THE INTERNET: CIRCA 1980
THE INTERNET: ~TODAY
<table>
<thead>
<tr>
<th>Time Period</th>
<th>Device</th>
<th>Model</th>
<th>Speed</th>
<th>Ports</th>
<th>Units (Percentage)</th>
<th>Ports (Percentage)</th>
<th>Cabling Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1994-1998</td>
<td>Asante 2072</td>
<td>10 Mb/s Shared</td>
<td>72 ports</td>
<td>17 Units</td>
<td>1,224 Ports</td>
<td>17 Units (0.6%)</td>
<td>Cat3 Cabling</td>
</tr>
<tr>
<td>1998-2000</td>
<td>Asante 5324</td>
<td>10 Mb/s Switched</td>
<td>24 ports</td>
<td>150 Units</td>
<td>3,600 Ports</td>
<td>150 Units (5.6%)</td>
<td>Cat3 Cabling</td>
</tr>
<tr>
<td>2000-2005</td>
<td>Cabletron 2200</td>
<td>100 Mb/s Switched</td>
<td>24 ports</td>
<td>931 Units</td>
<td>22,344 Ports</td>
<td>931 Units (34.8%)</td>
<td>Cat5 Cabling</td>
</tr>
<tr>
<td>2005-2008</td>
<td>Enterasys C2</td>
<td>1 Gb/s Switched</td>
<td>24 ports</td>
<td>224 Units</td>
<td>5,376 Ports</td>
<td>224 Units (8.4%)</td>
<td>Cat5 Cabling</td>
</tr>
<tr>
<td>2008-2010</td>
<td>Cisco 3560E</td>
<td>1 Gb/s Switched</td>
<td>48 ports</td>
<td>773 Units</td>
<td>37,104 Ports</td>
<td>773 Units (29.5%)</td>
<td>Cat6 Cabling</td>
</tr>
<tr>
<td>2010-Present</td>
<td>Cisco 3560X</td>
<td>1 Gb/s Switched</td>
<td>48 ports</td>
<td>583 Units</td>
<td>27,984 Ports</td>
<td>583 Units (11.7%)</td>
<td>Cat6 Cabling</td>
</tr>
</tbody>
</table>

1,332 units & 32,544 ports
Targeted for renewal
THE INTERNET OF EVERYTHING
MIT PHYSICAL INFRASTRUCTURE
TEL/DATA CLOSETS BEING RE-PURPOSED
TEL/DATA CLOSETS CREATIVELY USED IN DORMS
TODAY’S SECURITY LANDSCAPE

Cyber Crime

Hacktivism

Cyber Warfare
ZERO DAY EXPLOITS

(a) Attacks exploiting zero-day vulnerabilities before and after the disclosure (time = \( t_0 \)).
WHAT MIGHT THIS BE?
DDOS ATTACKS
DDoS Attacks

Recent DDoS

Border Traffic and Mitigation Bits for ALL

- In from Internet: 11.5991G
- Total Mitigated: 6.54862G
- Bivie Mitigated: 4.09312M
- Guard Mitigated

Out to Acfs Rtr: 11.5991G
Border Mitigated: 6.54862G
DPro Mitigated: 4.09312M

Graph showing traffic and mitigation bits.
PROTECTING MIT’S EXTERNAL WEB PRESENCE
MIT DOMAIN HIJACK
ATTACK #1 – THE INFRASTRUCTURE

• Routers
  • Target control plane
  • Disabling router disables all downstream resources

• Firewalls
  • Maintain state, which can be exploited
  • Reassemble packets by design
  • Often configured to log permit/deny actions
ATTACK #2 - MIT.EDU

R.I.P Aaron Swartz
Hacked by grand wizard of Lulzsec, Sabu
GOD BLESS AMERICA
DOWN WITH ANONYMOUS
MIT.EDU – THE ATTACK

Domain Name: MIT.EDU

Registrant:
Massachusetts Institute of Technology
Cambridge, MA 02139
UNITED STATES

Administrative Contact:
I got owned
Massachusetts Institute of Technology
MIT Room W92-167, 77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES
(617) 324-1337
cunt@mit.edu

Technical Contact:
OWNED NETWORK OPERATIONS
ROOT
US
DESTROYED, MA 02139-4307
UNITED STATES
(617) 253-1337
owned@mit.edu

Name Servers:
Fred.NS.Cloudflare.COM
Kate.NS.Cloudflare.COM

Domain record activated: 23-May-1985
Domain record last updated: 22-Jan-2013
Domain expires: 31-Jul-2013
MIT.EDU – WHAT HAPPENED
MIT.EDU – WHAT HAPPENED

Maintained by EDUCAUSE
MIT.EDU – WHAT HAPPENED

Maintained by EDUCAUSE
MIT.EDU - WHAT HAPPENED

dmit
From Gizmodo comments:

Hack went down like this:
1. Own the MIT NOC guy with a browser exploit
2. Get their educause logins, which were: [Redacted]
3. Create cloudflare account, set the dns records. (Deface was hosted on a multitude of servers one of them provided by harvard. (All of which are now down, DDoS? I don't know.))
4. Change their mail settings in cloudflare page.
5. At 12:00 EST we logged into the domain control panel and changed the DNS records and the password.

After that mit staff tried uselessly resetting the password but the email ended up on our servers. Eventually educause (the people that manage .edu domains) just locked the domain and took it all down.

Now the interesting part here is that cloudflare staff changed our domain name records in the middle of it all going down (They've previously stated that they wouldn't touch user data without a court order)
Soon after, we decided to troll Gizmodo and the rest of the media into preserving our access. The 'browser exploit' on MIT's NOC (http://gizmodo.com/5978039/hackers-incoherently-deface-entire-mit-website) never existed. We'd never show our full hand at once, we'd just lose access.

MIT certainly believed us though, despite their own reassurances otherwise. For confirmation, they contacted the root registrar for EDU domains (EDUCAUSE) after finally asserting that we got access to their EDUCAUSE account.

EDUCAUSE then made the fatal mistake of overlooking our complete access into the EDU TLD. Though, we can't say we expect much from a registrar running ASPX on their backend.
MIT.EDU – HOW IT HAPPENED

• EDUCAUSE registry was hacked
  • ~7000 .edu domains were vulnerable

EDUCAUSE SECURITY BREACH AND PASSWORD CHANGE INFORMATION

As of 2/19/13

In February 2013, EDUCAUSE discovered a security breach involving an EDUCAUSE server. Below are answers to questions about this breach.

Who was affected and what data was involved?

1. Individuals with an EDUCAUSE website profile
   1. Any information contained in individual EDUCAUSE website profiles (e.g., name, title, e-mail address, username, and hashed password) may have been compromised. As a result, individuals with an EDUCAUSE website profile must change their password.
   2. It is not necessary for InCommon account holders to update their institutional credentials because EDUCAUSE does not have access to, or store on any server, InCommon account information.

2. .edu domain accounts
   1. The breach may have compromised the hashed passwords of .edu domain holders. As a result, the designated administrative, technical, or billing contact must change the domain password. Administrative and technical contacts have already been notified by EDUCAUSE.

As a precaution, all passwords have already been deactivated; therefore, individuals do not need to create new passwords immediately.

Members and individuals who do not have an EDUCAUSE website profile or are not a .edu domain holder are not required to take action.
FUTURE SECURITY LANDSCAPE
QUESTIONS?