Global Information Assurance Certification Paper

Herbless - A Hachtivist Retires

Richard Grant

January 19, 2001

While European hackers cannot be stereotyped anymore than other groups, there are some traits that are common among them. Generally they have a need to bring public attention to some cause, but they also have a more practical goal. Often it is to improve their own careers or to increase their incomes. European hackers also more often have training in the computer sciences and therefore, unlike American counter-parts they tend to write their own code. They are more serious about their craft than American hackers; it is not just fun and games. Herbless, who is from the United Kingdom, is typical of the European school. He was first noticed at the beginning of August 2000. His very successful career ended about two months later with a self-proclamation of retirement. This paper will examine his exploits, method of attack, what is known about him personally, and finally, why he quit at the height of his career.

Herbless is a **Hacktivist**; someone who hacks computer systems websites to bring before the public deeply felt opinions on some issue. Generally a hacktivist does not wish to bring a target system down, he wishes only to leave a message of protest on the defaced sites. The sites are often chosen because of their relationship to the subject of the protest and may also just be targets of opportunity. Many issues are political and more often targets are government sites. Hachtivists should not be confused with cyber-terrorists. The goal of cyber-terrorists is to disrupt services and destroy data, often sites hacked are those of countries other than their own.

Herbless surfaced in August 2000. The sites Herbless defaced in early August were www.powellproperty.co.uk [12] on August 01, 2000 and then www.applied-tech.co.uk [3] on August 03, 2000. It appears that they have no relationship to the protest message. The messages left on the Powell Properties site was pretty typical, a little bravado and profanity sprinkled in the messages protesting fuel costs in the United Kingdom. Powell Properties appears to be a target of opportunity. The message Herbless left on the Powell Properties page indicated that this was not the first site hacked by Herbless. The message left on the website of Applied Technology Systems protested the government monitoring of cell phones conversations in the UK. The legitimate Applied Technology Systems web page includes the line "Applied Technology Systems offers you real peace of mind and service that is second to none", an irony that did not go unnoticed by Herbless. His message included "Hmm, maybe that statement was a bit ambitious guys. A bit of an exaggeration no?"[3] The Applied Technologies hack must have been particularly embarrassing to the company since they are in the information technology business.

Herbless then turned his attention to UK government sites and posted anti-smoking messages on the defaced websites he hacked. In this campaign Herbless hacked nine "gov.uk" websites in mid-August of 2000. The defaced web pages were later restored without much difficulty, in part due to his care in not damaging more than required. It is somewhat interesting that in a later communication Herbless apologized for hacking the government sites. Herbless, in his messages, said he wanted the government to wakeup to the dangers of smoking and do

something about the issue. He accused the government of only worrying about the tax revenues from smoking. The sites attacked included the Adult Learning Inspectorate, five local government councils, two charitable agencies and the Village of Binfield, Berkshire. It appears that the Binfield site was still under development; it had not yet been registered with Ukerna, the authority in the United Kingdom that registers Internet names that end with gov.uk and ac.uk.

Herbless struck again on September 11, 2000; this time he hit the website of www.legoland.co.uk and then several more sites within the next couple of days. This time protesting the fact that the Motion Picture Association of America was taking legal action against a young Scandinavian that created a program that decoded and allowed copying of DVD movies. Herbless, as part of his defacement, left copies of the DVD decoder program on some of the Legoland servers. [5] On the legoland.co.uk website Herbless also posted a picture of the Millennium Falcon from Star Wars (not the space shuttle as had been reported). This can be seen on Attrition.org's website [9], that has a large archive of hacked web pages mirrored there. Our hacktivist friend also left a copy of his code, a copy of the program for decoding DVDs and his email address on the defaced page. Then he left instructions for the administrative personal of the site on how to repair it!

Herbless changed his protest on September 13, 2000 to focus on the fuel price crisis in the United Kingdom. [4] The fuel price protest that had been started by truckers in the UK stirred Herbless to action. On September 14, 2000 he is credited with 168 sites hacked. The Security consulting firm MIS Corporate Defense Solutions confirmed on September 19, 2000 that the total number of sites hacked during this fuel protest reached 450 sites. The messages left at these defaced sites included comments indicating that 72 percent of the fuel cost in the United Kingdom is tax, and that fuel production costs in the UK are among the cheapest in Europe. [7] He encouraged others to join the protest in any way they could, as long as they did not resort to violence. He also requested any hacks for the cause to be 'non-abusive'. The use of the term non-abusive is an interesting one; Herbless considers the defacing of websites to be non-abusive! His message continued, "If you live near a picket line, go and give your support. Applaud the lorry drivers. Make cups of tea and sandwiches for the picketers. Write your MP pledging your support".[11] A visit to the MIS Corporate Defense Solutions website (www.MIS-cds.com) did not reveal any information about the sites hacked and the list of sites hacked was no longer available. The sites hacked in this attack all appeared to be commercial sites in the UK.

