts, exhausting the resources of the web server and crippling it.

Although The Jester's exact attack vector is unknown, many have speculated that his attacks are similar in nature to Slowloris, RUDY, or both. In the following section, we will examine his toolkits used in his attacks.

## 3.2. XerXes, Leonidis, and Saladin

In two separately released videos, The Jester publicized his toolkit known as XerXes (Freed, 2010). With a rather robust graphical user interface, the toolkit graphically depicts the attack in progress and allows The Jester to control it in real time. Both videos provide insight into the toolkit. It appears The Jester routes the traffic through an anonymous network such as TOR, with icons for both the entry and exit, and intermediate notes that route the attack, as shown in Figure 5. A supposedly leaked source code (which The Jester has publically denied) shows the use of cycling through TOR networks to attack, as shown in Figure 4.

```
void cycle_identity() {
        int r;
        int socket = make_socket("localhost", "9050");
        write(socket, "AUTHENTICATE \"\"\n", 16);
        while(1) {
                r=write(socket, "signal NEWNYM\n\x00", 16);
                fprintf(stderr, "[%i: cycle_identity -> signal NEWNYM\n", r);
                usleep(300000);
        }
}
```

**Figure 4:** Partial Leak of XerXes Source Code

Furthermore, the toolkit appears to allow The Jester to select attack options, the type of target server, and automatically post the results to the Twitter social media site.

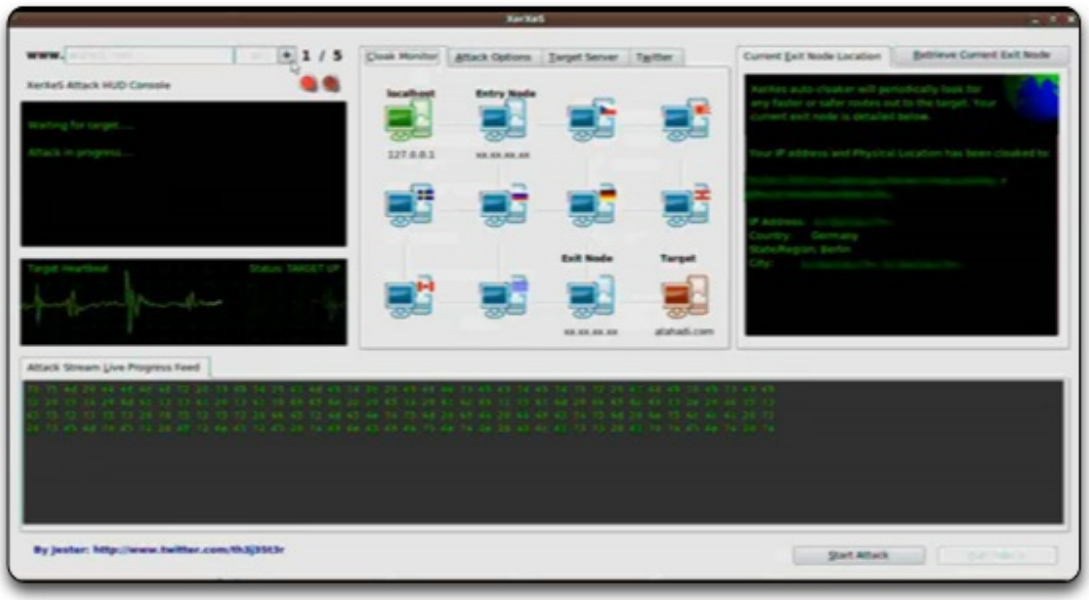


**Figure 5:** XerXes Denial of Service Toolkit

Early criticism of XerXes argued that the tool was only capable of hitting unhardened Apache webservers vulnerable to the SlowLoris and RUDY types of attacks. However, The Jester has publically stated via Twitter that since March 2010 XerXes has been capable of targeting IIS servers in addition to Apache. In a July 2011 posting shown in Figure 6, The Jester argued also that many of his targets have had a platform other than Apache.

**Fri Jul 08 21:14:10** +0000 2011,FTR: the purported 'XerXeS source' leak is bogus. Its not getting released, and isn't limited to Apache as has been demonstrated many times.

**Fri Jul 08 20:42:39** +0000 2011,@sambowne - come on Sam? We both know within my targets over the last 2 years Apache only features as it's prevalent, theres more than that.

**Thu Mar 11 22:57:57** +0000 2010,Jester releases 2nd video of enhanced XerXeS attack - http://bit.ly/90IaQd - read it and well...weep cuz it's not just Apache now.

**Figure 6:** Twitter Exchange about the XerXes Toolkit

In addition, The Jester has alluded to developing two separate toolkits named Leonidis and Saladin. Named after the first Sultan of Egypt and re-capturer of Palestine, Saladin has been used in at least five separate attacks since November 2011. http://anwar-alawlaki.com/ was the first target of Saladin. More powerful than a simple DoS toolkit,

The Jester bragged *Tango Down Permanently* after attacking anwar-alawlaki.com/. Furthermore, he hinted to the attack vector by stating because #saladin (XerXeS big bro) "*knows their p/w and changed it, and deleted you*."

Little is known about the Leonidis attack platform, named after the Spartan warrior-king most famous for his bravery during the Battle of Thermopylae. Other than referring to it during his Hacker Halted IRC Chat and a brief mention during an interview with Mr. Anthony Freed, The Jester has spoken little publically about the attack platform. While The Jester has his tools, let us use the next section to discuss how he back-doored the tools of his adversaries.

