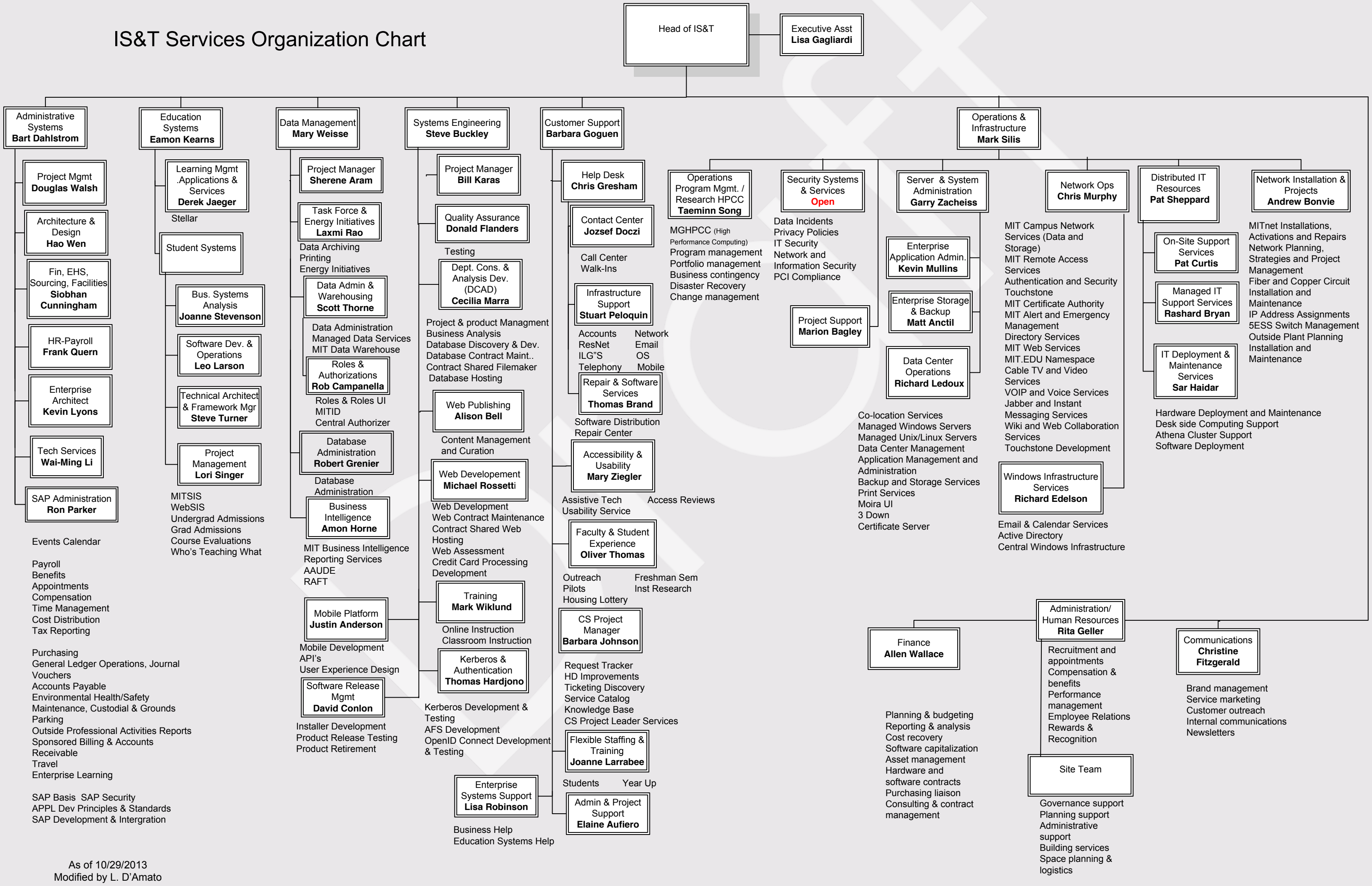
MIT NETWORK SECURITY

MARK SILIS & DAVE LAPORTE

ABOUT IS&T

IS&T Services Organization Chart



Head of IS&T

Executive Asst **Lisa Gagliardi**

Administrative Systems **Bart Dahlstrom**

- Project Mgmt **Douglas Walsh**
- Architecture & Design **Hao Wen**
- Fin, EHS, Sourcing, Facilities **Siobhan Cunningham**
- HR-Payroll **Frank Quern**
- Enterprise Architect **Kevin Lyons**
- Tech Services **Wai-Ming Li**
- SAP Administration **Ron Parker**

Events Calendar

Payroll
Benefits
Appointments
Compensation
Time Management
Cost Distribution
Tax Reporting

Purchasing
General Ledger Operations, Journal Vouchers
Accounts Payable
Environmental Health/Safety
Maintenance, Custodial & Grounds
Parking
Outside Professional Activities Reports
Sponsored Billing & Accounts Receivable
Travel
Enterprise Learning

SAP Basis SAP Security
APPL Dev Principles & Standards
SAP Development & Intergration

Education Systems **Eamon Kearns**

- Learning Mgmt .Applications & Services **Derek Jaeger**
  Stellar
- Student Systems
  - Bus. Systems Analysis **Joanne Stevenson**
  - Software Dev. & Operations **Leo Larson**
  - Technical Architect & Framework Mgr **Steve Turner**
  - Project Management **Lori Singer**

MITSIS
WebSIS
Undergrad Admissions
Grad Admissions
Course Evaluations
Who's Teaching What

Data Management **Mary Weisse**

- Project Manager **Sherene Aram**
- Task Force & Energy Initiatives **Laxmi Rao**
  Data Archiving
  Printing
  Energy Initiatives
- Data Admin & Warehousing **Scott Thorne**
  Data Administration
  Managed Data Services
  MIT Data Warehouse
  - Roles & Authorizations **Rob Campanella**
    Roles & Roles UI
    MITID
    Central Authorizer
- Database Administration **Robert Grenier**
  Database Administration
- Business Intelligence **Amon Horne**
  MIT Business Intelligence
  Reporting Services
  AAUDE
  RAFT
- Mobile Platform **Justin Anderson**
  Mobile Development
  API's
  User Experience Design
- Software Release Mgmt **David Conlon**
  Installer Development
  Product Release Testing
  Product Retirement

Systems Engineering **Steve Buckley**

- Project Manager **Bill Karas**
- Quality Assurance **Donald Flanders**
  Testing
- Dept. Cons. & Analysis Dev. (DCAD) **Cecilia Marra**
  Project & product Managment
  Business Analysis
  Database Discovery & Dev.
  Database Contract Maint..
  Contract Shared Filemaker
  Database Hosting
- Web Publishing **Alison Bell**
  Content Management and Curation
- Web Developement **Michael Rossetti**
  Web Development
  Web Contract Maintenance
  Contract Shared Web Hosting
  Web Assessment
  Credit Card Processing Development
- Training **Mark Wiklund**
  Online Instruction
  Classroom Instruction
- Kerberos & Authentication **Thomas Hardjono**
  Kerberos Development & Testing
  AFS Development
  OpenID Connect Development & Testing
- Enterprise Systems Support **Lisa Robinson**
  Business Help
  Education Systems Help

Customer Support **Barbara Goguen**

- Help Desk **Chris Gresham**
  - Contact Center **Jozsef Doczi**
    Call Center
    Walk-Ins
  - Infrastructure Support **Stuart Peloquin**
    Accounts Network
    ResNet Email
    ILG"S OS
    Telephony Mobile
  - Repair & Software Services **Thomas Brand**
    Software Distribution
    Repair Center
- Accessibility & Usability **Mary Ziegler**
  Assistive Tech Access Reviews
  Usability Service
- Faculty & Student Experience **Oliver Thomas**
  Outreach Freshman Sem
  Pilots Inst Research
  Housing Lottery
- CS Project Manager **Barbara Johnson**
  Request Tracker
  HD Improvements
  Ticketing Discovery
  Service Catalog
  Knowledge Base
  CS Project Leader Services
- Flexible Staffing & Training **Joanne Larrabee**
  Students Year Up
- Admin & Project Support **Elaine Aufiero**

Operations & Infrastructure **Mark Silis**

- Operations Program Mgmt. / Research HPCC **Taeminn Song**
  MGHPCC (High Performance Computing)
  Program management
  Portfolio management
  Business contingency
  Disaster Recovery
  Change management
- Security Systems & Services **Open**
  Data Incidents
  Privacy Policies
  IT Security
  Network and Information Security
  PCI Compliance
- Project Support **Marion Bagley**
- Server & System Administration **Garry Zacheiss**
  - Enterprise Application Admin. **Kevin Mullins**
  - Enterprise Storage & Backup **Matt Anctil**
  - Data Center Operations **Richard Ledoux**

  Co-location Services
  Managed Windows Servers
  Managed Unix/Linux Servers
  Data Center Management
  Application Management and Administration
  Backup and Storage Services
  Print Services
  Moira UI
  3 Down
  Certificate Server
- Network Ops **Chris Murphy**
  MIT Campus Network Services (Data and Storage)
  MIT Remote Access Services
  Authentication and Security
  Touchstone
  MIT Certificate Authority
  MIT Alert and Emergency Management
  Directory Services
  MIT Web Services
  MIT.EDU Namespace
  Cable TV and Video Services
  VOIP and Voice Services
  Jabber and Instant Messaging Services
  Wiki and Web Collaboration Services
  Touchstone Development
  - Windows Infrastructure Services **Richard Edelson**
    Email & Calendar Services
    Active Directory
    Central Windows Infrastructure
- Distributed IT Resources **Pat Sheppard**
  - On-Site Support Services **Pat Curtis**
  - Managed IT Support Services **Rashard Bryan**
  - IT Deployment & Maintenance Services **Sar Haidar**

  Hardware Deployment and Maintenance
  Desk side Computing Support
  Athena Cluster Support
  Software Deployment
- Network Installation & Projects **Andrew Bonvie**
  MITnet Installations, Activations and Repairs
  Network Planning, Strategies and Project Management
  Fiber and Copper Circuit Installation and Maintenance
  IP Address Assignments
  5ESS Switch Management
  Outside Plant Planning Installation and Maintenance

Finance **Allen Wallace**

Planning & budgeting
Reporting & analysis
Cost recovery
Software capitalization
Asset management
Hardware and software contracts
Purchasing liaison
Consulting & contract management

