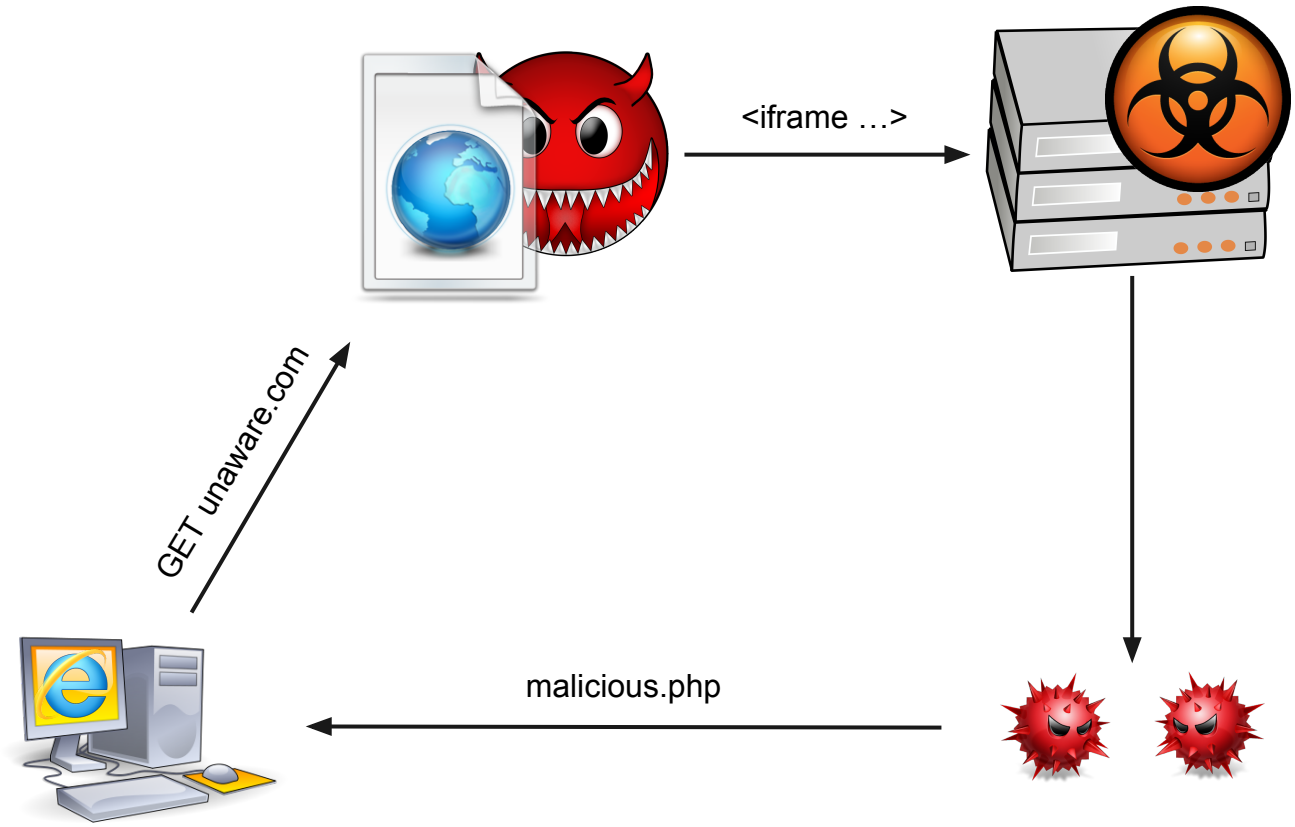
G. De Maio**, A. Kapravelos*, Y. Shoshitaishvili*, C. Kruegel*, G. Vigna*

