‘Invisible’ Hacker Enemy attacks FBI Affiliate

by Kismo *Saturday, Jun 4 2011, 11:28pm*
international / mass media / commentary

> Hackers and hacker groups are as invisible as they are amorphous, which highlights the ABSURDITY of the Pentagon approach, which is to declare CONVENTIONAL war on an INVISIBLE digital ENEMY -- military morons on parade for the public!

Goldman Sachs CEO, squinting

For the past THREE DECADES elite hackers have been able to launch completely anonymous or invisible attacks on any target they select. Methods and tools for disguising the source and launching attacks are freely available on most security sites as proof of concept listings today, though elite groups have no need of such rudimentary tools.

The invisibility factor is therefore a ‘known’ by military and other American moron regulators, so what is the REALITY behind the LIE or ruse of declaring conventional (ineffective) WAR on phantoms?

The obvious answer is dumbfuck US regulators could easily launch a ‘kiddie’ attack from spoofed addresses or millions of 'zombies' and then accuse ANYONE they wish for the attack – logs are only text files which are therefore open to complete or partial fabrication! The point is NO ONE on the PLANET would be able to establish in a court of law, beyond reason doubt, the source of any DIGITAL attack TODAY! BUT as is apparent in the Hague and local courts, the legal system is now thoroughly corrupt (legalised torture) and under the control of shadowy but KNOWN traditional criminal Banking/Financial elites – the same vile criminals that have instigated all the wars raging in the world today.

American State Institutions – principally the Pentagon and White House -- continue to advertise the fact that the US lags behind competing nations, groups and individuals in the digital arena. The absurd threat of launching a missile at suspected hackers will no doubt go down in history as one of the most stupid and thoroughly idiotic statements made by any high official anywhere; in this case it is clear the moron should have been put out to pasture years ago!

In any event, ‘hacker groups,’ or the US military pretending to be hackers, are now openly threatening attacks and DECLARING/indentifying their targets openly before the attack – a completely out of character situation and behaviour in elite hacking circles! What is the IGNORANT

public to think?

It is also widely known that elite hackers are a ‘breed;’ a fiercely independent, anarchic, anti-conventional, freedom-loving, maverick, genus that DETESTS the LYING, MASS MURDERING, vile Banking scum that (temporarily) exercise influence over the western world with their poisonous mass media spewing dis/misinformation venom daily.

Hackers for decades have been inside ‘the machine’ gathering data and highly sensitive information on the criminal scum that have been EXPLOITING the masses for centuries – THEY KNOW THE UGLY TRUTH or REALITY behind the LIES! It is only natural they should FIGHT the EVIL forces that reign needless death and destruction on the world – forces that are concentrated in the UK, USA and Western Europe.

Indeed, a digital war has been raging against these nefarious (State) forces for decades and I would inform the public -- perhaps for the first time -- that elite hackers are prevailing in this 'war.'

Largely unknown to the public are the billions of dollars lost to hackers by the ‘secure’ banks, an almost comical situation, as ‘kiddie’ hackers are able to compromise Bank security these days.

More important than financial hacking, which is nevertheless a means of UNLIMITED INCOME for hackers -- are the intrusions into sensitive data and military systems, of which American imbeciles are COMPLETELY UNAWARE -- an expert of equal or superior skill is required to even detect such intrusions. And as is well known and advertised today the Pentagon and other State regulatory organisations LACK skilled operators in this field.

The reality today is quite clear, it is not Hollywood created ‘Bin Laden terrorists’ or other phantasms manufactured by the powers to dupe the public into submission and compliance; it is the REAL FORCE of elite hackers that form the vanguard in the fight for REAL Freedom. Elite hackers unquestionably fight the most EFFICIENT and effective war against the criminal Banking and Financial forces that have hijacked Western Democracies today.

These traditional criminal forces are sweating blood even as I write, as they are acutely aware their end is certain – they have failed to appreciate that a new breed of digital warrior would inevitably overtake/vanquish them – perhaps they were too busy polluting and killing for profit to notice!

Fin.

[we extend our profound appreciation to the master, ‘ferrite,’ one of the first uber hackers – ur work and patience was not wasted; be comforted by the fact that the ‘man’ is on his knees.]