## 3.3. Reverse-Engineering Technical Skills

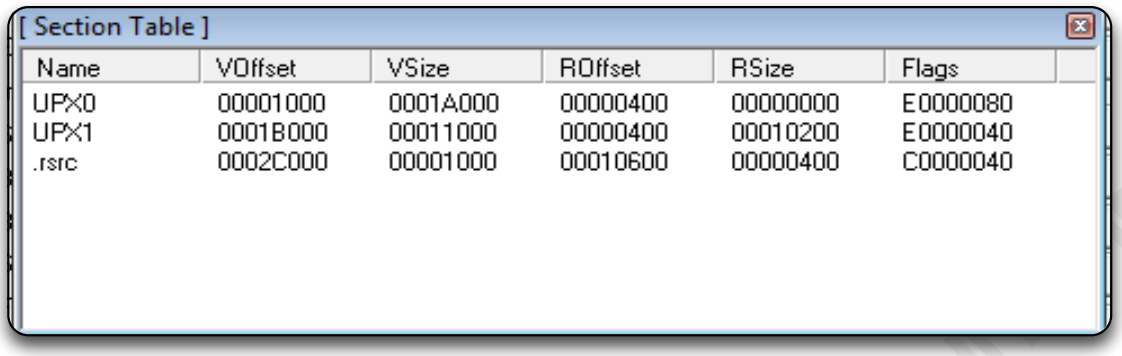
The December 2010 attack against Anonymous proved pivotal in defining The Jester's capabilities as a talented attacker. At this point in his cyber-warfare campaign, he removed any criticism of his technical skillsets. In his attack against the Hacker group Anonymous, The Jester falsely advertised a replacement tool for the group's Low Orbit Ion Canon (LOIC) DDoS toolkit and encouraged members of the group to download it, shown in Figure 7.

ADVANTAGES OVER LOIC:

*This tool supports DNS amplify attacks, which can make your DDOS attacks up to 70* as effective, by combining ip and mac source address spoofing, and trackers over TOR, anonymity is guaranteed*

**Figure 7:** ReadMe provided with DHN.zip toolkit

However, The Jester added a back-door routine to the toolkit so it would remove the anonymous functionality provided by the tool (Infosec, 2011). Anti-Virus systems employed by the hacker group would detect this activity. To hide his malicious activity, The Jester encoded the binary using a UPX packer to evade anti-virus activity. Thus, a virus detection engine could not find a static signature for malicious activity. The binary decrypted itself to run in memory, successfully evading anti-virus activity. Examining the portable executable section headers from the binary in Figure 8, it is clear it is UPX packed to evade anti-virus.


[ Section Table ]

| Name | VOffset | VSize | ROffset | RSize | Flags |
|---|---|---|---|---|---|
| UPX0 | 00001000 | 0001A000 | 00000400 | 00000000 | E0000080 |
| UPX1 | 0001B000 | 00011000 | 00000400 | 00010200 | E0000040 |
| .rsrc | 0002C000 | 00001000 | 00010600 | 00000400 | C0000040 |

**Figure 8:** UPX Packed DHN.exe Section Table

The Jester's ability to intercept the source code of the DHN.zip toolkit, remove functionality in the binary without drawing attention, and then repack the binary using a UPX packet to evade anti-virus detection proves worthy of praise. However, the quick rise to popularity and public support has been fueled by The Jester's savvy social media campaign.

## 3.4. Social Media Campaign

Arguably one of the most amazing abilities of The Jester is his social media campaign. Through his online campaign, The Jester garnered support from otherwise law-abiding citizens. Over two years, The Jester posted 918 independent tweets to his some 28,200+ followers. Additionally, The Jester maintains a fairly robust Wordpress blog, where he has outlined his activities in great technical depth. On his blog, shown in Figure 9, he discusses the motivations and technical aspects of his attacks. Just shy of 1 million unique visits (988,622 as of 9 January 2012), The Jester has a considerable following on his Blog.

Although The Jester's personal interviews have been far and few between compared to the omnipotence of his attacks, he has spoken on a couple occasions. First, he discussed his motivations and the XerXes toolkit with Mr. Anthony Freed (InfoSec Island) along with the ethical dilemmas he has faced. Next, Mr. Sam Bowne, ethical hacking instructor at City College San Francisco, has spoken to him numerous times in regards to specifics of Layer 7 DoS attacks. In addition, the 2600 IRC server has proved a safe haven for The Jester to occasionally entertain questions, as he routinely appears in the channel #jester.

TJ OConnor, toconnor@mastersprogram.sans.edu


**Figure 9:** The Jester's WordPress Blog

On October 26, 2011, The Jester spoke openly with conference attendees from Hacker Halted over an IRC channel (Infosec, 2011). The Jester candidly discussed the rationale behind his attacks, his desire to work alone, the specific attacks against Anonymous and the Libyan online press, and an incident where he mistakenly hit the wrong target. Using his very savvy social media skills, The Jester has garnered public support for his repeated attacks. In the next section, we will discuss the specific attack campaigns of The Jester.

# 4. Attack Campaigns

## 4.1. Disruption of Militant Jihadist Propaganda

On January 1, 2010, The Jester began his campaign to disrupt militant Jihadist web propaganda. At 11:26, he tweeted "*www.alemarah.info is now under sporadic cyber attack. This 'Voice of Jihad' served only to act as tool for terrorist. OWNED. By me, Jester.*" This began a sustained campaign against over seventy-five other targets over the next two years. Annex A1 contains a complete list of the sites attacked.

In an interview months later, The Jester described his desire to push militant Jihadists underground: "*If you take the position that online jihadi propaganda,*

*proselytization, and interaction is increasingly important in jihadi recruitment, then why is it bad to drive them back into the shadows online? That's a key principle of COIN* [Counter-insurgency]."