Administration/ Human Resources **Rita Geller**

Recruitment and appointments
Compensation & benefits
Performance management
Employee Relations
Rewards & Recognition

- Site Team
  Governance support
  Planning support
  Administrative support
  Building services
  Space planning & logistics

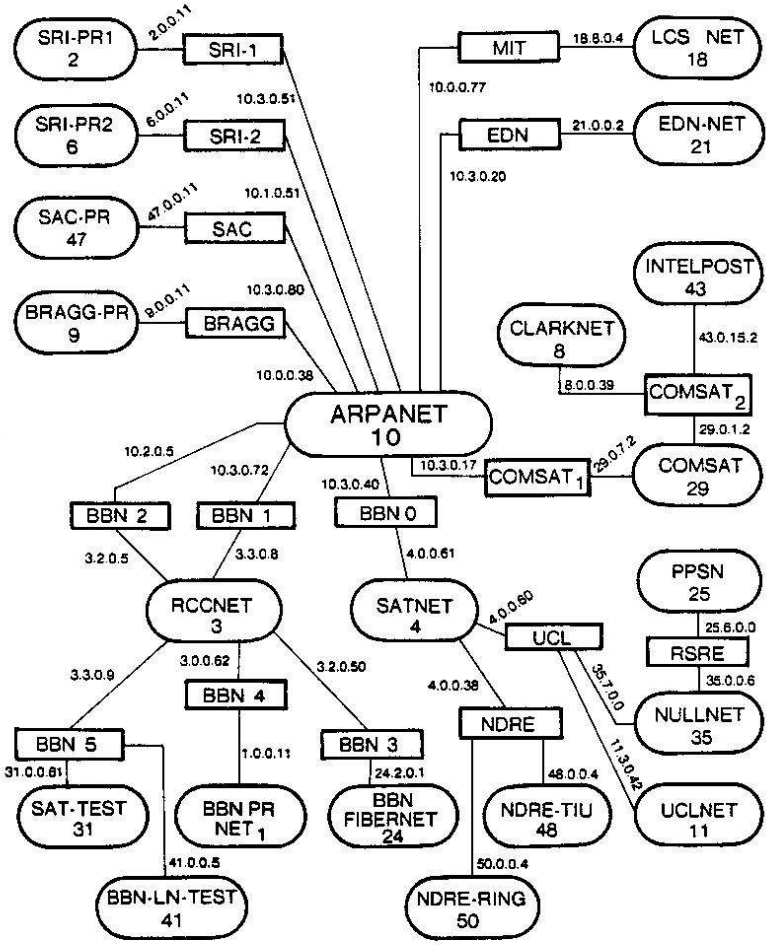
Communications **Christine Fitzgerald**

Brand management
Service marketing
Customer outreach
Internal communications
Newsletters

