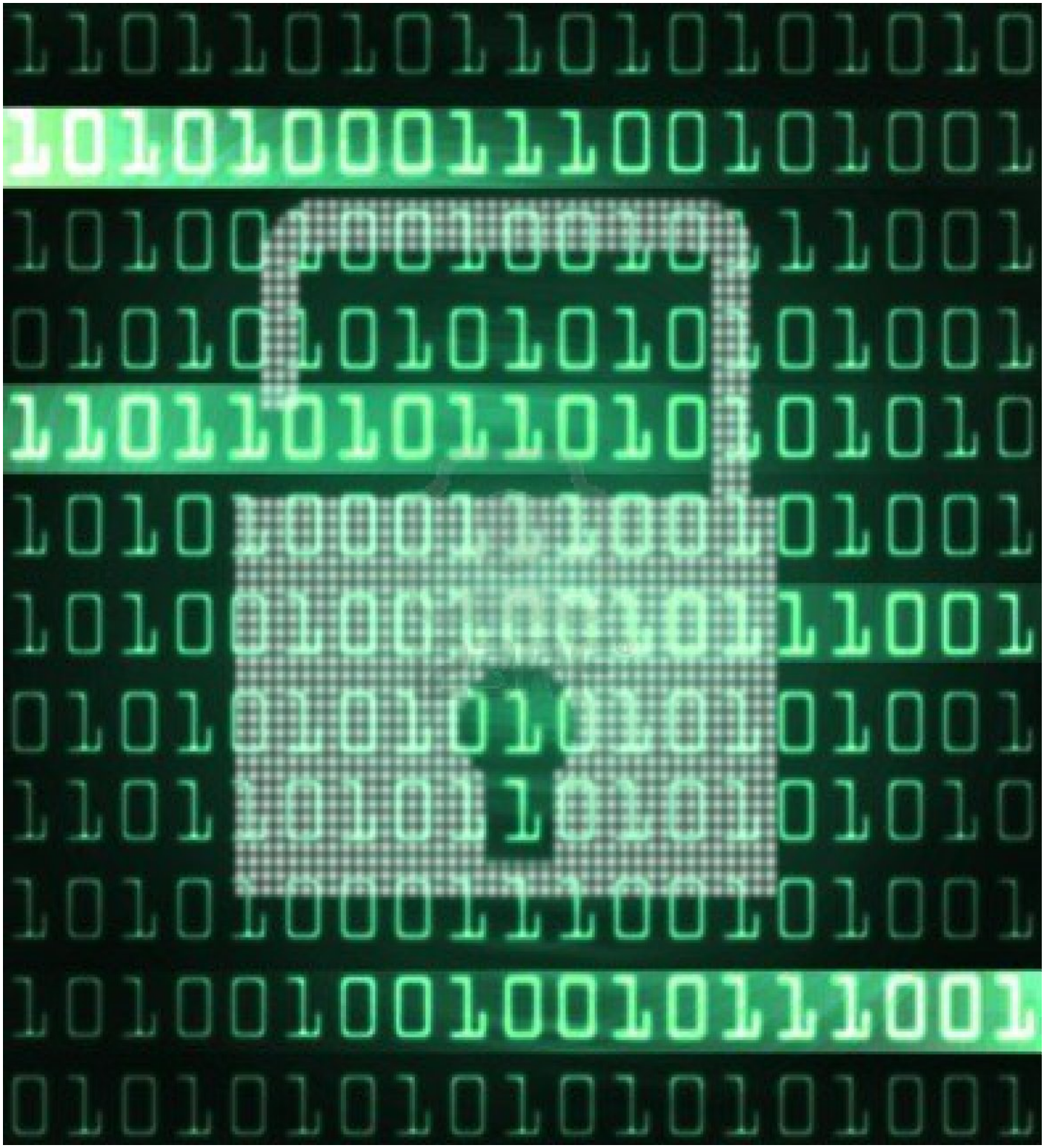
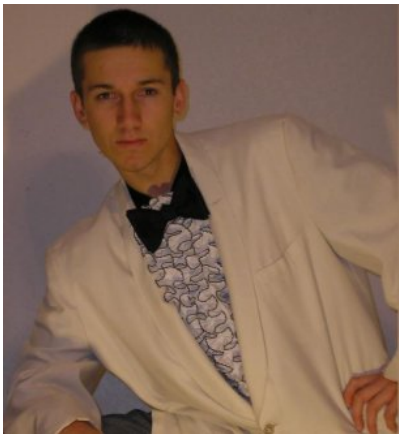


“The quieter you become, the more you are able to hear.”

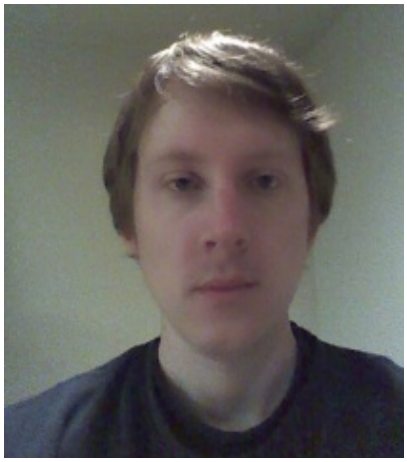
# 010100111001 Security

*Total intrusions since founding: 0*

Simply put, Erich Viebrock is a network security aficionado. He has several published articles in IEEE, as well as Wikipedia. He was the head of network security for google.com, yahoo.com, and facebook.com, all at the same time. Singer and songwriter Shakira, a seasoned hacker, once said, “Erich is just too good. I have no moves to get around him; no matter what method I use to exploit his websites, he has them well-protected. He has also consistently rejected my offers for dinner and a movie.”