Almost a year into his campaign against militant Jihadists, The Jester identified a target that posed a greater threat to US national security. In the following section, we will discuss his attacks against the Web site WikiLeaks.

## 4.2. Disruption of WikiLeak's Dissemination of Classified Data

On November 28, 2010, The Jester attacked the WikiLeaks Web site run by notorious hacker Julian Assange. Although originally launched in 2006, WikiLeaks gained public notoriety in October 2010 when it published over 400,000 classified documents about the Afghan war. US officials coordinated with Amazon, PayPal and MasterCard to prevent future funding of the WikiLeaks supporters. However, the US government did technically very little to successfully knock WikiLeaks offline.

In November of 2010, WikiLeaks coordinated to release US State Department Cables. At this point, The Jester weighed in with his public objection and disrupted WikiLeaks: "*www.wikileaks.org - TANGO DOWN - for attempting to endanger the lives of our troops, 'other assets' & foreign relations #wikileaks #fail."* During this attack, Sam Bowne claimed The Jester even paused the attack for a minute to prove he was behind it (Bowne, 2011).

The attack on WikiLeaks and subsequent fallout lead to an argument between the hacker group Anonymous, which backed WikiLeaks, and The Jester, who had attacked it. This began The Jester's campaign of personal attacks on members of Anonymous. In the next section, we will examine some of the key highlights of this campaign.

## 4.3. Tangles with the Anonymous Hacker Group

In late January 2011, a public war waged between The Jester and the hacker group Anonymous. This war waged over Twitter, WordPress blogs, and in private IRC channels controlled by both Anonymous and The Jester. On January 24th 2011, The Jester clearly objected to Anonymous' defense of WikiLeaks when he tweeted: "*#Wikileaks Rest in Peace http://t.co/bw4vfga #anonymous defending a corpse, peace out."*

In response, Anonymous targeted individuals who sympathized with those that wished to destroy WikiLeaks during Operation Payback. It was during this time that the group targeted Robin Jackson, claiming that he was The Jester, a claim The Jester later denied". They also attacked the Web sites of MasterCard, PayPal, and Amazon, which had removed the ability to send payments to WikiLeaks maintainers.

The Jester claimed an official victory in the war when he reverse-engineered and removed the anonymous functionality out of Anonymous's DHN.zip toolkit. To advertise his successful attack, The Jester posted:

> *That's right ladies and gents, trolls and trollettes, skiddie, wannabe, and poser…. The DHN files that you are downloading, using, and 'playing' with are altered versions of the original. These lovely beauties are, in fact, infected by none other than th3j35t3r. (Did Anonymous really think that they could remain anonymous with all their little toys.)*

## 4.4. Sustained Attack against Westboro Baptist Church

Another key indicator behind The Jester's motivation lies in his attack against the controversial Westboro Baptist Church. The Westboro Baptist Church, lead by Rev Fred Phelps, has staged protests at funerals ranging from slain gay college students to members of the US military killed in combat. The group typically uses inflammatory language to harass vulnerable victims such as the family members of deceased US military soldiers. Evidence of this is depicted in Figure 10, from the Westboro Baptist Church's official Web site, where they provided a flyer to protest the funeral of a fallen US soldier claiming to "*play taps to a fallen fool."* Clearly, this could fuel the anger of an individual such as The Jester, who claims to have served twice in frontline airborne combat units. Speaking over an IRC channel during Hacker Halted, The Jester stated his objections to the WestBoro Baptist Church: "*I draw the line in the sand…when they attempt to get in the face of the mourners of our military*" (InfoSec, 2011).

In February 2011, The Jester began an attack that took twenty Web sites of the Westboro Baptist Church down for four straight weeks.


**Figure 10:** WestBoro Baptist Church's Flagship Web site, GodHatesFags.com

A since-deleted Twitter post by The Jester hinted that the Anonymous hacker group had also assisted in the attack: "*AnonymousIRC The @th3j35t3r and #Anonymous cooperation on #WBC was an eclipse; we're still like Sun and Moon, following our own agendas.*" Considering that only a month earlier The Jester and Anonymous had gone to war, it definitely demonstrated both groups' desire to take the Westboro Baptist Church offline indefinitely. Officially, the Anonymous group denied any involvement in the attack. Regardless of Anonymous' activities, it appeared by spring 2011 that The Jester and Anonymous no longer shared the desire to attack each other. Instead The Jester moved onto a more substantial target in summer 2011, a target that troubled intelligence agencies and law enforcement agencies worldwide.

## 4.5. De-Anonymization of LulzSec

Known for successfully attacking the Central Intelligence Agency's web server, the hacker group LulzSec quickly rose to popularity in June 2011. LulzSec additionally attacked Fox News, PBS, Nintendo, pron.com, the NHS, Infragard, the US Senate, Bethesda, Minecraft, League of Legends, *The Escapist* magazine, EVE online, *The Times*, and *The Sun* newspaper (Pwnies, 2011).

During their reign of terror on the Internet, LulzSec came to the attention of The Jester. By mid-June 2011, The Jester indicated his intentions to discover the identities of the members of LulzSec when he tweeted: "Gloves off. Expect me. My silence is not an indication of weakness, as your mouth is an indication of yours." During his attack against LulzSec, it is believed that The Jester joined forces with a team of hackers known as Web Ninjas. These security professionals setup a blog, where they posted the identities of supposed LulzSec members at http://lulzsecexposed.blogspot.com. The Jester's motivation was fueled by his anger of LulzSec's dumping documents that contained the "*names of undercover operators in the field, exposing not only them, but their families*" (Th3J35t3r, 2010).

