The Exploit Kit Club

Charles Nicholas, Robert Brandon, Joshua Domangue, Andrew Hallemeyer, Peter Olsen, Alison Pfannenstein and John Seymour
Department of Computer Science and Electrical Engineering, UMBC

Bad Guys use Exploit Kits a Lot!

- According to recent estimates, most of the malware on the Web is from EKs
- Black Hole is still the most famous, but there are many others: Sweet Orange, Redkit, Nuclear, RIG, ...
- Can we attribute malware sites to specific EKs?
- How can we tell when new EKs come out?

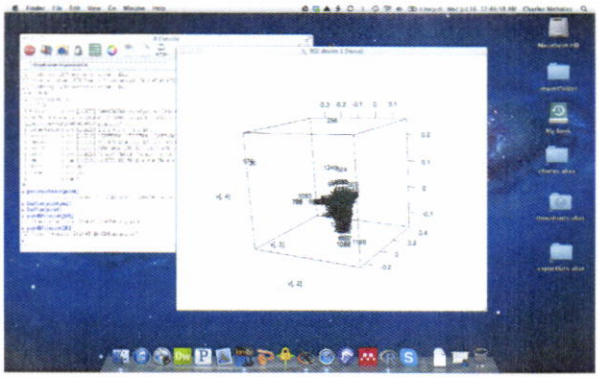
Our Hypotheses:

- If the Javascript code on landing pages is characteristic of the corresponding exploit kits, then similar scripts would be attributable to the same (or related versions of the same) exploit kit.
- Scripts unlike any seen before may indicate a new, unknown exploit kit.
- Landing page analysis may let us better understand this form of malware.

Progress

- Between early April to late July, we collected more than 4GB of pcaps from over 1600 malware domains
- Analysis of raw pcap data using 3-grams and SVD shows that the sessions are not all the same
- Analysis of tcpick output with 4-grams shows two almost duplicates, among other phenomena
- Suricata extracts specific files, including HTML with embedded Javascript, from sessions, analysis pending.

Analysis of tcpick Output



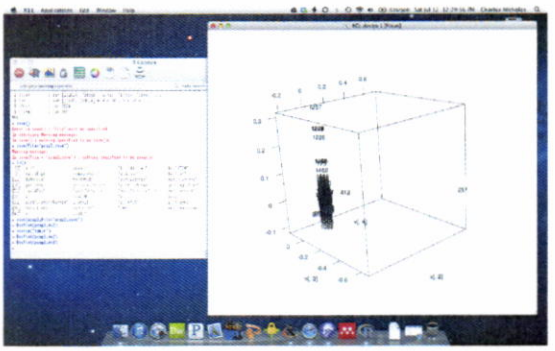
How do EKs Work?

- User is tricked into visiting an infected (but usually harmless) web site
- As a result of a few iframe redirects, such as <iframe src=http://badGuys.R.Us> the user's browser is sent to an EK web site
- A Javascript "landing page" is sent down
- The landing page looks at user's box and tries some exploits
- If any succeed, word is sent back to EK operators

Where to get data?

- Existing malware corpora are unsuitable, since they focus on malicious binary payloads, not on the Javascript code that GETs them
- With their consent, we scrape the web site http://urlquery.net which lists newly discovered malware sites
- When a new site is found, we send a browser inside a VM to go get infected (we hope!), and we capture the packets

Analysis of Raw PCAP



Future Work

- Analysis of extracted Javascript files is planned for near future
- Hoping to tie specific EKs to visual phenomena
- To request a copy of our latest tech report, send email to nicholas@umbc.edu,

MTEM 2014

UMBC
AN HONORS UNIVERSITY IN MARYLAND