
# 'MICROSOFT W

Mar 7, 2018

By Dennis Fisher

Share

*As the L0pht began to coalesce and become more well-known in the security community, the dynamics of the group evolved, too. The loft space in Boston's South End became a hangout and meeting spot for local hackers, and as some of the members flourished, others began to pull back from the group. At the same time, new members were brought into the L0pht, including Mudge (Peiter Zatko) and Dildog (Christien Rioux), who would collaborate on the team's seminal L0phtCrack tool, bringing an entirely new level of notoriety and attention to the L0pht. Software vendors, government agencies, and other hackers sat up and took notice. The ground began to shift under their feet.*

*(Read Part 1, Part 3, and Part 4.)*

**(Read Part 1, Part 3, and Part 4.)**

**Silicosis:** There's two different sides of the L0pht. You have the stuff that Brian was working on, Space Rogue, Kingpin. Then there was a security advisory piece that was coming out. It was different. That was definitely a change in the L0pht.

**Kingpin:** Brian and Count Zero were in one part of the original L0pht space in the South End, and Brian and John's girlfriends at the time were in the other half. So once I got arrested is when I started hanging out with them more, and then ultimately joined the L0pht later that same year. And it was amazing because my parents, instead of saying, "No computers, no nothing," they knew that that hacker culture was my life. So they couldn't take that away, or they didn't. And when I joined the L0pht, my parents started paying rent for me. It was $50 a month or something like that, and they were paying the rent. So they were supporting this positive endeavor, which was amazing.

**Weld Pond:** It was about a year into the L0pht starting as a physical space. It had already been set up. When I got there, there was already four or five guys, like Space Rogue and Count Zero and Brian were already there, and Kingpin was already there. Kingpin, probably because he didn't have a lot of money, was like, "I'll split my desk rent with Chris. We'll share the spot."

**White Knight:** We enjoyed being part of the blossoming hacker community but also the broader aesthetic that was wrapping itself around the hacker scene. We would have folks over all the time to hang out.

**Mudge:** White Knight was in the L0pht, so he invited me over to the L0pht, which had just formed and wasn't an actual organization per se. And Count Zero was there. I met him. I liked him. He had published a few articles. So I hung out with them for a little while. And White Knight was just really cool. He said, "Why don't you become a member of the L0pht?" Everybody paid to rent their little local space. And I was like, "Cool." So I shared a space with, I think, White Knight. I had my old NeXTcube there because I was interested in hacking that.

**Katie Moussouris:** One of the things that I remember talking to them about later was that when they invited members of the government to come and look, and members of law enforcement to come and look at what they had assembled, that actually changed the threat model for these organizations. Because they pretty much figured there was an economic barrier to most attackers uncovering security holes. And once they realized that no, actually people can just dumpster dive for the stuff that they can't afford, or they wouldn't have access to and do research on it and find vulnerabilities, they suddenly were like oh, revised! We have revised our threat model now, and it was because of a visit to the L0pht to look at what they had assembled there.

## We have revised our threat model now, and it was because of a visit to the L0pht.

Written by Mudge and adapted for Windows by Weld Pond, L0phtCrack became the go-to password-cracking tool for administrators and a major revenue source for the L0pht.

**Space Rogue:** Count Zero was there all the time. I was there as much as I could be. Brian was there a lot because Count Zero and Brian lived around the corner. I remember Kingpin would come by, usually on the weekends or after school because he was still in high school at the time. But his parents liked it too because it kept him out of trouble.

**Kingpin:** Those were formative years, and I feel like the other guys, I think they were maybe out of their formative years. I feel like they were just much more grounded at that point, and much more responsible, and balanced, and Count Zero had a job at Mass General. Brian Oblivion was at CompUSA. But the L0pht really was that center for me. I was still a punk kid.