The last known exploit in his career was his hack of the Hong Kong and Shanghai Banking Corp. and three of its subsidiaries on September 20, 2000. HSBC was previously known as Midland Bank and is one of the largest banking institutions in the UK. The sites hacked were www.hsbc.co.uk, the UK site, www.hsbc.es, the Spanish site, www.hsbc.gr, the Greek site and www.bach.co.uk, which is the British Arab Commercial Bank. HSBC quickly announced that these were informational websites and in no way related to their on-line banking system. HSBC also said that it appeared that no data was harmed and that HSBC was careful in restoring the hacked sites to be sure that everything was returned to the same configuration as before the defacement. Herbless, in an email to vnunet.com, made the point of saying that no data was altered in this hack, nor did he even look at any data. The banking system took a lot of heat for not fixing this vulnerability before they were defaced since Herbless' previous exploits were well

publicized. HSBC responded to the criticism saying the sites defaced were managed by a service provider and not by their own in-house technical people. These same in-house personnel were, by the way, responsible for the HSBC Internet banking system. The defacement on these sites included his standard political messages as well as a picture of the British Prime Minister saying "Trust Herbless he talks sense" [8].

The methods initially used by Herbless to hack into targeted sites are still in question. An early claim by Herbless was that he exploited a weakness in Windows NT that was previously unknown. Later he claimed to exploit vulnerability in Microsoft's SQL Server. He also claimed that the code he used was original and his own, although both of these points were at the time disputed by industry experts. He documented his claim on the www.ali.gov.uk defaced website. He usually left instructions to the administrators of the websites he hacked on how to restore them and to fix the weakness he exploited. Herbless left another hint on the www.bobbybrowns defaced web page, he said," Learn how to change passwords. Hint SQL Server doesn't just do SQL".[14]. From this information it is apparent that at that time he was exploiting the default (null) password embedded within the installed SQL Server.

Microsoft representative Nicholas McGrath blamed the administrators of the hacked sites for not changing the default SQL password; thus leaving the sites vulnerable. McGrath implied that the administrators had not read the SQL manuals and this sentiment was echoed by Herbless on some of the defaced web pages. There is also a possibility that the SQL could have been embedded within another software package and the administrators would not have been aware of the passwords at all. Microsoft in the installation for SQL Server does not prompt the installer to set a new password as they do in other product installations.

A tool that Herbless used was the LinSQL.c program utility. The LinSQL.c program is an all-in-one utility; using a built-in port scanner, the user finds hosts with SQL using its standard TCP port of 1443 and the "sa" account with the null password. The password option is configurable to accommodate other weak passwords. The program then logs into the target system and through the command line interface gains access to SQL databases and has the ability to upload files.

There is a default graphics database in SQL that Herbless used to upload his graffiti pages. Then he would rename the existing page; often an index page, and replace it with the one he had stored in the database. This is apparently how he was able to deface 450 websites in the September 14, 2000 timeframe. A document called explain.txt, which can be found on the Attrition.org site [18] was penned by Herbless and explains how he exploits SQL and the "sa" administrative account that by default has a null password. It also appears that the "sa" account has better than administrative access to the server; it actually has system level authority.

The explain.txt document is a good study of a hacker learning how to exploit a weakness he has found. Herbless discusses the development of LinSQL.c and the problems he encountered during the development. This document unveils the development of a hacker as he crafts his tool for exploitation and the problems he encounters in the process. This has been downloaded from the Packetstorm website almost 40,000 times by January 2001.[16] The explain.txt file is

compelling evidence to support his claim that LinSQL.c is all original code and his creation.

The identity of Herbless may never be known since he has retired with anominity. Herbless has been called a hactivist because unlike an activist he did not stay with one cause. He seemed to follow whatever issue stirred him at that time. The hacktivist role may be one he used to gain public support and to legitimize his activities. The issues also made good press.

It is also apparent that Herbless was interested in publicity and his image. He communicated several times with online news and information services such as Vnunet.com. It appears that he was more than willing to reply to Email interviews.

The LinSQL.c program appears to be well written and documented. This implies that, as with most European hackers, Herbless is well schooled in computer science. Herbless commented in one of his email interviews that he did not fit the Hollywood stereotype of a hacker. In 'techie' circles, was word that he was a relatively normal type of person who had several years of experience working in the Information Technologies community. It was implied that he was a professional who was not working during his hacking period. As the hacks continued, Herbless also showed a progression: he improved his program, he dropped the profanities, he used better grammar, his graphics became more sophisticated and he even became humorous (as in the picture of the Prime Minister Tony Blair saying "Listen to Herbless he knows what he says" left on the HSBC sites).

Finally, in the end, we do not know the age or even the sex of this individual. Herbless suddenly ended his black-hat career in October of 2000. He had gotten his protest messages before the public and he did achieve a fair amount of notoriety. In one communiqué, Herbless commented that he had received 180 emails from people and said, "I must be getting the word out".