Within a week of The Jester declaring "gloves off", Ryan Cleary was arrested on June 22, 2011, and charged with five offenses under the Computer Misuse Act (Vinograd, 2011). Cleary was discovered after "*someone with apparent links to the group posted Cleary's personal details on various websites – including his address, phone numbers, chat screen names and email address*" (Vinograd, 2011). Subsequently, on September 21, the FBI arrested Cody Kretsinger of Phoenix, Arizona, on the suspicion that he was a member of LulzSec during the attack on Sony Pictures (Eimiller, 2011). Furthermore, individuals within LulzSec were supposedly ousted in anonymous post to a pastebin account. These individuals included Sweden-based Daniel Ackerman Sandberg (aka Topiary), Iowa-based Wesley Bailey (aka Laurelai), New York-based EE (or Eekdacat), Britain-based Richard Fontaine (aka Uncommon), alleged leader Hector Xavier Monsegur (aka Sabu), and Netherlands-based Sven Slootweg (aka Joepie91), among others (IBTimes, 2011).

However, this attack was not without controversy. During his work with Team Web Ninjas, The Jester identified two separate individuals as #anonymousSabu, the leader of LulzSec. In July, based on information from an intercepted LulzSec IRC session, The Jester initially fingered Hugo Carvalho as the leader of LulzSec based on a domain name registration and other details. However, after gaining further information, The Jester retracted his accusation and instead pointed the finger at Xavier Monsegur.

## 4.6. Libyan Disinformation Campaign

In late March 2011, The Jester turned his attacks to the former Libyan strongman Muammar Gaddafi. During this campaign, The Jester once again changed tactics. Instead of his using his proven DDoS toolkits XerXes and Saladin, he used a psychological operations trick, possibly learned during his time in the military.

In an attempt to break the spirits of troops loyal to Muammar Gaddafi, The Jester injected two news stories into *The Tripoli Post* and a separate news story into the *Malta Independent Online*, shown in Figure 11. The stories were headlined "*Gadhafi loyal soldiers deserting and defecting as key off tows are lost to rebel forces*" and "*army abandoning posts across country as rebels advance further and further*." The Jester presumably intended for these stories to erode the morale of Gaddafi loyalists and inspire them to desert their posts. In subsequent Twitter postings, The Jester excitedly encouraged Libyan defections, including the Libyan Foreign Minister.


**Figure 11:** The Jester's Compromise of *The Tripoli Post Online*

In order to inject these stories into two separate newspapers, The Jester used a technique known as "bit.ly obfuscated intermediary-based code injection" (Freed, 2010). By examining a vulnerability in the PHP code of the two sites, The Jester discovered a method for injecting images of articles into a search query field of the pages. The Web sites then returned these images as direct results, thus appearing to come from the legitimate news sources instead of The Jester. Considering his technical competence, political agenda, and a proven track record, we will use the next section to discuss the overall effectiveness of The Jester's six campaigns of cyber war.

# 5. Assessment of Effectiveness

## 5.1. Demographics and Metrics of Targets

In twenty-four months, The Jester has performed over 200 attacks on seventy-five unique targets. This means on average that he nominates a new target three weeks and attacks a target just about twice every week. While this pace alone seems astounding, consider another detail: the heavy lifting of The Jester's work is done between 3:00 PM to midnight EST. Figure 12 shows a distribution of the times The Jester has tweeted "TANGO DOWN." Before noon EST, The Jester is almost absent from attack. This supports the assumption that The Jester may indeed hold at least a part-time job and perform his attacks after returning home.

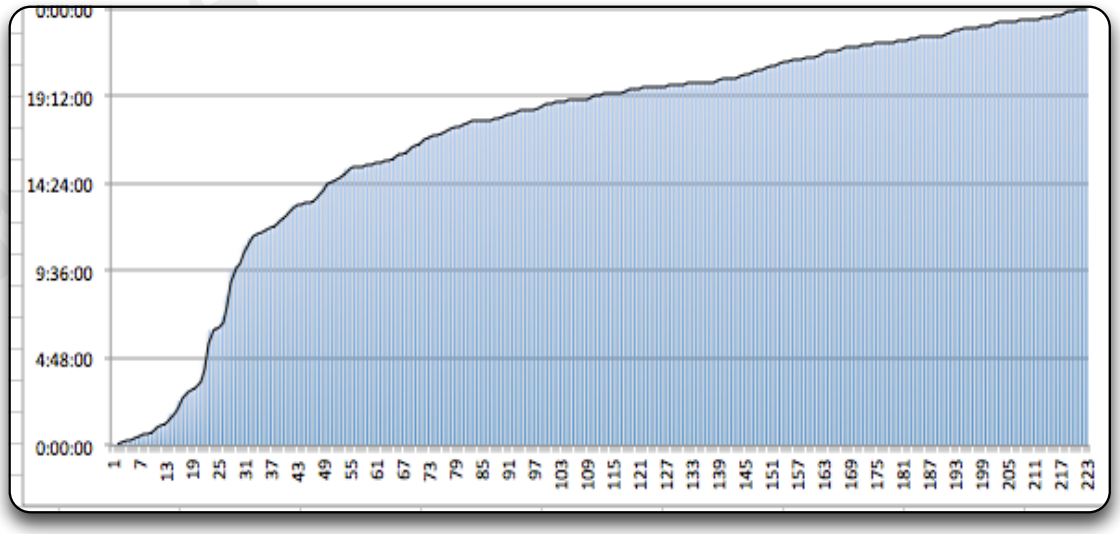



**Figure 12:** The Distribution of Times Jester Has Successfully Attacked Targets.

Figure 13 also supports this assumption. To create this figure, we totaled the unique attacks for each day of the week that The Jester has tweeted "TANGO DOWN." On Sundays he has attacked over 50 targets, almost double the weekly average. If The Jester works Monday through Friday, he may do his research and targeting activities primarily on Saturday and then attack the following day.