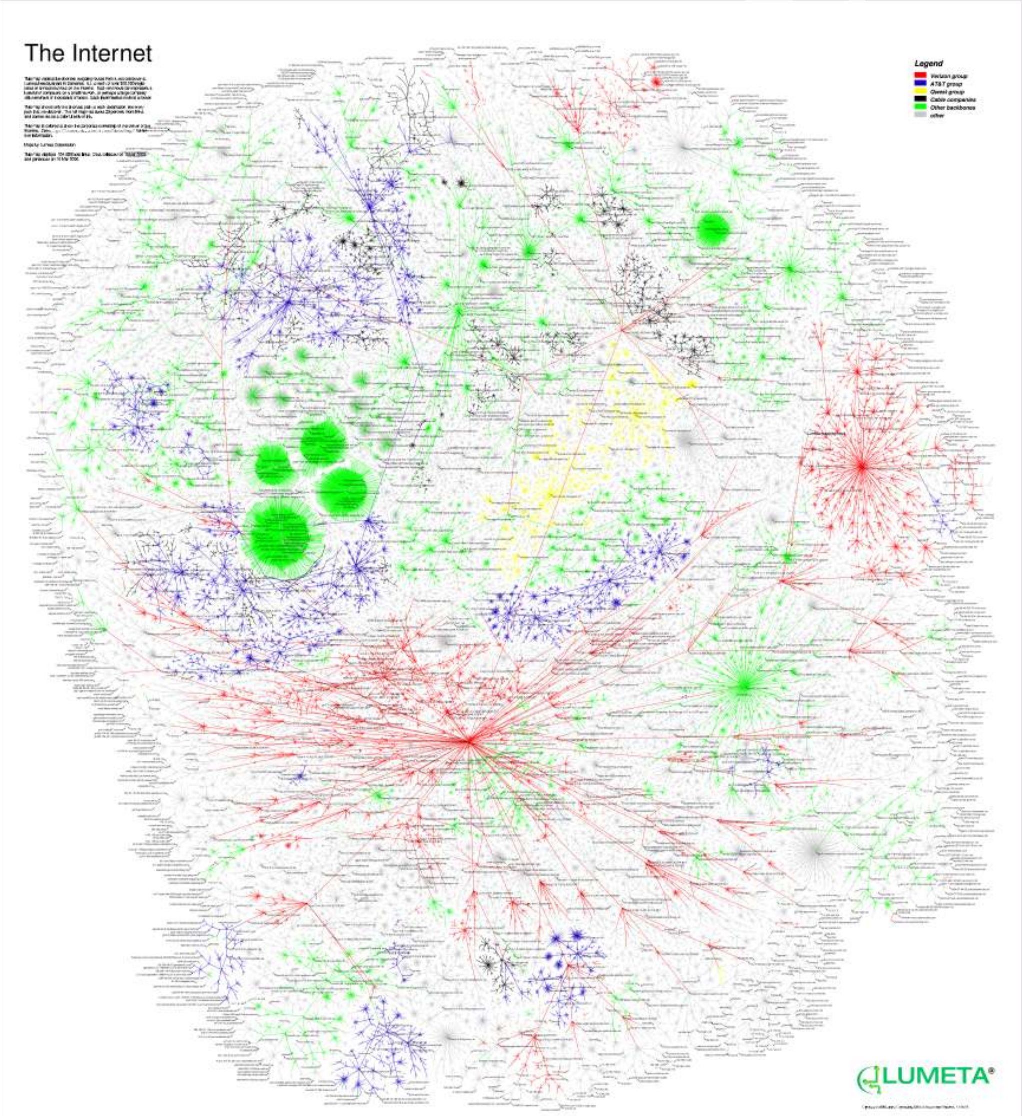
As of 10/29/2013
Modified by L. D'Amato

THE INTERNET: CIRCA 1980

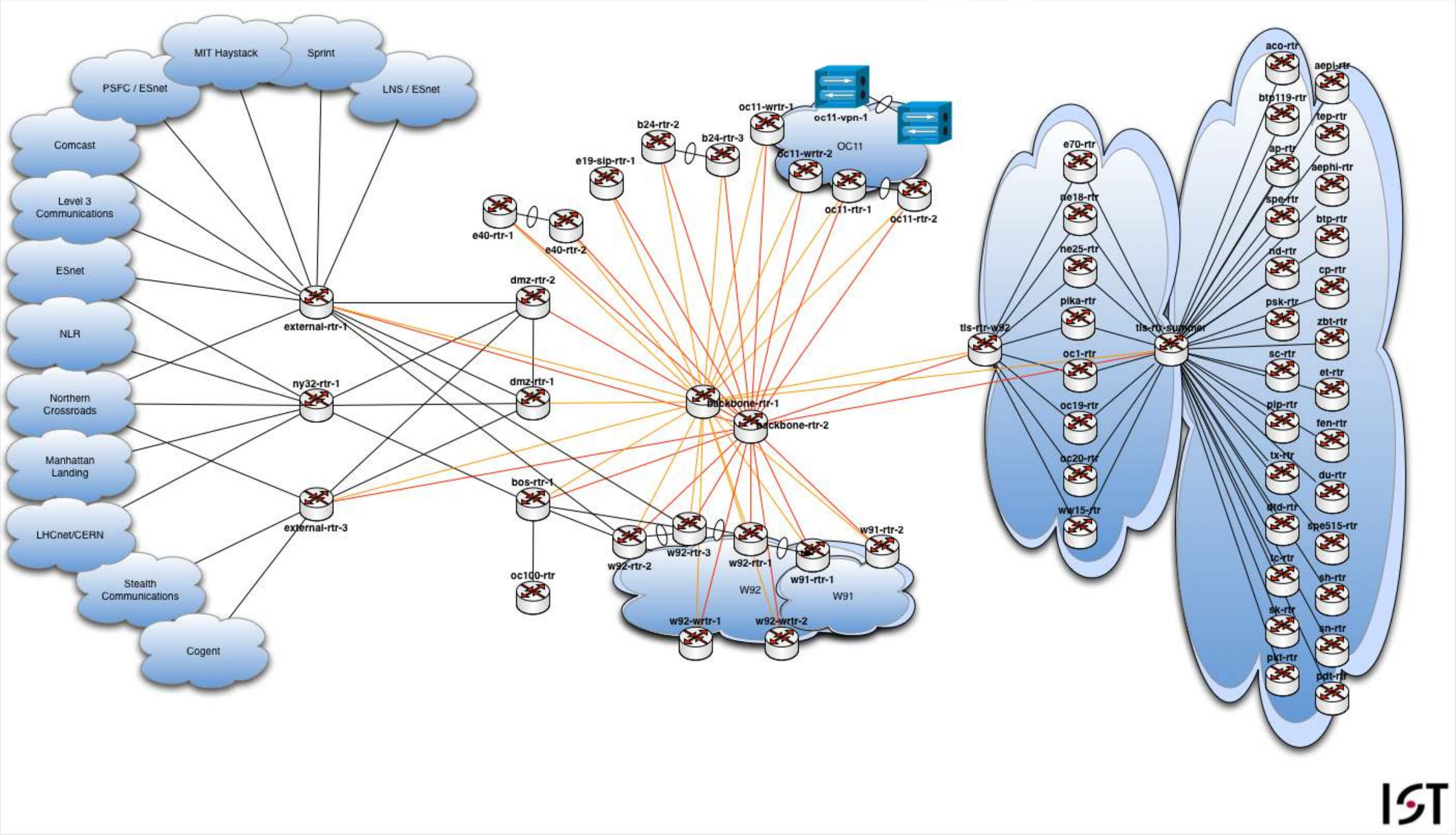
POSTEL 25 FEB 82



THE INTERNET: ~TODAY



MIT CAMPUS NETWORK



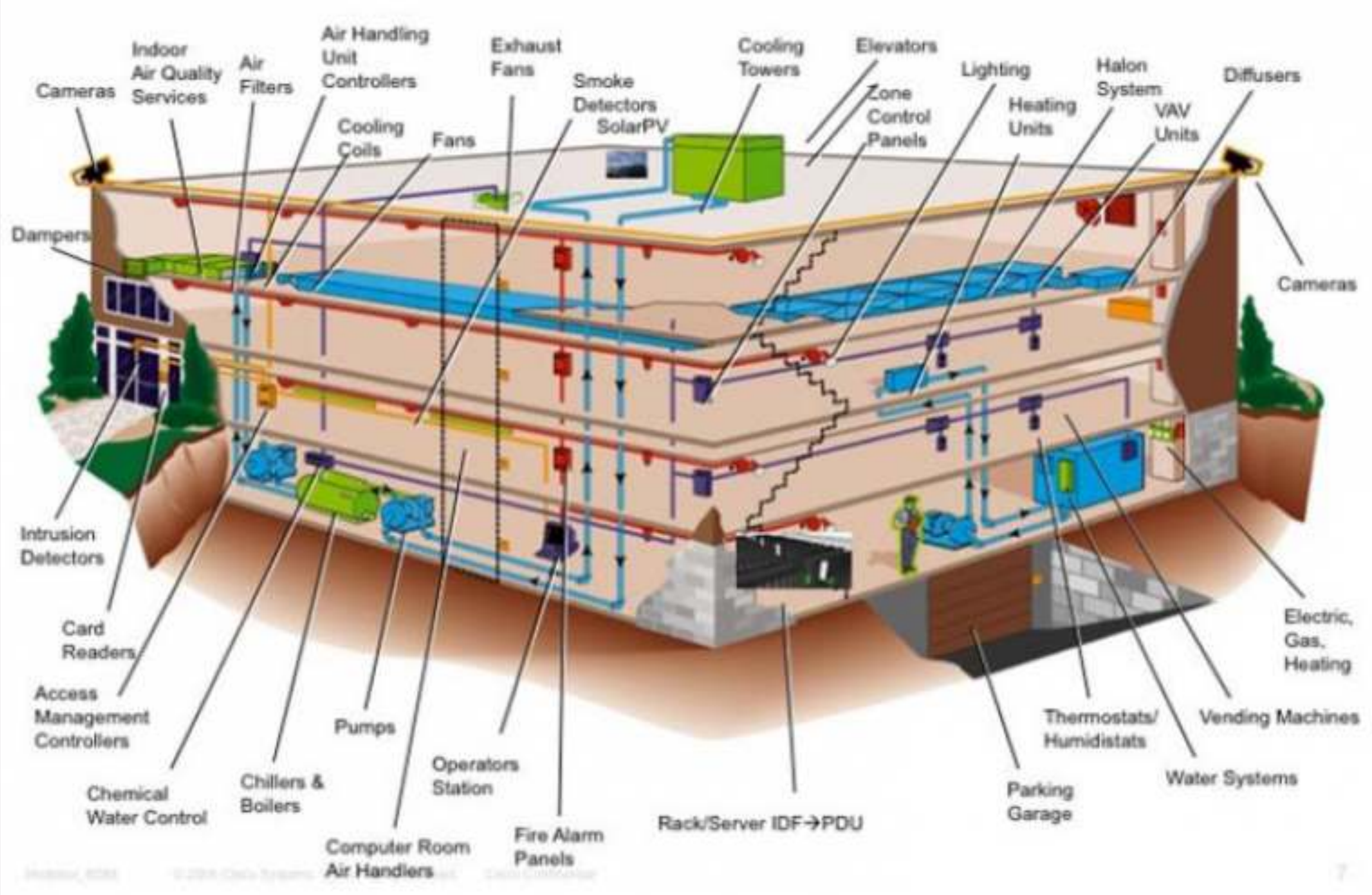
1994-1998	1998-2000	2000-2005	2005-2008
Asante 2072	**Asante 5324**	**Cabletron 2200**	**Enterasys C2**
10 Mb/s Shared	10 Mb/s Switched	100 Mb/s Switched	1 Gb/s Switched
72 ports ($80 per port)	24 ports ($100 per port)	24 ports ($145 per port)	24 ports ($175 per port)
17 Units (0.6%)	150 Units (5.6%)	931 Units (34.8%)	224 Units (8.4%)
1,224 Ports (1.25%)	3,600 Ports (3.7%)	22,344 Ports (22.9%)	5,376 Ports (5.5%)
Cat3 Cabling	Cat3 Cabling	Cat5 Cabling	Cat5 Cabling

2008-2010	2010-Present
Cisco 3560E	**Cisco 3560X**
1 Gb/s Switched	1 Gb/s Switched
48 ports ($140 per port)	48 ports ($110 per port)
773 Units (29.5%)	583 Units (11.7%)
37,104 Ports (38%)	27,984 Ports (28.7%)
Cat6 Cabling	Cat6 Cabling

