Comcast.net DNS Hijacking: What Could Have Happened

Tom Daly, CTO
tom@dyndns.com
What happened?

Two hackers managed to manipulate the DNS name server delegation for comcast.net to a set of alternate servers.
How did this happen?

• Hackers cracked comcast.net e-mail account (Domain Administrative Contact) to obtain a password reset token for NetSol admin portal?
• Hackers social engineered staff at Comcast to get them to give out the credentials.
• Hackers simply logged in with a weak password to NetSol?
• An exploit of security in the NetSol admin portal?
Known Effect on comcast.net
What could have happened?

• [www.comcast.net](http://www.comcast.net) - password harvesting
• Hijack MX records to intercept inbound e-mail.
• Hack other services that use [user@comcast.net](mailto:user@comcast.net) e-mail accounts as a trust token.
• *.hsd.comcast.net wildcard
  (ex: [www.bankofamerica.com.hsd.comcast.net](http://www.bankofamerica.com.hsd.comcast.net))
• Redirect internal comcast.net network management functions to other IP addresses (provisioning, databases, AAA servers), anything that connects via a hostname externally.
Root Problems

• Was WHOIS disclosure part of the login token for NetSol? Did it provide half of the credentials?

Administrative Contact:
Administrator, Domain Registration Contact
domregadmin@COMCAST.net
Comcast Corporation
1500 Market, West Tower
Philadelphia, PA 19102
US
215-320-8774 fax: 215-564-0132

• E-mail addresses are weak trust anchors for online services. What’s a better anchor to identify a user?
What could have stopped this?

• Fully validating DNSSEC resolvers, unable to forge the NS referral key from the .net TLD.

• But what if the hackers provided the TLD a new key?

• A better authorization system for domain name changes – let’s depend on something more than an e-mail address and password.
Thank You

Q & A