Insecurity breeds at home

- Vulnerabilities in SOHO routers

Amrita Center for Cyber Security
Amrita University
Small Office Home Office (SOHO) Routers
Problem at hand

• No technology available to detect/prevent attacks on Cyber Physical Systems

• No mechanism to assure security of basic Internet connection @ home

• Serious risk created by widespread SOHO router pharming
Small Office Home Office (SOHO) Routers

• Basic interface to Internet for home/small office networks

• Less cost, least secure

• Intended for novice users, designed with easy connectivity in mind

• Different vendors, same hardware
DNS Based Phishing

- Website
- Genuine Website
- Malicious Website
- DNS Server
- Home Router
- Malicious DNS Server
- Infected Home Router
- User
DNS Changer Malware

• First Surfaced in 2007, Phishing targeted at financial gain
• Affected 300,000 devices across Europe and Asia
• Redirecting DNS traffic to malicious servers in Estonia, New York and Chicago
• Common malwares involved – TidServ, Alureon, TDSS, TDL4
• Most of these malwares exploit default passwords being used
• Countermeasures undertaken by the US FBI in 2012 under “Operation Ghost Click” confiscating rogue DNS server and shutting them down
• Report by Rob Thomas from Team Cymru suggests presence of new rogue servers and 78% of the traffic to these servers are from INDIA
Methodology

• Monitor DNS traffic at ISP level to identify compromised routers as well as rogue DNS servers
  • Requires permission from ISPs and other authorities
  • Limited information on router level vulnerabilities
• Extract DNS information from vulnerable home routers
  • Running automated scripts to extract DNS settings information from routers online
  • Can collect detailed information on what vulnerabilities are there in each router
• We are not exploiting just extracting ... We value Ethics...
Methodology

Identification

• Scan for devices on the internet with known port (used by SOHO routers) open
• Extract headers and banners to look for signature of SOHO devices

Information Extraction

• Run the rom-0 exploit on the list of identified SOHO router IPs to extract password
• Run exploit script (automated telnet com) on vulnerable routers to extract DNS setting info and MAC address

Data Analysis

• Identify rogue DNS servers and services hosted by related malicious servers
Identification

• Scan devices running RomPager HTTP server (HTTP header will reveal the server)

• Scan the list of RomPager IP for known open ports (making sure it is a SOHO device)
Security of SOHO Routers

• Designed for easy connectivity not security
• Vulnerabilities listed at both firmware level as well as at user interface
• Common Vulnerabilities (44 CVEs listed for ZyXel hardware alone)
  • Rom-0 Vulnerability
  • Cross Site Scripting (XSS)
  • Cross Site Request Forgery (CSRF)
  • Denial of Service (DoS)
Rom-0 Vulnerability

• Attackers can download the backup configuration file (rom-0) without authentication

• Attack URL : http://<ip>/rom-0

• Reverse Engineer Rom-0 file to extract configuration file

• First line of the rom-0 file contains the admin password of the router

• Found in ZyNOS OS running RomPager HTTP server
Rom-0 Vulnerability

Vulnerable Router Models

- ZyXel
- TP-Link
- D-Link
- Micronet
- Tenda
- Binatone
Information Extraction

• Extracting Password
  • Scan the identified router IP list to check for rom-0 vulnerability
  • If vulnerable, download rom-0 file
  • Reverse engineer the file rom-0 file to extract the config file
  • First line of rom-0 file holds the admin password

• Extract DNS settings
  • ZyNOS devices has telnet access from external network
  • An automated telnet script can be used to extract DNS settings and MAC address of the router
-- Host: 122.162.11.85
[+] Testing Vulnerability...
[+] Downloading rom-0...
[-] Extracting Key...
[-] Password is: [redacted]
[-] Done :)
Results & Findings

• What we found …
  • Scanned 11,24,682 Unique IP in the Entire Indian ASN space running HTTP services
  • Identified 9,0733 devices running HTTP service
  • Identified 1,4209 devices with matching SOHO router signature
  • Identified and exploited 4515 routers running vulnerable ZyNOS firmware
  • 17% of routers forward DNS traffic to legitimate DNS servers
  • 556 routers redirects to known malicious DNS servers
Data in Google Maps
Results & Finding

• Why these many vulnerabilities …
  • Lack of security protocols followed during design by low end router manufacturers
  • Lack of Initiative form the part of ISPs
  • Lack of awareness from the part of users
Thank You…