**University of Salerno *UC Santa Barbara

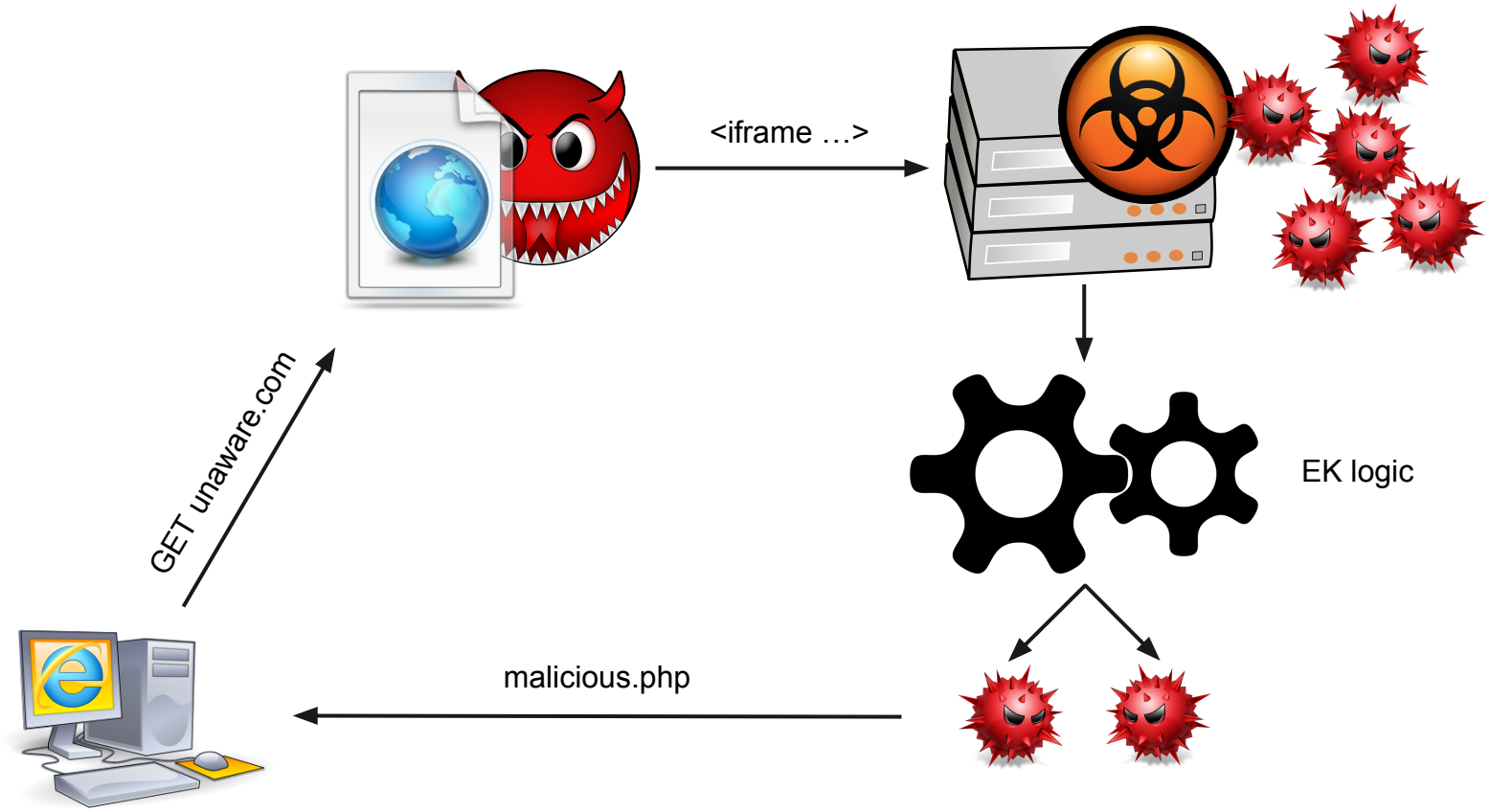
PExy

The Other Side of Exploit Kits

Drive-by download



Exploit Kits



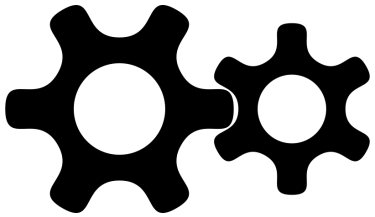
The other side

