Red Balloon Security

# Capabilities Summary

**Ang Cui**
CEO & Chief Scientist

**Aleksey Nogin**
Head of Research

**IARPA SoURCE CODE Proposers Day, October 5, 2023**

WHO WE ARE

# Red Balloon Security has expertise with embedded devices and provides innovative technologies to defend critical systems

For 10 years, Red Balloon Security has developed and advanced two core capabilities:

- Reverse engineering embedded hardware and firmware
- Modifying binaries to harden firmware by augmenting/reducing existing functionality and integrating runtime protection

**THREE BUSINESS LINES**

**1. COMMERCIAL**

**DEPLOYMENTS AND VERIFIED COMPATIBILITY**

hp · SIEMENS · Rockwell Automation · CISCO · BOSCH · APTIV · DENSO

**2. RESEARCH**
**3. GOVERNMENT SERVICES**

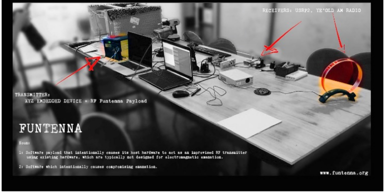
**U.S. GOVERNMENT ENGAGEMENTS**

DHS • DARPA • Air Force • Army • Navy • In-Q-Tel • NSF

SAMPLE OF RESEARCH FINDINGS

# RBS' embedded system expertise has led to novel & enhanced embedded security research techniques as well as findings to inform product security

## Funtenna: Data Exfiltration Using Malware Induced Compromising Emanation


RECEIVERS: USRP2, YE'OLD AM RADIO
TRANSMITTER:
XYZ EMBEDDED DEVICE + RF Funtenna Payload

FUNTENNA

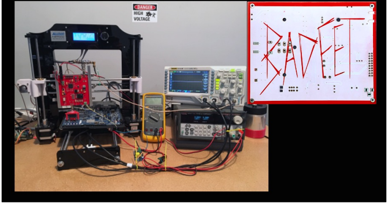
Noun:

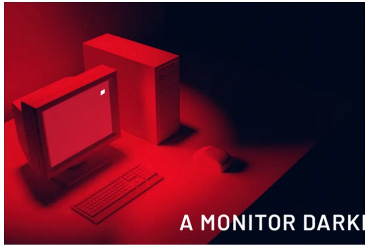
1: Software payload that intentionally causes its host hardware to act as an improvised RF transmitter using existing hardware, which are typically not designed for electromagnetic emanation.

2: Software which intentionally causes compromising emanation.

www.funtenna.org

## BADFET: Defeating Modern Secure Boot Using Second-Order Pulsed Electromagnetic Fault Injection





### A MONITOR DARKLY

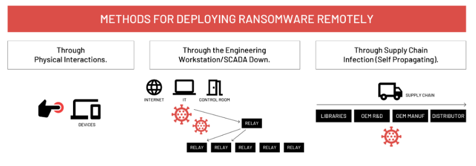
**Is your monitor displaying the truth?**

Reversing and exploiting ubiquitous on-screen display controllers in modern monitors.

### THRANGRYCAT

**Defeating Cisco's secure boot**

Red Balloon discovered a vulnerability which allows an attacker to persistently bypass Cisco's proprietary secure boot mechanism and lock out future updates.


METHODS FOR DEPLOYING RANSOMWARE REMOTELY
Through Physical Interactions.
Through the Engineering Workstation/SCADA Down.
Through Supply Chain Infection (Self Propagating).
DEVICES
INTERNET
IT
CONTROL ROOM
RELAY
RELAY
RELAY
RELAY
RELAY
RELAY
SUPPLY CHAIN
LIBRARIES
OEM R&D
OEM MANUF
DISTRIBUTOR

Red Balloon Security's groundbreaking research has found a means of implementing ransomware on a protection relay. The process is repeatable — and general to embedded devices.

## Critical Architectural Vulnerabilities in Siemens SIMATIC S7-1500 Series Allow for Bypass of All Protected Boot Features

ofrak

# OFRAK enables advanced control of binaries across 4 key areas during development and operation, increasing security and work efficiency & decreasing time and cost

| | OPEN FIRMWARE REVERSE ANALYSIS KONSOLE | | | |
|---|---|---|---|---|
| | **UNPACKING/REPACKING** | **ANALYSIS** | **MODIFICATION** | **PATCHING** |
| **PRIMARY USE CASES** | Unpack and repack file formats, from ELF executables and filesystem archives, to compressed and checksummed firmware<br>Extendable to proprietary file formats | Extract binary information and discover firmware components, including proprietary file formats<br>Identify known CVE/CWEs in a binary<br>Identify vulnerabilities through taint analysis | Modify device features at the binary-level<br>Find and create free space in binaries<br>Remove unused or unwanted features directly from binary<br>Develop binary exploitation  for testing | Update and patch compiled binaries (e.g., patching legacy software, adapting a kernel module to a new Linux environment) |
| **BENEFITS** | Save time with reusable and automated scripts – no more one-off code<br>Interact with almost any binary file format | Gain device assurance with low-level visibility, generating SBOM and FBOM<br>Build firmware component genealogy of previously opaque systems | Add security directly into binaries - no dependencies or recompilation necessary<br>Reduce attack surface at binary-level | Patch vulnerabilities before vendor patches are available<br>Write and test patches faster and easier |
| **SECURITY SUPPORT** | Attack Surface Management<br>Supply Chain Risk Management | | Hardening & Remediation<br>Secure Software Development Lifecycle | |
| **CORE FEATURES** | **GUI**<br>Explore binaries interactively with an intuitive visual frontend | **Python API**<br>Access to readable and reproducible scripts that apply to entire classes of binaries | **Disassembler Backends**<br>Utilize multiple analysis backends integrated into OFRAK (Ghidra, IDA, Binary Ninja) | **Extensibility**<br>Leverage a common interface to easily write new components for a new file format or binary patching operation |

**Ang Cui**
CEO & Chief Scientist

**Aleksey Nogin**
Head of Research

**Please contact us at research@redballoonsecurity.com**
https://www.redballoonsecurity.com