1,332 units
&
32,544 ports

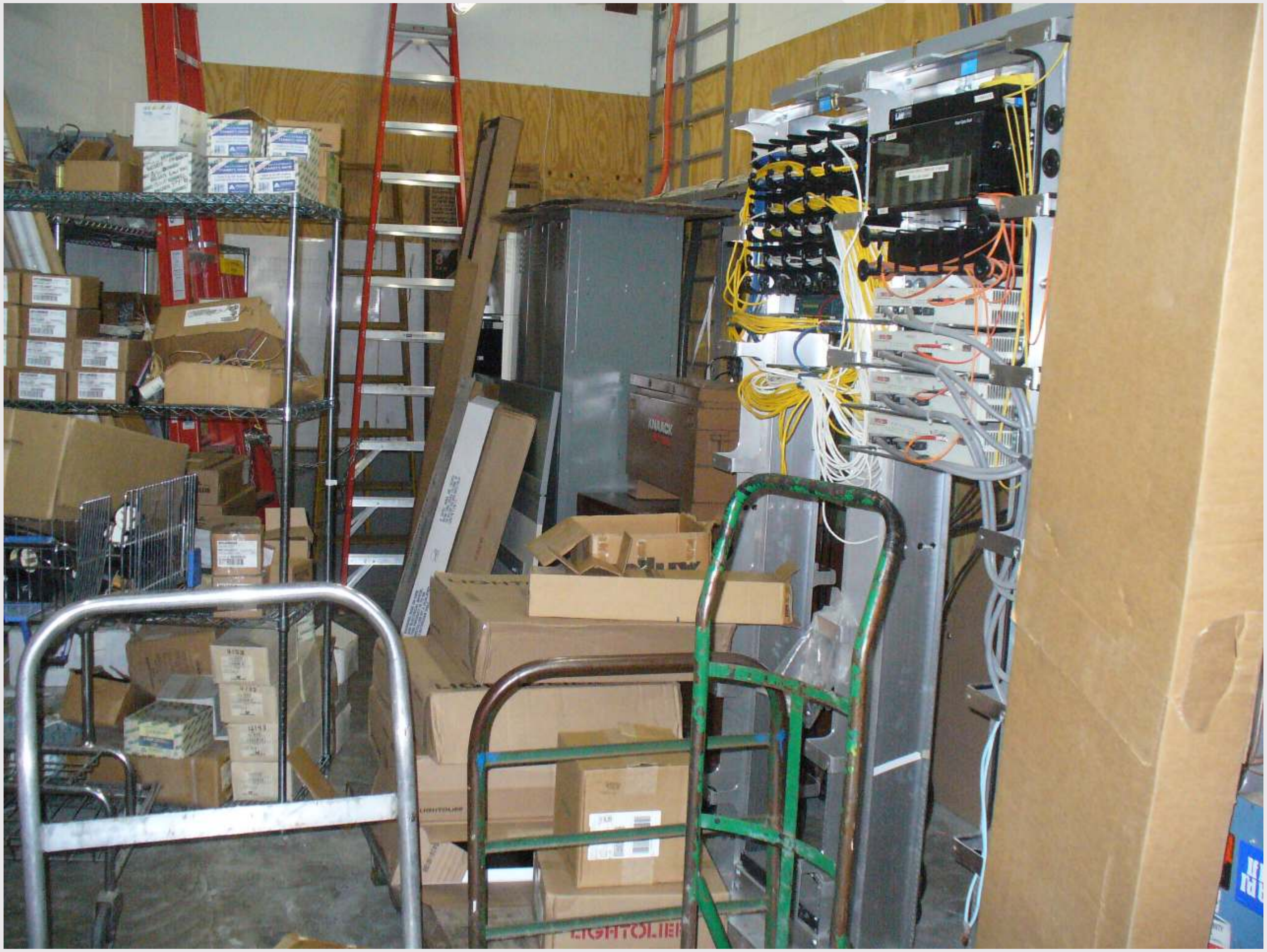
Targeted for renewal

THE INTERNET OF EVERYTHING

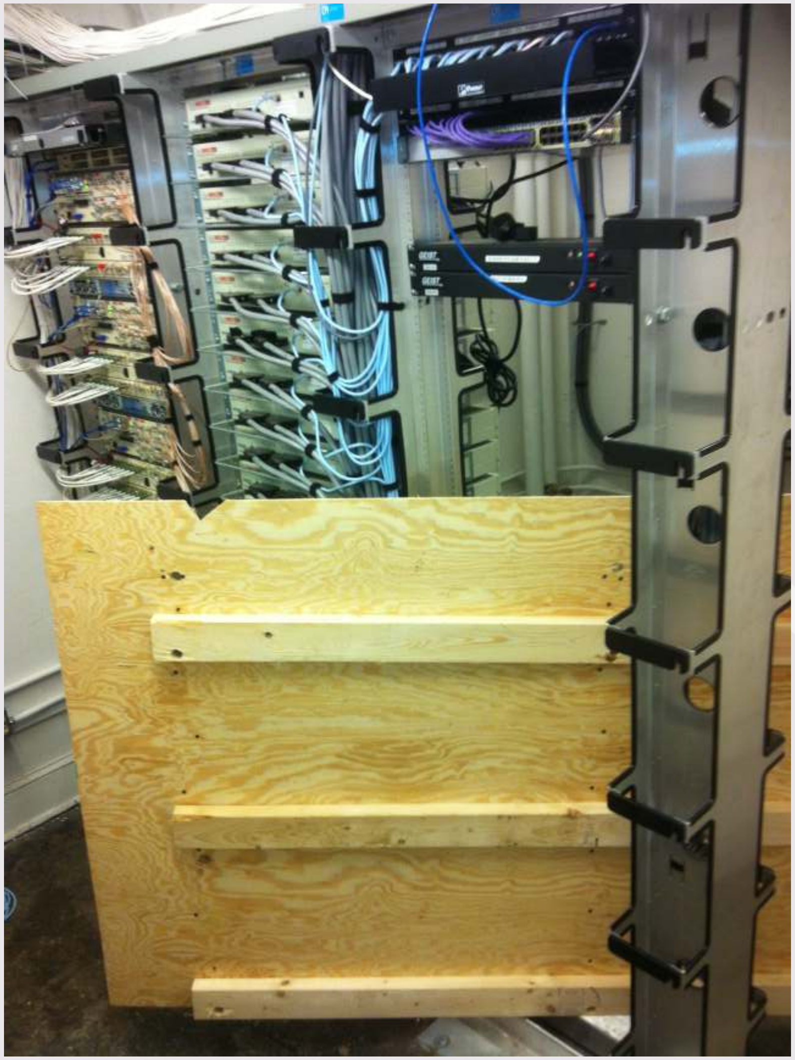


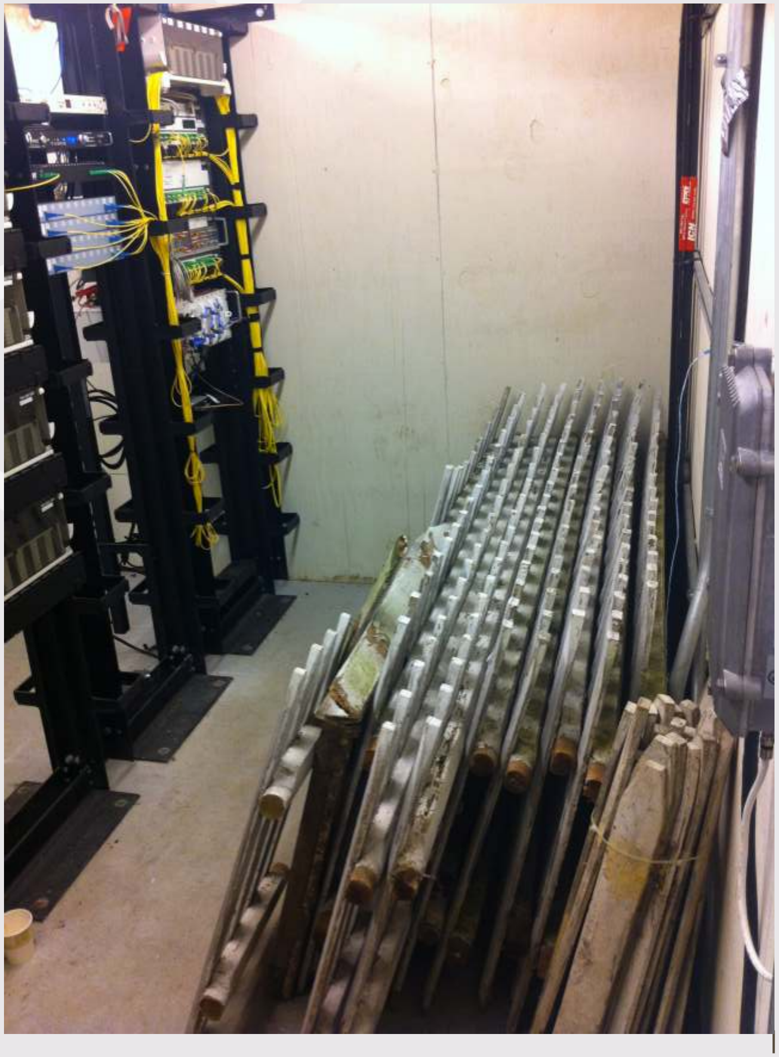
MIT PHYSICAL INFRASTRUCTURE

TEL/DATA CLOSETS BEING RE-PURPOSED



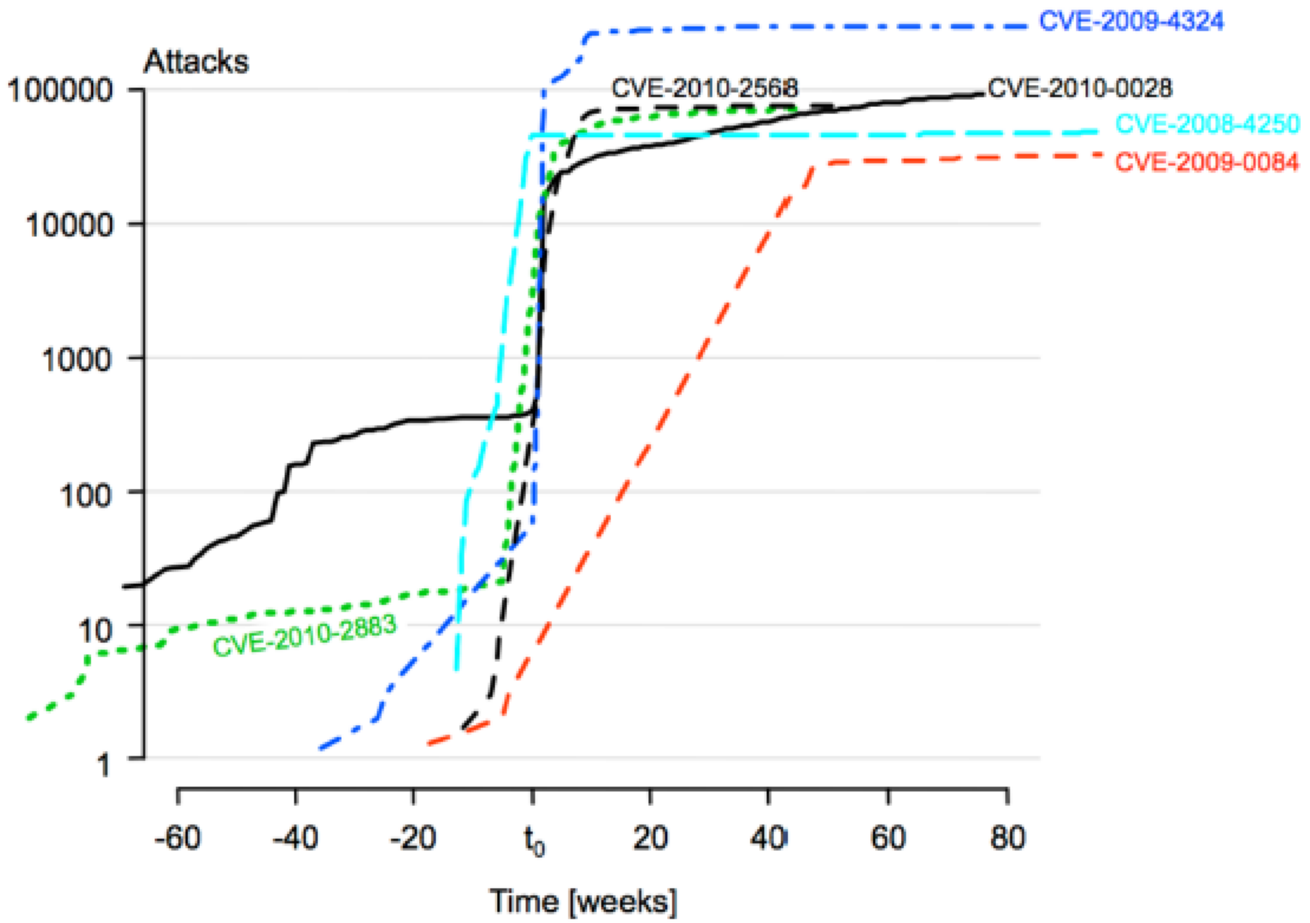
TEL/DATA CLOSETS CREATIVELY USED IN DORMS





