01:090:101 Section 51 Hill 120 Tuesday, 3:20-4:40

02: How to get infected. Phishing. Spearphishing. d0xed game.
03: Discuss the game. Erasing data forever. Lying.
04: The web of you. Who has it? What can they do with it? Good practices. Class presentation description.
05: Class presentations picking. What can I do with a little bit of you? Why the web can lie forever – wikipedia.
06: Social media. What’s good and bad practices.
07: The other side of the curtain – what are the responsibilities of the holders of data?
09: Presentations, part 1 (randomly selected.)
10: Presentations, part 2 (randomly selected.)

Dr. Casmir Kulikowski (kulikows@cs.rutgers.edu)
Not-at-all-Dr. Charles McGrew (mcgrew@cs.rutgers.edu)
You are currently using Google Chrome to browse the web. An outdated video player may be slowing the browser’s performance.

We recommend that you update to the latest version.

- Watch HD movies online
- HD video performance with hardware acceleration of video
- Support for full screen mode with multiple monitors
- Bug fixes and security enhancements

Accept and Install
Unusual Activity

Your account access has been locked for security purposes.

To unlock your account access, click: Sign in to My Verizon and proceed with the verification process.

Thank you for using My Verizon.
Upon further analysis...

The mail came from "windstream.net" (somewhere in Alabama, Arkansas, Florida, Georgia, Kentucky, Minnesota, Mississippi, Missouri, Nebraska, North Carolina, South Carolina, New Mexico, New York, Ohio, Oklahoma, Pennsylvania, South Carolina or Texas), lying about who they were saying they were "mail1.com" (actually a google address).

The windstream address relayed it to mailartel.intra.ar-tel.it -- in Italy.

mailartel.intra.ar-tel.it sent it to "dragon.rutgers.edu" (cs mail server) - to me.

Note that it forged an email address expectation ('noreply@mail1.com')

... and, of course, it intended me to go off to a server in Poland to steal my credentials. (Which would have looked, on the face of it, as the verizon web site.)
Received: from [151.13.120.245] (HELO mailartel.intra.ar-tel.it)
  by dragon.rutgers.edu (CommuniGate Pro SMTP 6.0.9)
  with ESMTP id 118201454 for mcgrew@cs.rutgers.edu; Sat, 20 Dec 2014 15:06:45 -0500
Received-SPF: softfail
  receiver=dragon.rutgers.edu; client-ip=151.13.120.245; envelope-from=noreply@mail1.com
Received: from localhost (localhost [127.0.0.1])
  by mailartel.intra.ar-tel.it (Postfix) with ESMTP id B07FE38214C;
  Sat, 20 Dec 2014 21:06:29 +0100 (CET)
Received: from localhost (localhost [127.0.0.1])
  by localhost (mailartel.intra.ar-tel.it [127.0.0.1]) (amavisd-new, port 10032)
  with ESMTP id gOwmWZvb6Rdj; Sat, 20 Dec 2014 21:06:14 +0100 (CET)
Received: from localhost (localhost [127.0.0.1])
  by mailartel.intra.ar-tel.it (Postfix) with ESMTP id 69E07382138;
  Sat, 20 Dec 2014 21:06:14 +0100 (CET)
X-Virus-Scanned: amavisd-new at mailartel.intra.ar-tel.it
Received: from mailartel.intra.ar-tel.it ([127.0.0.1])
  by localhost (mailartel.intra.ar-tel.it [127.0.0.1]) (amavisd-new, port 10026)
  with ESMTP id BBd2q3qKZnnE; Sat, 20 Dec 2014 21:06:14 +0100 (CET)
Received: from mail1.com (h82.84.29.71.static.ip.windstream.net [71.29.84.82])
  by mailartel.intra.ar-tel.it (Postfix) with ESMTPA id 7293D3820D8;
  Sat, 20 Dec 2014 21:06:10 +0100 (CET)
Reply-To: noreply@mail1.com
Good News!

Your account access has been locked for security purposes. To unlock your account access, click: http://asenizacja.krakow.pl/wp-includes/js/jquery/ui/v1/index.html

Thank you for using My Verizon.

