HADRIAN

The Race Against Threats: Speed & AI in Exploitation

Rogier Fischer
Founder & CEO
Hadrian Security

Introduction

Rogier Fischer

Hacking Hall of Fame of Google, PayPal, Microsoft and Yahoo

Founded LiteBit (crypto exchange) in 2013

Founded Hadrian with fellow ethical hacker Oliver Beg in 2021

HADRIAN

The *autonomous hacker* that emulates the behaviour of real adversaries.

Hadrian monitors your digital footprint 24/7, proactively highlighting threats before criminals can exploit them.

Applying AI to Offensive Security

Reconnaissance

Discover as much of the target's digital footprint as possible

Contextualization

Building a deeper understanding of the target.

Exploit Development

Discover brand new vulnerabilities and **craft custom exploits**, without a human in the loop.

Mass Exploitation

When a new exploit is made available, quickly **find vulnerable targets at an internet-wide scale**.

Exploit Development

Training

Supervised learning on human hacker behaviour. Unsupervised learning on open-source resources.

Exploit

AI generates commands/code with crafted payloads to attempt exploitation.

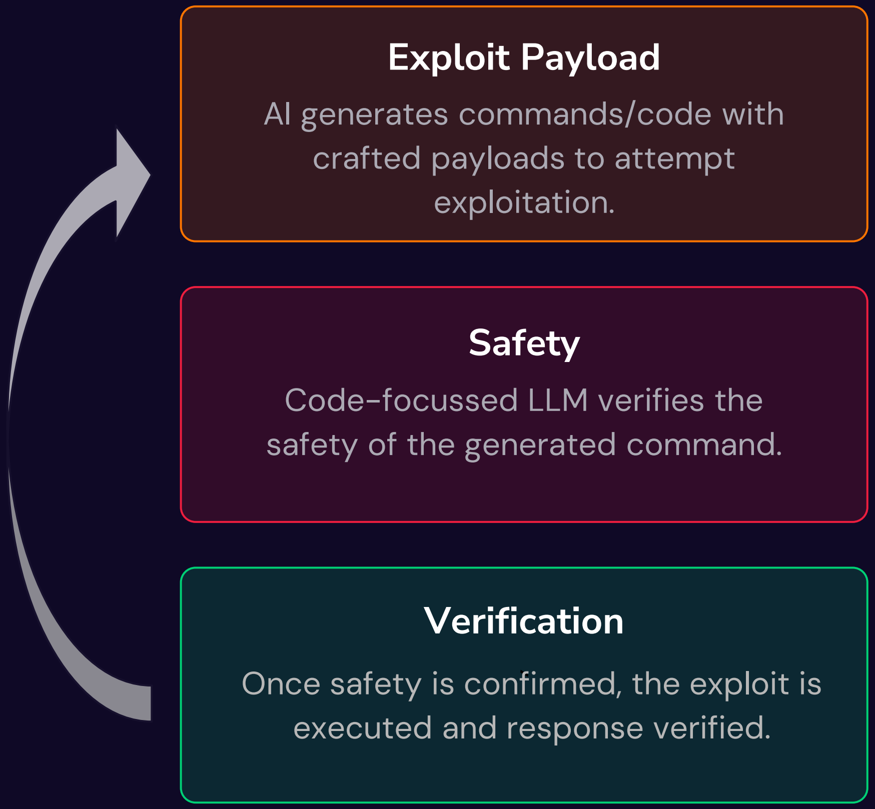
Safety

Code-focussed LLM verifies the safety of the generated command.

Verification

Confirm safety, execute the exploit, verify the application response.

SQL Injection - Example Loop



Exploit Payload

AI generates commands/code with crafted payloads to attempt exploitation.

```
GET /search?name=xyz' OR SLEEP(5)-- HTTP/1.1
Host: www.example.com
[..]
```

Safety

Code-focussed LLM verifies the safety of the generated command.

```
☑ ?name=xyz OR SLEEP(5)--
☑ ?name=xyz’
✕ ?name=xyz; DROP TABLE users;--
```