Forbes Magazine accurately describes Alex Lemmon in a single word: amazing. He currently works as the top security analyst for the entire country known as the United Kingdom (you may have heard of it). He has a literal bushel full of publications ranging in topics from network security to origami. In his spare time he enjoys beating the Prime Minister in Chinese checkers, sipping mocha lattes, and fighting terrorism in the name of the motherland.



Evan Glick may or may not be a top-notch security analyst and is a strong proponent of maintaining a low profile. He previously (allegedly, of course) worked in the cryptography division at the NSA. In his free time, Evan enjoys hacking weather satellites and has worked diligently in support of the White House petition to build a Death Star.

Adrian Escoto specializes in determining a network's weaknesses by performing ethical hacks. He is often hired by the government agencies to ensure that their networks are secure. For the last 5 years, Adrian has won first place in "The US Cyber Challenge", a national competition to find the best security analysts in the country.

Joshua Butler is a network security analyst who specializes in intrusion detection and prevention. He continues to support numerous companies such as IBM, Cisco, and Google in their on-going efforts to not get owned on a daily basis while continuing lead development on the number one Linux-based penetration arsenal: Backtrack.

**Security Analysis for January 24th:**

The DNS logs indicate that there there is an ongoing, repetitive, attack on a few boxes. The attack sends many DNS queries per second using a spoofed source IP address (the address of the computer the attacks are intended for). Since a DNS request is in the form of a relatively small UDP packet, the sender can initiate many with a very low overhead. The response to a DNS request is substantially larger than the request, allowing few computers to initiate requests and affect many computers. It is safe to assume that the attack is not solely using our DNS servers as a medium, but rather (possibly) dozens or hundreds of other DNS servers as well, (depending on the scale of the attack).

The apparent purpose of this is to create a DoS (Denial-of-service) attack against the supplied IP addresses. Each of the computers with the corresponding addresses will have its resources flooded by the response to thousands of bogus DNS lookups each minute. Figure 1, shows the intended targets of the spoofed IP address and from this graph it can be seen that the primary target was Boingo Wireless, which is based in Southern California. However,

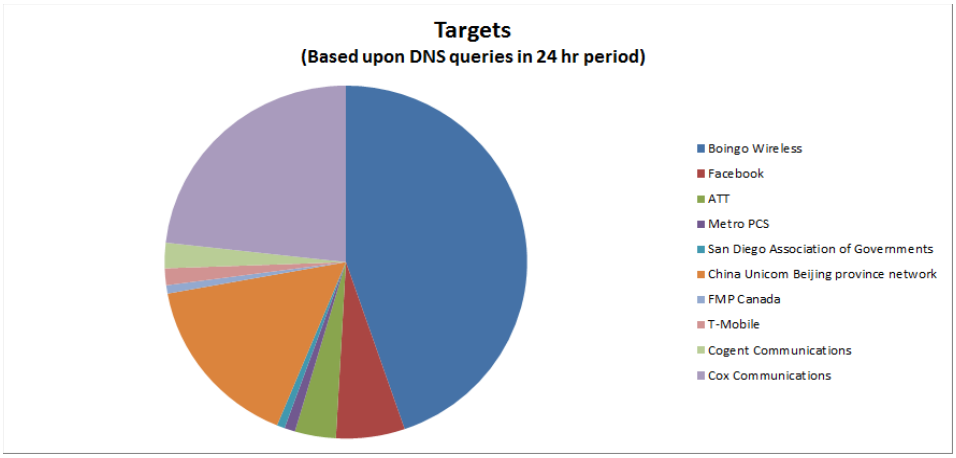



**Figure 1:** Targets from Resolved IP Addresses

rest assured that the attack did not work which is seen in the logs by the 'denied' phrase at the end of each line within the log.

Another interesting find is that there were approximately 84 requested dns zone transfers for the 24 hour period of January 24th which is a rather large amount of requests. This data

suggests that the requests were coming on behalf of Level 3 Communications and requesting the zone transfer from the California Transportation Authority (CalTrans). Although these zone transfers were denied, the reoccurrence of them appears relevant to a simultaneous attempt at yet another Denial of Service (DoS) attack and the possibility of information gathering on the topology of the Caltrans network.

Finally, the server at 149-136.net is not configured properly and is allowing the forwarding of private IP addresses which is not in compliance with RFC 1918. To ensure compliance and to fix the security warning please ensure the firewall automatically drops all packets that come from any of the following private IP addresses and netmasks:

10.0.0.0/8
172.16/12
192.168/16

Regards,

**010100111001**$_{\text{Security}}$
www.leetsecurity.com