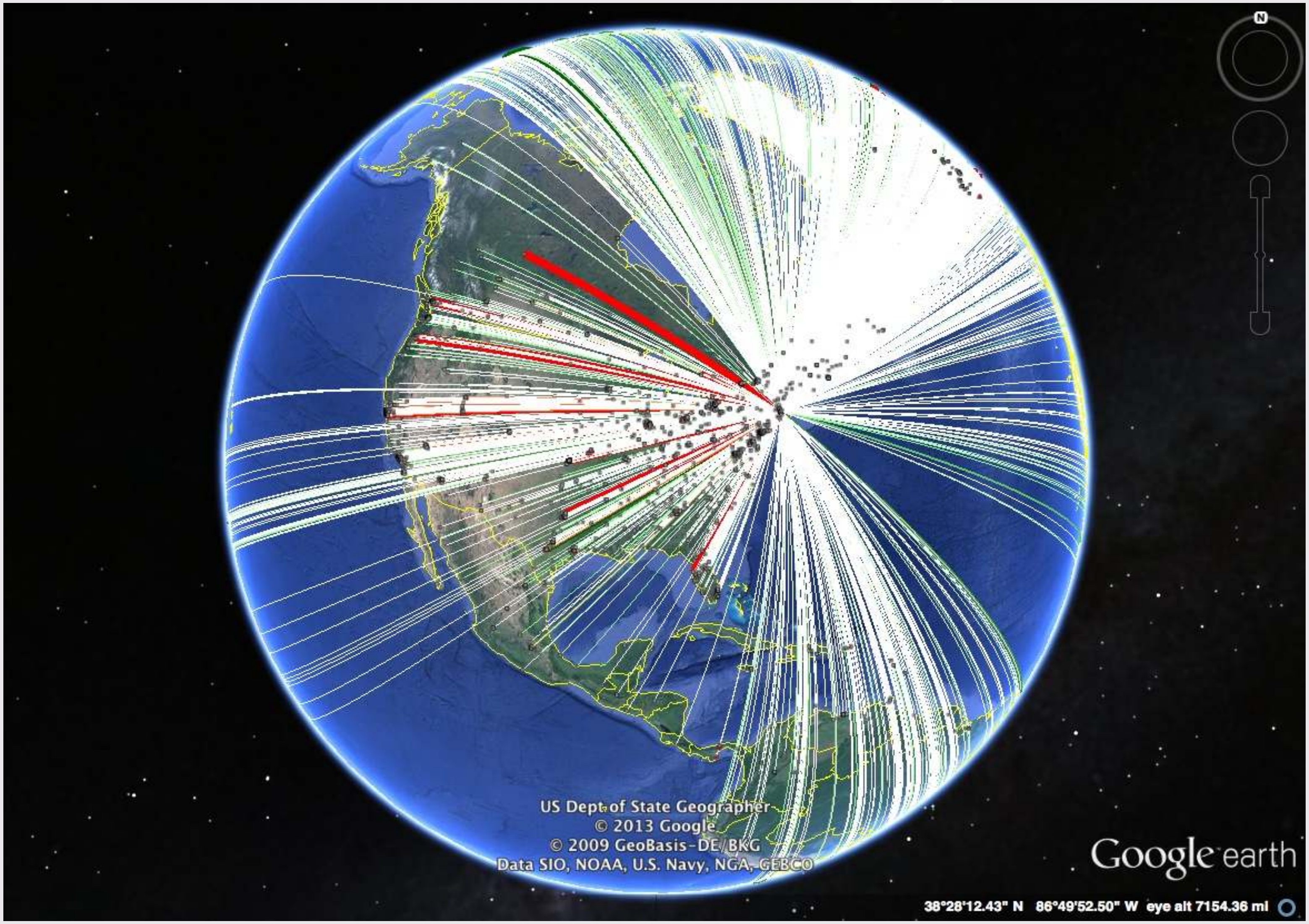
TODAY’S SECURITY LANDSCAPE

ZERO DAY EXPLOITS

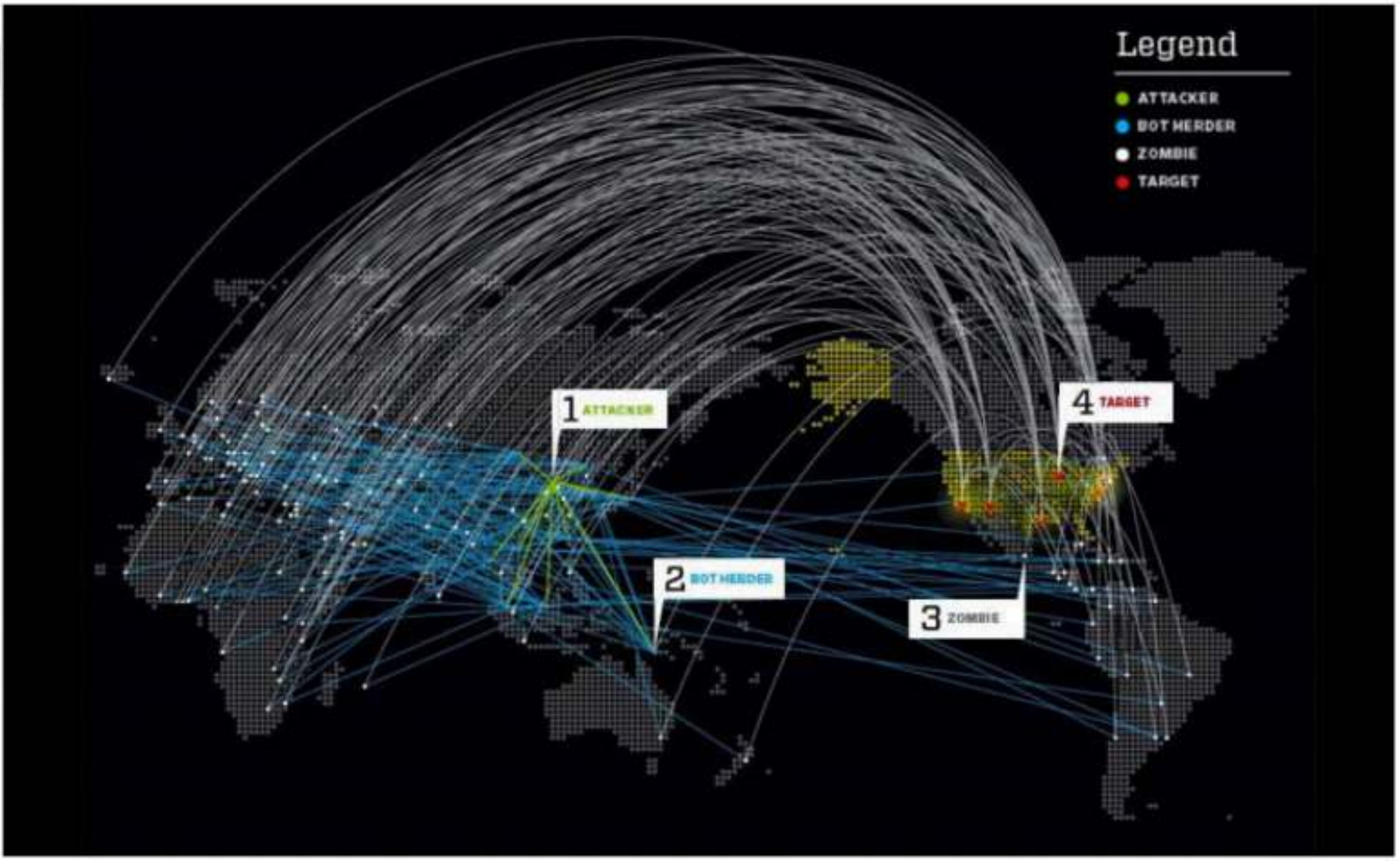


(a) Attacks exploiting zero-day vulnerabilities before and after the disclosure (time = t_0).

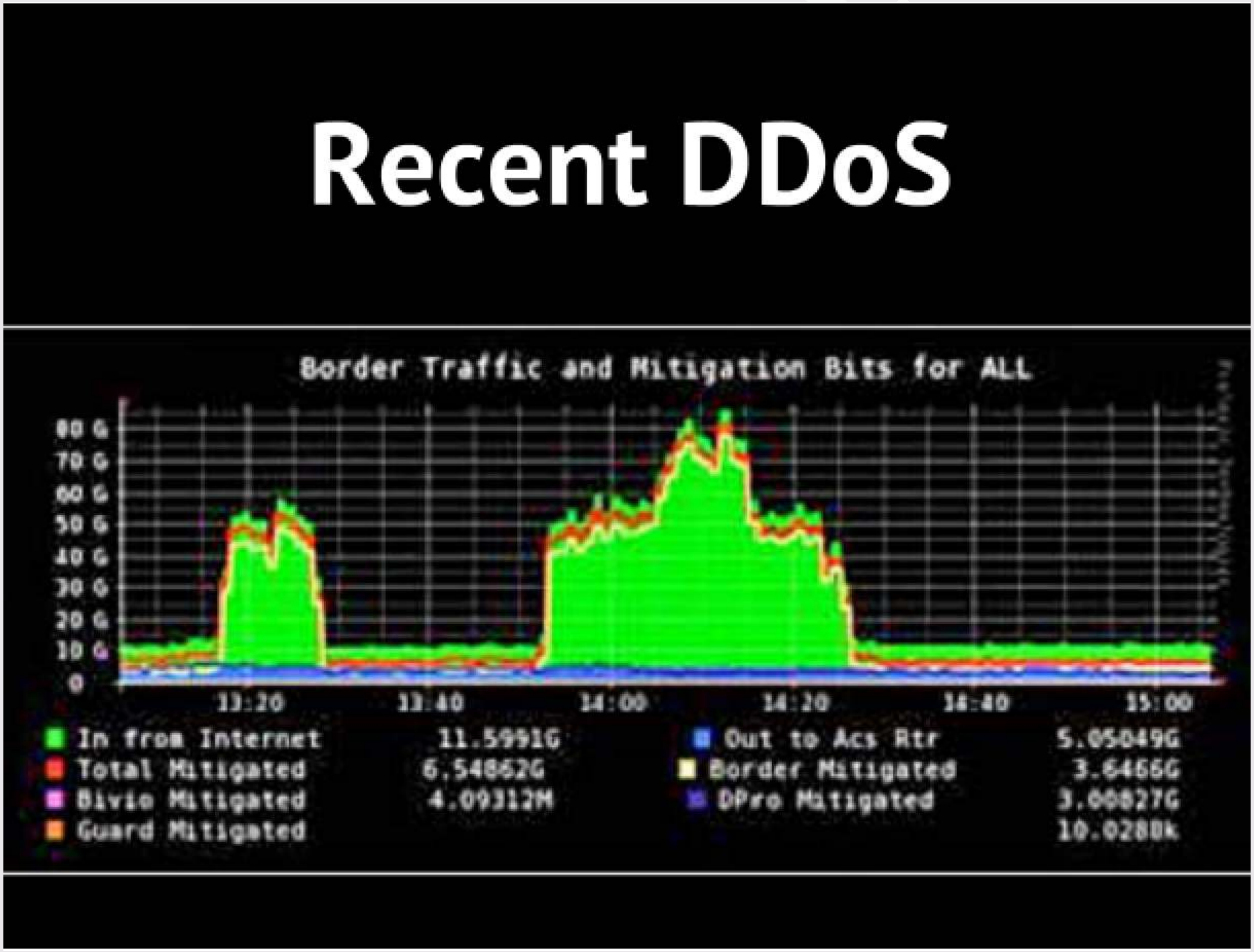
WHAT MIGHT THIS BE?