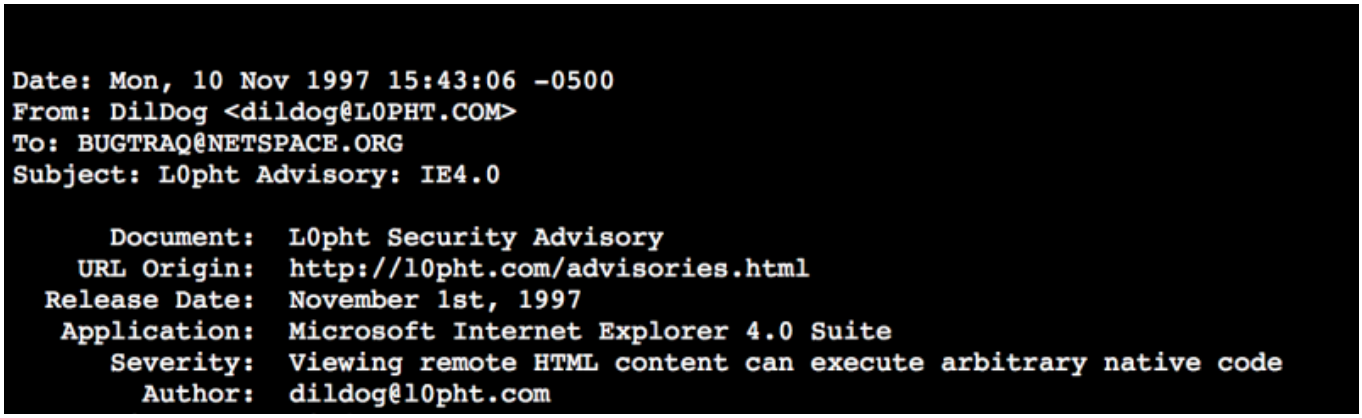
**Mudge:** I saw a lot of potential, and I started writing a few quasi-advisories and some other sorts of things. And I was like, "Well, this is kind of silly. We have a lot of potential here,"

primarily in that we all like each other and that we're all interested in similar things. And my goal all my life has just been to make a difference, so somehow have some positive impact. That's where the motto for the L0pht of make a dent in the universe came from. And the first thing of doing that is to find like-minded folks and get that movement going. It's really difficult to do it on your own.

**Weld Pond:** Dildog had a buffer overflow in IE4, which was really bad to have that in a browser, where someone could click on a link and then you owned their machine, right? He published it with proof of concept. We did a proof of concept where people could click on our site and it would just lock up their CPU. It was an easy way of showing, demonstrating it without we're not actually exploiting anything. We're just showing we can run instructions on your CPU. He published the exploit right in the advisory. This was a full disclosure thing.

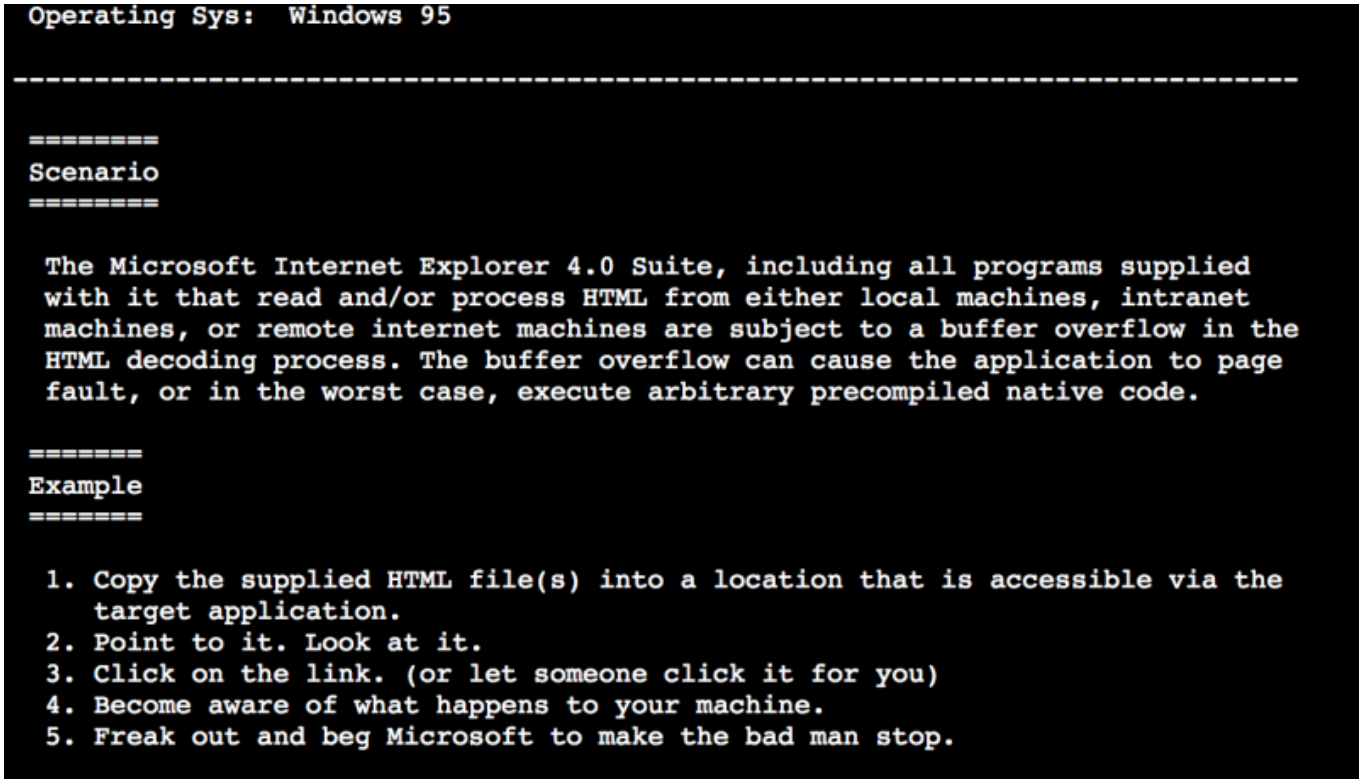
**Dildog (Christien Rioux):** I kind of got into the culture of security, but my first IT/network job was administrator for my fraternity, which at MIT was actually a bigger responsibility than you'd imagine. Yeah, it was only 50 people, but we were allocated entire class B of address space because MIT owned all of the /18 class A at the time. I could make whole class C's appear and disappear at will, which gave me a lot of flexibility in terms of just routing whatever I wanted on the Internet. My grades started to suffer around my junior year because I was spending more and more time with the hacking and security stuff I had taken on the Dildog moniker at that point. It was starting to publish things on Bugtraq about Internet Explorer and Windows hacking. I had written the first buffer overflow exploit for Windows.

