

CAC INTELLIGENCE, LLC



[Iranian Cyber Army]

09 January 2010

[Disclaimer: This document is the property of CAC Intelligence, LLC and is intended for the specified audience only. It is not intended for redistribution.]



Introduction to the Iranian Cyber Army

In December 2009 Twitter users were shocked to find the Iranian flag and a warning message from the Iranian Cyber Army (ICA) in place of their usual sign-in page. Within minutes, the now-famous hack became a loud introduction to a previously unknown group of hackers, and the ICA became a shadowy new power among Iranian hacker groups.

Overall Threat Assessment

Although the ICA is not very technically savvy, it does command some brute force capabilities and enjoys popularity among a young Iranian generation and tacit support from the Iranian regime, both of which are rife with anti-western sentiment. The group's lack of technical knowledge is balanced out by their boldness and unique position of government support that allows them to hack major high-traffic targets with few repercussions. As its cyber attack capabilities and skills improve, however, it will become easier for the ICA to find vulnerable systems to exploit, with only time standing between the ICA and another high-profile attack on a major western target.

Background

Despite a veil of anonymity afforded by the Internet, some information is known about the ICA. It is an underground criminal organization that focuses on defacing websites, and the group as a whole is far more organized than the typical hacker group, which is often a loose coalition of attackers with similar goals and interests.

ICA members regularly post on one of Iran's most popular hacker forums, run by the Ashiyane Digital Security Team. The leader of Ashiyane, who goes by "Behrooz_ICE," is a man named Behrooz Kamalian, a young and motivated idealist leading a business under the name of Ashiyane Digital Security. It provides web hosting services, dedicated servers, network penetration testing, and other cyber security solutions. What is unique about Ashiyane is that it does not hide the fact that it conducts criminal activity online. The website defacement database Zone-h indicates that the group has hacked at least 21,000 websites.

According to Iftach Ian Amit, an Israeli Air Force cyber expert, the ICA are active posters on the Ashiyane forums site, meaning they are at the very least part of Ashiyane's criminal network. A close look at Kamalian and Ashiyane as a whole reveals that ICA attacks use very similar methodology as Ashiyane attacks, in terms of targeting and execution. Their close ties in terms of types of attack and interests, as well as their confirmed constant contact, suggest that Ashiyane and the ICA are very likely to collaborate on attacks and may even share some members.



Ashiyane also claims to have ties to the Iranian government, which is likely true. The Iranian government has actively sought to increase its cyber attack capabilities, as well as its popular support. Allying with a group such as Ashiyane would meet both of these objectives. Furthermore, the government has yet to deny ties to Ashiyane or counter the group's openness about such relations. The ICA is not only staunchly pro-regime but also has close ties to Ashiyane and is possibly even a part of it, suggesting that it is likely also tied to the Iranian government. Some experts have even suggested that the government helps coordinate the ICA's attacks, partly because of the timing of the attack on Twitter. It occurred on the same day that the Iranians seized an Iraqi oil well along the border. As a result of the cyber attack, the other event went relatively unnoticed.

Given the regime's propensity to crack down heavily on illegal activities, the ICA appears to enjoy a degree of immunity and is, at the very least, a state-sponsored hacking group whose payment is in the form of special treatment by the state. The ICA is allowed to operate with impunity as long as it only attacks foreign enemies.

Iranian officials have also hinted that the ICA's relationship with the regime is even stronger than merely sponsorship. In particular, an Iranian military commander, Ebrahim Jabbari, suggested that the Iranian regime had been successful in establishing a cyber army. After this, Commander Javani, head of the Revolutionary Guards political bureau, claimed that the ICA aims to "prevent the destruction of Iran's cultural and social system" and seemed to imply that it may even be an integral part of the Iranian military. The commander claimed that while Iran's enemies seek to weaken the state through "cyber activities," the ICA has "powerfully entered this arena to prevent any damage to the cultural-social infrastructure of the country." This implicit admission of collaboration between the ICA and military suggests that Iran does indeed have very close ties with the ICA.

Demographics

It is suspicious that prior to the 2009 Twitter attack, no one had heard of a group called the Iranian Cyber Army, and it is therefore possible that the ICA is simply a cover for hackers of various criminal underground gangs coming together to conduct major attacks under a unified name. This would also fall in line with Ashiyane's methodology, as it frequently conducts "capture the flag" games wherein it chooses a website or organization to attack and commands its horde of criminal hacker followers to attack that organization. The ICA could be a cover for their high-stakes "capture the flag" targets. It should be noted here that the ICA's membership remains highly secretive, and any statements about membership are necessarily speculative.



