

L21: Security intro

Nickolai Zeldovich
6.033 Spring 2012

Private data routinely leaked

Utah's Medicaid Data Breach

www.informationweek.com/news/healthcare/security-privacy/232900128

Utah's Medicaid Data Breach Worse Than Expected

Utah Department of Technology Services (DTS) reveals 780,000 individuals have been affected by the theft of sensitive Medicaid information. That's far worse than initial estimates.

By [Nicole Lewis](#) InformationWeek
April 11, 2012 11:38 AM

A new tally of files stored on a server that contained Medicaid information at the Utah Department of Technology Services (DTS) reveals that 780,000 individuals have been affected by the theft of sensitive information. That's far worse than initial estimates.

The data breach occurred on March 30, when a configuration error occurred at the password authentication level, allowing the hacker, located in Eastern Europe, to circumvent DTS's security system.

More Healthcare Insights

Webcasts

- [Learn how Kettering Health Network maximized clinician patient time by virtualizing clinician access to data](#)
- [Self-Encrypting Drives: The Evolution of Encryption](#)

"The server was a test server and when it was put into production there was a misconfiguration. Processes were not followed and the password was very weak," Stephanie Weiss, spokesperson for DTS, told *InformationWeek Healthcare*.



Master's Degree Programs For IT Pros And Clinicians

(click image for larger view and fo

Users tricked by impersonators

Top Federal Lab Hack... x +

www.wired.com/threatlevel/2011/04/oak-ridge-lab-hack/

Top Federal Lab Hacked in Spear-Phishing Attack

By Kim Zetter | April 20, 2011 | 1:16 am | Categories: Breaches, Crime, Hacks and Cracks

