Your $$$ or your data

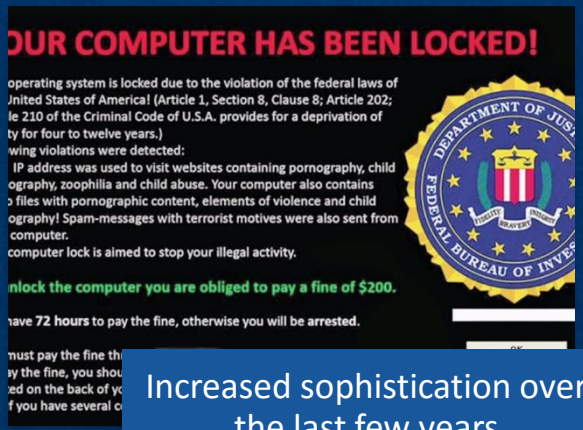
Protecting yourself against ransomware

(and a few other things while we have your attention)

Duke UNIVERSITY

What is ransomware?

Malware that encrypts files and demands a payment to unencrypt them



Increased sophistication over the last few years

Ransom costs vary and must be paid with “cryptocurrencies” like Bitcoin

Access is restored after payment … or not …

Duke UNIVERSITY

This is not new, and it affects everyone!

A single ransomware server could yield $33,600 per day in ransoms

The Town of Greenland, New Hampshire had a similar attack in 2014 that resulted in the loss of 8 years worth of electronic records

In 2015, the FBI received more than 2,400 ransomware complaints, which totaled $25M in damages

The City of Durham was recently the victim of a similar ransomware attack, but was able to quickly recover

Duke UNIVERSITY

Ransomware is popular

93% of phishing emai

Credit: Steve Traynor

As of the end of March, 93 percent of all p
contained encryption ransomware, accorc
released today

Cerber ransomware earns $2.3mil with 0.3% response rate

Credit: Bet_Noire / iStock

The fast-growing Cerber ransomware earned nearly $200,000 in July despite a payment rate of just 0.3 percent as a result of its affiliate distribution model, according to a new report by Check Point

MORE LIKE THIS


Cerber ransomware rakes in cash by recruiting unskilled hackers


The history of ransomware


93% of phishing emails are now ransomware

on IDG **Answers**
How does 5G compare to 4G and when will it be available?

[789% increase](#) in phishing over Q4 2015.

Duke UNIVERSITY

Can it happen here?

Yes … and it has!

- Small ransomware infections have occurred in some areas
- Fortunately, the damage has been limited…so far

Duke UNIVERSITY

Ransomware Attack - July 15, 2016

From: Francisca Hurley [mailto:Hurley.08@seeyouonskype.com]
Sent: Friday, July 15, 2016 4:43 AM
To: [redacted]
Subject: RE:

How is it going?
Please find attached document you asked for and the latest payments report

Hope that helps. Drop me a line if there is anything else you want to know

--
Warm regards,

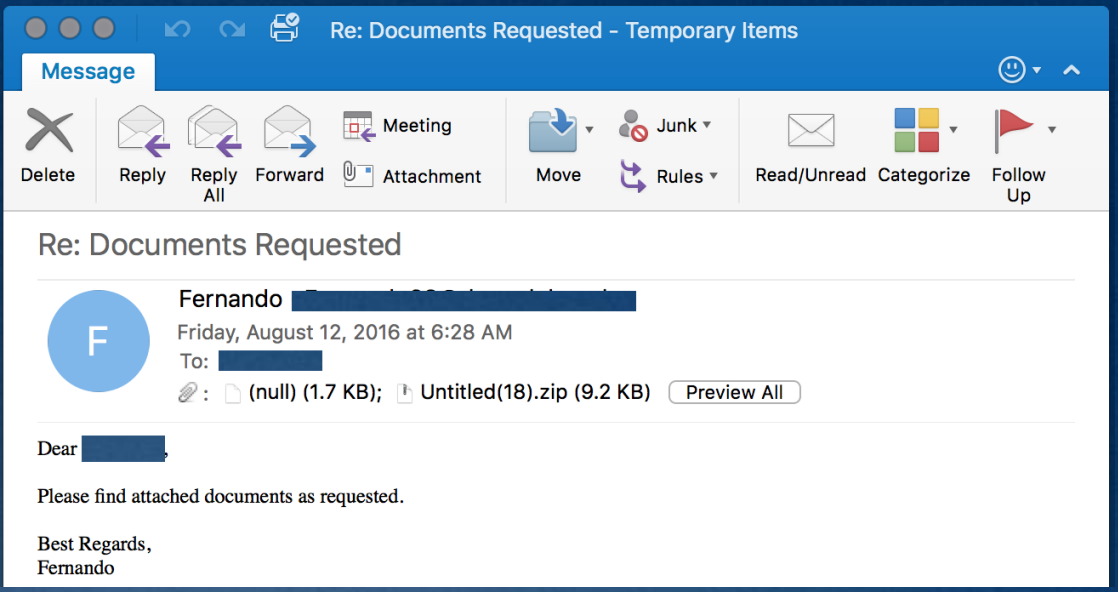
Francisca Hurley
IMMUPHARMA
Phone: +1 (304) 781-49-34
Fax: +1 (304) 781-49-70

