SECURITY RESEARCHER · REVERSE MALWARE ENGINEERING

Orion Wallace

CLEARANCE
TS / SCI
Active since Aug 2017

P 309-205-1983 E 0xdevbot@protonmail.com IN linkedin.com/in/orion-wallace-34167998 GITLAB gitlab.com/0xdevbot

Summary

Reverse engineer and security researcher with nine years across DoD cyber operations and defense-industrial software development. Active TS/SCI clearance, with deep work against Chinese state-sponsored APTs and Russian-nexus malware operations. Equally comfortable carving payloads out of memory, leading end-to-end incident response, emulating named adversaries as red team lead, and briefing senior stakeholders on national-security risk. Specializes in malware reverse engineering, threat intelligence, and DFIR from initial triage through attribution, detection authoring, and executive reporting.

Experience

Principal Cyber Threat Intelligence Analyst (Security Researcher)

2024 - Present

U.S. Air Force Reserve · 835th Cyber Operations Squadron

TS/SCI

- Led a 15-person Cyber Threat Intelligence team as Senior Analyst and squadron SME on Chinese state-sponsored cyber actors.
- Served as Lead Digital Forensics Analyst for the Incident Response Team across 15+ engagements spanning intrusion triage, host and memory forensics, and attribution.
- Hand-selected as Cyber Red Team Scenario author and Team Lead/Operator for Red Flag Alaska 26-2 — directed 10 operators emulating APT29 across a four-phase kill chain against a simulated air-defense network.
- Engineered the full kill chain: CVE-2023-22527 Confluence exploit, a custom libsysctl.so Linux rootkit (ld.so.preload hijack), and bespoke nginx-reverse-proxy C2 chosen over Sliver / Cobalt Strike to defeat known beacon YARA/SIGMA; post-ex via fodhelper UAC bypass into in-memory LSASS + SAM credential theft, PrintNightmare lateral movement, and a fratricide-watch dead-man's switch protecting impact actions against Early Warning systems.
- Reverse-engineered memory-resident malware via Volatility, uncovering an initial-access zero-day later attributed to a state-sponsored APT.
- Authored 100+ production detections via CVE research, PoCs, and isolated-sandbox adversary emulation; modernized the Threat Intelligence Lifecycle, cutting analyst reporting time by a month and saving the USAF an estimated $100K annually.
- Designed and published four C++ threat-hunting tools covering CTI automation, IR log enrichment, memory analysis, and network characterization.

Senior Software Engineer

2023 - 2025

Northrop Grumman · Advanced Mission Program (AMP)

TS/SCI

- Developed secure C++ for multi-billion-dollar embedded systems delivering strategic capabilities tied to U.S. national security.
- Conducted static and dynamic code audits inside a DevSecOps SDLC; reproduced and resolved critical defects via fuzzing, x64dbg, and behavior-driven testing.
- Served as technical lead for feature-development teams shipping high-reliability mission software in classified environments.

Cyber Threat Intelligence Analyst

2017 - 2023

U.S. Air Force Reserve · 42nd Cyber Operations Squadron

TS/SCI

- Produced 200+ finished CTI products characterizing nation-state threats against critical infrastructure; conducted threat and vulnerability assessments of high-value targets.
- Discovered a previously-unknown initial-access vector (zero-day) that would have enabled Malicious Cyber Actor (MCA) access to critical assets.
- Authored a 27-page Annex A intelligence report for a USCYBERCOM Operation; covering the zero-day, a supply- chain attack with full reverse-malware analysis (performed personally), 835 COS' first intel-driven hunt, and 12 assessments including 3 Red Team Scheme of Maneuvers, multiple HIGH-confidence near-peer assessments, mission-partner security-posture assessment.
- Led a joint effort with the Cyber Threat Emulation team and host operators to establish new 835 / 42 COS TTPs for memory forensics and APT attribution; drafted a companion 1N0 (All-Source Intelligence) integration white paper for Cyber Protection Teams.
- Delivered intelligence briefings across multiple echelons — including an impromptu in-mission brief to 67th Cyberspace Wing command staff during 853 CPT operations, translating tactical adversary actions into near-peer strategic-objective context.