N
US Dept of State Geographer
© 2013 Google
© 2009 GeoBasis-DE/BKG
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
Google earth
38°28'12.43" N 86°49'52.50" W eye alt 7154.36 mi

DDOS ATTACKS

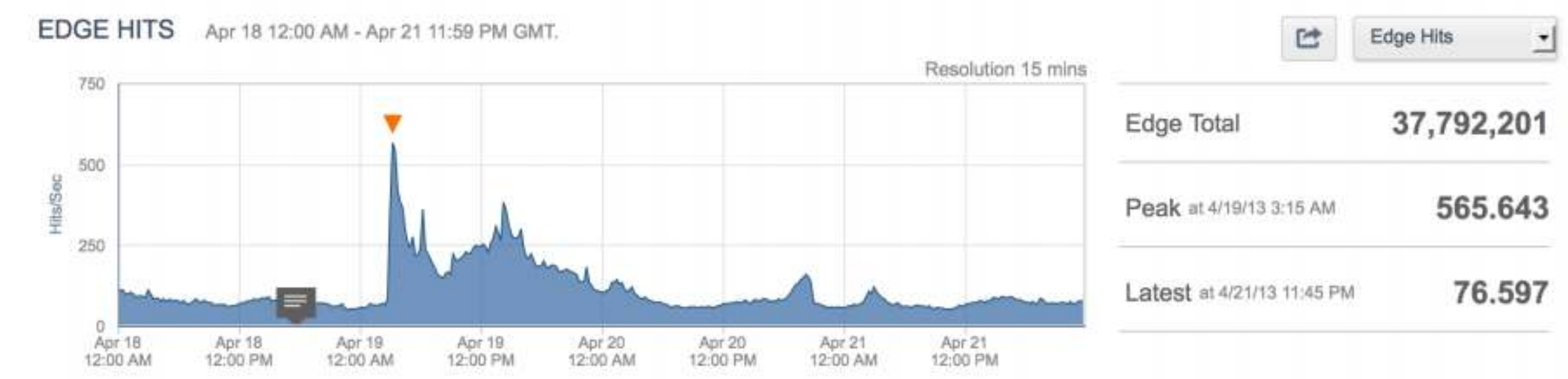


DDOS ATTACKS



PROTECTING MIT'S EXTERNAL WEB PRESENCE

Akamai



EDGE HITS Apr 18 12:00 AM - Apr 21 11:59 PM GMT.