obfuscation
administration
storage

similarity
blacklisting
fingerprinting

decision-making code

Fingerprinting



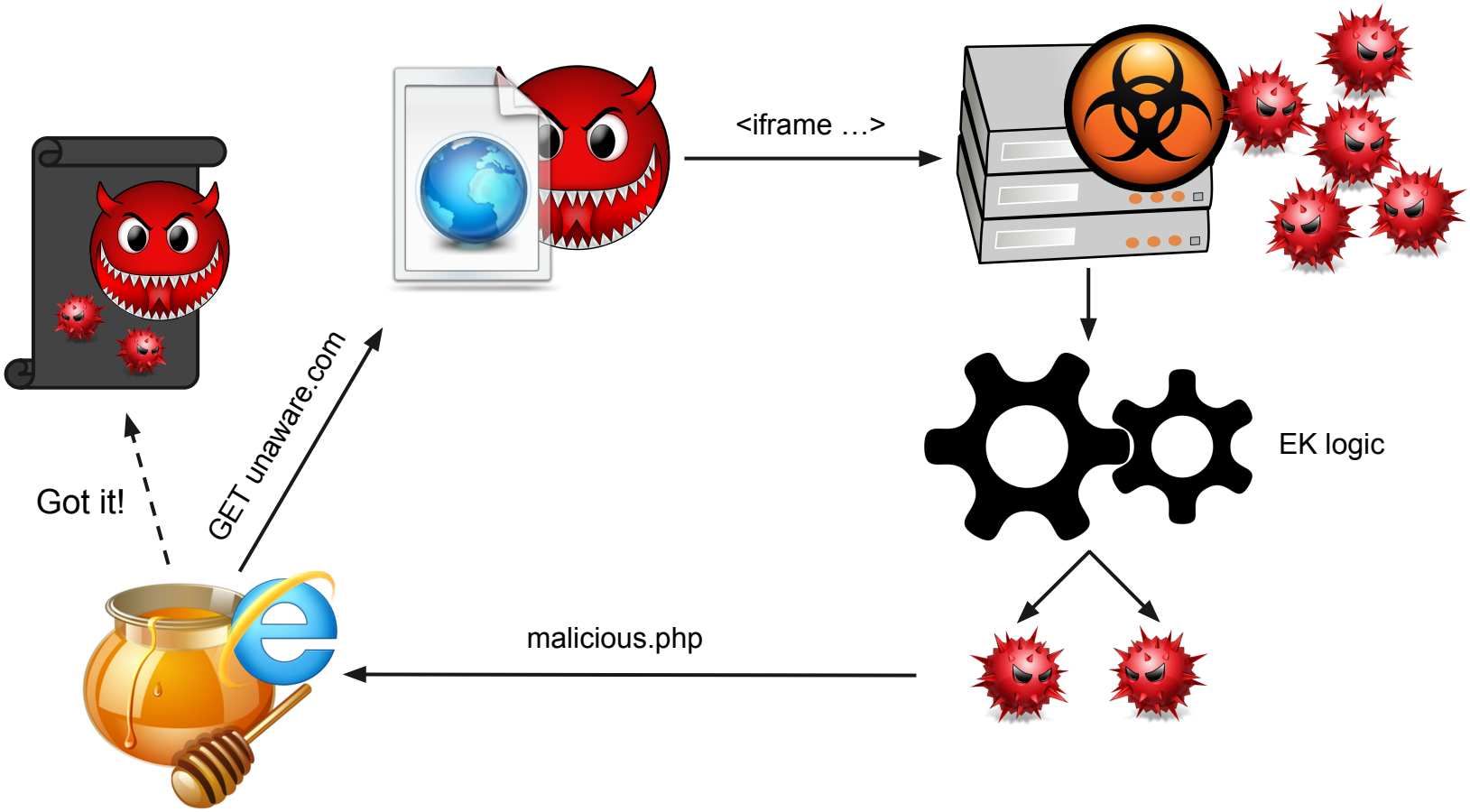
GET malicious.php?jre=1.7.0_6&fl=11.7.700.275