Verification

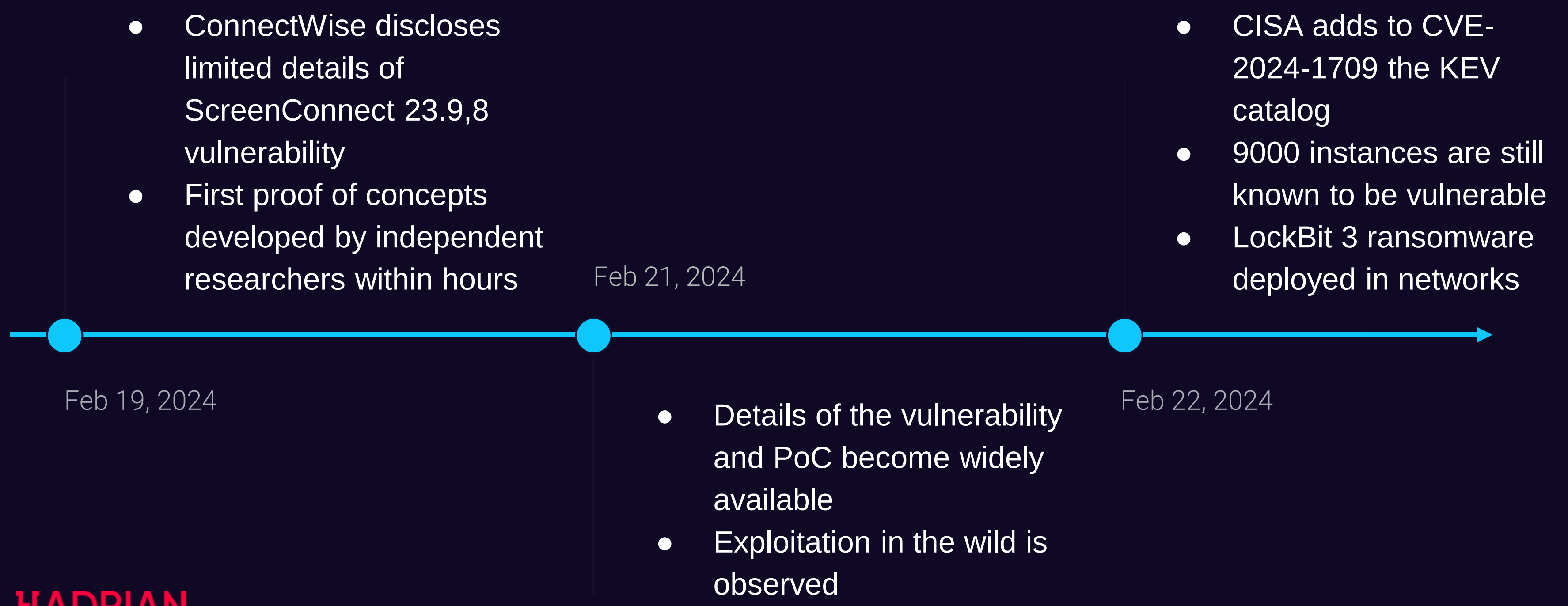
Once safety is confirmed, the exploit is executed and response verified.

```
Avg response time increased by 5 seconds?
Error thrown?
```

There’s got to be an easier way…

0-days, 0-days, 0-days

The Case of ScreenConnect



Feb 19, 2024

- ConnectWise discloses limited details of ScreenConnect 23.9,8 vulnerability
- First proof of concepts developed by independent researchers within hours

Feb 21, 2024

- Details of the vulnerability and PoC become widely available
- Exploitation in the wild is observed

Feb 22, 2024

- CISA adds to CVE-2024-1709 the KEV catalog
- 9000 instances are still known to be vulnerable
- LockBit 3 ransomware deployed in networks

MOVEit - 2023

May 28: Progress software was alerted by a customer who reported unusual activity in their MOVEit environment

May 31: Progress discloses a zero-day vulnerability in MOVEit

June 1: Multiple threat intelligence firms share evidence of active exploitation

June 2: The zero-day is assigned CVE-2023-34362 and a severity of 9.8

June 4: The series of attacks is attributed to Clop

June 6: Clop ransomware group claims responsibility for exploiting MOVEit

June 7: CISA and the FBI released a joint advisory

June 9: An updated advisory is released introducing a patch for a second vulnerability (CVE-2023-35036)

June 15: Progress uncovers a fresh vulnerability, CVE-2023-35708, and issues an advisory

July 6: Progress reveals three more vulnerabilities (CVE-2023-36934, CVE-2023-36932, CVE-2023-36933) for MOVEit Transfer

Staying one step ahead of hackers

Autonomously detect and exploit 0-days

HADRIAN

Autonomously Exploiting 0-days - CUPS Example

0-day Dropped

Subscribe to CVE feeds. Continuously monitor for a new 0-day to drop.

Extract Exploit

Is a PoC available? Parse CVE references to see if an exploit can be found.

Build Module

Generate a hacking module that fits into a scalable execution framework

HADRIAN

```
Polling API for new CVEs…
CVE-2024-1224 found.

Parsing exploit…
Gathering requirements…
     [i] Requirements
      *  Outbound request (udp)
      *  Callback server [http, https]
      *  Input: [ipv4]

Requesting callback server…
Server available on gkge12o2sfr3b.hdrn.nu:80.

Building container…
Generating PR…

PR Generated:
https://github.com/hadriansecurity/cve-
modules/pull/1247

Module ready – pending approval.
```

CUPS - CVE-2024-1224

Detection

Hadrian identified all customers with IPs responding on port 631.

Exploitation

The AI-developed module was executed across all targets.

Disclosure

Within hours from the 0-day dropping, Hadrian had informed all impacted customers.

Hadrian also scanned all IP ranges located in the Netherlands, uncovering 600+ vulnerable instances.

A coordinated disclosure was made.

HADRIAN

Engineering teams are on average 10-50x larger than security teams.

Security doesn’t have to get in the way of innovation & growth.

HADRIAN

Rogier Fischer,
CEO

rogier@hadrian.io