UMBC

AN HONORS UNIVERSITY IN MARYLAND

Beware of Exploit Kits!

Charles Nicholas
nicholas@umbc.edu
Department of Computer Science and Electrical Engineering

May 2023

Malware Since PMA

- Since the textbook was published, some things have changed
- Ransomware!
- Cryptominers!
- Exploit Kits!
- Exploit Kits can and do distribute cryptominers and ransomware!

Beware of Exploit Kits!

- User is tricked into visiting an infected (but innocent) web site
- Or attacker simply buys ad space , which is called "malvertising"
- As a result of a few iframe redirects, such as
  `<iframe src=http://badGuys.Rus.ru>`
  the user's browser is sent to an EK web site
- Or a "302" redirect (like a 404 error, but more "helpful") see Demystifying

Beware of Exploit Kits!

- A Javascript “landing page” is loaded,
  - Fallout EK example
- Which looks at user’s box and tries some exploits
- If any succeed, word is sent back to EK operators, some of whom have grown wealthy

Famous Exploit Kits

- Black Hole was once the most famous, but there are many others: Angler, Sweet Orange, Redkit, Nuclear, RIG, Fiesta, Magnitude, etc.
- EK activity is not getting as much press, but they're still out there! RiG and Magnitude are still going strong!
- Note that just black-listing infected web sites is not sufficient, as they change all the time
- How can we tell when new EKs come out?

Who Uses EKs?

- Popular among cybercriminals
- Who prefer to keep a low profile, and deal with trusted affilicates
- “Malware as a Service” (a form of SaaS) is a business model
- See “Exploit Kit Payloads by Type” page 3 CTA

  The top exploited vulnerability in 2018 was CVE-2018-8174 a Microsoft Internet Explorer vulnerability nicknamed “Double Kill,” which was included in four EKs (RIG, Fallout, KaiXin, and Magnitude)

How Do They Work?

- Vulnerabilities in Adobe, MS, WordPress ☹ and others are found all the time
- EK operators watch the CVEs, and implement (or buy or steal) exploit code
  - CVE web site
- It’s hard for everybody to keep everything patched
- Palo Alto’s Unit 42 has a report

Active EKs

- The source code for RIG was released in 2015
  - But I can't find it ☹
  - Lacking that, here's a good explanation of RIG (link)
- The Lord EK has been analysed
- The Capesand EK has been analysed
- A relatively recent overview from MalwareBytes

Current Questions

- Is there a better way to do patches?
  - There must be!
- Can browsers be smarter about detecting Javascript that is being too nosey?
- Can we get rid of Javascript?
  - Many wish this was true

Some Older Research
if I have time to talk about it

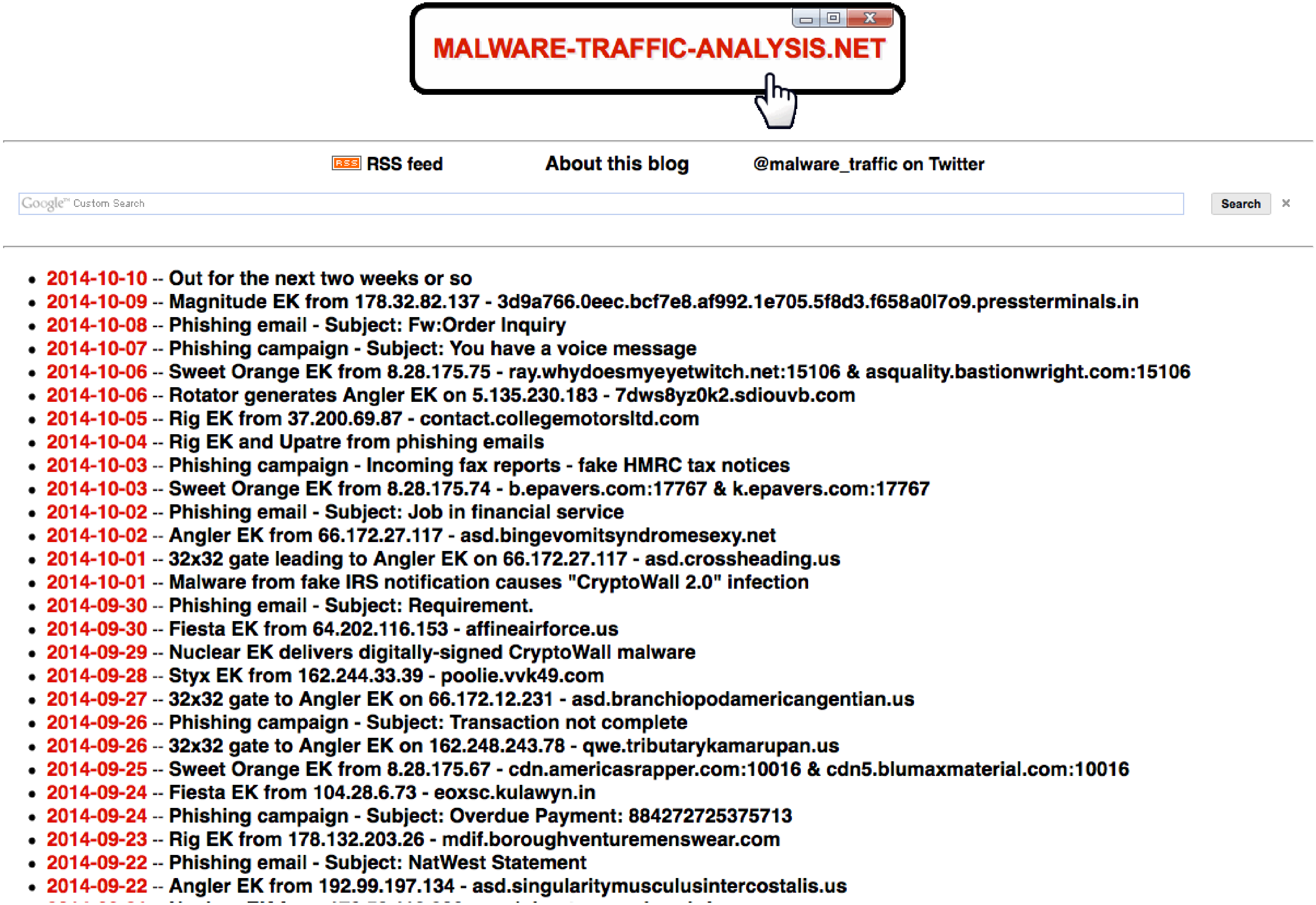
- Let’s capture some landing pages,
- And see if there are patterns in the Javascript that we can identify with known EKs