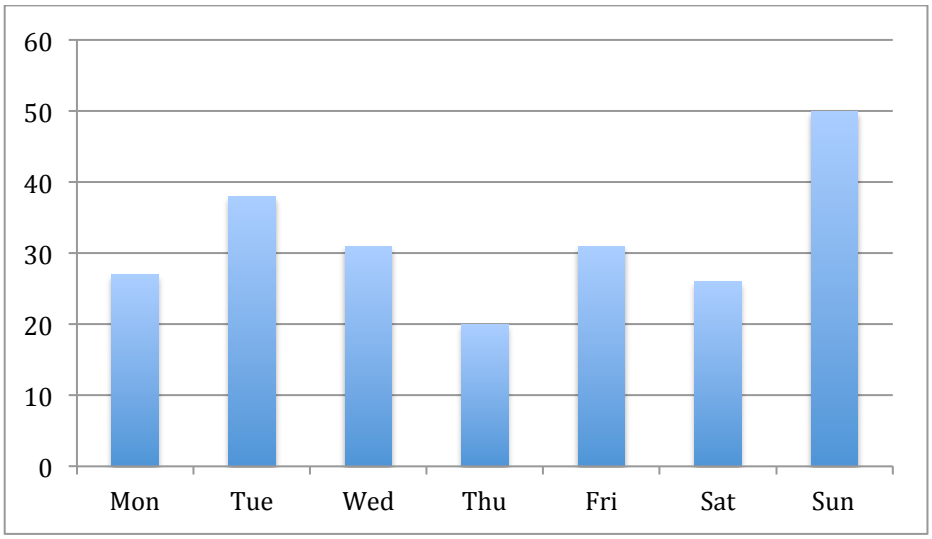



**Figure 13:** Distribution of Days that Jester Has Successfully Attacked Targets.

Figure 14 depicts the months of The Jester's attacks. March, July, and November stand out predominantly. Could this support the notion that The Jester is somehow involved with academia? Typically, academic institutions offer Spring Break in late March and early April, with summer leave in July and multiple holidays during the month of November. Could The Jester be a member of academia using these block leave dates for the bulk of his attacks? We may never know, which still remains the greatest strength of The Jester. In the next section, we will examine how he has been able to remain anonymous for over two years.

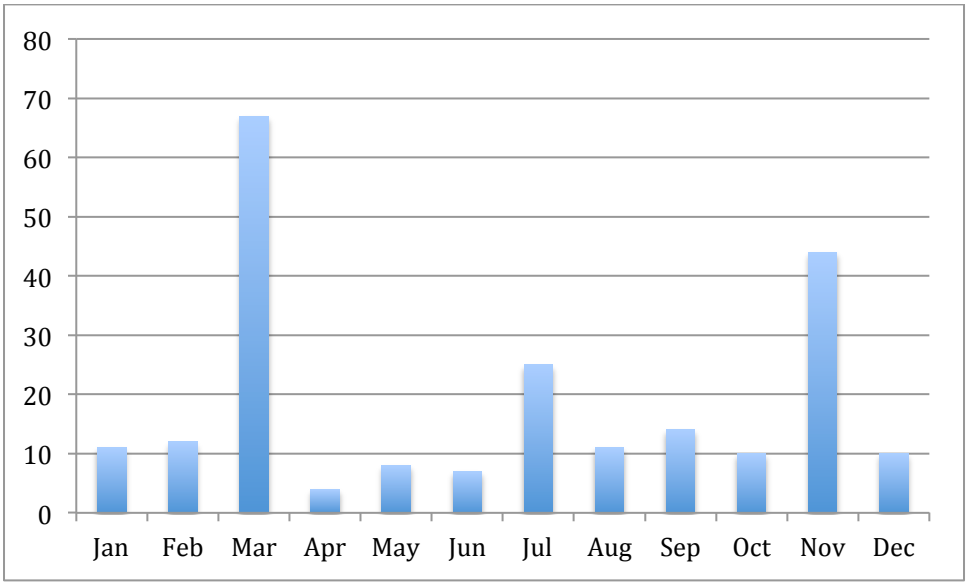



**Figure 14:** Distribution of the Months that Jester Has Successfully Attacked Targets.

## 5.2. Non-Repudiation of Attack, Ability to Remain Anonymous

In a message to Anonymous spokesman Barrett Brown, The Jester described the difficulty in concealing his true identity:

> *Let me break it down for you Brown, I have been operating for 2 YEARS ….alone. In that time I have had 'over 9000' anons trying to find me, along with multiple Law Enforcement Agencies, not to mention an Army of Muslim Extremists who would love nothing more than to saw my face off on cam, with a rusty nail.*

The Jester's words are certainly inflammatory and meant to incite support to his cause. Nonetheless, his words accurately describe his scenario. Consider the victims of The Jester for a moment. He has attacked militant Jihadists for two straight years, remotely shut down WikiLeaks, attacked a ministry of hatred, psychologically operated against a Libyan strongman, and aided in the arrest of members of the hacker group Anonymous and its elite splinter cell LulzSec.