server-side ⟵ **client-side**

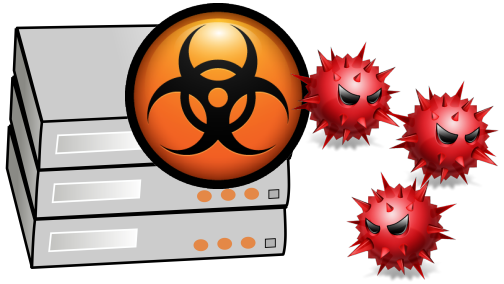
OS
browser
geolocation

plugins
other software

Honeyclients vs EKs



Honeyclients vs EKs

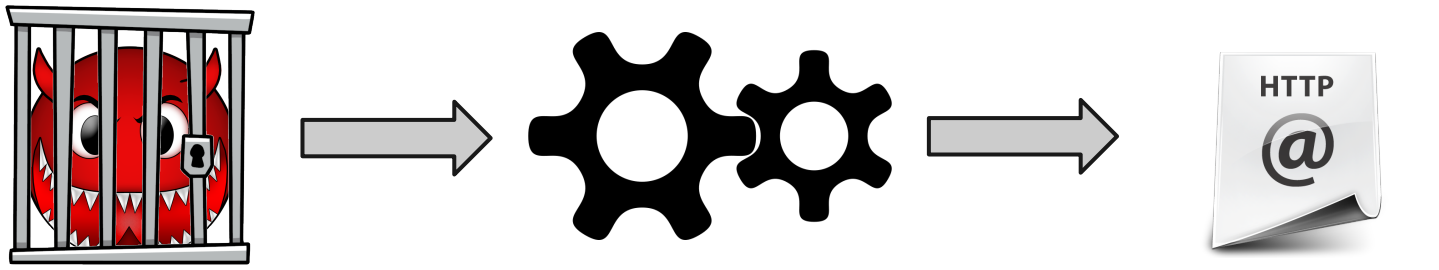


are we missing something?

~~brute-force~~

Exploit milking

idea (1)



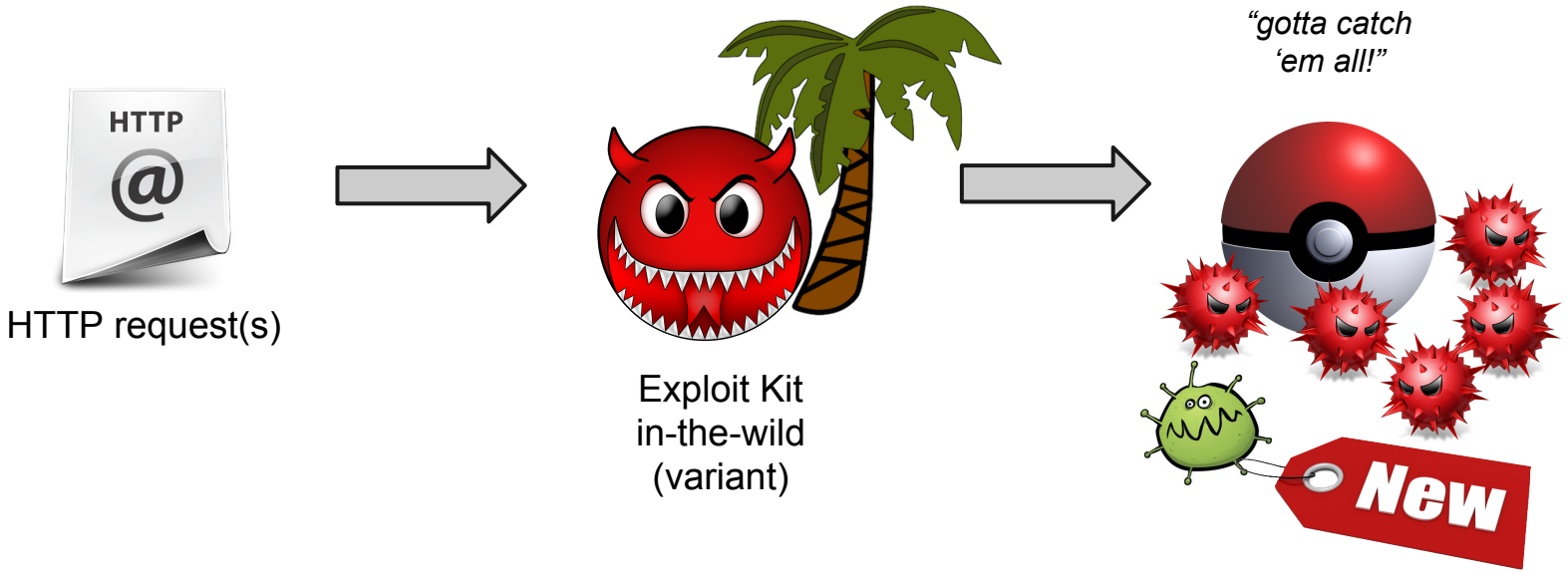
Exploit Kit sample

Static Analysis

HTTP request(s)