Targets

Whereas many hacker groups are opportunistic, with individuals hacking any website they can and posting personalized messages, the ICA selects a single target to be the focus of the entire group and propagates a unified political message. Media sources and online databases indicate that the ICA's targeting is politically motivated. The group has hacked various websites, including:

- Iranian opposition websites of the "Green Movement"
- Farsil Satellite Radio, accused by Iranian officials of being a western plot to turn Iran against its regime
- Other news and media sites that are critical of the regime
- Major high-traffic sites such as Twitter and the Chinese search engine Baidu

Forum postings from the ICA indicate that they have moved on from merely hacking websites and have begun to build a botnet, which they could use for cyber espionage and distributed denial-of-service (DDoS) or "flood" attacks. A botnet would also provide them with mass amounts of bandwidth and computing power for operations such as brute-force or "password guessing" attacks.

Some estimates indicate that the ICA's botnet includes at least 400,000 compromised machines, and as many as a few million. Botnet sizes are often exaggerated but it is likely that the ICA has - or will soon have - control of a considerably large botnet, as this has become commonplace among those whose goal is to disrupt websites. As such, they could become a dangerous force in cyberspace and could possibly take down medium to large-sized sites through DDoS attacks.

Moreover, the attacks that the ICA is currently capable of could, with some minor upgrades, become full-scale cyber attacks. In particular, the redirection of hundreds of thousands of Internet users, as was the case in the Twitter attack, could easily be used to build a more extensive botnet. If the page to which the ICA directed Twitter users had served malicious code, for example one that exploited a weakness in web browsers to automatically drop a Trojan on the user's PC to make it part of a botnet, they could build an army of infected zombie computers in a matter of minutes.

Furthermore, they could drop additional malware on the infected computers that could be used to better spy on the user. As Twitter users are from a diverse set of age groups and professional experience, this could easily be used for cyber espionage purposes.



Modus Operandi

When the ICA hacked the Twitter website, they displayed an image of the Iranian flag, along with a message that read:

"U.S.A. Think They Controlling And Managing Internet By Their Access, But They Don't, We Control And Manage Internet By Our Power, So Do Not Try To Stimulation Iranian Peoples To....

NOW WHICH COUNTRY IN EMBARGO LIST? IRAN? USA?

WE PUSH THEM IN EMBARGO LIST

Take Care."

The text that showed up when doing a Google search for Twitter was (translation): *"In the name of God, As an Iranian this is a reaction to Twitter's interference sly which was U.S. authorities ordered in the internal affairs of my country..."*

The initial text about stimulating the Iranian people is a clear reference to the use of Twitter by anti-regime activists during the 2009 Iranian election. Twitter was used as a means for staging and organizing online and physical protests during and after the election. Though the exact nature of the accusation in the Google search for Twitter is unclear, the ICA is claiming that the US had a hand in deliberately propagating the use of Twitter by anti-regime activists.

While westerners may find the ICA's messages almost comical, with their poor English grammar and dramatic threats, younger generation of anti-western Iranians see such attacks as a way to strike back at the enemy from the comfort and safety of one's personal computer. This phenomenon, along with the fact that Iran is focusing on building its cyber power, will likely result in Iran growing from an up-and-coming cyber power to a major cyber power, with the ICA acting as a catalyst for the development of young Iranian hackers, providing an outlet for anti-western sentiments and a place for them to strike back at their enemy with little consequence.

Its current capabilities, however, are relatively limited. The ICA boasts the Twitter attack and a similar attack against the widely-used Chinese search engine Baidu as its major achievements. In the underground hacker community, however, website defacement is generally considered a low-level attack that does not afford much credibility.

Furthermore, upon a closer analysis of the Twitter attack, it becomes apparent that it was not highly sophisticated. No custom exploitation methods, or complex programming was required for the attack, and in





fact, the ICA did not even truly break into the Twitter administrative interface. Rather, the attack merely used valid administrative credentials for Twitter's main domain name system (DNS) server. In reality, Twitter was not broken into at all, only the Twitter DNS. As such, the hack was far less dangerous and complex than originally assumed and did not result in compromise of any sensitive user information. Even with control of a botnet and the ability to deface websites, therefore, the ICA appears relatively limited in its technical capabilities.

The ICA's repertoire of attacks includes: building a botnet and conducting DDoS attacks; direct attacks on some smaller/medium-sized websites using technical exploitation; and attacks on larger websites using social engineering. While none of these require a great deal of technical skill, the ICA has shown the ability to use low-level, minor attacks on strategic targets that generate mass media attention and cause fear of loss of personal data among the general public.

Perhaps the ICA's greatest strength is that it is based in and supported by Iran. This affords the group both domestic and international impunity, as Iran is highly unlikely to allow any foreign investigation into the ICA's activities. The ICA's unique position to commit highly visible transnational crimes without having to leave its home country makes it a unique and dangerous enemy. Furthermore, the Iranian regime is likely to increase its support for the ICA in response to US and UK efforts to build up their cyber attack capabilities. The regime may even subsume these hacker groups and offer them official training and explicit permission to run operations in cyberspace, thus turning the ICA into the actual Iranian cyber army.