Current Research

Zera Info-Stealer Malware Campaign — LEAD REVERSE ENGINEER · CINDR SECURITY RESEARCH

- Identified andled analysis as one of the first researchers tracking the campaign. Peeled backmultiple layersofencryption, decoy functions, and dead-code branching on a multi-stage Electron payload (main.js → crypted.js + Discord-desktop injector); recovered strings cross-referenced cleanly to ComRAT, Turla, and SAINT BEAR TTPs, supporting a likely Russian-nexus attribution. Coordinated disclosure with Discord, PayPal, and Stripe.
- Reconstructed the privilege-escalation primitive: main.js shells elevate.vbs for a UAC prompt, with an in-payload UAC bypass fallback inside crypted.js on decline.
- Documented a six-vector concurrent persistence stack — Defender exclusions; a scheduled task masquerading as Microsoft autochk SQM telemetry; an HKCU Run entry; a Startup .lnk overwriting OneDrive / Edge / Spotify / Discord; a WMI CommandLineEventConsumer(daily 08:00); and a COM CLSID hijack keyed by FNV-1a(hostname + username) — all wrapped inasingletry/catchsopartial-success implantation survives individual control failures.

Current Software Project

CINDR Intelligence Suite — FOUNDER · LEAD DEVELOPER

Modular CTI tooling that compresses the malware-triage-to-attribution-to-detection workflow from hours to minutes for DFIR teams and SOCs. Two production tools are field-proven on live engagements: a cloud-native triage engine (Azure Functions, Python, C++) that returns structured JSON static + behavioral analysis across 25+ file types in under 5 minutes per file; and TTP Mapper, which ranks probable threat-actor attribution via weighted F1 scoring against the full MITRE ATT&CK dataset. Three tools in active development (IOC Enrichment Hub, Threat Report Extractor, and Detection Rule Builder) extend the pipeline through bulk indicator enrichment, open-source CTI ingestion, and automated Sigma/YARA rule generation.

Software Projects

ConnToProc

C++

Windows Native API tool that watches new host connections, traces them back to the originating process, and emits custom events into an ELK stack for down stream hunting.

CVEScout

PYTHON

Cyber Threat Intelligence tool that generates a CVE Crosswalk and per-actor risk assessments for a given network surface. can be scoped to specific actors, software, or campaigns. Project delivered to 67th Cyberspace Wing and distributed to 15 Cyber Operations Squadrons

InfrastructureScan

C++

OSINT Purple Team software that uses publicly available infrastructure data or IoCs to programmatically discover and map networks. Originally designed for Security Research to uncover Malicious Cyber Actor infrastructure based on IoCs. But, found application for Red/Blue Teams.

Certifications

CISSP 2026
Certified Information Systems Security Professional

GREM (FOR610) 2025
Reverse-Engineering Malware: Analysis Tools & Techniques

GCFA (FOR508) 2024
Advanced Incident Response, Threat Hunting & Digital Forensics

GCTI (FOR578) 2023
Cyber Threat Intelligence Analysis

Security+ 2022
CompTIA Security+

Awards

Air & Space Medal — 2024

Awarded for identifying 89 previously-unknown IoCs and attributing them to nation-state APTs — materially improving DoD cyber defense posture.

NCO of the Year — 2024

Selected from a field of 100+ for modernizing the Air Force CTI program and authoring the SOP for analysts embedded with incident response.

Education

B.S. Computer Science
Lincoln Land Community College

A.S. Computer Science
Lincoln Land Community College

A.S. All-Source Intelligence
Community College of the Air Force

Skills

REVERSE ENGINEERING	Ghidra · x64dbg · static / dynamic analysis · deobfuscation · exploit development · fuzzing
DFIR	Volatility 2/3 · KAPE · memory forensics · registry artifacts · incident response · threat hunting
THREAT INTELLIGENCE	MITRE ATT&CK · kill-chain analysis · APT attribution · IoC enrichment · CTI reporting
RED TEAM & DETECTION	adversary emulation · C2 development · lateral movement · YARA / Sigma
SOFTWARE ENGINEERING	C++ 11/17/20 · Python · PowerShell · Windows API · secure SDLC · code auditing
PLATFORMS	Azure Functions · Elastic Stack (ELK) · Linux · Windows internals