THE RUSSIANS, YAHOO AND RANSOMWARE: A YEAR OF NETWORK SECURITY

David Carpenter
Huffman ISD
June 8, 2017
DNC HACK/GRIZZLY STEPPE
What Happened

- Two separate groups (APT 28 and APT 29) compromised the systems of the Democratic National Committee

- Both groups remained active in the systems for several months without being detected

- Attackers made off with a large number of emails and likely other data without causing any noticeable damage
How’d they do it?

- APT 29 used phishing campaigns with links to malicious files
- APT 28 used phishing campaigns to trick users into entering their credentials
What Can we Learn

- People are your weak point
- It may not be obvious you have been hacked
- Pay attention to what is leaving your network
- Be conscious of what you write down
YAHOO ACCOUNT HACK
What Happened

- This year Yahoo announced that in 2013 and 2014 they were hacked and account credentials were stolen.

- The first heist got 1 Billion User Accounts and the second 500 Million.

- All 1 Billion user account details (name, email, hashed password, security questions) were listed for sale for $200,000.
What’s that mean for Education?

- How much is your data worth?
Student Records - $4

★★★ ★★★ USA KIDS SSN - DOB YEAR 1998 UPTO 2015 [ALL STATES] ★★★

This listing is for USA Kids Profiles ( NO CC ). TAX Fraudsters knows the benefits of having children in the tax records when filing, here you are gents and sexy ladies, young american Kids and there parents if you want for you to make maximum profits on. SSN: DOB: First Name: Last Name: Address: City: State: Zip: Country + PARENTS info without SSN and DOB [First Name: Last Name: Address: City:]

Sold by TuttiFrutti_store - 3 sold since Mar 29, 2017
22 items available for auto-dispatch

★★★ ★★★ USA KIDS SSN + DOB 1998 UPTO 2016

★★★ 50% discount on my Hansa Market shop http://hansamkt2r6nfg3.onion/vendor/wakawaka/ ★★★ ----- READ FULLY BEFORE ORDERING------ . Welcome to our Listing. Please read till the END Before placing an order This listing is for USA Kids Profiles ( NO CC ), TAX Fraudsters knows the benefits of having children in the tax records when filing, here you are gents and sexy ladies, young american Kid...

Sold by wakawaka - 303 sold since Jun 25, 2015

Kids Fullz + SSN [] 1.5yrs - 15yrs ***Minimum order***

This listing is for Kids Fullz (First, Last, Address ZIP, DOB & SSN) 1.5yrs-15yrs. Looking listing: http://peach7bo6iu2pu.onion/listing.php?id=178641

Sold by Ramhart - 148 sold since Oct 19, 2016

KIDS SSN RANDOM - 1 days - USD +0.00 / item

Purchase price: USD 6.00

KIDS SSN RANDOM - 1 days - USD +0.00 / item

Purchase price: USD 9.00

Choose Below for DOB or GENDER Requests - 1 days - USD +0.00 / item

Purchase price: USD 9.00

Qty: 1

Buy Now

Buy Now

Queue

0.00022 BTC / 0.1247 XMR
ID Scans - $10
Value of a Student Information System

- 3,432 Current Students - $13,728
- 5,204 Former Students - $20,816
- 2,901 Staff Records - $2,901

$37,445

- How much are you spending to defend your Student Information?
THE RISE OF RANSOMWARE
What Happened

- In May Hundreds of Thousands of people in 150 countries were infected by WannaCry

- Britain’s NHS, FedEx, Telefonica, Renault, Deutsche Bahn and the Russian Interior ministry all experienced shutdowns

- WannaCry to date raked in $148,000
What’s this mean for Education?

- Patch your systems
- Signature Based Anti-virus is not sufficient any more
- Consider the entire emergency management cycle in your security plan
What’s this mean for Education?
What Happened

- Shadow Brokers is a hacking organization that found a cache of NSA hacking tools on a third party server they compromised
  - Never before seen exploits and tools are now for sale outright or available as a subscription with a few free samples available

- Vault 7 is the name of a cache of CIA hacking tools that WikiLeaks acquired
  - So far what has been released is mostly documents about hacking tools and vulnerabilities, not the tools themselves
What it means for Education

- You are more vulnerable than you know
- A sufficiently dedicated and well funded attacker cannot be stopped
- The right tools in the wrong hands could be disastrous
- Encryption works