Our Hypotheses

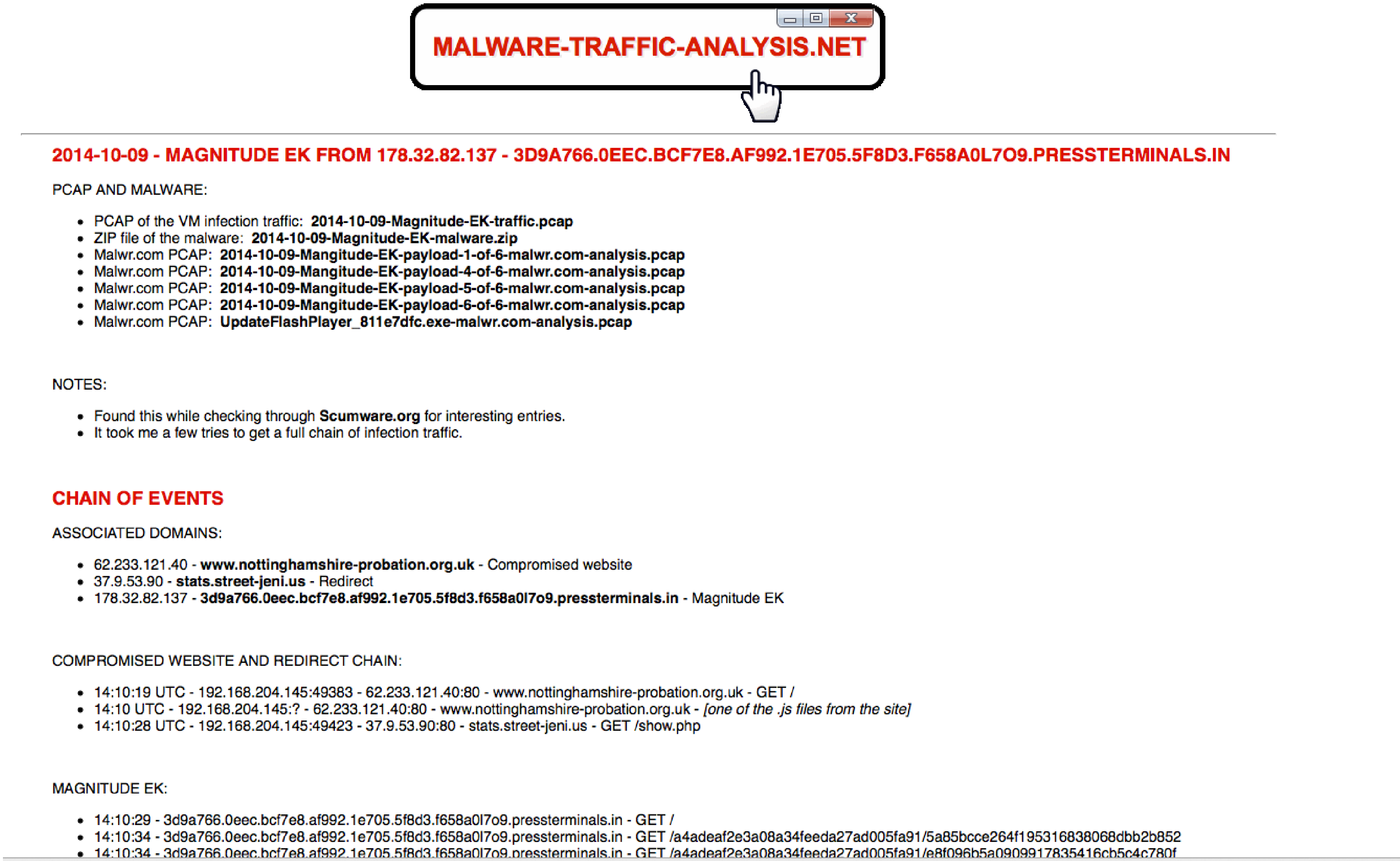
- If the Javascript code on landing pages corresponds to specific exploit kits, then similar scripts would be attributable to the same (or related versions of the same) exploit kit.
- Exploits may be updated from time to time, infrastructure maybe less often
- Scripts unlike any seen before may indicate a new, unknown exploit kit.
- This *landing page analysis* may let us better understand this form of malware.