## Microsoft was freaking out about it.



```
Date: Mon, 10 Nov 1997 15:43:06 -0500
From: DilDog <dildog@L0PHT.COM>
To: BUGTRAQ@NETSPACE.ORG
Subject: L0pht Advisory: IE4.0

      Document:  L0pht Security Advisory
    URL Origin:  http://l0pht.com/advisories.html
  Release Date:  November 1st, 1997
   Application:  Microsoft Internet Explorer 4.0 Suite
      Severity:  Viewing remote HTML content can execute arbitrary native code
        Author:  dildog@l0pht.com
```



```
Operating Sys:  Windows 95

------------------------------------------------------------------------------

 ========
 Scenario
 ========

  The Microsoft Internet Explorer 4.0 Suite, including all programs supplied
  with it that read and/or process HTML from either local machines, intranet
  machines, or remote internet machines are subject to a buffer overflow in the
  HTML decoding process. The buffer overflow can cause the application to page
  fault, or in the worst case, execute arbitrary precompiled native code.

 =======
 Example
 =======

  1. Copy the supplied HTML file(s) into a location that is accessible via the
     target application.
  2. Point to it. Look at it.
  3. Click on the link. (or let someone click it for you)
  4. Become aware of what happens to your machine.
  5. Freak out and beg Microsoft to make the bad man stop.
```

The original advisory for Dildog's buffer overflow in Internet Explorer 4.

**Weld Pond:** Microsoft was freaking out about it. Eventually we got an email from Microsoft that said, "Hey guys, you know what? If you send us this information before you publish it, we'll fix it, and we'll put out a patch. Then you can publish it." We're like, "Maybe that's not a bad idea." This was the first time, it was actually which we call it now coordinated disclosure, where both the finder, the bug and the company were both working towards knowing when a fix was out.

**Silicosis:** I think we were responsible for that. We did not just kind of blow out proof of concepts or advisories. We would always work with the vendor and make sure they actually had a patch, and we'd coordinate the release. That made us different. Half the L0pht worked at BBN at one point or another. It was fascinating. We'd find all these vulnerabilities, because we were responsible for security at BBN. I mean, these were the guys that built the internet back in the '60s and '70s. We were constantly taking software from vendors, breaking it apart, finding vulnerabilities, and trying to get the vendors to actually fix the issues that we found. Early on, they wouldn't do anything.

**Dildog:** I was a big proponent of full disclosure. That attracted the L0pht's attention and I ended up meeting with them at 2600 and 2621, which is our drinking and hanging out sharing exploits

up meeting with them at 2600 and 2021, which is our drinking and hanging out sharing exploits kind of thing, knitting circle for hackers. We hung out at that point and I got to know Brian Oblivion and Mudge and Weld and all those guys. Kingpin. They had heard of me through Bugtraq and I had brought a few exploits with me to share. We just hung out and talked and we started up a friendship at that point and invited me over to the L0pht to hang out. Later they caught on to the idea that maybe I could help with L0phtCrack.

