Heimdall

Vulnerable host discovery and lifecycle monitoring toolkit

Toronto, 02 October 2018
Dr. Andrea Braschi
Computer Engineering @ Politecnico di Milano
Past experience in antifraud-team for more than 3 years
Security Engineer @ Secure Network

andrea.braschi@securenetwork.it
www.linkedin.com/in/AndreaBraschi90
• Servizi Professionali di Information Security
  • Security Assessment
  • Information Security Management
  • Security Training
  • Digital Forensics

• 2004 - Stefano Zanero & Alvise Biffi

• Via Copernico 38 – Milano
• www.securenetwork.it
Table of contents

- Cyber Fraud Schema
- Heimdall
- Heimdall Architecture
- Bifrost
- Applications
- Conclusions and Q&A
Table of contents

- Cyber Fraud Schema
  - Threat Scenarios
  - Overview of a phishing campaign
  - Black market eco-system
  - A "special" kind of free hosting solution
  - Threat sources

- Heimdall
- Heimdall Architecture
- Bifrost
- Applications
- Conclusions and Q&A
• Outside your firewalls there are:
  • Malware
  • Fake sites
  • Ransomware
  • Trojan horses
  • Crawlers
  • Abusive crypto miners

All these threats have as common factor the source:

Vulnerable machines in the web
Overview of a phishing campaign

At least three machines are needed in this process.
Black market eco-system

• Who uses the kit is not who made it
• Not deeply technical people can buy those kits
• What they need:
  • The payload (clone kit, ransomware, trojan, etc)
  • A bot-net
  • A way to build their own botnet
• They may take their supplier from different vendors
• In the short period a criminal gang will use the same set of vulnerabilities
A «special» kind of free hosting solution

New vulnerabilities discovered

Attacker

Custom scanner

Heimdall
Hence every non-patched or misconfigured machine represents a source of threat
# Table of contents

- Cyber Fraud Schema
  - Heimdall
    - Why don’t we do the same?
    - Eingineering
    - GoogleDorks
    - Google Hacking Database (GHDB)
    - Shodan
    - Nmap
    - Masscan
    - Custom Script
  - Heimdall Architecture
  - Bifrost
  - Applications
  - Conclusions and Q&A
Why don’t we do the same?

Now we can track all the most interesting vulnerabilities
Build lists of possible sources of threat
Act on them but more systematically
Re-engineer the process used by criminals in order to prevent their moves
• Takes advantage of the right technology to monitor the web
• Takes advantage of proper instruments to handle big-data
• Automate all the analysis on a very large scale
• All built on an engine that can evolve quickly
• With a high scalability requirements
Google Dorks

- Advanced query for Google
- Query used to exploit Google's power to look for interesting things on the web
- Term introduced by Johnny Long at DefCon13 ([https://youtu.be/fo1BR9itwOY](https://youtu.be/fo1BR9itwOY))
- For instance: `inurl:"spaw2/dialogs/"
- Often used to detect new vulnerable machines
Google Hacking Database (GHDB)

- [https://www.exploit-db.com/google-hacking-database/](https://www.exploit-db.com/google-hacking-database/)
- A collection of queries leading to interesting machines or file into the web:
  - Vulnerable Files
  - Vulnerable Servers
  - Advisories Vulnerabilities
  - File containing usernames or passwords
  - And more....
- A total of 4500 query to start with!
Shodan

- Continuously crawling the internet collecting machine banner
- Useful to identify vulnerable software
- One step ahead of criminals
- Also useful to map IoT device with default credentials
NMAP

• One of the most common opensource tool for network scan
• Banner grabbing functionalities
• Easy to script and integrate
• Needs to use our resources to scan the whole web
Masscan

- Mostly similar to Nmap but optimized for large horizontal scans
- Easy to script and integrate
- Needs to use our resources to scan the whole web
Custom Script

- Heimdall is thought to be integrated, possibly with any script
- Simple interface to implement in order to be invoked by Heimdall
- Attention should be paid to be sure that those plugins are harmless
Custom Script – An Example

- An RCE in one of the most common application server
- Exploit code released after patch
- But....