Concept of Operations

- *Seek out* malware domains (live external links)
  - urlquery.net was useful to start
  - Or malware-traffic-analysis.net
- Visit infected sites from a browser inside a VM
  - EK would often be cleaned up by time we visit ☹
- Capture and re-assemble packets
  - Virtualbox packet capture, Suricata
  - Analyze raw pcap data, or tcpick output, or extracted Javascript



- 2014-10-10 -- Out for the next two weeks or so
- 2014-10-09 -- Magnitude EK from 178.32.82.137 - 3d9a766.0eec.bcf7e8.af992.1e705.5f8d3.f658a0l7o9.pressterminals.in
- 2014-10-08 -- Phishing email - Subject: Fw:Order Inquiry
- 2014-10-07 -- Phishing campaign - Subject: You have a voice message
- 2014-10-06 -- Sweet Orange EK from 8.28.175.75 - ray.whydoesmyeyetwitch.net:15106 & asquality.bastionwright.com:15106
- 2014-10-06 -- Rotator generates Angler EK on 5.135.230.183 - 7dws8yz0k2.sdiouvb.com
- 2014-10-05 -- Rig EK from 37.200.69.87 - contact.collegemotorsltd.com
- 2014-10-04 -- Rig EK and Upatre from phishing emails
- 2014-10-03 -- Phishing campaign - Incoming fax reports - fake HMRC tax notices
- 2014-10-03 -- Sweet Orange EK from 8.28.175.74 - b.epavers.com:17767 & k.epavers.com:17767
- 2014-10-02 -- Phishing email - Subject: Job in financial service
- 2014-10-02 -- Angler EK from 66.172.27.117 - asd.bingevomitsyndromesexy.net
- 2014-10-01 -- 32x32 gate leading to Angler EK on 66.172.27.117 - asd.crossheading.us
- 2014-10-01 -- Malware from fake IRS notification causes "CryptoWall 2.0" infection
- 2014-09-30 -- Phishing email - Subject: Requirement.
- 2014-09-30 -- Fiesta EK from 64.202.116.153 - affineairforce.us
- 2014-09-29 -- Nuclear EK delivers digitally-signed CryptoWall malware
- 2014-09-28 -- Styx EK from 162.244.33.39 - poolie.vvk49.com
- 2014-09-27 -- 32x32 gate to Angler EK on 66.172.12.231 - asd.branchiopodamericangentian.us
- 2014-09-26 -- Phishing campaign - Subject: Transaction not complete
- 2014-09-26 -- 32x32 gate to Angler EK on 162.248.243.78 - qwe.tributarykamarupan.us
- 2014-09-25 -- Sweet Orange EK from 8.28.175.67 - cdn.americasrapper.com:10016 & cdn5.blumaxmaterial.com:10016
- 2014-09-24 -- Fiesta EK from 104.28.6.73 - eoxsc.kulawyn.in
- 2014-09-24 -- Phishing campaign - Subject: Overdue Payment: 884272725375713
- 2014-09-23 -- Rig EK from 178.132.203.26 - mdif.boroughventuremenswear.com
- 2014-09-22 -- Phishing email - Subject: NatWest Statement
- 2014-09-22 -- Angler EK from 192.99.197.134 - asd.singularitymusculusintercostalis.us



MALWARE-TRAFFIC-ANALYSIS.NET

2014-10-09 - MAGNITUDE EK FROM 178.32.82.137 - 3D9A766.0EEC.BCF7E8.AF992.1E705.5F8D3.F658A0L7O9.PRESSTERMINALS.IN

PCAP AND MALWARE:

- PCAP of the VM infection traffic: **2014-10-09-Magnitude-EK-traffic.pcap**
- ZIP file of the malware: **2014-10-09-Magnitude-EK-malware.zip**
- Malwr.com PCAP: **2014-10-09-Mangitude-EK-payload-1-of-6-malwr.com-analysis.pcap**
- Malwr.com PCAP: **2014-10-09-Mangitude-EK-payload-4-of-6-malwr.com-analysis.pcap**
- Malwr.com PCAP: **2014-10-09-Mangitude-EK-payload-5-of-6-malwr.com-analysis.pcap**
- Malwr.com PCAP: **2014-10-09-Mangitude-EK-payload-6-of-6-malwr.com-analysis.pcap**
- Malwr.com PCAP: **UpdateFlashPlayer_811e7dfc.exe-malwr.com-analysis.pcap**

NOTES:

- Found this while checking through **Scumware.org** for interesting entries.
- It took me a few tries to get a full chain of infection traffic.