LulzSec successfully attacked the Central Intelligence Agency of the United States. WikiLeaks, in turn, has amassed the largest public collection of stolen classified documents. The WestBoro Baptist Church found a way to hold a soldier's family financially accountable for attempting to disrupt a protest at their son's funeral. (Grinberg, 2010) The Jester's targets are all empire-builders. In his fight against them,

The Jester acted as David slaying Goliath, not once but six separate times. With his enemies fallen, not one has identified his true identity. Not a single law enforcement agency has detained and arrested The Jester or issued an arrest warrant with his true identity.

How has The Jester accomplished such a feat? Even the very competent and elite hackers of LulzSec eventually were de-anonymized and captured. How can a single patriot hacker remain anonymous in his attacks and continue to operate for two years undetected? The answer lies in his lack of reliance upon anyone else. While #anonymousSabu counted on the technical competence of members of his elite group and the savvy political skills of Topiary to promote their cause, The Jester essentially performs all his work. He continues to perform his own reconnaissance, targeting, promotion, and research and development. Over 200 successful attacks against seventy-five different independent targets in two years and The Jester remains anonymous. In the next section we will discuss how he maintains this tempo and success rate by in-house research and development.

## 5.3. Research and Development Capabilities

Consider for a moment the initial criticisms of The Jester. Some argued that he was only capable of only adding a GUI to a well-known attack against Apache Webservers. His critics argued that The Jester lacked any real knowledge of attacks and was simply bold enough to perform attacks. However, time and again The Jester has silenced this criticism. (Jeter, 2011)

Consider the moments when The Jester changed tactics. In January 2011, The Jester applied reverse-engineering techniques by crippling the software of Anonymous. In March 2011, he invented a technique for inserting stories into two separate international newspapers. By summer 2011, he joined forces with a powerful group that used sound investigative and reconnaissance skills and tools to de-anonymize the elite hacker group, LulzSec. Yet, as all these operations continued, The Jester successfully developed two new tools: Leonidas and Saladin. By December 2011, The Jester successfully launched Saladin against a target.

Anyone that has served a day in any military knows that you have an operations planning cell, a targeting cell, and then men who are actually the boots on the ground. The Jester continues to attack while at the same time doing his own targeting, planning, and development of tools. This itself is an incredible feat. However, consider the fact that The Jester most likely also has a 9-to-5 job. Certainly his patriot hacking provides no financial incentive, so these attacks are most likely carried out in his free time. This assumption is supported by the knowledge that Sunday appears to be the most prominent day for his attacks, with fifty independent attacks occurring on Sundays versus an average of 28.3 attacks occurring on each of the remaining days of the week.

The Jester has proven incredibly resourceful in research and development. In 2011, The US cyber-security budget spent $139 million for US Cyber Command and received a $105 million increase from previous years (Kruzel, 2010). Yet, at best we can tell The Jester receives no official funding or support, and has continued to attack over a two-year span. His unflagging ability to morph tactics while still attacking remains one of his greatest strengths.

## 5.4. Cyber-Fratricide Incidents

Clearly, The Jester is a controversial figure. While some information security professionals may support The Jester's cause, his activities have lead to personal attacks on fifteen innocent individuals, including Robin Jackson. Additionally, The Jester falsely accused Hugo Carvalho as the leader of the hacker group that took down the Web site of the Central Intelligence Agency. We can only imagine that this fingering did and continues to significantly impact Mr. Cavalho's personal life.

Arguably The Jester does interfere with ongoing cyber operations by intelligence and government agencies tasked with those missions. On a bureaucratic level, a great deal of effort is made before the US government can perform any cyber mission to prevent cyber fratricide on a target. In contrast, The Jester receives no official authority and therefore is exempt from asking permission. This does mean his attacks can occur swiftly, such as we saw in the attack on WikiLeaks. One would imagine it would be in the best interest of the US government to shut down that particular Web site. However, officially, The Jester remains the only individual capable of carrying out such an activity.

Does The Jester's ability to strike precisely and quickly outweigh his lack of coordination with intelligence and government agencies? It appears to do so in his utilitarian mind. However, consider a hypothetical attack by The Jester on the Web site www.baghdadsniper.net. This Web site served as a recruiting ground for militant Jihadists. The Jester's attack disrupted this Web site and drew attention to it. This type of activity most likely pushed underground the operators of the Web site and individuals interested in visiting it. The Jester's attack could hypothetically cost intelligence agencies actable intelligence on a target that could lead to the capture of a militant Jihadist recruitment team. While this is a purely hypothetical example, it does highlight the problem with a rogue patriot hacker who receives no official authority.

## 6. Conclusions

In conclusion, we have addressed the storied history of patriot hacker, The Jester, and his campaign of unmanaged, asymmetric cyber warfare. Without a doubt, The Jester has succeeded in his campaign of cyber warfare over a two-year span. He has accomplished in his intentions to push militant Jihadists underground and deny them safe haven on the Internet.

His attacks have mutated, supporting multiple different types of targets, while at the same time his tactics have morphed as well. While maintaining a considerably fast operating tempo of three unique targets every month and discrete attacks every week, The Jester has found a way to perform reconnaissance, targeting, research and development, and publicized his attacks. In discussing his different campaigns, we have come to realize that he has acted as David slaying a few giants, including members of Anonymous and their elite splinter cell LulzSec, the WestBoro Baptist Church, militant Jihadists using the web to spread propaganda, and Libyan strongmen. Additionally, The Jester's strengths lie in his ability to remain anonymous in denied sanctuary. Two hundred attacks in two years, and we still do not have an identity for this hacker. As we discussed in section 5, we can only really hypothesize the effects The Jester has had on intelligence community activities. However, we discussed possible cyber-fratricide incidents and the impacts The Jester may have had on ongoing intelligence collection operations.