His willingness to talk to the media probably reflects several motives. First, he wanted to become known; and second he did not want to have a negative image. He was careful to condemn malicious hackers and 'script kiddies' to distance himself from the dark side of the hacking craft. He also let it be known that he felt compelled to expose poor security practices and was helping companies better secure their networks, again showing that he was not a bad person and skilled with computer systems. While he did invade target systems he was always careful to note that he never altered or misappropriated data on the sites he hacked. He tried to down play illegal activities and dress them with some respectability. All of this is evidence that his goals went beyond what his political messages implied. Russ Cooper the developer of NTBugtrap said, "That in Europe it is all about getting a better job and building your career" [17]. In statements about his retirement from hacking Herbless said that he hoped to land some paid work [17]. He has indicated that he already helped some companies fix their web servers.

Herbless, as evidence seems to indicate, wants to become an ethical hacker. Ethical hackers are those who work for the owners of computer systems as security experts. It is their jobs to hack computer systems to test and improve the security of those systems. They are also known as "White Hats". He has gone to great efforts to let everyone know that he knows the

difference between right and wrong. Herbless' exploits prove that he possesses good knowledge of corporate computer systems. Why did he quit? Perhaps Herbless was concerned that the authorities were focusing in on him. Hacking in Europe is a very serious activity. Both European governments and organized crime have been known to try to promote their goals by pressuring European hackers to use their hacking skills for those ends. Perhaps some of these factors have encouraged Herbless to retire while he had his health and his freedom. While the name Herbless may never appear on another defaced web page it does not guarantee that the person may not continue hacking under another alias. A hacker's past black hat activities makes it difficult for companies to trust them with the security of their computer systems.

Sources

[1]Gold, Steve. "Anti-Smoking Hacker Stubs Out UK Govt. Sites".8/16/00. URL: www.infowar.com/hacker/00/hack_081600b_j.html (8/16/00)
[2]Lynch, Ian. "Hacker attacks UK government websites". 8/17/00. URL: www.vnunet.com/NEWS/1109018 (12/29/2001)
[3] URL:www.attrition.org/mirror/attrition/2000/08/03/www.applied-tech.co.uk/index.htm
[4] Lynch, Ian. "Herbless – five weeks of hacktivism". 9/21/2000.
URL: www.vnunet.com/NEWS/1111249 (12/22/2000)
[5] Knight, Will. "Cheesed off cracker strikes again". 9/12/2000.
URL: www.zdnet.co.uk/news/2000/36/ns-17841.html (12/22/2000)
[6]Evans, Dave. "How harmless is Herbless?". 10/02/2000.
URL: vnunet.com/Analysis/1111951(12/22/2000)
[7]Gold, Steve; Newsbytes. "UK Anti-smoking Protester Hacks Over 100 Web Sites".
9/15/2000. URL: www.infowar.com/hack_091500a_j.shtml (12/22/2000)
[8] Ticehurst, Jo. "HSBC internet sites hacked".9/20/2000.
URL: www.vnunet.com/NEWS/1111217 (1/02/20001)
[9] URL: www.attrition.org/mirror/attrition/2000/09/10/www.legoland.co.uk;
[10]Ananova. "Bank criticised after hacker breaches website".9/20/2000
URL: www.ananova.com/news/story/sm_64694.html (12/22/2000)
[11]Lynch,Ian. "Fuel protestor hacks 168 websites".9/15/2000.
URL: www.vnunet.com/NEWS/1110938 (1/02/2001)
[12] URL:www.attrition.org/mirror/attrition/2000/08/01/www.powellproperty.co.uk
[13] Network News. "Herbless hacker turns government security to ashes". 9/27/2000.
URL:www.vnunet.com/NEWS/1111667 (12/22/2000)
[14] www.attrition.org/mirror/attrition/2000/09/15/www.bobbybrowns.co.uk
[15]Sullivan, Bob; MSNBC. "High-stakes hacking, Euro-style". 10/23/2000.
URL:www.msnbc.com/news/479105.asp (12/22/2000)
[16] "LinSQL-MS-SQL Server checkup tool". 8/16/2000.
URL:www.securiteam.com/tools/LinSQL_-_MS-SQL_Server_checkup_tool.html (1/08/01)
[17]"Herbless the Hacker goes legitimate". 11/21/2000.
URL:uk.news.yahoo.com/001121/15/apm2f.html (12/22/2000)
[18] Herbless. "The attack method:". 9/10/2000. URL:
www.attrition.org/mirror/attrition/2000/09/10/www.legoland.co.uk/explain.txt (1/08/01)

[19] Anderiesz, Mike; Daily Telegraph. “UK: It Takes A hacker To Catch One”. 12/10/2000. URL: www.infowar.com/hacker/00/hack_101300a_j.shtml (12/22/2000)