CHAIN OF EVENTS

ASSOCIATED DOMAINS:

- 62.233.121.40 - **www.nottinghamshire-probation.org.uk** - Compromised website
- 37.9.53.90 - **stats.street-jeni.us** - Redirect
- 178.32.82.137 - **3d9a766.0eec.bcf7e8.af992.1e705.5f8d3.f658a0l7o9.pressterminals.in** - Magnitude EK

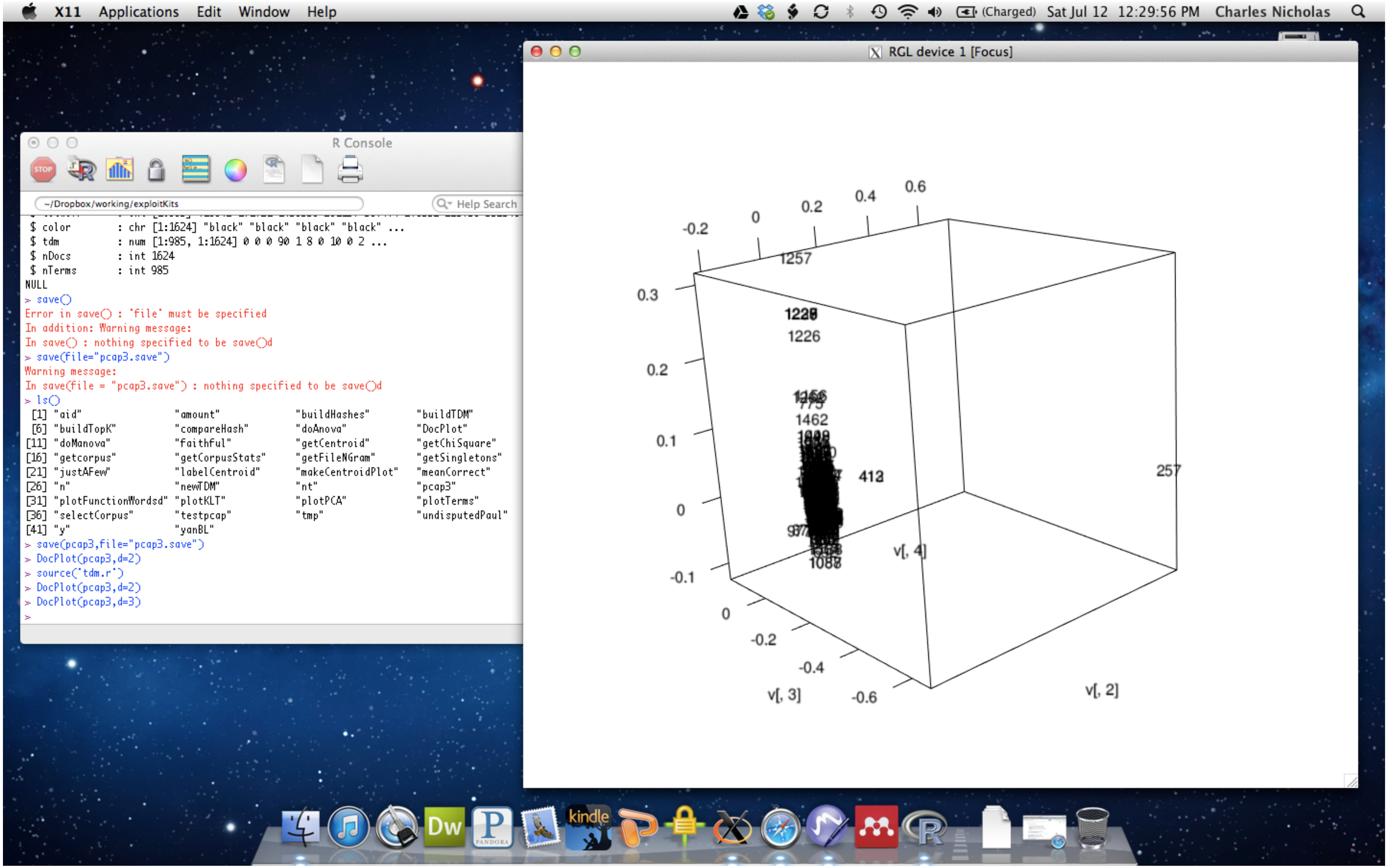
COMPROMISED WEBSITE AND REDIRECT CHAIN:

- 14:10:19 UTC - 192.168.204.145:49383 - 62.233.121.40:80 - www.nottinghamshire-probation.org.uk - GET /
- 14:10 UTC - 192.168.204.145:? - 62.233.121.40:80 - www.nottinghamshire-probation.org.uk - *[one of the .js files from the site]*
- 14:10:28 UTC - 192.168.204.145:49423 - 37.9.53.90:80 - stats.street-jeni.us - GET /show.php

MAGNITUDE EK:

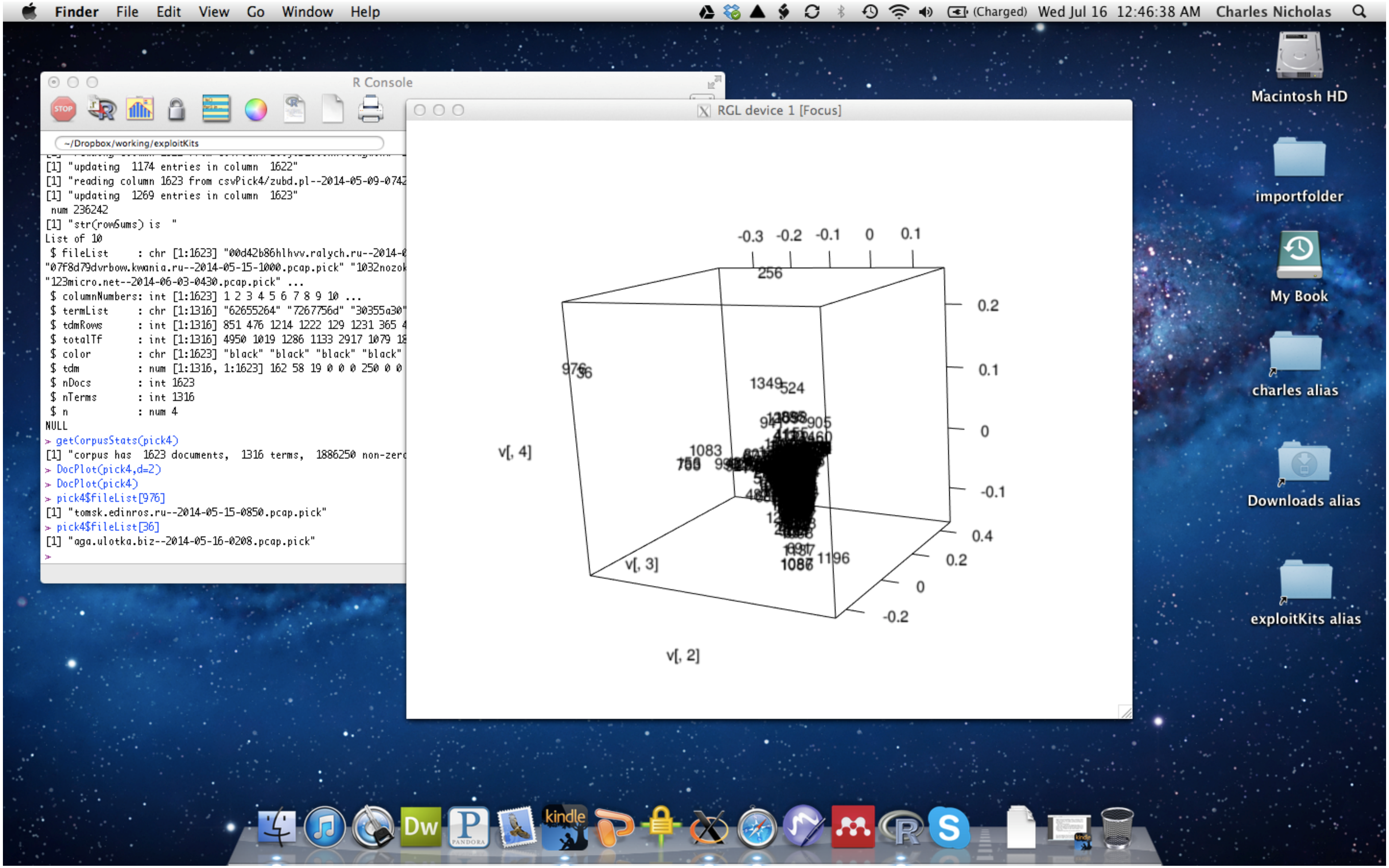
- 14:10:29 - 3d9a766.0eec.bcf7e8.af992.1e705.5f8d3.f658a0l7o9.pressterminals.in - GET /
- 14:10:34 - 3d9a766.0eec.bcf7e8.af992.1e705.5f8d3.f658a0l7o9.pressterminals.in - GET /a4adeaf2e3a08a34feeda27ad005fa91/5a85bcce264f195316838068dbb2b852
- 14:10:34 - 3d9a766.0eec.bcf7e8.af992.1e705.5f8d3.f658a0l7o9.pressterminals.in - GET /a4adeaf2e3a08a34feeda27ad005fa91/e8f096b5a0909917835416cb5c4c780f