© 2014 Verizon Wireless
From: "Verizon Wireless" <noreply@mail1.com>
Subject: Unusual Activity
Date: 20 Dec 2014 15:07:26 -0500
Message-ID: <20141220150726.753D7B86A9897984F@mail1.com>
MIME-Version: 1.0
Content-Type: text/html; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<html> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>Good News</title> </head> <body>
<table border="0" cellspacing="0" cellpadding="0" align="center" width="640">
<tbody><tr>
<td width="636" height="661" align="left" valign="top"><table border="0" cellspacing="0" cellpadding="0" width="91%">
<tbody><tr><td width="100%"><table border="0" cellspacing="0" cellpadding="0" width="100%"><tbody><tr><td width="95%"><img src="http://asenizacja.krakow.pl/wp-includes/js/jquery/ui/v1.png" width="223" height="41" border="0" /> <br><br></td></tr></tbody></table></td></tr></tbody></table></td></tr><tr><td><img src="http://asenizacja.krakow.pl/wp-includes/js/jquery/ui/v1.png" width="636" height="65" /></td></tr><tr><td><table width="100%" cellspacing="10" border="0" cellspacing="0" cellpadding="0"><tbody><tr><td width="100%" align="left" bgcolor="#FFFFFF"><table border="0" cellspacing="0" cellpadding="0" width="100%">
<tbody><tr>
<td width="637" height="117" valign="top"><table border="0" cellspacing="0" cellpadding="0">
<tbody><tr>
<td><b><font face="arial" size="2">Your account access has been locked for security purposes. To unlock your account access, click: <a href="http://asenizacja.krakow.pl/wp-includes/js/jquery/ui/v1/index.html">Sign in to My Verizon</a> and proceed with the verification process.</font></b></td></tr>
<tr><td>&nbsp;</td></tr>
<tr><td><font face="arial" size="2">Thank you for using My Verizon.</font></td></tr>
<tr><td>&nbsp;</td></tr>
</tbody></table></td></tr></tbody></table></td></tr><tr><td><br><br>A9 2014 Verizon Wireless</td></tr></tbody></table></td></tr></tbody></table></td></tr><tr><td><table border="0" cellspacing="0" cellpadding="0" align="center" width="100%">
<tbody><tr><td align="center"><font face="arial" size="1">© 2014 Verizon Wireless</font></td></tr></tbody></table></td></tr></tbody></table>&nbsp;
Ever get one of these?

Subject: LOOKING FOR PARTNERSHIP IN BUSINESS

Engr David Koni.
(BOARD OF CONTRACT AWARD COMMITTEE.)
Cotonou Republic Du Benin.

Sir/Madam,

It is my great pleasure to write to you and present my business proposal for your consideration and possible acceptance which you will find mutually beneficial to both parties.

I am Engr. David Koni, the Chairman of the Contract Award Committee, Cotonou Republic Du Benin W.Africa, We need a trust-worthy partner to assist us in the transfer of (US$11,5M) ELEVEN MILLION, FIVE HUNDRED THOUSAND UNITED STATES DOLLARS for further investment in your country,

You will be required to:
(1) Assist us in the transfer of this sum to your bank account in your Country.

(2) Advise on areas for potential future investment in your country

(3) Assist us in carrying out the feasibility study before actual investment. If you decide to render your service to us in this regard, you will be paid 20% of the total funds for assistance. Reply back this email if you are willing to work with us.

Respectfully,
Engr. David Koni.
Chairman Contract Award Committee {BCAC}
... the Spanish Prisoner cropped up in the aftermath of the French Revolution. It went like this: A letter arrived describing an aristocrat in exile, say, the Marquis de _______, who in escaping from revolutionary violence had thrown a chest full of jewels into a lake. His faithful servant, now writing this heartfelt letter, had come back to retrieve it and unfortunately ended up in prison. With just a little help from you, a fellow Frenchman, to aid in the servant’s bail or escape, you’d earn a portion of the loot. The scheme worked: “Of a hundred such letters” sent by French confidence tricksters, “twenty were always answered,” wrote Eugène Vidocq, the French criminal turned detective.

Search Request

• www.amazon.com

• I am Angus Q. Customer, auto purchase allowed.

• Give me search results for “Buckaroo Banzai”
Reply from Amazon.com

• “The Adventures of Buckaroo Banzai” (price, graphic, rating, etc.)
• “Adventures of Buckaroo Banzai Across the 8th Dimension” (etc.)
• “The Adventures of Buckaroo Banzai Across the 8th Dimension (etc.)
• “Astronomy 101 Collection” (huh?)
• More of permutations on BB.
• Big Trouble in Little China (why?)
• “Cherry 2000”
• “Ice Pirates”
• Lots more
The Adventures Of Buckaroo Banzai • 1984  PG  CC

Shop Instant Video
$2.99 - $14.99
Rent or Buy movie
Watch instantly on your PS3, Xbox, Kindle Fire, iPad, PC and other devices.