Resolution 15 mins

Edge Total 37,792,201

Peak at 4/19/13 3:15 AM 565.643

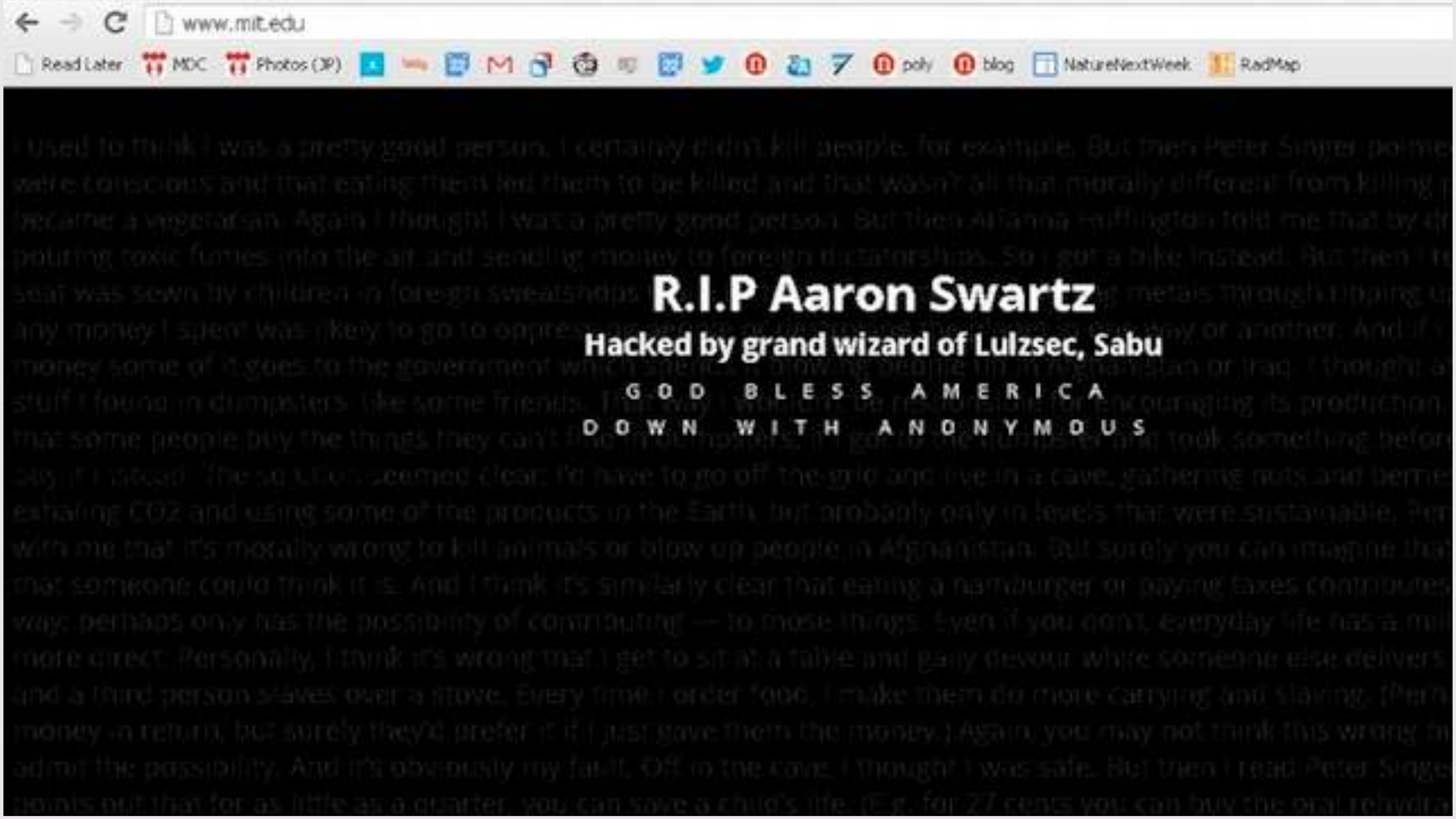
Latest at 4/21/13 11:45 PM 76.597

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



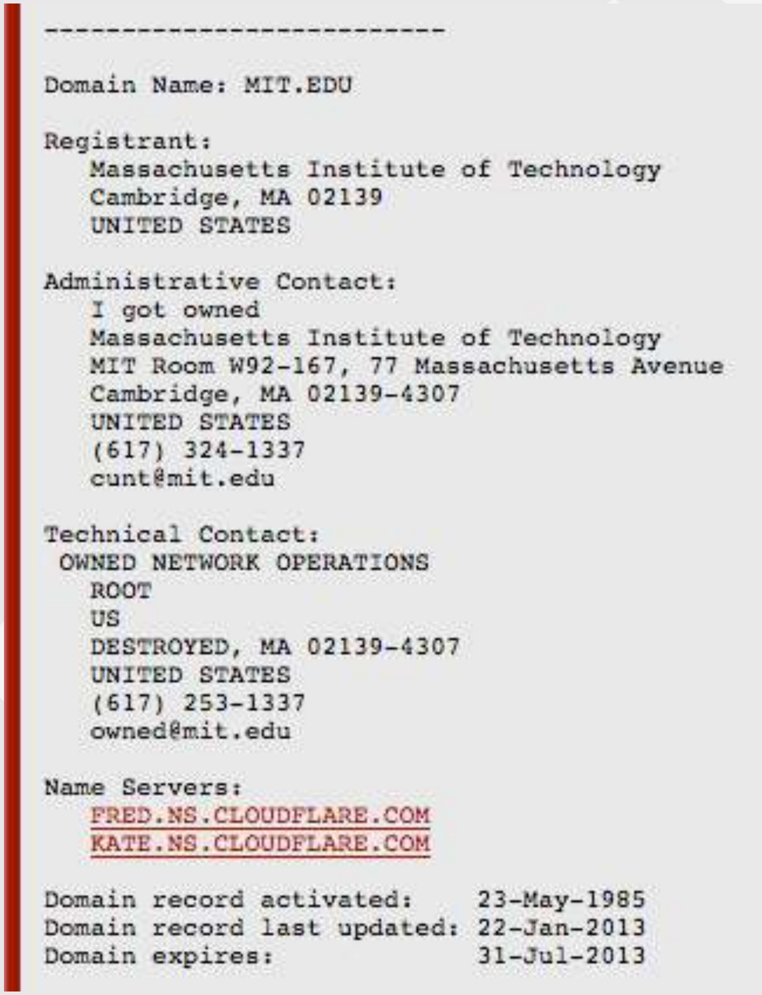
R.I.P Aaron Swartz

Hacked by grand wizard of Lulzsec, Sabu

GOD BLESS AMERICA

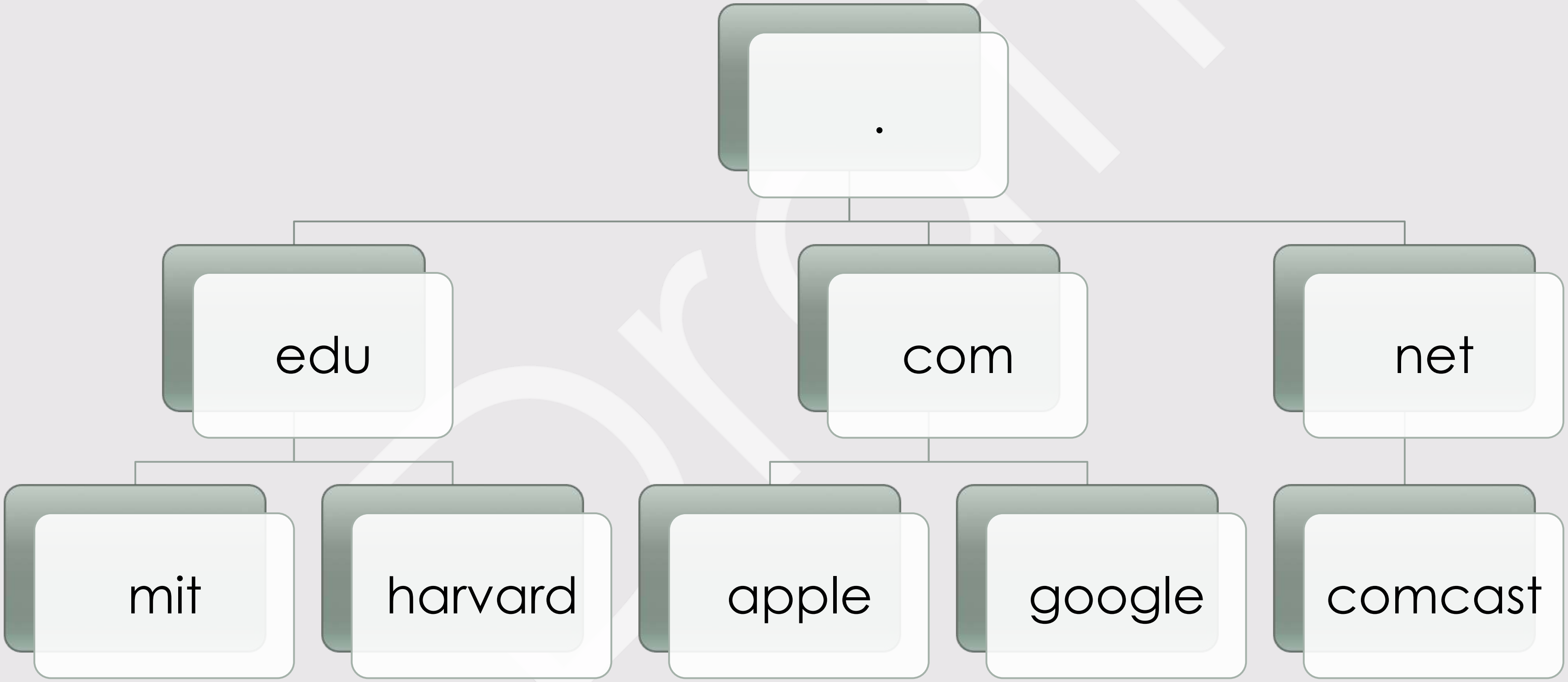
DOWN WITH ANONYMOUS

MIT.EDU – THE ATTACK



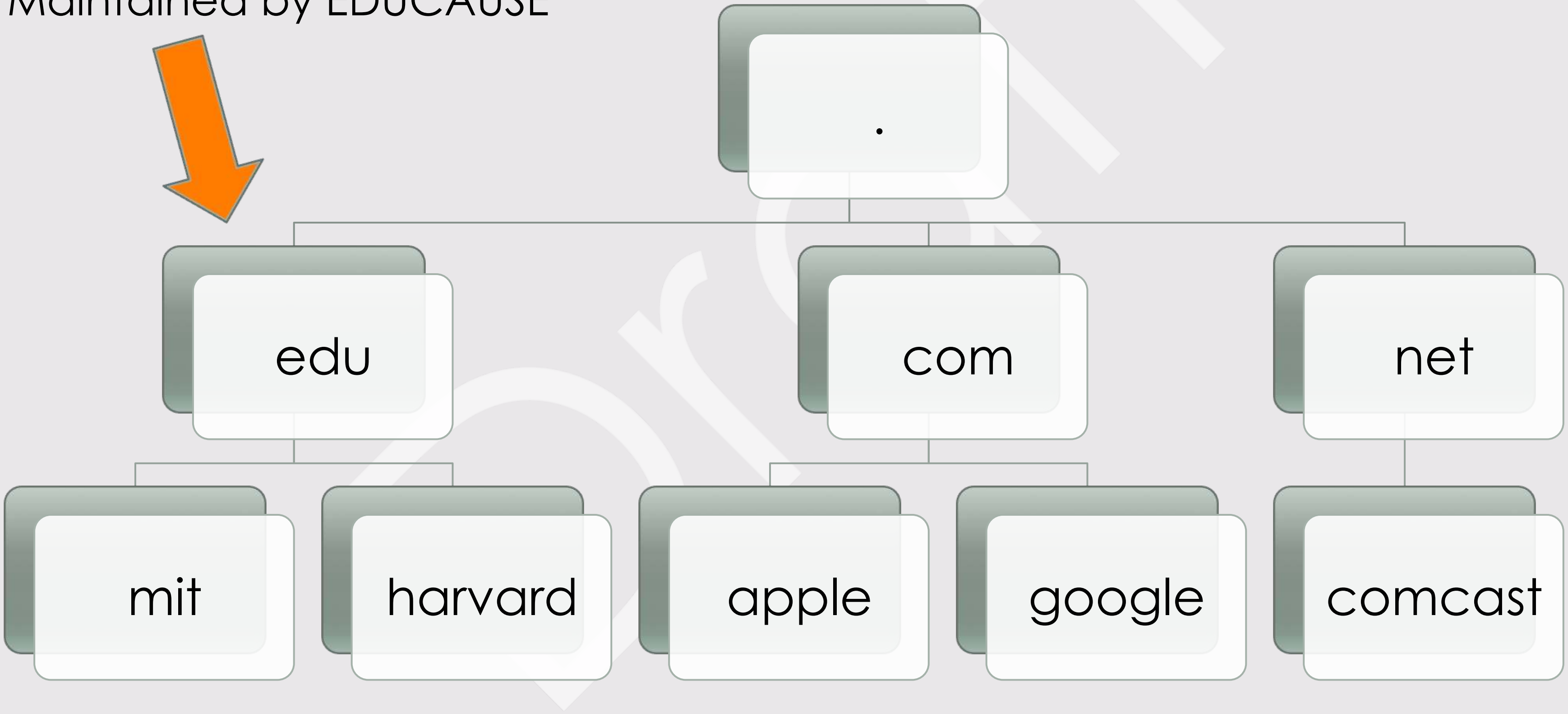
```
--------------------------

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