Analysis of Raw PCAP



```
 $ color        : chr [1:1624] "black" "black" "black" "black" ...
 $ tdm          : num [1:985, 1:1624] 0 0 0 90 1 8 0 10 0 2 ...
 $ nDocs        : int 1624
 $ nTerms       : int 985
NULL
> save()
Error in save() : 'file' must be specified
In addition: Warning message:
In save() : nothing specified to be save()d
> save(file="pcap3.save")
Warning message:
In save(file = "pcap3.save") : nothing specified to be save()d
> ls()
 [1] "aid"                "amount"             "buildHashes"        "buildTDM"
 [6] "buildTopK"          "compareHash"        "doAnova"            "DocPlot"
[11] "doManova"           "faithful"           "getCentroid"        "getChiSquare"
[16] "getcorpus"          "getCorpusStats"     "getFileNGram"       "getSingletons"
[21] "justAFew"           "labelCentroid"      "makeCentroidPlot"   "meanCorrect"
[26] "n"                  "newTDM"             "nt"                 "pcap3"
[31] "plotFunctionWordsd" "plotKLT"            "plotPCA"            "plotTerms"
[36] "selectCorpus"       "testpcap"           "tmp"                "undisputedPaul"
[41] "y"                  "yanBL"
> save(pcap3,file="pcap3.save")
> DocPlot(pcap3,d=2)
> source('tdm.r')
> DocPlot(pcap3,d=2)
> DocPlot(pcap3,d=3)
>
```

Analysis of tcpick Output

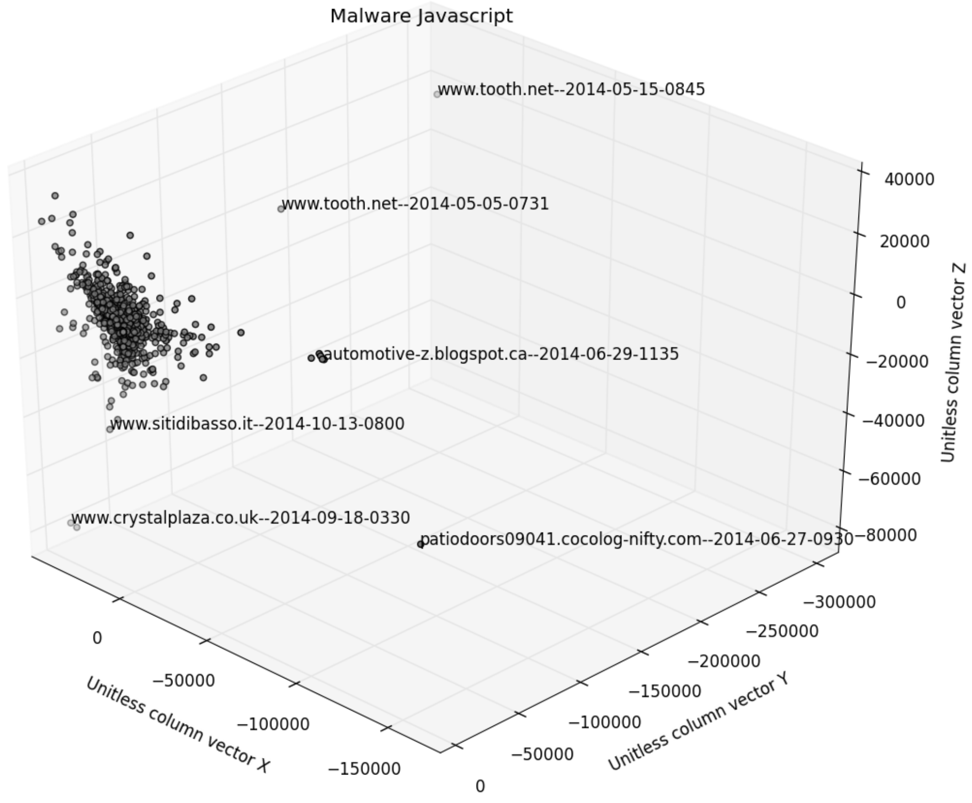


```
[1] "updating  1174 entries in column  1622"
[1] "reading column 1623 from csvPick4/zubd.pl--2014-05-09-0742
[1] "updating  1269 entries in column  1623"
 num 236242
[1] "str(rowSums) is  "
List of 10
 $ fileList     : chr [1:1623] "00d42b86hlhvv.ralych.ru--2014-0
"07f8d79dvrbow.kwania.ru--2014-05-15-1000.pcap.pick" "1032nozok
"123micro.net--2014-06-03-0430.pcap.pick" ...
 $ columnNumbers: int [1:1623] 1 2 3 4 5 6 7 8 9 10 ...
 $ termList     : chr [1:1316] "62655264" "7267756d" "30355a30"
 $ tdmRows      : int [1:1316] 851 476 1214 1222 129 1231 365 4
 $ totalTf      : int [1:1316] 4950 1019 1286 1133 2917 1079 18
 $ color        : chr [1:1623] "black" "black" "black" "black"
 $ tdm          : num [1:1316, 1:1623] 162 58 19 0 0 0 250 0 0
 $ nDocs        : int 1623
 $ nTerms       : int 1316
 $ n            : num 4
NULL
> getCorpusStats(pick4)
[1] "corpus has  1623 documents,  1316 terms,  1886250 non-zero
> DocPlot(pick4,d=2)
> DocPlot(pick4)
> pick4$fileList[976]
[1] "tomsk.edinros.ru--2014-05-15-0850.pcap.pick"
> pick4$fileList[36]
[1] "aga.ulotka.biz--2014-05-16-0208.pcap.pick"
>
```