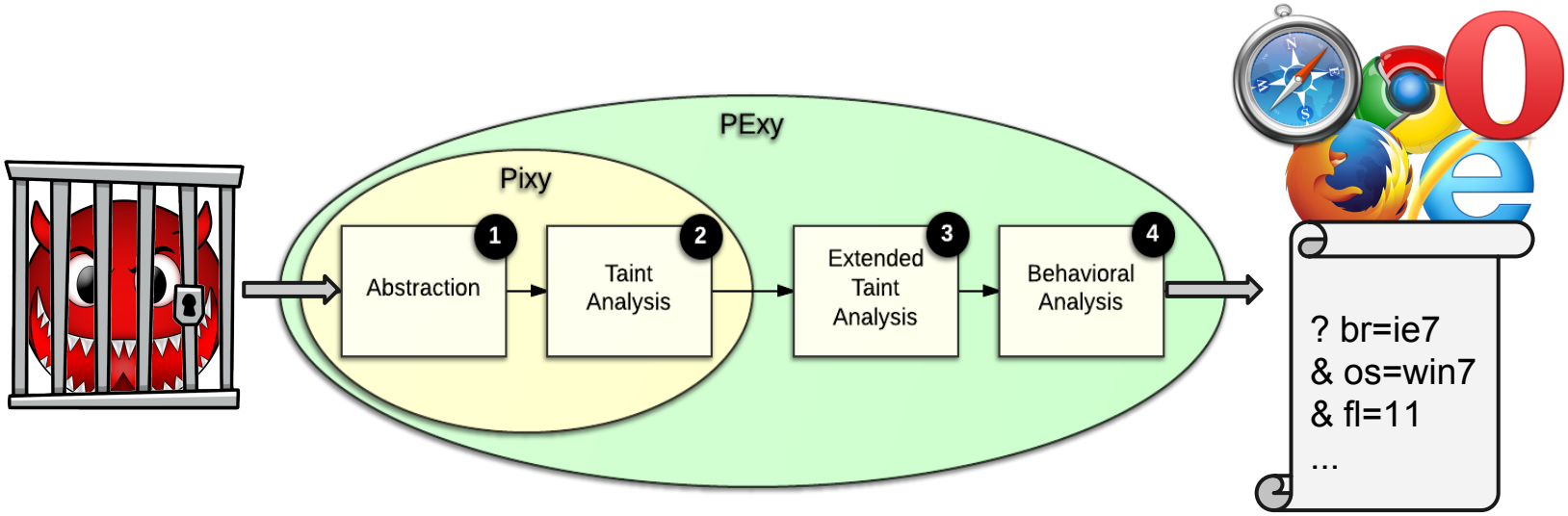
Exploit milking

idea (2)



