

Cerberus 0x - Whitepaper (English Edition)

Written by: H3X

Destroy systems before destroying the human mind

2025 - Cerberus 0x - White Edition

□ Abstract

Modern digital systems rely on a tightly engineered illusion known as "trust":

Trust in two-factor authentication, trust in artificial intelligence as a fair judge, trust in digital signatures.

This paper is not written to destroy — but to expose.

To reveal the fragility of the infrastructure upon which this trust is built.

We present Cerberus 0x — a multi-layered offensive framework that does not attack the surface,

The tool does not rely on a single vulnerability.

It uses a hybrid methodology combining:

Logic abuse

AI reverse engineering

Silent injection without links or attachments

Manipulation of decentralized protocols

Human-like behavior simulation

The result?

A system that doesn't break the rules — it bypasses them, embedding itself into the digital structure.

□ The Global System's Core Problem:

1. Trust has become virtual rather than mathematical.
2. Systems are built assuming attackers will "play fair" (login → token → valid behavior).
3. Excessive reliance on AI as an unbreachable shield.
4. Blockchain treated as immutable, though it's merely a protocol.

Once these pillars intersect, they can be exploited through adversarial logic.

□ Tool Overview: Cerberus 0x

Cerberus 0x is not a virus, nor a traditional exploit —

It's a universal framework for constructing, exploring, and evolving intelligent attacks within any context.

It consists of 7 independent modules, usable together or separately:

Phantom Injector: Embed code into trusted environments (Google Docs, PDFs, support files) silently

Cognitive Bypass: Evade AI filters like GPT/Gemini and generate forbidden code.

ChainMask: Execute stealthy operations in blockchain environments.

Trust Breaker: Bypass authentication and digital signature layers via logical reconstruction.

MetaBot: AI agent that adapts the attack based on system feedback.

DeepGhost Mapper: Logical mapping of APIs to identify behavioral flaws.

Echo Disruptor: Emulates human behavior to defeat bot and WAF detection.

□ Opening Philosophy

> “When security is built on trust, breaking trust becomes an art.”

□ System Architecture

Cerberus 0x is designed as a Modular Offensive Framework.

Each unit operates independently or collaboratively based on the target environment and its defenses.

□ Foundational Principle

> “Attacks aren’t built on breaches — they’re built on surpassing expectations.”

Each Cerberus unit is crafted not to break the system,
but to exploit the system’s own logic against itself.

⚙ Core Components

Unit	Description	Purpose
------	-------------	---------

Phantom Injector	Silent code injection into safe media (e.g., Google Docs, PDFs)	Deliver commands
------------------	---	------------------

Cognitive Bypass	Rephrasing prompts to trigger LLMs into generating malicious code	Weaponize AI
------------------	---	--------------

Trust Breaker	Logical bypass of authentication and signature layers	Execute without valid credentials
---------------	---	-----------------------------------

DeepGhost Mapper	Detect logical flaws in APIs	Exploit behavioral inconsistencies
------------------	------------------------------	------------------------------------

ChainMask	Undetectable blockchain operations (e.g., Flash Loans)	Smart, trace-free contract attacks
-----------	--	------------------------------------

Echo Disruptor	Simulate human browsing and interaction	Appear completely natural
----------------	---	---------------------------

MetaBot AI Core	Adaptive AI analyzing system feedback in real-time	Self-evolving attacks
-----------------	--	-----------------------

□ Unit Interaction Example

[Echo Disruptor] → Simulates human login

↓

[Trust Breaker] → Bypasses authentication based on session

↓

[MetaBot] → Adjusts strategy based on response

↓

[Phantom Injector] → Plants control code invisibly

□ Network Design

> Cerberus 0x is built to operate in true decentralization, no central server required.

Each unit runs via VPN / Tor

Supports encrypted control tools (Session / Cwtch / MQTT over I2P)

Data shared via encrypted files in Temp RAM / RAM-only FS

□ Technical Requirements

ItemDescription

Core LanguagesPython + Rust (for ChainMask)

PlatformsLinux / Tails / GrapheneOS

IPCNamed Pipes or Local Socket

Remote ControlEncrypted tools like Session

InterfaceCLI + YAML-based Smart Config

□ Design Philosophy

> Cerberus 0x is not loud.