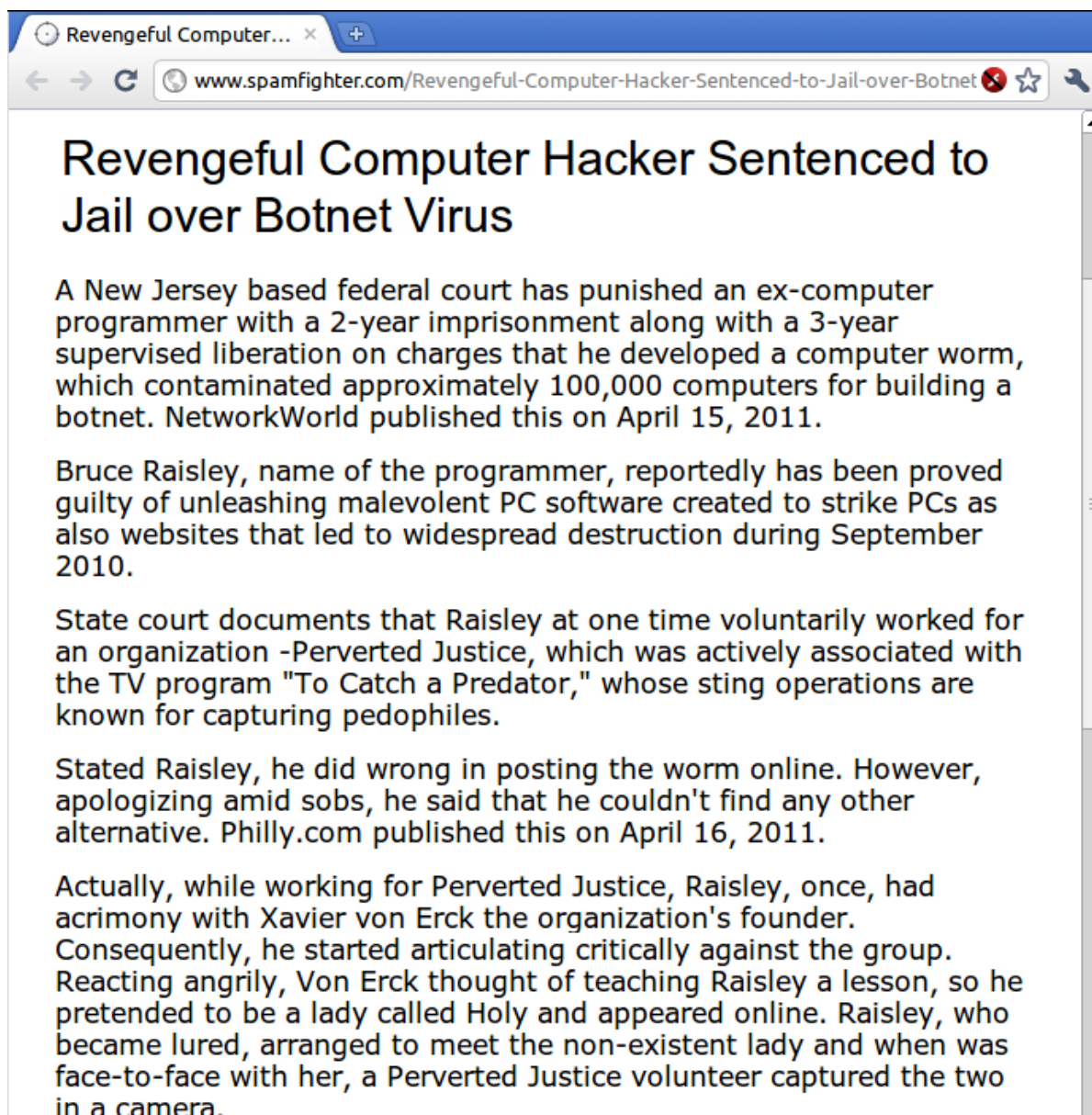


The image shows an aerial view of the Oak Ridge National Laboratory campus. The facility consists of several large, multi-story brick buildings with flat roofs, arranged around a central courtyard. The courtyard features a large, white, circular fountain. The campus is surrounded by lush green trees and a well-maintained lawn. A road with a red truck is visible in the foreground, and a parking lot with several cars is located near the central buildings. The background shows more industrial structures and a forested hillside.

The Oak Ridge National Laboratory was forced to disconnect internet access for workers on Friday after the federal facility was hacked, and administrators discovered data being siphoned from a server.

Only a "few megabytes" of data were stolen before the lab discovered the breach and cut internet

Botnets control millions of PCs



The image is a screenshot of a web browser window. The address bar shows the URL: www.spamfighter.com/Revengeful-Computer-Hacker-Sentenced-to-Jail-over-Botnet. The page title is "Revengeful Computer Hacker Sentenced to Jail over Botnet Virus". The article text is as follows:

A New Jersey based federal court has punished an ex-computer programmer with a 2-year imprisonment along with a 3-year supervised liberation on charges that he developed a computer worm, which contaminated approximately 100,000 computers for building a botnet. NetworkWorld published this on April 15, 2011.

Bruce Raisley, name of the programmer, reportedly has been proved guilty of unleashing malevolent PC software created to strike PCs as also websites that led to widespread destruction during September 2010.

State court documents that Raisley at one time voluntarily worked for an organization -Perverted Justice, which was actively associated with the TV program "To Catch a Predator," whose sting operations are known for capturing pedophiles.

Stated Raisley, he did wrong in posting the worm online. However, apologizing amid sobs, he said that he couldn't find any other alternative. Philly.com published this on April 16, 2011.

Actually, while working for Perverted Justice, Raisley, once, had acrimony with Xavier von Erck the organization's founder. Consequently, he started articulating critically against the group. Reacting angrily, Von Erck thought of teaching Raisley a lesson, so he pretended to be a lady called Holy and appeared online. Raisley, who became lured, arranged to meet the non-existent lady and when was face-to-face with her, a Perverted Justice volunteer captured the two in a camera.

Computer worm used to sabotage

Clues Suggest Stuxne... x +

← → ↻ www.wired.com/threatlevel/2010/11/stuxnet-clues/

Clues Suggest Stuxnet Virus Was Built for Subtle Nuclear Sabotage

By [Kim Zetter](#) November 15, 2010 | 4:00 pm | Categories: [Cybersecurity](#)



New and important evidence found in the sophisticated “Stuxnet” malware targeting industrial control systems provides strong hints that the code was designed to sabotage nuclear plants, and that it employs a subtle sabotage strategy that involves briefly speeding up and slowing down physical machinery at a plant over a span of weeks.

“It indicates that [Stuxnet’s creators] wanted to get on the system and not be discovered and stay there for a long time and [change the process subtly, but not break it,](#)” (.pdf) says Liam O Murchu, researcher with Svmantec Security Response, which published the new information in an updated paper on Friday.