Apache Struts Remote Code Execution Flaw (CVE-2018-11776)
Custom Script – An Example

http://localhost:8080/superhero/superman/fly.action

Namespace

WAR

Action
Custom Script – An Example

“If Struts can't find any namespace for the given action, it will take a **user-specified namespace** and evaluates it as a **OGNL** expression, allowing the attacker to exploits a **Remote Command Execution** on the web application”
Custom Script – An Example

```bash
~$ test >>> curl -v 'http://localhost:8080/$%7b2%2b2%7d/help.action'
*   Trying ::1...
*   TCP_NODELAY set
*   Connected to localhost (::1) port 8080 (#0)
>   GET /$%7b2%2b2%7d/help.action HTTP/1.1
>   Host: localhost:8080
>   User-Agent: curl/7.54.0
>   Accept: */*
>
<   HTTP/1.1 302 Found
<   Server: Apache-Coyote/1.1
<   Location: /4/help.action
<   Content-Length: 0
<   Date: Fri, 24 Aug 2018 14:49:26 GMT
<
*   Connection #0 to host localhost left intact
```

${2+2}
Custom Script – An Example

- The exploit is not harmless
- We do not know how critical is the infrastructure scanned by Heimdall
- We cannot integrate this plugin...let’s look ad Apache struts version number!
### Table of contents

- Cyber Fraud Schema
- Heimdall
  - **Heimdall Architecture**
    - Architecture
    - Core
    - Storage solution
    - Plugin modules
- Bifrost
- Applications
- Conclusions and Q&A
Who is Heimdall?
Core

- Main components invoking periodically all the plugins
- Invoke scan method for every plugin
- Store results produced by the plugin
- Directly store JSON into Elasticsearch
- Natively offers JSON APIs to export data
- Ease of integration
- Ease of scalability
- Designed for big-data
- Easily integrable with Kibana for statistics and charts
Plugin modules

- Basilar interface that has to be implemented by every Plugin static class
- Implemented a module which monitor a configurable set of GoogleDorks
- Implemented a module which monitor a configurable set of Shodan Queries
Table of contents

- Cyber Fraud Schema
- Heimdall
- Heimdall Architecture
  - Bifrost
    - Custom Dashboards
    - Demo
  - Applications
- Conclusions and Q&A
Custom Dashboards
Custom Dashboards
Table of contents

- Cyber Fraud Schema
- Heimdall
- Heimdall Architecture
- Bifrost
  - Applications
    - Vulnerabilities lifecycle
    - Threat intelligence
    - Prevention
  - Conclusions and Q&A
Vulnerabilities Lifecycle

- Monitor time vulnerabilities takes to disappears (from SE indexed web)
- Eventually identify patterns vulnerabilities follows before disappearing
- Study Geographical diffusion of certain vulnerabilities
- Identify those events that have more impacts in evicting vulnerabilities
Threat Intelligence

- Identify new sources of threat (e.g.: group of criminals typically using machine affected by a certain vulnerability)
- Corporate perimeter Assessment
Preventions

- Sources for WAF and firewalls rules
- For National CERT to conduct “Patching campaigns”
- To evaluate the health status of corporate/national networks
Table of contents

• Cyber Fraud Schema
• Heimdall
• Heimdall Architecture
• Bifrost
• Applications

• Conclusions and Q&A
  • Results
  • Next steps
  • Questions
Results

- Integration with Google and Shodan
- First dashboards and tools
- Currently monitoring 26 vulnerabilities or misconfigurations
Monitored Vulnerabilities

✓ Vulnerable WordPress Gallery
✓ Joomla! com_joomanager - Arbitrary File Download
✓ Upload Vulnerability Elfinder 2.0
✓ Oracle Reports likely vulnerable to DB user/password disclosure
✓ cpanel and ftp cracker
✓ webapp vulnerable to SQL injection
✓ view phpMyAdmin of web sites
✓ asp.net shells
✓ w3tc dbcache
✓ Locus7shell
✓ intranet admin
✓ spaw2 arbitrary upload
✓ Vulnerable Wago devices
✓ Xitami servers distributed with a script for testing server-side includes
✓ Vulnerable moxa devices
✓ mgl-instagram-gallery plugin of WordPress Vulnerable to XSS
✓ Heartbleed Bug
✓ PHP framework Open redirect
✓ PHP framework Open redirect 2
✓ leovslideshow remote shell upload
✓ mobile detector remote shell upload
✓ Drupal Arbitrary File Upload Vulnerabilities
✓ dummy apache
✓ webcam with password password
✓ default password
✓ unauthenticated FTP
Next Steps

- Increase the number of Monitored Items
- Follow an entire vulnerability life-cycle
- Add new plugins
- Partnerships and/or community support
- Configurable Alarms (*Gjallahorn* on network perimeter)
- IP/URL list export API
- Automatic import of new dorks or Shodan query
QUESTION
Thank you!