RISE
Enable • Protect
Research-centric Information Security Enablement Program

BSD
Information Security Office
Cybersecurity
Newsletter

March 2016 SECURITY.BSD.UCHICAGO.EDU Volume 2, Issue 3

Computer for Ransom

Ransomware is a growing problem on both PC and Mac computers. As with other types of malware, you can avoid it by *never* installing software that you don't recognize or that didn't come from a reputable source. It's also another reason to regularly and frequently back up your files, so that hackers can't hold your valuable information hostage. Please read the following story about how Grant became a victim of a ransomware attack.

It wasn't like the movies. There was no note made from letters cut out of magazines, no phone calls to trace. No angry Liam Neeson, no team of eccentric detectives. When Grant shut down his laptop the previous night, it was working just fine. But this morning, when he booted up, something was definitely not right.

When he went to open the Word document he was working on yesterday, the file had a strange new suffix: ".encrypted." When he clicked on the file, he was prompted to enter a private key he had never heard of before. Even worse, every single file in his documents folder now had the same ".encrypted" added to the file name. And his photos. And his music. It was everywhere.

But one new object, a small .txt file, had mysteriously appeared in all of these folders. When he clicked on it, a simple text message explained that his files had been locked, and that they would be deleted in three days if he didn't pay $300 via a strangely garbled web address.

Grant couldn't believe it, and didn't know where to turn. He quickly ran a web search -- at least his browser was still working, he thought -- and discovered this was an increasingly common form of hacking, called ransomware. Further digging didn't provide much good news: the type of malware Grant's hacker used didn't have any known solutions, and unless he'd backed up his files, it was pay up or lose them forever.

The damage could be even worse, Grant found out. A hospital in Los Angeles had its computers infected with a similar program, and ended up paying $17,000 to the hackers. Grant felt lucky that at least it didn't happen on his work computer, where it could have gotten into the university's system.

Unfortunately, Grant's research also made it clear how the ransomware had gotten in -- articles said that most people got it from pirated software or...more personal downloads. That video game that he had downloaded a few nights ago from a less than reputable site turned out to be not so free after all, he thought in dismay, biting his lip and pulling out his credit card.

Protective Measures

- The STA-01-BSD Minimum Security Standards for Systems specify that all important data should be backed up to a BSD-approved network storage.
- Laboratory system admins must establish a regular, procedure to carry out and verify regular backups.
- Labs should document restoration procedures, and periodically execute trial restores to ensure data continuity.
- The Center for Research Informatics can help meet these standards by housing your data and preventing unauthorized access by outside parties and providing automatic backup services. For more on the CRI, visit http://cri.uchicago.edu.

New Information Security Policies

The BSD, UCM and University Information Security Offices have collaboratively developed a set of cyber security policy documents that will direct and guide our organizations through the new landscape of cyber security threats and regulations. The BSD and UCM Security Offices have undertaken this project with the support of senior leadership and are committed to establishing a single set of policies for use within both the BSD and UCM. Our goal is to replace the existing and outdated policies with a set of robust policies that will enable the organization to:

- Compete for new research opportunities and grants
- Safeguard patient, student and staff information
- Support critical business processes

The Organizations have 3 new policies available for review and comment:

- **System and Communications Protection Policy**
- **Data Classification Policy and Handling Procedures**
- **System and Information Integrity Policy**

How to review and comment:
To access the policy documents, go to the BSD Information Security Office Policies webpage and click on the Policy Name. You will receive a prompt to log in with either your BSDAD or UCHAD account (for BSDAD accounts, please login using the syntax "BSDAD\<username>" and your BSDAD password).

To comment on the policies, select "Open in Word" from the top left hand corner of the screen and use the Microsoft Word "Insert Comment" feature (on the Review tab, in the Comments group, click New Comment). To access this feature, highlight the section of text you would like to comment on, go to "Review" and select "New Comment." In the process of your review and commentary, we ask that you consider the following to guide your comments:

- Is the policy readable and understandable?
- Is the policy acceptable, or are there items of particular sensitivity that should be further considered?
- What advice would you give to implement the policy?

What to do if you become aware of an information security incident?

Contact the BSD ISO Team via email at security@bsd.uchicago.edu.