Ways to access grades.txt

Ways to access grades.txt

- Change permissions on grades.txt to get access

Ways to access grades.txt

- Change permissions on grades.txt to get access
- Access disk blocks directly

Ways to access grades.txt

- Change permissions on grades.txt to get access
- Access disk blocks directly
- Access grades.txt via web.mit.edu

Ways to access grades.txt

- Change permissions on grades.txt to get access
- Access disk blocks directly
- Access grades.txt via web.mit.edu
- Reuse memory after Frans's text editor exits, read data

Ways to access grades.txt

- Change permissions on grades.txt to get access
- Access disk blocks directly
- Access grades.txt via web.mit.edu
- Reuse memory after Frans's text editor exits, read data
- Read backup copy of grades.txt from Frans's text editor

Ways to access grades.txt

- Change permissions on grades.txt to get access
- Access disk blocks directly
- Access grades.txt via web.mit.edu
- Reuse memory after Frans's text editor exits, read data
- Read backup copy of grades.txt from Frans's text editor
- Intercept network packets to file server storing grades.txt

Ways to access grades.txt

- Change permissions on grades.txt to get access
- Access disk blocks directly
- Access grades.txt via web.mit.edu
- Reuse memory after Frans's text editor exits, read data
- Read backup copy of grades.txt from Frans's text editor
- Intercept network packets to file server storing grades.txt
- Send Frans a trojaned text editor that emails out the file

Ways to access grades.txt

- Change permissions on grades.txt to get access
- Access disk blocks directly
- Access grades.txt via web.mit.edu
- Reuse memory after Frans's text editor exits, read data
- Read backup copy of grades.txt from Frans's text editor
- Intercept network packets to file server storing grades.txt
- Send Frans a trojaned text editor that emails out the file
- Steal disk from file server storing grades.txt

Ways to access grades.txt

- Change permissions on grades.txt to get access
- Access disk blocks directly
- Access grades.txt via web.mit.edu
- Reuse memory after Frans's text editor exits, read data
- Read backup copy of grades.txt from Frans's text editor
- Intercept network packets to file server storing grades.txt
- Send Frans a trojaned text editor that emails out the file
- Steal disk from file server storing grades.txt
- Get discarded printout of grades.txt from the trash

Ways to access grades.txt

- Change permissions on grades.txt to get access
- Access disk blocks directly
- Access grades.txt via web.mit.edu
- Reuse memory after Frans's text editor exits, read data
- Read backup copy of grades.txt from Frans's text editor
- Intercept network packets to file server storing grades.txt
- Send Frans a trojaned text editor that emails out the file
- Steal disk from file server storing grades.txt
- Get discarded printout of grades.txt from the trash
- Call sysadmin, pretend to be Frans, reset his password

Ways to access grades.txt

- Change permissions on grades.txt to get access
- Access disk blocks directly
- Access grades.txt via web.mit.edu
- Reuse memory after Frans's text editor exits, read data
- Read backup copy of grades.txt from Frans's text editor
- Intercept network packets to file server storing grades.txt
- Send Frans a trojaned text editor that emails out the file
- Steal disk from file server storing grades.txt
- Get discarded printout of grades.txt from the trash
- Call sysadmin, pretend to be Frans, reset his password
- ... when should we stop thinking of more ways?

paymaxx.com (2005)

- <https://my.paymaxx.com/>
 - Requires username and password
 - If you authenticate, provides menu of options
 - One option is to get a PDF of your W2 tax form

paymaxx.com (2005)

- <https://my.paymaxx.com/>
 - Requires username and password
 - If you authenticate, provides menu of options
 - One option is to get a PDF of your W2 tax form
- <https://my.paymaxx.com/get-w2.cgi?id=1234>
 - Gets a PDF of W2 tax form for ID 1234

paymaxx.com (2005)

- <https://my.paymaxx.com/>
 - Requires username and password
 - If you authenticate, provides menu of options
 - One option is to get a PDF of your W2 tax form
- <https://my.paymaxx.com/get-w2.cgi?id=1234>
 - Gets a PDF of W2 tax form for ID 1234
- get-w2.cgi forgot to check authorization
 - Attacker manually constructs URLs to fetch all data

Layer interactions: naming

```
athena% cd /mit/bob/project  
athena% cat ideas.txt  
Hello world.  
...  
athena%
```

Layer interactions: naming

```
athena% cd /mit/bob/project
```

```
athena% cat ideas.txt
```

```
Hello world.
```

```
...
```

```
athena% mail alice@mit.edu < ideas.txt
```

```
athena%
```

Layer interactions: naming

```
athena% cd /mit/bob/project  
athena% cat ideas.txt  
Hello world.
```

...

```
athena% mail alice@mit.edu < ideas.txt  
athena%
```

Bob changes ideas.txt
into a symbolic link to
6.033's grades.txt

Summary

- Security is a negative goal – hard to achieve
 - Policy: desired goal
 - Threat model: assumptions about what can go wrong
- Guard model
 - Authentication
 - Authorization