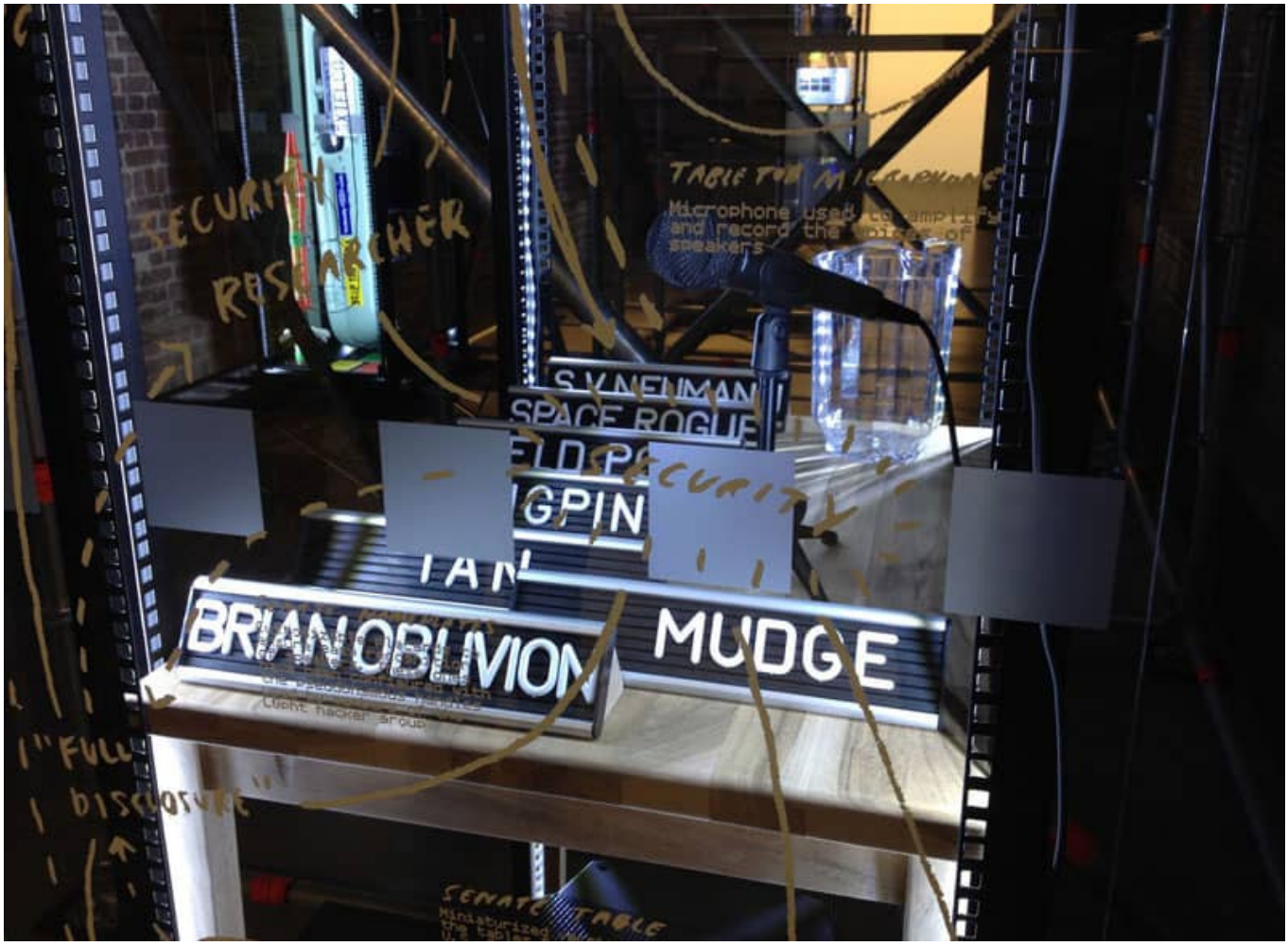
**Weld Pond**: L0phtCrack really kind of put us on Microsoft's radar.