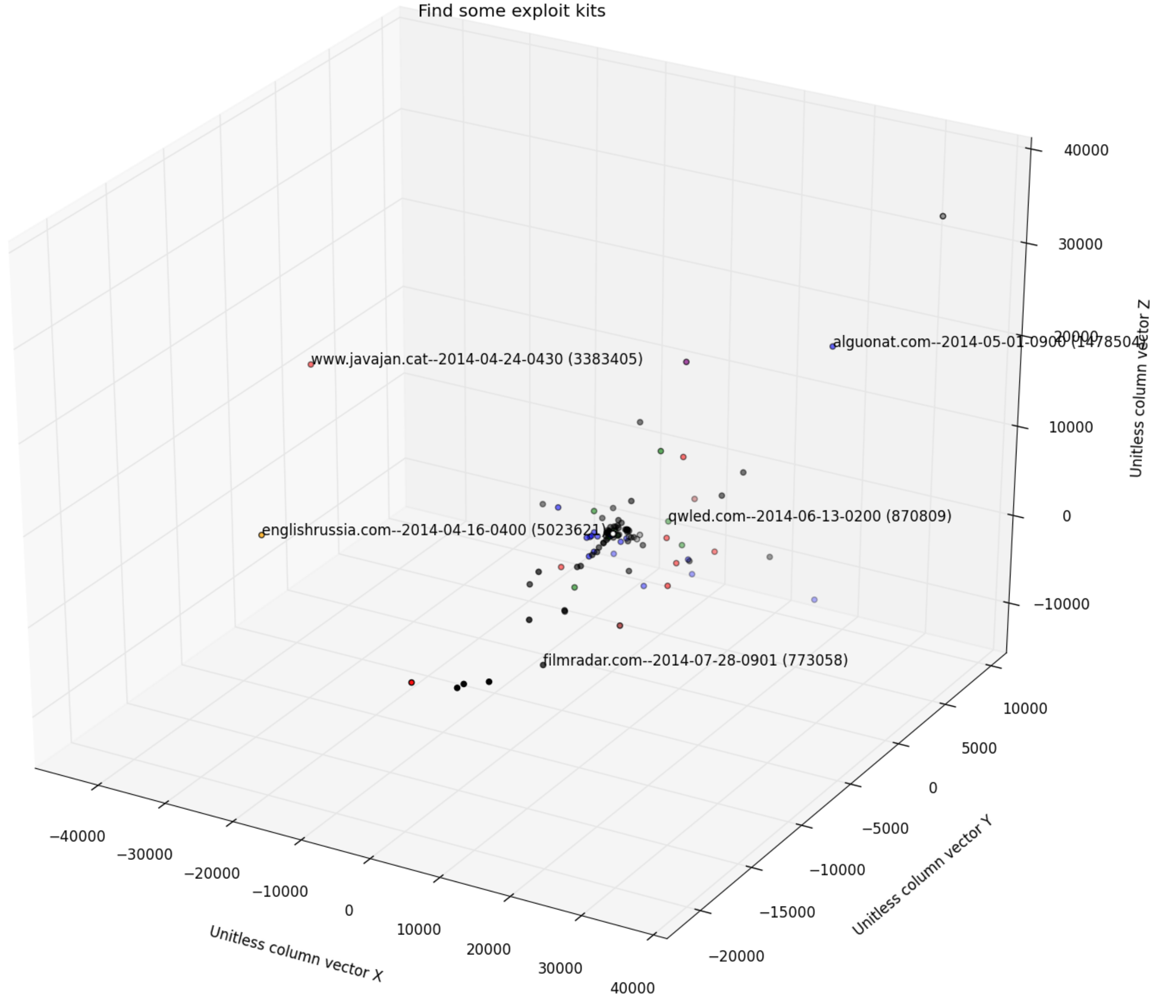
Discussion

- Analysis of raw pcap data might be used to spot outliers, or near duplicates.
- Analysis of tcpick output with 4-grams shows two almost duplicates, among other phenomena
- Suricata extracts specific files, including HTML with embedded Javascript, from specific sites and timestamps, as shown