Adventures of Buckaroo Banzai Across the 8th Dimension • 1984
Blu-ray
$19.17  $37.99  Prime
Only 19 left in stock - order soon.
More Buying Choices
$14.77 used & new (16 offers)

The Adventures of Buckaroo Banzai Across the Eighth Dimension • 1984  PG
DVD
$50.99  Prime
Only 15 left in stock - order soon.
More Buying Choices
$6.97 used & new (55 offers)

See All Formats •

Astronomy 101 Collection • 1987  PG
DVD
Killer Klowns from Outer Space / Spaceballs / The Adventures of Buckaroo Banzai Across the Eighth Dimension
$12.47  $19.98  Prime
Only 6 left in stock - order soon.
More Buying Choices
$0.49 used & new (48 offers)

The Adventures of Buckaroo Banzai Across the 8th Dimension • 1984  Unrated
Blu-ray
The Adventures of Buckaroo Banzai Across the Eighth Dimension - NON-USA FORMAT, Blu-Ray, Reg.B Import - Germany
$19.60 used & new (13 offers)

See All Formats •

Adventures of Buckaroo Banzai Across the 8th Dimension DVD
DVD
Region 0 Pal Import
Send to Amazon

• Buy me the 2\textsuperscript{nd} one on the list. Here’s my credit card number 9890767465897907

• Expiration date is 10/2017
Answer from Amazon

• Okeedokee!
Hi, amazon, I’m about to send you a request, using the encryption method I will mention, but you should use the decryption side of a public/private key thingie we both know about already. Here’s my public key.

- Jdflkajdfljajfjdjal;jfl;ajdf;ljdf;ljafl;jouy9ru1034urio fh9f8u1-98yru-30fj09fh-30jpih02 ejfn efyu31pejf9 fuj30pfn93jfp39enf93ufp93oufhpioehfpoqwhpo
Presearch, Amazon replies

• Got it. Here’s mine

• Lfkjaj;djf9 -13u10d bocgckoas l;dbcjvq0u[sdbciuousdc[pdib 08qed99u0qvbsdcj908cv809eifn oinpaiosdghc0qwoehubfnpiqwudjncpoqf
Public Key and Private Keys

The Public and Private key pair comprise of two uniquely related cryptographic keys (basically long random numbers). Below is an example of a Public Key:

3048 0241 00C9 18FA CF8D EB2D EFD5 FD37 89B9 E069 EA97 FC20 5E35 F577 EE31 C4FB C6E4 4811 7D86 BC8F BAFA 362F 922B F01B 2F40 C744 2654 C0DD 2881 D673 CA2B 4003 C266 E2CD CB02 0301 0001

The Public Key is what its name suggests - Public. It is made available to everyone via a publicly accessible repository or directory. On the other hand, the Private Key must remain confidential to its respective owner.

Because the key pair is mathematically related, whatever is encrypted with a Public Key may only be decrypted by its corresponding Private Key and vice versa.

For example, if Bob wants to send sensitive data to Alice, and wants to be sure that only Alice may be able to read it, he will encrypt the data with Alice's Public Key. Only Alice has access to her corresponding Private Key and as a result is the only person with the capability of decrypting the encrypted data back into its original form.
Search Request

• www.amazon.com

• I am jsalfjlsdfopfadjadjo912ru019287wueiosdj
• I have the ability to aldjfaldflnvkv9hlklal

• Please search for adjflajdl;ajdoanerh09y9udv
Amazon Reply

• Your answer is

• aflJOIJPOJoipojPOIJNklnkgUgfiuoigOllkbuYGhlkhLKbnbKJBLKhoiughOlInlknOlg87yiohbjHvbiUgObl0OhLJhvUihIlUgLKbhKhpoJ98y8hiY980hiB Ngh;bOlgoihlkBlknpo8Y85876rt566YigjkhI;m’,

• ‘,lhjiGYiugiHiogtUFGoihJPOy9876rutD67rt7CVt d lhGFIOUh
Customer Sends

- I want to buy (**&YU()&IHKKHKHLJHKOH

- My credit card is
  *OUOPUYOUKJKGHUYTUTIHIUOIUPOIU

- Expiration is (**&())*POY(YHIGJHohhhklhgiughh

- Address is
  8(**&9079sfyidfhkahiahioiahoajhoahhdoadfpouap ouadpofuadpofuapsodifjpodijfpoas
Amazon replies

- alkdjhasdjpa8yv9asdkhbkvljnvlk
After Two Days of Internet Problems, Rutgers Admits Its Computer Network Was Attacked

University is Only Saying it Did Not Detect a Breach of Confidential Information

NEW BRUNSWICK, NJ
—An email sent at 2:29pm on March 29 was the first official communication that tens of thousands of students got from Rutgers University, after more than two days of service interruptions involving the school’s computer network.