In conclusion, The Jester has taught us quite a bit about cyber warfare. This domain is one that favors David over Goliath. Fully functional teams like LulzSec succeed in the short term with precision strikes, as we saw in their campaign of terror; however, they ultimately fail when personalities inside or attached to the group crumble. In contrast, individuals excel and continue to remain anonymous because they do not count on outside resources and significantly reduce their threat vectors. The Jester has proved that a single individual is very capable of waging cyber war at a level we previously attributed only to intelligence agencies or crime syndicates.

# 7. References

Bentham, J., & Lafleur, L. J. (1948). An introduction to the principles of morals and legislation. New York: Hafner Pub. Co.

Bowne, S. (2011, August 4). Three generations of DoS attacks. *Defcon 2011*. Retrieved from https://media.defcon.org/dc-19/presentations/Bowne/DEFCON-19-Bowne-Three-Generations-of-DoS-Attacks.pdf

Bowne, S. (2011, April 18). Mid-Pacific ICT Center: Why the Jester and Anonymous are Both Wrong. Mid-Pacific ICT Center. Retrieved January 21, 2012, from http://mpictcenter.blogspot.com/2011/04/why-jester-and-anonymous-are-both-wrong.html

Eimiller, L. (2011, September 22). Member of hacking group LulzSec arrested for June 2011 intrusion of Sony Pictures computer systems. Federal Bureau of Investigation. Retrieved from www.fbi.gov/losangeles/press-releases/2011/member-of-hacking-group-lulzsec-arrested-for-june-2011-intrusion-of-sony-pictures-computer-systems

Finkle, J. (2011, December 30). Stratfor Hack: Anonymous-Affiliated Hackers Publish Thousands Of Credit Card Numbers. Breaking News and Opinion on The Huffington Post. Retrieved January 21, 2012, from http://www.huffingtonpost.com/2011/12/30/stratfor-hack-anonymous_n_1176726.html

Freed, A. (2010, March 11). Hacker releases second video of enhanced XerXeS DoS attack on Apache vulnerability. *InfoSec Island*. Retrieved from www.infosecisland.com/blogview/3258-Hacker-Releases-Second-Video-of-Enhanced-XerXeS-DoS-Attack-on-Apache-Vulnerability-.html

Freed, A. (2010, January 27). Hacktivist tactics raise ethical questions. *Infosec Island*. Retrieved from http://www.infosecisland.com/blogview/2695-Hacktivist-Tactics-Raise-Ethical-Questions.html

Freed, A. (2011, March 20). Patriot hacker The Jester's Libyan psyops campaign. *Infosec Island*. Retrieved from http://www.infosecisland.com/blogview/12745-Patriot-Hacker-The-Jesters-Libyan-Psyops-Campaign.html

Greene, R., & Hughes, N. (2010, October 29). "Hacktivist for good" claims WikiLeaks takedown. *CNN U.S.* Retrieved from http://articles.cnn.com/2010-11-29/us/wikileaks.hacker_1_wikileaks-computer-hacker-cyber-attack?_s=PM:US

Grinberg, E. (2010, March 30). Dead Marine's father ordered to pay protesters' legal costs. *CNN U.S.* Retrieved from http://articles.cnn.com/2010-03-30/justice/westboro.baptist.snyder_1_military-funerals-albert-snyder-westboro-baptist-church?_s=PM:CRIME

Hacktivist confirms infecting Anonymous DHN.zip file. (2011, January 19). *Infosec Island*. Retrieved from http://www.infosecisland.com/blogview/11140-Hacktivist-Confirms-Infecting-Anonymous-DHNzip-File.html

Hacktivist maintains attack on Westboro Baptist Church. (2011, April 11). *INFOSEC INDIA*. Retrieved from http://infosecindia.com/2011/04/02/ hacktivist-maintains-attack-on-westboro-baptist-church/

Jeter, C. (2011, December 12). Cyberwarfare Roshambo: th3j35t3r Profiled - SC Magazine. IT Security News and Security Product Reviews - SC Magazine. Retrieved January 21, 2012, from http://www.scmagazine.com/cyberwarfare-roshambo-th3j35t3r-profiled/article/194123/

Kruzel, J. (2010, February 4). Defense.gov news article: Cybersecurity seizes more attention, budget dollars. US Department of Defense. Retrieved from http://www.defense.gov/news/newsarticle.aspx?id=57871

LulzSec attacks CIA web site, taunts The Jester. (2011, June 16). *InfoSec Island*. Retrieved from http://infosecisland.com/blogview/14496-LulzSec-Attacks-CIA-Website-Taunts-The-Jester.html

McCullagh, D. (2009, December 17). U.S. was warned of predator drone hacking. *CBS News*. Retrieved from http://www.cbsnews.com/8301-504383_162-5988978-504383.html.