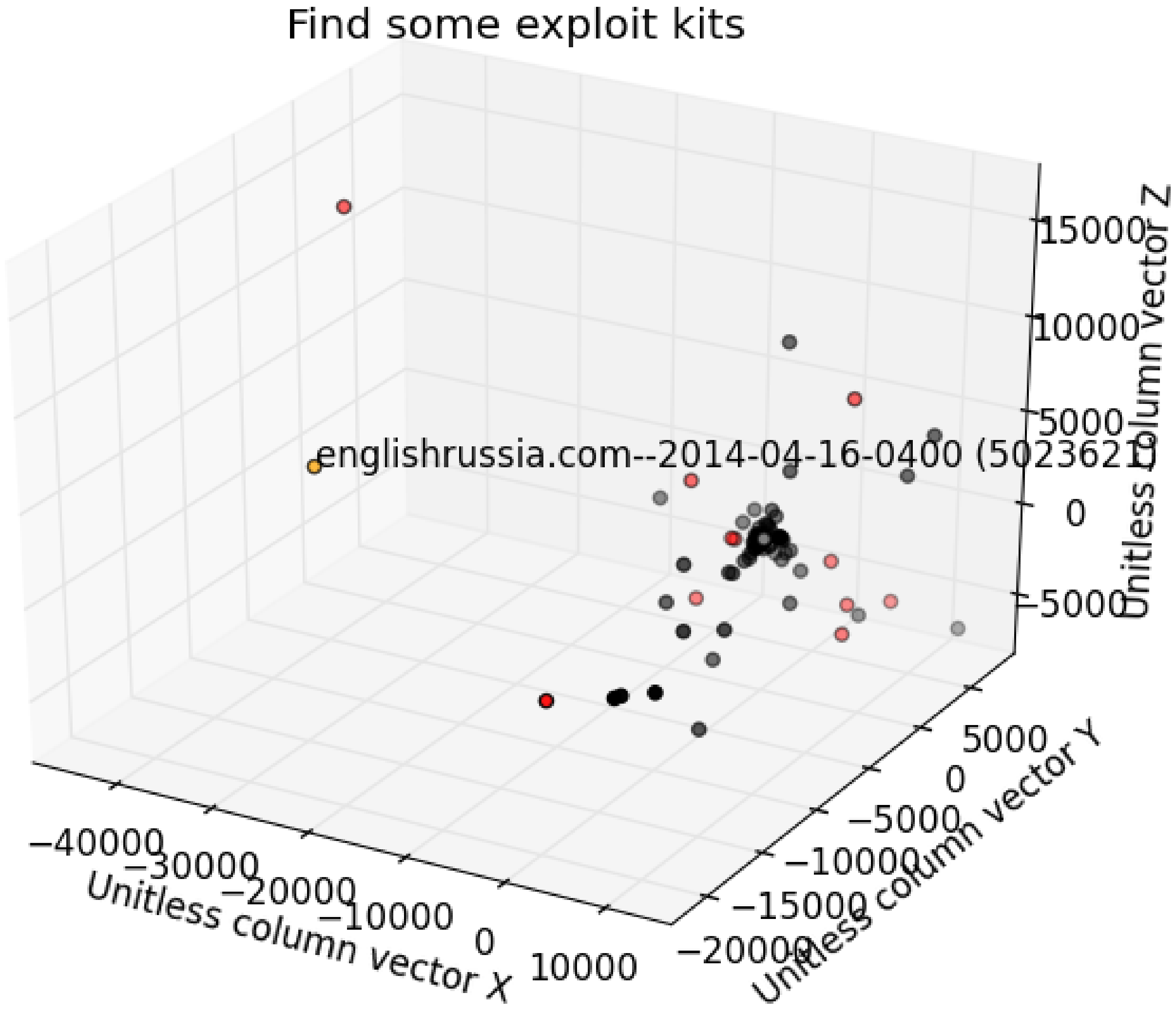
Plotting of Packets



Javascript with Kit Labels



Sweet Orange, Redkit, and Blackhole



~~Original~~ Revised Research Results

- We built a system to seek out EKs, visit them, and record the packets
- We parsed the Javascript files
  - we can spot unusual specimens
  - not yet able to associate Javascript syntax with specific EKs (n-grams may not be up to this task)
- Many EKs out there, but only a few are popular at a given time

Discussion

- Lots of exploit kits exist, but only a few are popular
- Outliers can provide insight, but discard them to drill deeper
- Too many n-grams carry too little information
  - This is old news
  - There seems to be lots of Blackhole activity
  - Perhaps other EK activity is being drowned out
  - So select better (or fewer) features

Limitations

- This approach is naïve, in the sense of using little or no domain knowledge
  - File structure information? No
  - N-grams ➔ machine instructions? No
  - N-grams ➔ Javascript language constructs? No
  - Specifying n-grams “of importance”? No
  - Similarity to “known” specimens? Some
  - Collection-related metadata? No
  - Knowledge of known actors? No

Machine Learning

- We’ve shown examples of unsupervised ML
- Other forms of ML, especially deep learning, are used in ongoing research
  - Neural nets, especially convolutional neural nets
    - Can we build neural nets to distinguish malware from benign is a related problem
  - Long short-term memories, or LSTMs
    - To discern what functions do, not just opcodes
  - Quality data sets for training is important!

Selected Publications and Presentations

- Charles Nicholas, Robert Brandon, Joshua Domangue, Andrew Hallemeyer, Peter Olsen, Alison Pfannenstein and John Seymour, “The Exploit Kit Club”, Malware Technical Exchange Meeting, July 22-24, 2014, Albuquerque, NM. (poster session)
- Diganth Bhagya Channegowda, "Exploratory Analysis of Exploit Kit Javascript", M.S. Thesis, July 2015.

continued

- Charles Nicholas, Brian Hillsley, Robert Brandon, Diganth Channegowda, Tobechukwu Ezekwenna, Andrew Hallameyer, Jacob Kogan, Cameron Lee, Edward Mukasey, Peter Olsen, Alison Pfannenstein, John Seymour, Payal Singh, Brendan Stryker, “From AlphaPack to Zuponcic: a Survey of Exploit Kits”, Malware Technical Exchange Meeting, June 17-19, 2015, Boston, MA. (poster session)