The university acknowledged its network was the victim of a cyber-attack that took down internet service in dormitories, and rendered many online services used by students and staff unusable. Shortly after 1pm, the main Rutgers University website had been taken offline for at least 15 minutes.
Arizona State, Rutgers battle web blockages a week before finals

By Jenny Ung, Arizona State University  May 4, 2015 2:41 pm

As students rush to finish up assignments during the week before finals, two apparent Distributed Denial of Service attacks (DDoS) blocked web access to both Arizona State University (ASU) and Rutgers University systems.

Both ASU and Rutgers are working to make appropriate accommodations to students affected by the situation, such as asking faculty to extend deadlines and change final exam dates.

But not all professors are on board, according to Chris Broom, an Arizona State University student completing his courses remotely from Seattle, Wash. While his Women's History professor did not make exceptions to the outage, his African American Literature professor gave the class three
Regarding DDoS Attacks On Rutgers  by exfocus in rutgers

anonimize yourself

permalink  context  full comments (23)

DDoS On Rutgers Again  by exfocus in rutgers

not nice

permalink  context  full comments (14)

exfocus ddos moar pls?  (self.rutgers)

submitted 5 months ago by exfocus to /r/rutgers

permalink  context  share

DDoS On Rutgers Again  by exfocus in rutgers

sry

permalink  context  full comments (14)

DDoS On Rutgers Again  by exfocus in rutgers

:(

permalink  context  full comments (14)
Regarding DDoS Attacks On Rutgers by exfocus in rutgers

- anonymize yourself

DDoS On Rutgers Again by exfocus in rutgers

- not nice

exfocus ddoes moar pls? (self.rutgers)

DDoS On Rutgers Again by exfocus in rutgers

- sry

DDoS On Rutgers Again by exfocus in rutgers

- :(  

DDoS On Rutgers Again by exfocus in rutgers

- sorry, my stop command doesn't work... my bots's uplinks get saturated while attacking and don't receive the stop attack cmd. most are not full duplex smh
On Monday morning, Rutgers University was still trying to recover from a distributed denial of service (DDoS) attack that had been launched against it over the weekend, according to media reports. The attack, which began on Friday afternoon, interrupted Internet service for Rutgers.
Rutgers adopts ‘emergency grading’ policy due to cyber attack

By Dan Alexander May 1, 2015 6:38 AM

With final exams set to begin, the Rutgers University Information Technology team says they have successfully ended “persistent” cyber attacks that have crippled the school’s internet network.

A Friday morning update posted on the Office of Information Technology’s website reported that “network services are continuing to return to normal.”

However, in an email sent to students and staff just before 12 noon from Chancellor Richard L. Edwards, Ph.D. was not as optimistic. “While we are optimistic that our IT teams will resolve this situation soon, I have been working with the academic deans to assist our faculty in preparing contingency plans to minimize the impact potential further disruptions may have on your coursework this semester, focusing, in particular, on courses that plan to offer online exams or those that rely heavily on online resources for final assignments,” wrote Edwards.

Chancellor Nancy Cantor and Provost Todd R. Clear of the Rutgers Newark campus announced an emergency grading policy for the spring semester. In an online post Thursday, they said the move is aimed at preventing students’ grades from being “victimized” by the Denial of Service (DDoS) attacks that have
Rutgers Hit With DDoS from China and Ukraine

Posted: Apr. 02nd, 2015 at 2:55 pm under Watch Desk

Rutgers University suffered a widespread distributed denial-of-service (DDoS) attack against its servers on March 27 to 30 coming from botnets in China and Ukraine. The attack took down the university's secured and unsecured wireless networks, the online learning platform, and the university's home webpage.