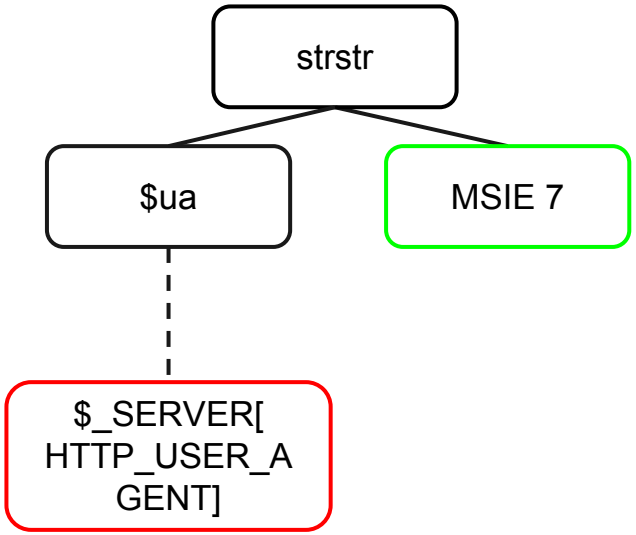
PExy

overview



Pixy

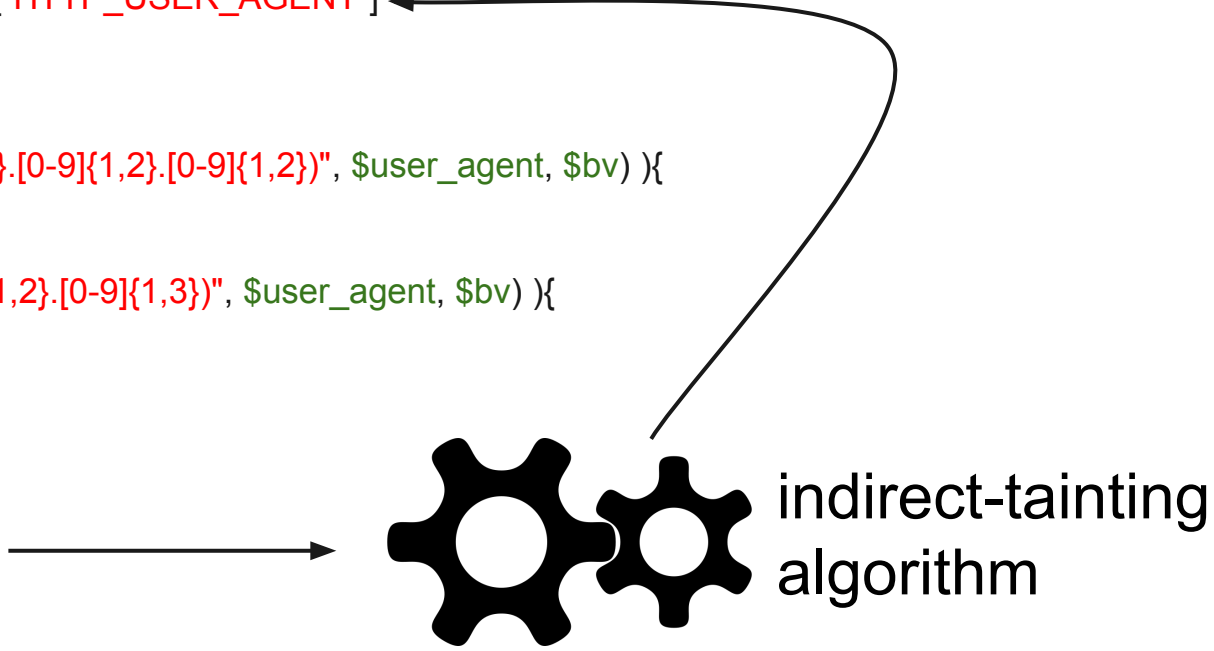
```
$ua = $_SERVER[“HTTP_USER_AGENT”]

…

if ( strstr($ua, “MSIE 7”) ){
        include("ie.php");
}
```



“Pixy: A Static Analysis Tool for Detecting Web Application Vulnerabilities,” Oakland 2006

Branch identification

```
$user_agent = $_SERVER[“HTTP_USER_AGENT”]

...

if ( eregi("(firefox)/([0-9]{1,2}.[0-9]{1,2}.[0-9]{1,2})", $user_agent, $bv) ){
        $br = 2;
}
elseif ( eregi("(msie) ([0-9]{1,2}.[0-9]{1,3})", $user_agent, $bv) ){
        $br = 1;
}

…

if ( $br == 1 && … ){
        include("ie.php");
}
```



Branch classification

```
$deny = $_GET[“d”]
...

if ($deny){
        die(“This page is benign!”);
}

…

$flash_ver = $_GET[“fl”]
if ($flash_ver < 13){
        print($flash_exploit);
}
```

embedded PHP

print statements

file inclusion

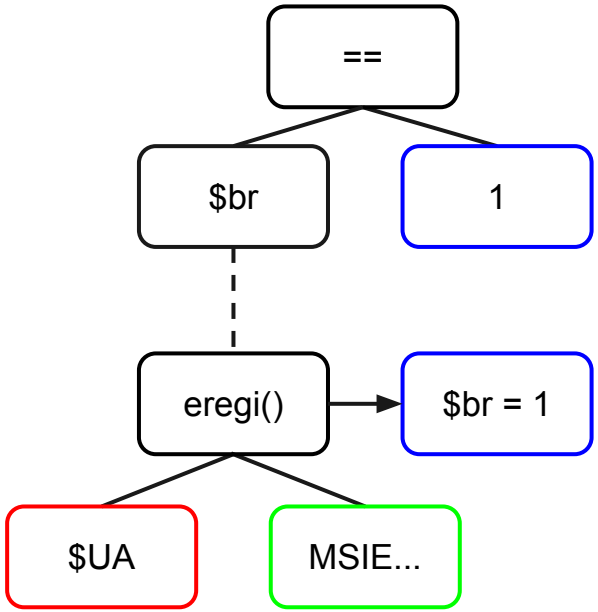
header manipulation

string manipulation

functions...

