Global Information Assurance Certification Paper

Which Hat Is DilDog Wearing?

Ryan Shaw

April 2, 2000

In the world of hacking, there has long been a separation between good and bad intentioned hackers. Good, or white hat hackers are described as hackers "who, upon discovering a vulnerability in a computer system, alerts the system vendor to the Problem" (McFedries). A bad, or black hat hacker is labeled as one "who exploit system security breaches for nefarious ends" (McFedries). The advent of security hacking groups such as L0pht and the Nomad Mobile Research Centre have stirred a new debate regarding a third group: gray hat hackers. These individuals are defined as those "who supply information about a security issue both to the vendor and to crackers" (McFedries). It is the purpose of this paper to examine the case of one hacker in particular, DilDog, and determine where he fits into the hacker spectrum. DilDog is a member of L0pht and the Cult of the Dead Cow, two groups who are very high profile in the security and hacking communities. Based upon DilDog's history in these organizations, I pose the question: which hat is he wearing?

L0pht Heavy Industries, www.l0pht.com, was founded in 1992. Since that time, L0pht has made many newsworthy contributions to the security field including: L0phtCrack (a Windows password cracking utility), AntiSniff (a proactive security monitoring tool), and SLINT (a source code security analyzer). L0pht's policy on announcing their findings is well summarized on the soap box page of their website. "Vulnerability information is extremely valuable both to attackers and customers. Companies and organizations that release this information openly and as soon as possible are doing the security community a service. Those who choose to use the information for their own purposes first put customers at risk" (L0pht Trends). Based upon these guidelines, L0pht has made numerous vulnerabilities known throughout the technology industry as soon as they were discovered and validated. The publication of the exploit, instead of taking advantage of its use, qualifies L0pht as gray hat hackers. DilDog has been a member since 1998, although he did submit an advisory as a non-member in 1997. Since he joined, he has co-authored L0phtcrack 2.5 and AntiSniff and posted six security vulnerability advisories. These include:

Date	Application	OS	Vulnerability
11/10/97	MS IE 4.0	Win 95	Viewing remote HTML content can execute arbitrary native code
01/14/98	MS IE 4.0	Win 95/NT	Viewing remote HTML content can execute arbitrary native code
02/18/99	MS NT 4.0	Win NT	Any local user can gain administrator privileges and/or take full control over the system
01/04/00	userhelper and PAM	RedHat 6.x	A local user can gain root access
01/08/00	LPD	RedHat 4.x, 5.x, 6.x	A remote user can execute arbitrary code
03/06/00	Office 2000	Win 95, 98, NT, 2000	Viewing file executes arbitrary code

The Cult of the Dead Cow (cDc), www.cultdeadcow, was formed in 1984. The cDc currently has 23 members, which has included DilDog since August 1998. The cDc's web site boasts:

> …but have we ever disrupted communications on two continents by moving telecommunications satellites? Mhm. Hacked computing resources belonging to the three-letter agencies and the Pentagon? Yep. Electronically altered environmental controls in local malls? Done that. But unlike other hacker groups you've undoubtedly read about, we've never been caught (cDc Who).

The cDc site is littered with statements of this nature. The cDc manages to redefine the word arrogance; arrogance that is the trademark of black hat hackers. They make no attempt to hide their efforts to break into well-known computer networks. Their most popular applications are Back Orifice and Back Orifice 2000. Back Orifice was written by Sir Dystic and released in 1998. The original version was able to control Windows 95 and 98 based machines. It was upon this foundation that DilDog began work on Back Orifice 2000 (BO2K). BO2K was released on July 10, 1999 at DEFCON in Las Vegas. The features of the new release include: "runs under Windows NT, as well as Windows 95/98, utilizes strong cryptography to ensure secure network administration, has extended plugin architecture to allow for greatest flexibility, and is completely open-source and made freely available under the GNU Public License" (DilDog FAQ). The release of Back Orifice 2000 caused tremendous concern throughout the technology industry, as it made remote administration of computers by hackers much easier. In addition to his development of BO2K, DilDog wrote, The Tao of Windows Buffer Overflow. In this HTML based tutorial, DilDog explains how to find and exploit Windows buffer overflow vulnerabilities.