A final note to the Pentagon (the military arm of Corporatism): you are first required to detect or LOCATE an 'enemy' or target; then you are faced with the daunting task of engaging a known but amorphous opponent which is impervious to conventional warfare!

The only missiles you are launching against this perceived ‘enemy’ are missiles of gross STUPIDITY and INCOMPETENCE, you imbecilic brutes!

Make what you will from the following article (propaganda) from Digital Trends:

> **LulzSec hacks FBI affiliate, Infragard**

by Andrew Couts

After hacks on PBS.org and SonyPictures.com, hacker group LulzSec has a new target: The FBI.

Hacker group Lulz Security (aka LulzSec) is on a war path. Following their highly public hacks of the PBS website and SonyPictures.com, LulzSec has now set its sights on the top law enforcement agency in the United State: The Federal Bureau of Investigations.

In a press release posted to anonymous message board PasteBin.com, the group announced that it hacked the website of the Atlanta chapter of Infragard, a non-profit that serves as a partnership between the FBI and private business, which the American Civil Liberties Union describes as "a corporate TIPS program, turning private-sector corporations...into surrogate eyes and ears for the FBI." LulzSec also uploaded Infragard Atlanta's user database to the Internet. The group says that the attack was launched in retaliation for NATO and the Pentagon officially declaring hacking an act of war.

"It has come to our unfortunate attention that NATO and our good friend Barrack Osama-Llama 24th-century Obama have recently upped the stakes with regard to hacking. They now treat hacking as an act of war. So, we just hacked an FBI affiliated website (Infragard, specifically the Atlanta chapter) and leaked its user base," wrote LulzSec. "...Most [Infragard members] reuse their passwords in other places, which is heavily frowned upon in the FBI/Infragard handbook and generally everywhere else too."

With the user login info at its disposal, LulzSec explains that it then hacked the private Gmail account of one Karim Hijazi, a "whitehat" hacker who owns data security firm Unveillance. LulzSec hacked Unveillance, too, and "briefly took over, among other things, their servers and their botnet control panel," LulzSec writes.

"After doing so, we contacted Karim and told him what we did. After a few discussions, he offered to pay us to eliminate his competitors through illegal hacking means in return for our silence. Karim, a member of an FBI-related website, was willing to give us money and inside info in order to destroy his opponents in the whitehat world," writes LulzSec. "We even discussed plans for him to give us insider botnet information."

This exchange has, in some ways, been confirmed by Hijazi, who posted a statement about the breach and his contact with LulzSec members on the Unveillance website. One glaring difference between the opposing accounts of their discussions remains, however: While LulzSec claims Hijazi tried to pay them to "destroy his opponents," Hijazi says he was simply extorted by LulzSec.

"Over the last two weeks, my company, Unveillance, has been the target of a sophisticated group of hackers now identified as 'LulzSec," writes Hijazi. "During this two week period, I was personally contacted by several members of this group who made threats against me and my company to try to obtain money as well as to force me into revealing sensitive data about my botnet intelligence that would have put many other businesses, government agencies and individuals at risk of massive Distributed Denial of Service (DDoS) attacks.

"In spite of these threats, I refused to pay off LulzSec or to supply them with access to this sensitive botnet information. Had we agreed to provide this data to them, LulzSec

would have been able to grow the size and scope of their DDoS attack and fraud capabilities."

Hijazi also posted a chat log between himself and two members of LulzSec, identified in the chat as "Ninetales" and "hamster_nipples." The back-and-forth explicitly shows Ninetales mention the word "extortion," and shows the pair's attempts to be paid for their "silence."

"While I do get great enjoyment from obliterating whitehats from cyberspace, I can save this pleasure for other targets," writes LulzSec's Ninetails. "Let's just simplify: you have lots of money, we want more money."

LulzSec says they were simply trying to "stringing [Hijazi] along to further expose the corruption of whitehats."

Regardless of who's telling the truth, it would seem that LulzSec's war has only just begun, so stay tuned.

http://www.digitaltrends.com/computing/lulzsec-hacks-fbi-affiliate-infragard/