[redacted].zip

- Made it through Proofpoint
- Seven people opened it
- Resulted in encryption of user workstations and a file share
- Zip file contained a windows executable
- Malware known as Zepto

Duke UNIVERSITY

Ransomware Attack – August 12, 2016



- Mail server did not make use of ProofPoint as an email gateway
- Resulted in encryption of user workstations and a file share
- Ransom demand was $2,000
- Malware was Zepto again

Duke UNIVERSITY

How can YOU prepare?

1. Patch and update all the things!
2. Use Symantec with:
   - Insight (file reputation)
   - SONAR (application behavior)
3. Don't open unexpected attachments
4. Avoid enabling macros when opening documents, unless you trust the source
5. Have good backups
6. Bonus: Run an adblocker (ublock origin).
7. Bonus: Remove Flash, Silverlight, Java, etc.

Note: Duke IT support teams, DHTS, and OIT are doing these things for many Duke computers.

But, this is the 21st century. Ransomware is all I have to worry about now, right?

Duke UNIVERSITY

Let's talk about your passwords

Passwords are a prime target for attacks:

- Malware
- Social Engineering
- Phishing
- 0-days

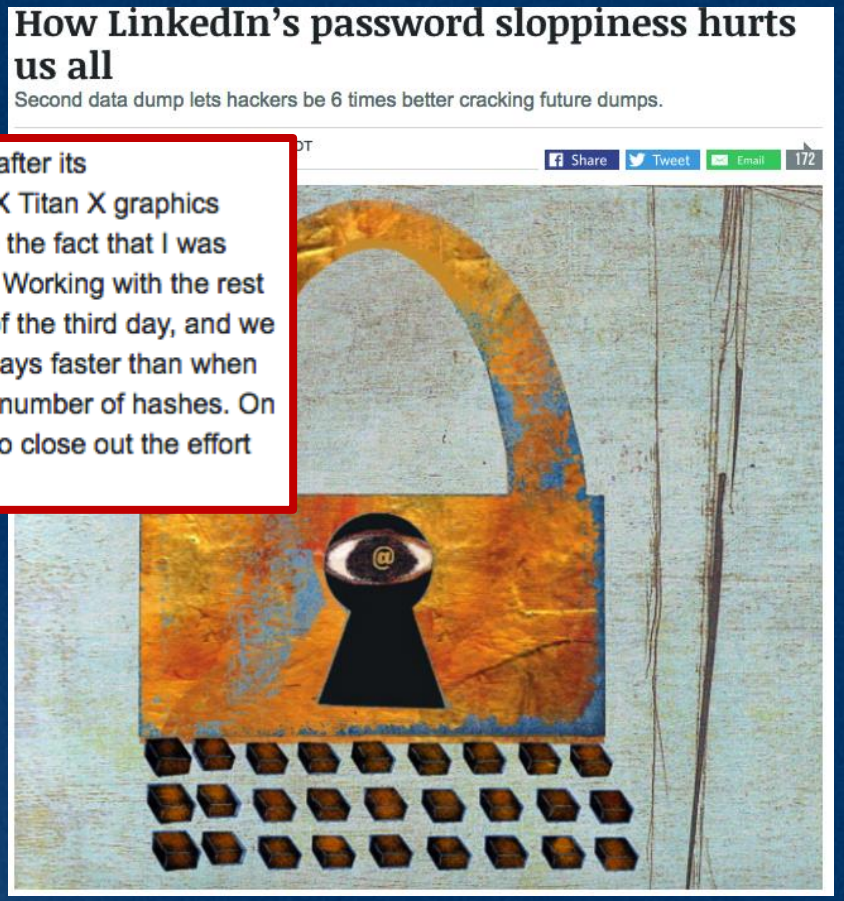
Reused passwords allow access other accounts. Attackers will:

- Take the information from the accounts
- Use the accounts to target others

Duke UNIVERSITY

Password mega-breaches: 1 billion and counting!