Nominations for the pwnie awards. (2011, July 20). pwnies.com. Retrieved from http://pwnies.com/nominations/

Post-shipwreck LulzSec is cornered by FBI and hackers—Leader Sabu outed. (2011, June 29). *IBTimes New York*. Retrieved from http://newyork.ibtimes.com/articles/171674/20110629/lulzsec-leader-sabu-identity-anonymous-antisec-disband-topiary-outed.htm

Raviv. (2010, October 20). R-U-Dead-Yet. *HybridSec.* Retrieved from http://hybridsec.com/tools/rudy/

RSnake. (2010, December 1). Slowloris HTTP DoS. ha.ckers.org web application security lab. Retrieved from http://ha.ckers.org/slowloris/

Special Forces Mission. (2012, January 10). Special forces groups—Green Berets. Retrieved from http://www.groups.sfahq.com/command/mission.htm

Th3J35t3r [The Jester]. (2010, January 1). Jester's court: Official blog of Th3j35t3r. Retrieved from http://th3j35t3r.wordpress.com/

Th3J35t3r [The Jester]. (2010, December 30). Message to #anonOOPS « . Jester's court. Retrieved from http://th3j35t3r.wordpress.com/2010/12/30/message-to-anonoops/

U.S. Special Operations Command. (2012, January 10). GlobalSecurity.org—Reliable security information. Retrieved from http://www.globalsecurity.org/military/agency/dod/socom.htm

Vance, A. (2010, December 4). WikiLeaks struggles to keep a step ahead of hackers. *New York Times.com*. Retrieved from http://www.nytimes.com/2010/12/04/world/europe/04domain.html

Vinograd, C. (2011, June 22). Ryan Cleary, suspected teen LulzSec hacker, charged with cybercrimes in U.K. *The Huffington Post*. Retrieved from http://www.

huffingtonpost.com/2011/06/22/ ryan-cleary-lulzsec-hacker-charged-cybercrime-uk_n_882453.html

Who is th3j35t3r? « T3h H3r0d07u5 R3p0r7. (2010, December 17). *T3h H3r0d07u5 R3p0r7*. Retrieved from http://h3r0d07u5.wordpress.com/2010/12/17/who-is-th3j35t3r/

# A1. Appendix A1: Jester's Targets

| | |
|---|---|
| 4chan.org | www.cablegatesearch.net |
| jixad.tk | www.einladungzumparadies.de |
| muslimsagainstcrusades.com | www.falojaa.net |
| www.3bwat.info | www.fatwa1.com |
| www.absba.org | www.godhatesfags.com |
| www.abu-qatada.com | www.h-alali.net |
| www.al-amanh.net | www.hizb-america.org |
| www.al-islam.com | www.iaisite-eng.org |
| www.albasrah.net | www.ikhwan.net |
| www.alboraq.info | www.imamtv.com |
| www.alboraqforum.info | www.islam-ucoii.it |
| www.albukhari.com | www.islamicawakening.com |
| www.alemara1.com | www.islamicboard.com |
| www.alemarah-iea.net | www.islamicemirate.com |
| www.alemarah.co.tv | www.itaqulaah.com |
| www.alemarah.info | www.jihadunspun.com |
| www.alfaloja.net | www.kalamullah.com |
| www.alfidaa.info | www.kavkaz.org.uk |
| www.alghurabaa.org | www.lulzsecurity.com |
| www.aljahad.com | www.majahden.com |
| www.almadad1.com | www.mmagreb.com |
| www.almaghrib.org | www.modawanati.com |
| www.almaqdese.net | www.mojahden.net |
| www.almedad.com | www.mtj.tw |
| www.almedad.net | www.muslimdefenseforce.islamicink.com |
| www.almoslim.net | www.muslimsagainstcrusades.com |
| www.alqimmah.net | www.muslm.net |
| www.alqoqaz.net | www.rjfront.info |
| www.altartosi.com | www.sawtaljihad.org |
| www.annabaa.org | www.shahamat-english.com |
| www.anonyops.com | www.sharia4belgium.webs.com |
| www.ansar1.info | www.talabeyes.com |
| www.ansarullah.co.cc | www.tawhed.net |
| www.aqsatv.ps | www.tawhed.ws |
| www.as-ansar.com | www.tawheedmedia.com |
| www.at-tawbah.net | www.theunjustmedia.com |
| www.atahadi.com | www.way2allah.com |
| www.baghdadsniper.net | www.wikileaks.org |

# A2. Appendix A2: Jester's WBC Release

GODHATESFAGS.COM - Tango down 1 Month and counting. (THAT'S 4 WEEKS)

Also all of the Westboro Baptist Church secondary domains (listed below) - Also their 3rd party hosted blog hosted at:

http://blogs.sparenot.com/index.php/godsmacks - TANGO DOWN

That's one whole month WBC???? I thought you guys were just rebooting? Also why did ya remove all ya websites from your official letterhead:

http://twitter.com/#!/th3j35t3r/status/48508992082808833

Americaisdoomed.com - TANGO DOWN
priestsrapeboys.com - TANGO DOWN
godhatesireland.com - TANGO DOWN
godhatesmexico.com - TANGO DOWN
godhatescanada.com - TANGO DOWN
Godhatesfags.com - TANGO DOWN
sparenot.com - TANGO DOWN
thebeastobama.com - TANGO DOWN
yourpastorisawhore.com - TANGO DOWN
godhatestheworld.com - TANGO DOWN
godhatessweden.com - TANGO DOWN
Jewskilledjesus.com - TANGO DOWN
godistheterrorist.com - TANGO DOWN
godhatesamerica.com - TANGO DOWN
godhatesthemedia.com - TANGO DOWN
signmovies.com - TANGO DOWN
signmovies.net - TANGO DOWN
fredthemovie.com - TANGO DOWN
hatemongers.com - TANGO DOWN

stay frosty

th3j35t3r

There's an unequal amount of good and bad in most things. Trick is to figure out the ratio and act accordingly.

http://twitter.com/th3j35t3r
http://th3j35t3r.wordpress.com

Last Updated: May 22nd, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| **SANSFIRE 2017** | **Washington, DC** | **Jul 22, 2017 - Jul 29, 2017** | **Live Event** |
| **SANS Network Security 2017** | **Las Vegas, NV** | **Sep 10, 2017 - Sep 17, 2017** | **Live Event** |