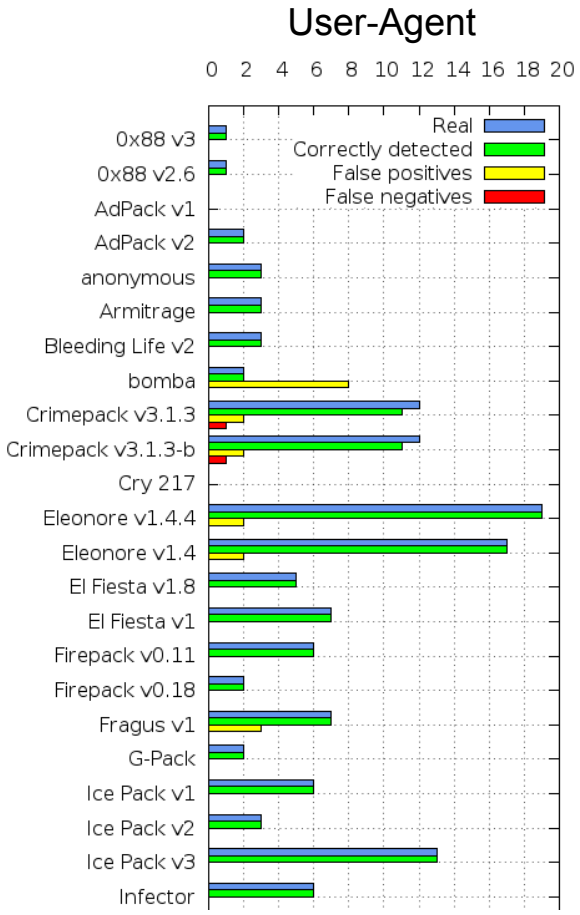
Parameters extraction

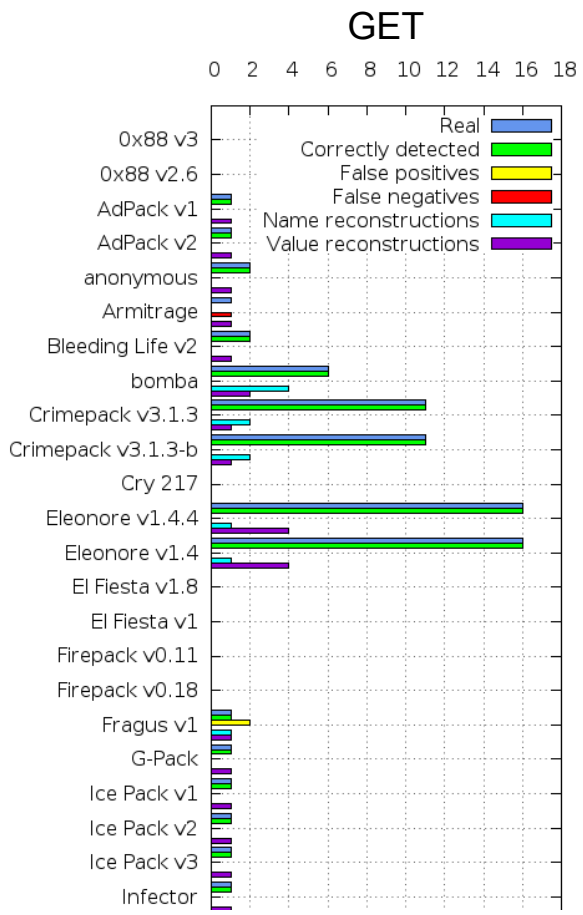
```
elseif ( eregi("(msie) ([0-9]{1,2}.[0-9]{1,3})",
    $user_agent, $bv) ){
        $br = 1;
}

…

if ( $br == 1 && $bv[2] < 9 ){
        include("ie.php");
}
```



~ extended dependency graph

PExy: results





Limitations

source code of EK

obfuscation

Conclusions

- identification
- milking
- honeyclient setup
- limitations

Thank you!