As in 2012, I was lucky to get my hands on this new LinkedIn data about a week after its announcement. Using a single Sagitta HPC Brutalis packed with eight Nvidia GTX Titan X graphics cards, I managed to recover 85 percent of the passwords on the first day, despite the fact that I was cracking so many passwords so quickly that the whole system slowed to a crawl. Working with the rest of the Hashcat development team, we managed to reach 88 percent by the end of the third day, and we crossed the 90-percent threshold on the fourth day. This all happened a full two days faster than when working with the first LinkedIn dump, which contained only a small fraction of the number of hashes. On the sixth day, we teamed up with rival password cracking team CynoSure Prime to close out the effort at a solid 98 percent, cracking a total of 173.7 million passwords.



Breaches include:

- MySpace (360 million users)
- LinkedIn (167 million)
- Tumblr (65 million)
- Twitter (32 million)
- Dropbox (68 million)
- Yahoo (400 million)

Duke UNIVERSITY

Password recommendations

- Don’t reuse passwords!
- Get a password manager (LastPass)
- Use multi-factor everywhere you can: https://twofactorauth.org
- Check “Leaked Source” regularly: https://www.leakedsource.com/
- Check “Breach or Clear” regularly: http://breachorclear.jesterscourt.cc/
- Subscribe to “Have I Been Pwned?”: https://haveibeenpwned.com/

Duke UNIVERSITY

USB Drive Risks

GEEK TECH

FOLLOW GEEK

SC Magazine > Blogs > The Data Breach Blog > Indiana University Health Arnett Hospital loses USB drive with 2

led malware-
of offices

Doug Olenick, Online Editor

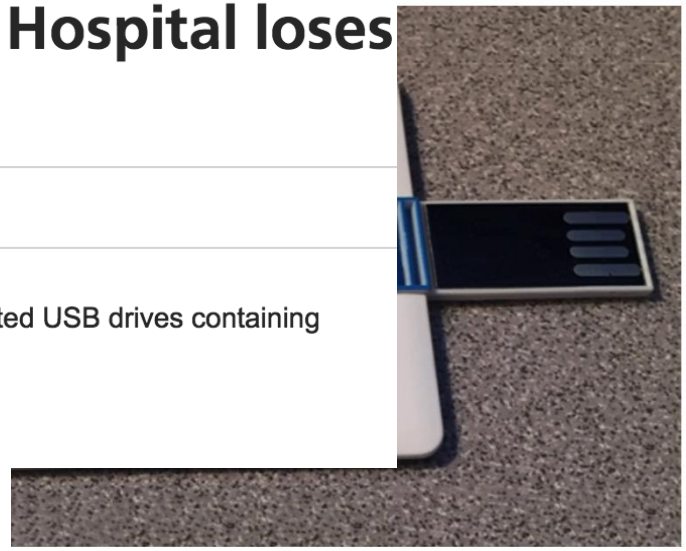
Follow @DougOlenick

January 11, 2016

0 SHARES

Indiana University Health Arnett Hospital loses USB drive with 29K records

Share this content:



DATA CENTER SOF

Indiana University Health Arnett Hospital reported the loss of an unencrypted USB drives containing information on 29,000 emergency room patients.

Security

How many victims? 29,324

Half of peo parking lot

Why do we even bother with security software?

11 Apr 2016 at 21:09, Shaun Nichols

527

A new study has found that almost half the people who pick up a USB stick they happen across in a parking lot plug said drives into their PCs.

Why USB Drives?

We recommend that you use Duke Box unless it does not work for your particular situation. For example, if you need to …

- Transfer data from one location to another where reliable Internet access is not available.
- Store or back up files during field work/travel where reliable Internet access is not available.
- Temporarily access your work on another computer where reliable Internet access is not available.

In these cases, we recommend the use of an encrypted USB flash drive to safeguard your work and Duke's data.

https://oit.duke.edu/comp-print/storage/flashdrives.php

Duke UNIVERSITY

Encrypted USB Drive Recommendations

Again, we recommend that you use Duke Box unless it does not work for your particular situation. If you need to use a USB drive, Duke Stores sells the the Kingston DataTraveler Vault Privacy USB drives, tested by Duke OIT and DHTS.

Key features of these drives include:

- Password required to access drive
- Drive self-erases after multiple failed passwords
- Read-only option to allow sharing of data without exposure to viruses or malware
- Multiple sizes, from 8 GB to 64 GB

http://www.dukestores.duke.edu/

Duke UNIVERSITY

Closing Thoughts

- Simple steps to protect yourself from MOST attacks
  - Apply software updates
  - Don’t click the bright shiny thing (or the unverified urgent thing)
  - Good password practices (Lastpass and multifactor)
  - Browser protections (adblocker, https everywhere)
  - Use encrypted USB drives
- Accept there are some things from which you can’t protect yourself
  - For these, have good backups!

Duke UNIVERSITY