So which hat is DilDog wearing? While the textbook definition would lead you to label him a gray hat, a closer examination of his intent will prove otherwise. DilDog has long harbored bad feelings towards industry giant Microsoft. Not only is this grudge apparent in his professional work, it was evident during his years at the Massachusetts Institute of Technology. While in college, DilDog announced a vulnerability in Microsoft's Internet Explorer v3.01a. As with numerous of his more recent security hole findings, DilDog did not provide advanced warning to the software developer. Instead, the media and newsgroup readers were the first to find out. In an interview with CMP Media, when asked how well Microsoft responded to the problem, DilDog responds, "They have not yet been informed of the bug. I suppose as soon as the media jumps on it, and on Microsoft, they might actually get SERIOUS about fixing the gaping problems with Internet Explorer. (which from a developer's point-of-view, I can't see how the hell they didn't expect this to happen!)" (CMP Media). In one instance, George Roettger of www.nthelp.com made the following accusation regarding DilDog's February 18, 1999 release of the KnownDLL's hack:

> I'd also like to point out that MS had the cure for this posted to the same maillist that dildog posted to within hours, so it's pretty obvious that dildog never even took the time to notify Microsoft before posting the exploit. This isn't exactly ethical behavior on the security mailing lists where it's customary to notify the vendor at least a week before posting to give them time to patch the systems. It was also posted on a friday, no doubt to force programmers to work the weekend. Come on dildog, I respect L0pht, don't give them a bad name (Roettger).

The release of Back Orifice 2000 is another example of DilDog's failure to provide the standard week of advance notice to the vendor. The fanfare with which BO2K was released only drew more attention to DilDog and the cDc's blatant attempts to make Microsoft look bad. In his work and in his words, DilDog makes no attempt to hide his contempt for Microsoft. The FAQ for Back Orifice 2000 explains why:

> 2. Who wrote BO2K? Why was it written?
>
> BO2K was written by DilDog of the Cult of the Dead Cow. Many of the commands that BO2K comes with were directly ported from Sir Dystic's original Back Orifice source code. It was written with a two-fold purpose: To enhance the Windows operating system's remote administration capability and to point out that Windows was not designed with security in mind (Dildog FAQ).

While many agree with this statement, most choose a more positive route of making change. Numerous technology workers have used flaws in Microsoft's operating systems (OS) to justify switching personal and corporate desktops and servers to Linux. This switch is slowly causing Microsoft to lose their stranglehold on the OS market. All of these factors demonstrate the "nefarious ends" DilDog is out to achieve. While the implied goal is improved security, DilDog's actions speak clearly about his primary intention, the embarrassment and weakening of Microsoft. Maybe DilDog's future work will include the removal of his vindictive black hat and a movement towards white or gray hat hacking. It is important to note that DilDog's findings have caused Microsoft and others to correct significant security lapses in their software and networks. Put to use in a positive manner, DilDog's talent could help provide a secure OS we could all benefit from.

Works Cited

CMP Media Interview. URL: http://www.cmpnet.com (6 April 2000).
Complete URL withheld for privacy concerns.

Cult of the Dead Cow (cDc). Who are we? Cult of the Dead Cow Homepage. March 2000. URL: http://www.cultdeadcow.com (30 March 2000).

Cult of the Dead Cow (cDc). cDc Homepage. March 2000. URL: http://www.cultdeadcow.com (30 March 2000).

DilDog. Advisories. L0pht Homepage. 6 March 2000. URL: http://www.l0pht.com/advisories.html (2 April 2000).

DilDog. Back Orifice 2000 Homepage. 8 October 1999. URL: http://www.bo2k.com (2 April 2000).

DilDog. FAQ for Back Orifice 2000. Back Orifice 2000 Homepage. 8 October 1999. URL: http://www.bo2k.com/indexnews.html (2 April 2000).

L0pht Heavy Industries, Inc. L0pht Homepage. 24 March 2000. URL: http://www.l0pht.com (2 April 2000).

L0pht Heavy Industries, Inc. Trends In 'Press Release' Security Advisories. L0pht Homepage 10 May 1999. URL: http://www.l0pht.com/~oblivion/soapbox/index.html (2 April 2000).

McFedries, Paul. W Listings. The Word Spy. 4 October 1999. URL: http://www.logophilia.com/WordSpy/w.html (2 April 2000).

Penenberg, Adam L. Defcon Live! Forbes.com. 16 July 1999. URL: http://www.forbes.com/tool/html/99/jul/0716/feat2.htm (6 April 2000).

Roettger, George. Known DLL Hack. NT Help. February 1999. URL: http://www.nthelp.com/40/knowndll.htm (2 April 2000).