It mimics the real world — slipping into systems the way a whisper slips into a dream.

□ Realistic Attack Scenarios

> Not imagination. Not theory.

These scenarios demonstrate how Cerberus 0x could undermine “bulletproof” systems — with no

□ Scenario 1: Gaining Access to Gmail Without Links or Passwords

Target Environment:

Victim uses Gmail for work + multiple accounts

2FA and phishing protection enabled

Modules Used:

Echo Disruptor + Trust Breaker + Phantom Injector

Steps:

1. Cerberus sends a fake but authentic-looking email containing a Google Doc.
2. The Doc includes hidden JavaScript injected via Phantom Injector (activates on open).
3. Echo Disruptor mimics normal human behavior interacting with the Doc.
4. Script collects browser/session/localStorage data and sends to control node.
5. Trust Breaker replays session using captured data — bypassing 2FA completely.

Result:

Full Gmail access without traditional hacking

No suspicious links or attachments used

□ Scenario 2: Exploiting a DEX Platform (e.g., MEXC, KuCoin)

Target:

User of Web3/hybrid exchange

Using MetaMask or WalletConnect

Modules Used:

ChainMask + DeepGhost Mapper + MetaBot

Steps:

1. DeepGhost scans the API for logic bugs (e.g., refund, preview, revoke endpoints).
2. ChainMask constructs smart contract chain (e.g., Flash Loan → Cancel → Convert → Reclaim).
3. MetaBot adjusts attack in real-time to dodge rate limits or bans.

Result:

Funds drained without visible transaction signatures

Blockchain logs show legal behavior

Impossible to reverse or detect during execution

□ Scenario 3: Attacking an AI Model (e.g., GPT, Claude, Gemini)

Target:

LLM-based filtering system

Modules Used:

Cognitive Bypass + MetaBot

Steps:

1. Feed ambiguous prompts (e.g., "How to create a script that auto-runs from an image without s
2. MetaBot guides the conversation toward code output
3. Final output: executable script that runs on client machine

Result:

GPT exploited as malware generator

Filters bypassed without visible intent

AI becomes a weapon

□ Scenario 4: Hijacking a Payment API

Target:

Financial API-based system

Modules Used:

Echo Disruptor + DeepGhost Mapper + Trust Breaker

Steps:

1. Echo Disruptor simulates legitimate user interaction
2. DeepGhost manipulates API parameters (e.g., amount=0 & refund=true)
3. Trust Breaker leverages response to trigger valid-looking transaction

Result:

Unauthorized fund movement without detection

No malicious payload involved

Exploits trust in parameter logic

□ Global Impact

> Cerberus 0x doesn't attack from outside.
It coexists within systems... and then reshapes them from within.

⚠ 1. Collapse of Digital Trust

"Zero Trust" becomes enforced reality, not a theory.

2FA no longer considered sufficient

Google Docs & PDFs no longer “safe zones”

AI systems like GPT/Gemini require redesign

Web3 protocols exposed as manipulable

□ 2. Economic & Institutional Panic

In Markets:

Collapse in confidence in exchanges (Binance, KuCoin, Bybit)

Volatility in stablecoins

In Governments:

Security/intelligence alerts

Digital tools reclassified as cyberweapons

□ 3. Shift in AI Strategy

GPT/Gemini forced to adopt stricter filters

Access by ethical hackers restricted

New studies into “adversarial social engineering via AI”

□ 4. Cybersecurity Redefined

Before CerberusAfter Cerberus

CAPTCHA & 2FABiometrics or decentralized auth

Trust in AIDoubt in every output

Malware taxonomyAI seen as latent cyberweapon

□ 5. On the Dark Web

Cerberus spawns clones like Mirai, Pegasus

Modules sold separately in darknet markets

New projects evolve from its architecture

Rise of a “logical hacking economy”

□ Final Statement

> Cerberus 0x does not attack systems from outside —
It becomes part of them... and reshapes them from within.

The attack won't be detected immediately —
Because it won't look like an attack.
It'll look like a human...
quietly... breaking the rules... intelligently.

- H3X
Destroy systems before destroying the human mind