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 elements. 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. Casimir Kulikowski (kulikows@cs.rutgers.edu)
Not-at-all-Dr. Charles McGrew (mcgrew@cs.rutgers.edu)
The Hack Yesterday

“...Despite these enhancements, today’s attack, which lasted from about 10:00 a.m. until mid-afternoon, was disruptive and annoying. We apologize for any inconvenience.

You should know that we are working with state and federal law enforcement officials on this matter.”

From what we’ve (LCSR) have seen, it was an attack on every (reachable) Rutgers machine individually at once.
FROM

<table>
<thead>
<tr>
<th>Country</th>
<th>Country</th>
<th>Country</th>
<th>Country</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Norway</td>
<td>India</td>
<td>Russia</td>
<td>Moldova</td>
<td>Poland</td>
</tr>
<tr>
<td>Taiwan</td>
<td>Indonesia</td>
<td>Brazil</td>
<td>Mexico</td>
<td>Romania</td>
</tr>
<tr>
<td>Spain</td>
<td>Chile</td>
<td>Italy</td>
<td>Thailand</td>
<td>Uruguay</td>
</tr>
<tr>
<td>Portugal</td>
<td>Ukraine</td>
<td>Bulgaria</td>
<td>Philippines</td>
<td>Turkey</td>
</tr>
<tr>
<td>Israel</td>
<td>Serbia</td>
<td>Columbia</td>
<td>Cambodia</td>
<td>Argentina</td>
</tr>
<tr>
<td>Paraguay</td>
<td>Bolivia</td>
<td>Curacao</td>
<td>Kenya</td>
<td>Greece</td>
</tr>
<tr>
<td>Andorra</td>
<td>New Zealand</td>
<td>Sweden</td>
<td>Malaysia</td>
<td>France</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Ireland</td>
<td>Macedonia</td>
<td>Bangladesh</td>
<td>South Africa</td>
</tr>
<tr>
<td>Canada</td>
<td>Japan</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

... And of course, the US of A. At least.
....so a different attack from last time

• Rather than attack specific services to try and put them out of action and trigger a multi-day cutoff by the Internet Provider...
• Attack every known host, and overwhelm the services by making it (apparently) harder to choke off, and hopefully trigger a multi-day cutoff by the Internet Provider.
• Worked for about three hours; the amount of time we’ve had outages for a downed telephone pole on River Road in the past.
• “burned” (exposed as infected) a LOT more attacking hosts than last time.
• No finesse at all. Not a rapier; a brick.
It was the second time in one week the popular site went down.

Facebook restored access to its social media website after a 40-minute outage on Monday, the second time in a week that the site went down.

Users saw an error message that read "Sorry, something went wrong. We're working on it and we'll get it fixed as soon as we can."

Company shares were down nearly 4% at $89.25 (£58.83) shortly after the site went down. It also crashed on Thursday.

The social networking site is used by nearly 1.5 billion people worldwide.

Dave Lee, BBC North America technology reporter

Alright, alright - the world is still spinning.
What can we draw from this?

• If I could cause Facebook to cut out for even a short amount of time, and know that the stock will go down as a result, what can I do?

• Is Facebook fragile?
I know the stock will go down, so...

• Profit #1 – sell short

• “Selling short” is a deal you make with your broker to ‘loan’ you a stock (from their own inventory), which you then sell, with the proviso that you will buy it back and return it to the broker (typically in a short time-frame)

• If the stock goes down, you can buy it at the (new) lower price, return it to the broker, and keep the difference.

• Believe it or not, this is legal.
I know the stock will go down, so...

• Profit #2 – blackmail

• I tell facebook that I can crash them at will, and make them believe it (by, for instance, crashing them for 40 minutes.)

• I tell them I can do it at will and often, unless they pay me not to (a.k.a. “protection money”)

I know the stock will go down, so...

- Profit #3 – help a competitor

- I tell facebook’s competitor that I can crash them at will, and make them believe it (by, for instance, crashing them for 40 minutes.)

- I tell them I can do it at will and often, and the competitor will pay me to make facebook look bad, to the competitor’s advantage.

- Of course, facebook doesn’t really have a major competitor at the moment.
... and another way to get hacked

Yet another pre-installed spyware app discovered on Lenovo computers

A factory refurbished Thinkpad shipped with Windows 7 and a scheduler app that ran once a day, collecting usage data about what you do with your computer and exfiltrating it to an analytics company.
Don’t break in, \textit{start} in

- Windows installer, it turns out, will (intended for anti-theft mechanisms) copy executables from the ‘firmware’ at install time.
- Lenovo put spyware on that would keep track of what you were doing, and send it to an “analytics company” (‘Omniture’) once a day.
- If you reinstall windows entirely, it comes back!
Class Presentations

• Find something interesting in the way of computer security. An incident from the past, or current events, or even a science-fictional story (*not one you wrote*)
• Research it, with the intention of writing a one or two page abstract of the event
• Present it to the class. 10 minutes at most.
• Be interesting!
Next week...

• Present one-sentence description of what you’ve come up with.
• If it’s not good enough, we’ll give you something.
• If you don’t come up with anything, we’ll give you something harder.
• Play the game.
Cover at least

• Who was hacked?
• Whose information/money was stolen
• How did it work?
• Were they caught?
• Was anything changed because of it?
• Could it happen again?
Adblocking

- Nobody likes to look at ads
- Ads allow web providers to painlessly (more or less) pay for what is to the users free (except the tax-of-time for ads)
- Blocking ads costs website publishers revenue, but speeds up web-browsing for readers.
- Most everybody ‘self-edits’ out ads they don’t want to look at anyway. We recognize ads as ads, and decide for ourselves whether to ‘block’ them from our attention.

- So are ad-blockers a good idea, on balance?
A new(ish) way of intrusion detection

• Most intrusion detection is a look-at-a-packet-and-decide (based on rules) to alert somebody
• This works to spot infected machines ‘checking in’ with a control node, for instance, or specific kinds of attacks.
• How about a more ‘contemplative’ approach, using a GPU to allow massive parallelization of the traffic analysis?
• This might allow us to do traffic-over-time analysis to spot port-scanners, or attacks directed at specific hosts, or types of services.
Is it a good idea?

• Well?