**Mudge**: I was working at BBN Technologies, the company that actually under a DARPA contract invented TCP/IP and the Internet. And they were just starting to introduce Windows systems into their environment. It was still mostly Solaris SunOS boxes for the most part. I knew how to audit and I knew how to control and I knew how to configure and harden and monitor the Unix boxes because I'd been a Unix admin for some time at that point, but the Windows one, I'm like, "I don't know how to do this. I don't even know how to test whether the passwords are strong. I wrote it at BBN, just kind of over one night. I remember I had the flu because I remember I was just downing cough syrup. So I just stayed up for like 24 hours and wrote it, which there's a whole bunch of nuances in it which are kind of funny that people didn't understand. I brought it in, and BBN didn't want ownership of it or anything, and I was like, "Great."

**Dildog**: Mudge had written L0phtCrack 1 and Weld had written L0phtCrack 2, which had a Windows GUI, but it wasn't selling very well. They were trying to commercialize it, so they were like, "You're a software developer, not just a hacker. You actually write Windows code all day. Want to help with L0phtCrack and make a new version and help us make it better?" I was just like, "Okay." I was a L0pht employee before I was a L0pht member.

**Weld Pond**: It became a tool that administrators could use, but that also meant anyone could use it. It ended up being the tool that you demoed password cracking with, because it was visually interesting. It had a graphical interface, and so a lot of people bought it. It was pretty big.

## L0phtCrack really kind of put us on Microsoft's radar.




L0pht members' placards. (CC By 2.0 license photo by Joe Grand.)

**Mudge:** Nobody cared about it [at first]. So it had been out for a while. We released it from the L0pht. And Weld said, "Hey, I want to try writing some Windows GUI stuff." I said, "Write a GUI for L0phtCrack." So I put the license agreement in place that the source code was free for non-commercial use. I didn't write it as a Windows tool. We were like, "If you make us write Windows code, you're going to have to pay for the pain that we had to go through." So we put in a little timeout and said just a modest, it was like twenty bucks. Don't care what size of company you are. I think the entire Air Force got a license for twenty bucks

**Dildog:** MIT had never done a computer security class. It was just up-and-coming. I sit down in class and the first day, they pop up on the projector my exploit for Windows Internet Explorer. It was coursework for everybody else and myself to study this and to understand what's going on. They didn't know I was in the room because my name was Dildog on the thing and it was

Rioux in the classroom. They just popped this thing up on the screen and holy shit, there's my freakin' exploit right there.

**Mudge:** So I said to them, "Hey, it's really kind of a drain for everybody just to be paying. We have fun, but it seems like there's a lot more that we can do. What if we put together a plan [so] we move into a different place? It would be a little easier to do actual projects. We have some goal of sharing those projects, of making it a cohesive unit to focus on computer security.

**Count Zero:** One thing that happened over time was like some folks were really into making it kind of like focused on computer security, and more kind of a businessy kind of a thing. And at the time, I wasn't interested in that at all. I was purely at the time really focused in terms of my work on the stuff I was doing at Mass General, doing neuroscience research. And I was really into the social side of things.

**Space Rogue:** Basically, we decided that we needed to move the L0pht because there were too many people hanging out there, sleeping on the couch, people who weren't members of the L0pht. We gotta get bigger, we gotta get better. We wanna do something with this, we wanna make it pay for itself. We need a new space. Anyway, we decided we had to say goodbye to Count Zero.


The L0pht space in Watertown.

**Count Zero:** Everything changes and evolves over time, and I remember the way the L0pht was evolving, there was a change. I was very much at the time wanting to be part of this kind of anarchic kind of crazy thing with no clearly defined purpose to it. I was more interested in it as a very loose hacker collective kind of thing. I was just probably not that fun to be around in some times to be honest. And so at some point, it was one of those, "Okay, this ... I'm not going to be part of this anymore." And people at the L0pht were like, "John, you're not really into this kind of stuff that we're trying to do." And so I just parted ways. And the Watertown move, I wasn't part of any of that. And there were more people coming in too, who were very much programmers. Mudge came in.

**Dildog: My first L0pht events and stuff were in Watertown. I went there every day, drank far too much Mountain Dew, wrote L0phtCrack, and eventually got turned on to writing Back Orifice 2000 for Cult of the Dead Cow. I had met the cDc members at New Hack City in Allston back when that was the thing. I really wanted to do a highly optimized open source kind of thing that did the BO2K thing. I figured I could make a bigger deal by hitting Windows NT.**

*Tomorrow: Part 3. Read Part 1 here.*

L0pht