Visit: http://cms1.gre.ac.uk/research/csafe

School of Computing & Mathematical Sciences
UNIVERSITY of GREENWICH

November 15, 2012 Issue #3

This issue:

CSAFE Short Courses

- Computer Forensic Evidence and the Law (Legal Aspects)
- Computer Forensics for Lawyers
- EnCase Computer Forensics 1 and 2 Certification (EnCE©)
- Introduction to Computer Forensics
- Penetration Testing and Vulnerability Assessment

Who's Anonymous these days?

By Ryan Heartfield, CSAFE Contributing Writer

Just exactly who are the Anonymous hackers?

The question is very difficult to answer of course, which leaves no coincidence as to why the "loose" group have named themselves so. Starting in 2008, this elusive collective have been regularly associated with collaborative Hacktivism on an international scale, with online protests and retaliatory operations against anti-digital piracy campaigns by the motion picture and industry trade associations. Many of these attributions have been founded by individuals claiming Anonymous hand in these attacks.

Whilst Anonymous describe them as freedom fights of the internet, likening to a kind of digital Robin Hood, others have personified Anonymous as a group anarchic cyber guerrillas. Regardless the question remains as to who the people behind this group really are. Anonymous describe themselves as follows:

Anonymous is not an organisation, or a group of people. It most certainly is not a group of hackers. Anonymous is an online living consciousness compromised of different individuals with at times coinciding ideals and goals. Anonymous is decentralized and as such is free.

It would be fair to assume that from this statement, that Anonymous may not be a single entity as such, but rather a group of separate entities - enclaves even working together when the need for a common goal must be achieved.

A person known only as "Commander X" provides interview and videos for Anonymous and therefore can be considered to be a spokesman of sorts. In 2011 he was involved in an investigation into Anonymous by Aaron Barr - who claimed to have identified this man as a San Francisco gardener...not your average hacker! Commander X was said to call himself a "peon", and not a leader of the group as Aaron Barr suspected.

However he did claim to be a skilled hacker and a founding member of an allied organisation - Peoples Liberation Front whom are a collection of hacktivists. PLF have acted with AnonOps, which are another sub-group of Anonymous who carry out denial of service attacks against government websites. Interestingly Commander X likened the relation with the PLF and Anonymous as that between NATO members where a member could opt out of specific projects or operations.

Hacktivism or Terrorism?

So now we have a vague idea of how Anonymous are organised, from the mouth of one of their own in “Commander X”. Therefore should Anonymous be a collection of many sub groups with a common goal, it can be assumed that their motivations are somewhat relevant to the group leading the current “project”. Which raises the question: can the actions of Anonymous be considered a collaborative community or rather a clever umbrella for those who wish to divert attention from their own groups’ real profile and intentions? We are made to believe that those whom contribute to Anonymous activity are fighting for the freedom of the internet and so Anonymous can be any number of supporters willing to join in order to complete a goal or mission. However let us consider a scenario where this true, yet at the same time, hardcore hackers groups are sitting behind this smokescreen to exhibit data theft and serious organised crime over the internet. With recent high profile attacks such as those on SOCA, Mastercard, Visa and Paypal it is would seem that there is a far more sinister motivation, more so than the community label that has been used as a propaganda mechanism for impressionable hacker wannabes - especially when we look at the evident relation between attacks and Wikileaks to maintain release of secret government cables...

SOFTWARE

“RAPPORT”

RAPPORT is an internet web browser plugin that secures your browser session against malware and phishing attacks. This is achieved by preventing attacks such as Man-in-the-Browser and Man-in-the-Middle. It secures credentials and personal information by locking down communication between the browser and selected web server when activated.

It is able to block malware installations and remove existing infections; providing in particular secure communication with financial websites whom have a backend server instance of RAPPORT. RAPPORT is free to download and install and does not affect browser performance at all. For more information please visit:

www.trusteer.com

ISCIS 2012 Paris - On the Feasibility of Automated Semantic Attacks in the Cloud

Ryan Heartfield, alumni of the University of Greenwich, presenting at The 27th International Symposium on Computer and Information Sciences in Paris. The paper presented is an investigation into automating semantic attacks (a special form of social engineering) with the Cloud.

To read this paper click on the icon below:

About the Author

This month's author:

Ryan Heartfield

Ryan is an alumni of the University of Greenwich and founding writer of CSAFE e-publication.

Anatomy of a DDOS Attack (Distributed Denial of Service)

By Ryan Heartfield, CSAFE Contributing Writer

Distributed Denial of Service is seemingly the weapon of choice for many cyber criminals... but what makes this attack so difficult to defend?

Typically a denial of service attack consists of a vast number of web requests (generally genuine HTTP, ICMP) to a specific web server, originating from a collection of nodes. These nodes generate so much traffic that either the web server becomes extremely slow in operation or it crashes completely because the server is overloaded with requests. This type of attack is very old and can be prevented by either filtering the offending nodes or slowing down incoming traffic. However each node is static and must initiate the denial of service attack individually.

Distributed Denial of Service is somewhat more sophisticated and coincidently more difficult to prevent or protect against. DDOS implements the use of a network of compromised computers called zombie which are contacted and controlled by a master computer whom the attacker is instructing the zombies via. The attacker directs his botnet of compromised machines to contact a server or website repeatedly thus generating enormous amounts of traffic that either slow the web server down or again crash it completely.

This causes the issue where the compromised hosts (yours and mine computers), of which there may be thousands, would initially appear to be producing legitimate requests to the victim web server.

Again we can try to use filtering and statistical analysis techniques to profile traffic requests in order to locate attackers and drop traffic from the source.

However there are also methods to execute DDOS by using uncompromised hosts. This is done through the use of "Reflectors", a method in which the attacker uses his botnet to contact a host of innocent computers, where the message appears to originate from the victim web server. In this scenario the legitimate hosts respond to the message but send the response to the victim as it appears to have originated from that server.

Looking at this type of DDOS it is clear that from the perspective of the victim web server it appears that the reflectors attacked the system. Also from the reflectors perspective it appears that the victimised system requests the packets. Ultimately the zombie computers remain hidden from the victim and the attacker becomes more or less untraceable.

Members of Anonymous are known to use a software application that acts as a network stress package called LOIC (Low Orbit Ion Cannon). This application is used to execute DDOS attacks against targets - however it can be likened to a "voluntary botnet" as it incorporates a "Hive Mind" feature which allows the user to relinquish control of the LOIC application to the operator of an IRC channel and thus setup a DDOS as that described in the previous two scenarios through willing participants.

Fig.1 Typical DDOS Scenario