The university sent out an email to students and staff saying, “The first attack started around noon on the 27th. Since the initial attack, there have been multiple follow-up attacks. The attacker(s) are focusing on one service for a while, then another, then another. OIT has addressed each attack as it was detected (detection was immediate in each instance), but as fast as we fix one service, the next gets hit. Sakai [the Rutgers online learning platform], CAS (authentication), and the dorms have been targeted by the attacker(s). Other services have also been affected. The attacks are coming from China and eastern Europe.”

“Overall, the students and faculty were very frustrated with the situation,” said Rutgers senior Ishani Sen. “Many of us have exams around this time and couldn't prepare properly. Many professors had to give students extensions or push exams back in order to deal with the problem.”

The attack comes shortly after the university announced a new $1.95 million grant from the federal government to fund a homeland security study program.
Why did Exfocus Take Down Rutgers? An Interview & Analysis

Since Friday, March 27th Rutgers students have been experiencing intermittent service interruptions. Students have been unavailable to access Rutgers related websites including Sakai, Ecollege and others.

In the interim, a mysterious figure who goes by the handle Exfocus (or @ogexfocus) has popped up on Twitter and the /r/Rutgers subreddit claiming credit for the interruptions & inaccessibility for much of the Rutgers community.

His first post to Reddit consisted of a cryptic interface showing the bandwidth output of his “botnet” (an army of compromised computers which do their masters’ bidding).
Here is an abridged & cleaned up version of our conversation with this shadowy figure.

*How much are you getting paid?*

$500 an hour.

*Are you for real? Why would you do an interview with us if you’re getting paid?*

Normally I don’t show myself, but the entity paying me has something against the school. They want me to “make a splash”.

*Have you compromised any servers? To what extent?*

In Rutgers itself? No. I have hundreds of exploited servers though. I’m connecting through a proxied one right now in fact.

*On your twitter account, you posted some super private information including Social Security numbers & addresses. Where did those come from?*

The ssn dump was from a school in Texas. Not from Rutgers. : I haven’t been ddosing anything for a while now, I stopped three hours ago.

*Why can’t students access Sakai right now – if you’re not DDOSING it?*

Your internet is down because RU is probably scared about overages with their transit provider. Whenever I do a ddos all rutgers websites that are still public facing (like rutgers.edu) go offline because their network port with
Rutgers University to Spend $3 Million on Cybersecurity

Following a spate of recent cyberattacks targeting the university last year, officials now say Rutgers University is expected to spend up to $3 million on cybersecurity this year.

Rutgers University was targeted at least four separate times during the last school year, and the school has hired multiple cybersecurity firms to help secure their networks and computer systems against more cyber attacks, reports NJ.com.

The information was made available through documents gathered due to New Jersey’s Open Public Records Act. The firms involved are tasked to run a Threat Assessment Test of the university’s
What really happened?

• Doofus sent 60Gb/sec from a (purchased) network of zombies
• Old ISP couldn’t deal with it, dropped rutgers as a source and destination (why?), and turned away all traffic to/from it. Suddenly we’re off the net.
• New ISP could deal with it (and react to DDOS-type attacks before the traffic gets near rutgers. We’re on the net!
What to remember

• The doofus bought his “weapons” from organized crime. He’s no more a ‘hacker’ than I am. He didn’t ‘outsmart’ anyone, or “stick it to the man”, or be a modern incarnation of “Neo”, or any of that. He’s just a doofus.

• He did it for money. He’s a criminal-for-hire. Hired by someone who had enough money to try and buy his or her way out of not being ready for finals. And he or she decided that damaging everybody else’s chances of graduating was entirely uninteresting; that everyone else was far less important than she or he was. And the doofus helped.

• Doofus didn’t make anything like what he says he did on the deal, he’s just bragging (to raise his price later.) Either that, or the person that hired him is really, really stupid. (Which is, based on the evidence, quite possible.)

• This could have happened to any of our old ISP provider’s customers, and we’d have been just as affected.

• This kind of thing happens all the time (github, Sony, MIT, Penn State, Xbox, “Wurm Online”…)

• When your machine is hacked, normally nothing seems to happen. But it goes into someone’s back pocket, to be used when he or she wants to damage someone. For money.

• http://www.digitalattackmap.com
Current Efforts - Google

GFE = Google Front End Server

SSL Added and removed here!

Traffic in clear text here.
Next Week

D0x3d (or whatever its called)

Have a look at

http://www.cs.rutgers.edu/~mcgrew/Byrne/

For rules and examples