.

edu

com

net

mit

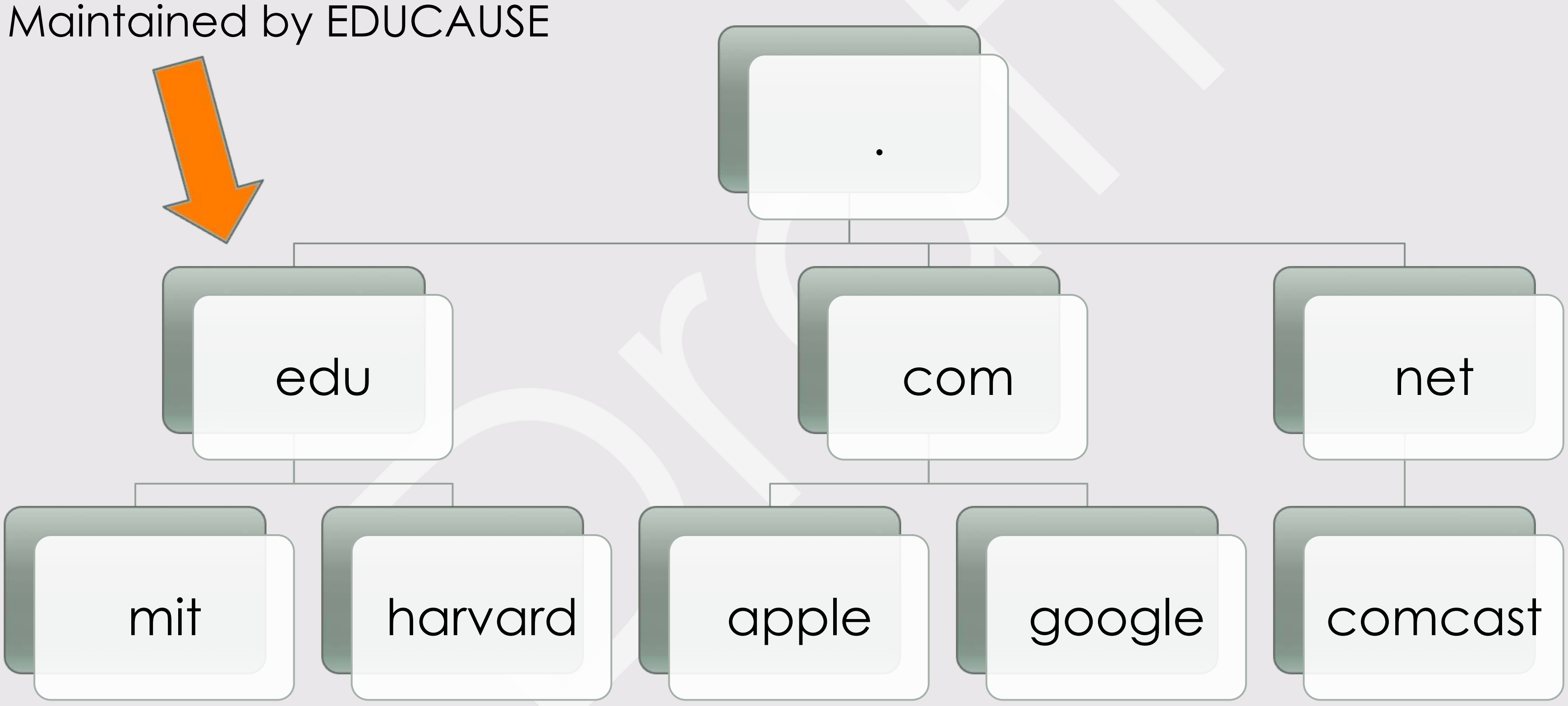
harvard

apple

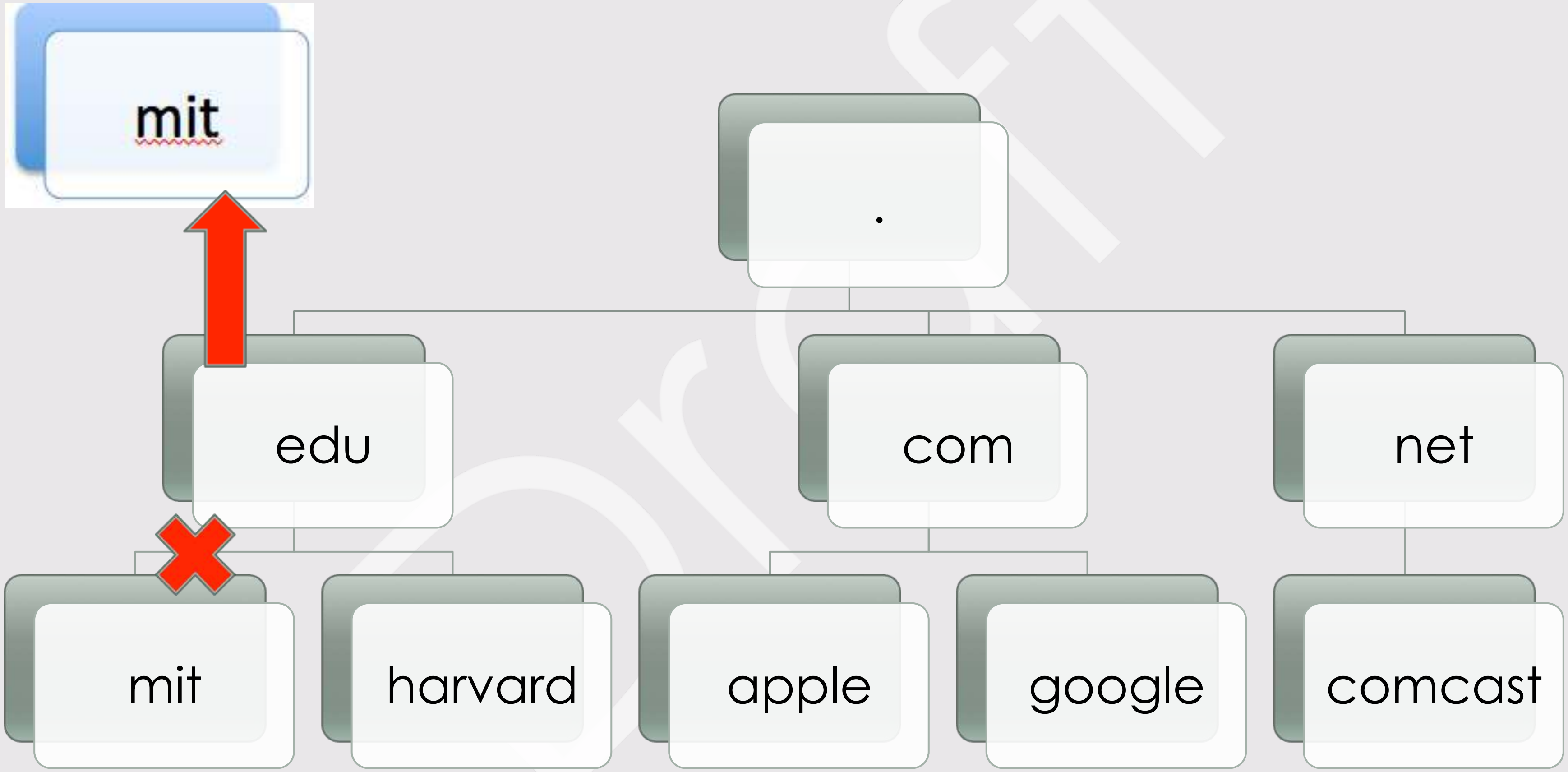
google

comcast

MIT.EDU – WHAT HAPPENED

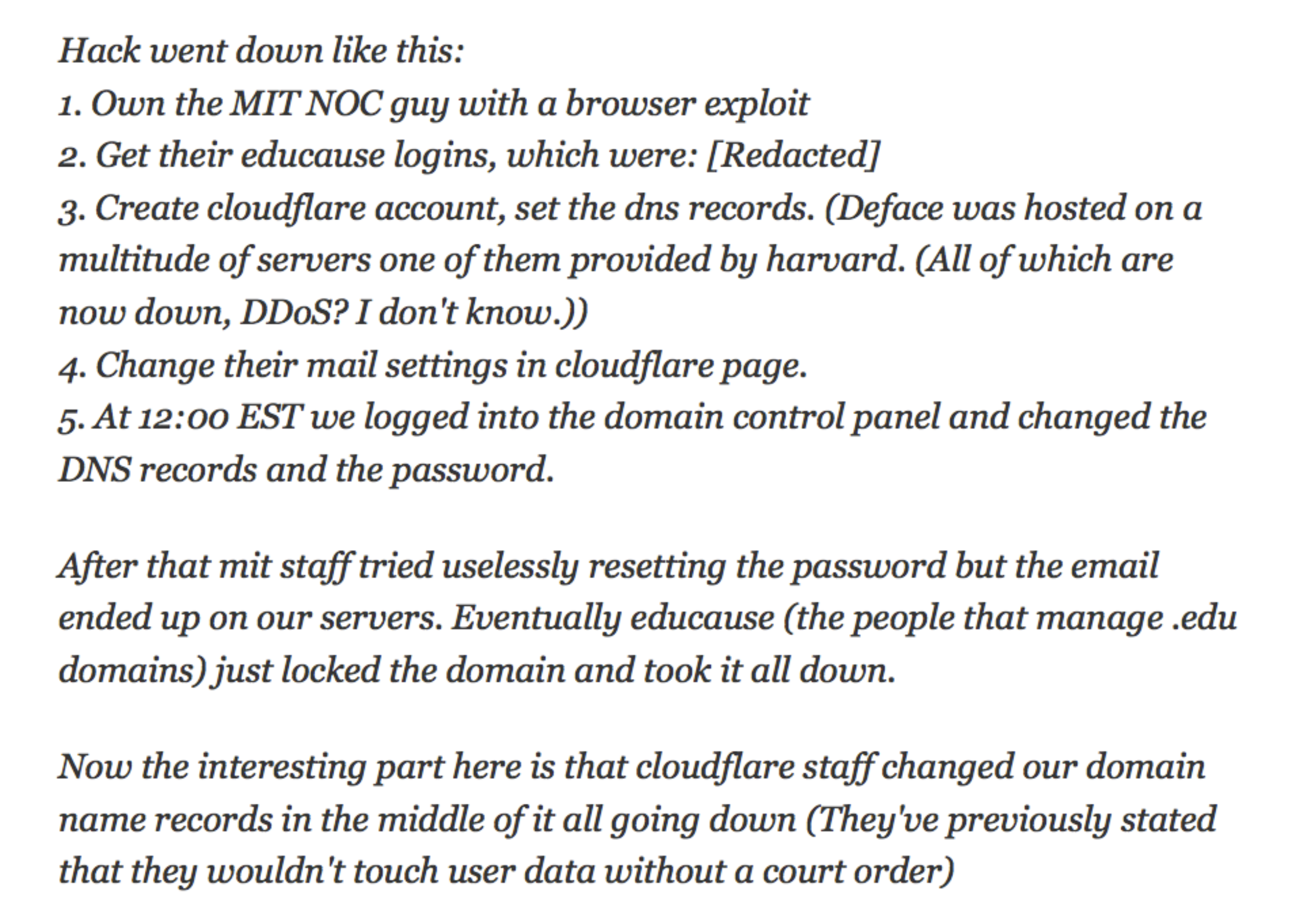


MIT.EDU – WHAT HAPPENED



MIT.EDU – THE TROLL

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)

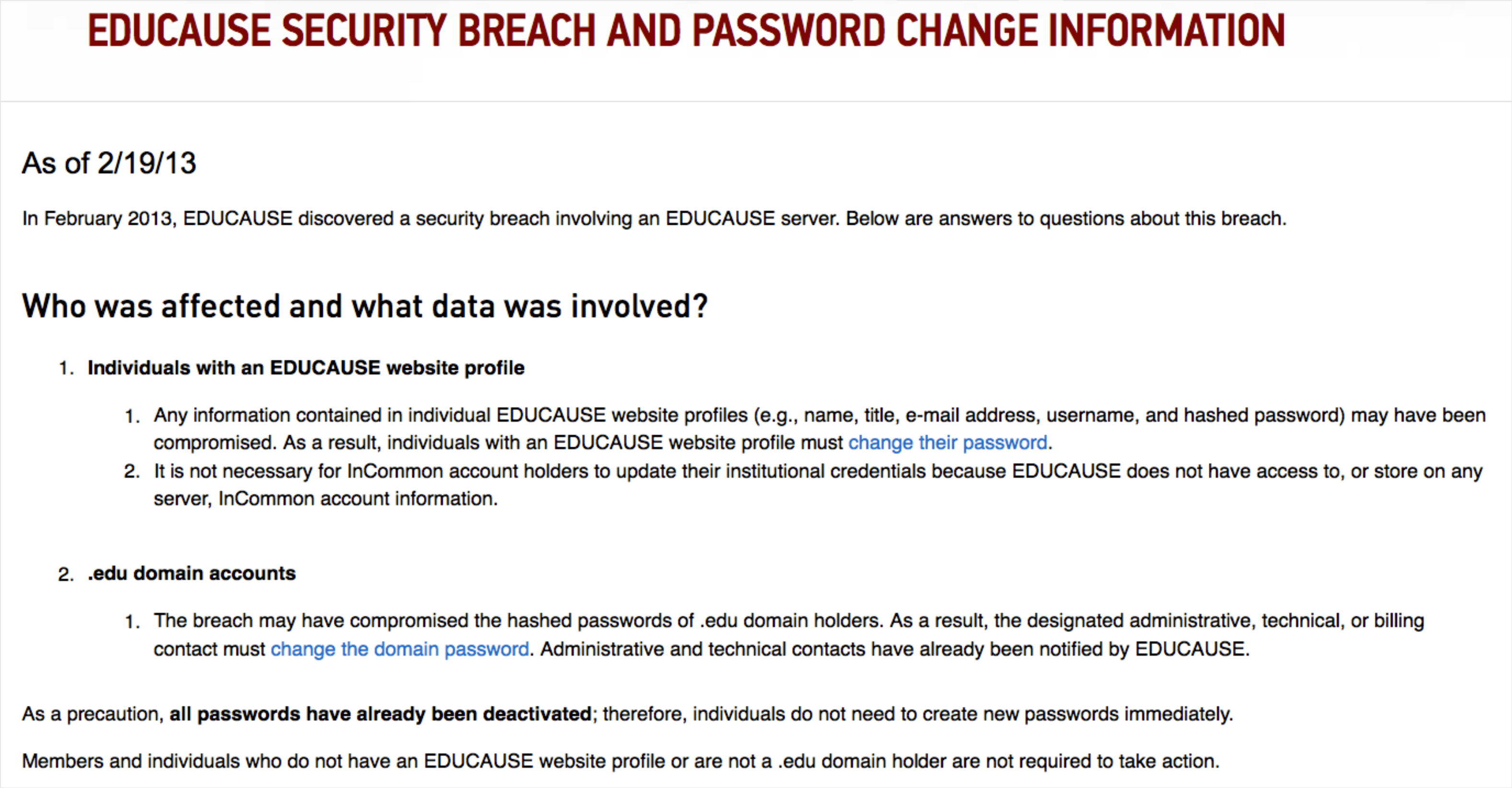
MIT.EDU - HOW IT HAPPENED

From HTP Zine 5 (http://www.exploit-db.com/papers/25306/):

> 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?