GraVitoN:

A Cross Platform Malware Development Framework

Author : Sina Hatef Matbue, Arash Shirkhorshidi

29th July 2012 ,India Habitat Center, Delhi

If it exists, the **GraVitoN** is expected to be

mass-less...

which gives it the power to

move to and from universes...

THE HACKERS CONFERENCE

Sina Hatef Matbue

VP of Software Development in ChallenGe Security

AND

Funder of The GraVitoN Project

THE HACKERS CONFERENCE

Arash Shirkhorshidi

CEO at ChallenGe Security Co.

THE HACKERS CONFERENCE

ABOUT GraVitoN

A beautiful combination of simple and smart ideas

THE HACKERS CONFERENCE

Malware Development Framework

Cross platform

Highly Customizable

Virus

Trojan

Worm

Why GraVitoN

C++ and ASM → Fast execution

Object Oriented → Easy to understand

GCC Support → Cross Platform

Doxygen → Well documented code

©License → GPLv3 → Free Software (Free as in freedom) → Hosted at Savannah

Technical Details

Self Exploitable Code

Main Idea

Load your payload assembly code as an unsigned char array to memoy

Jump into your payload start address

Let’s Go Code

Initialize Payload Memory

Initialize jumper as a C++ function

Let’s Go Code!

Copy our payload assembly code into memory of our function

And…

Jump!

Let’s Go Code!

Put things together

target: Windows 7 32 bit

payload: payload/windows/messagebox

IDE: dev-cpp

Compiler: g++

THE HACKERS CONFERENCE

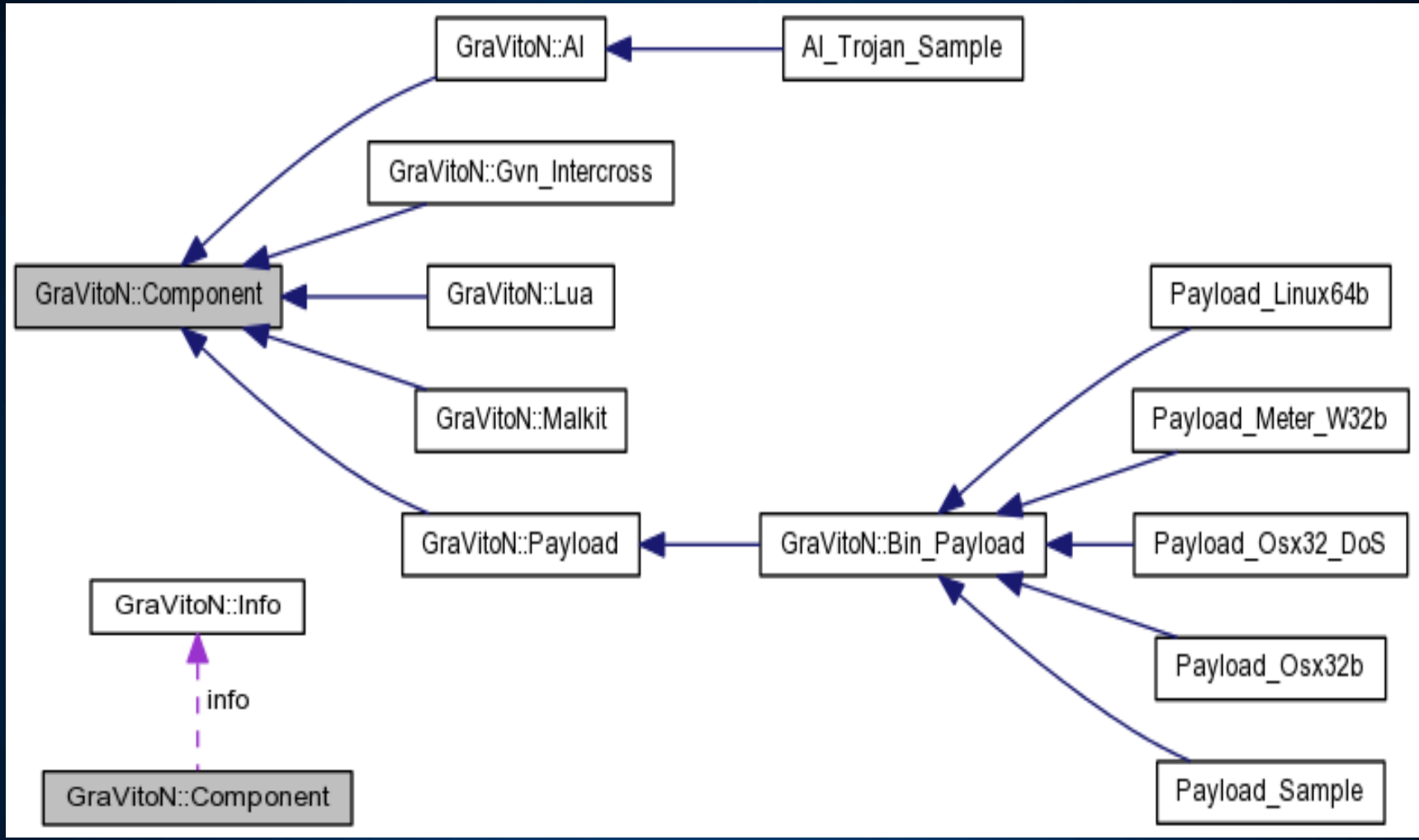
GraVitoN Framework

Component

Definition

Single piece which forms part of a larger whole

Big daddy of all other components of the GraVitoN


GraVitoN::AI
AI_Trojan_Sample
GraVitoN::Gvn_Intercross
GraVitoN::Component
GraVitoN::Lua
Payload_Linux64b
GraVitoN::Malkit
Payload_Meter_W32b
GraVitoN::Payload
GraVitoN::Bin_Payload
Payload_Osx32_DoS
GraVitoN::Info
Payload_Osx32b
info
Payload_Sample
GraVitoN::Component

Let’s Go Code!

Component Class

Info

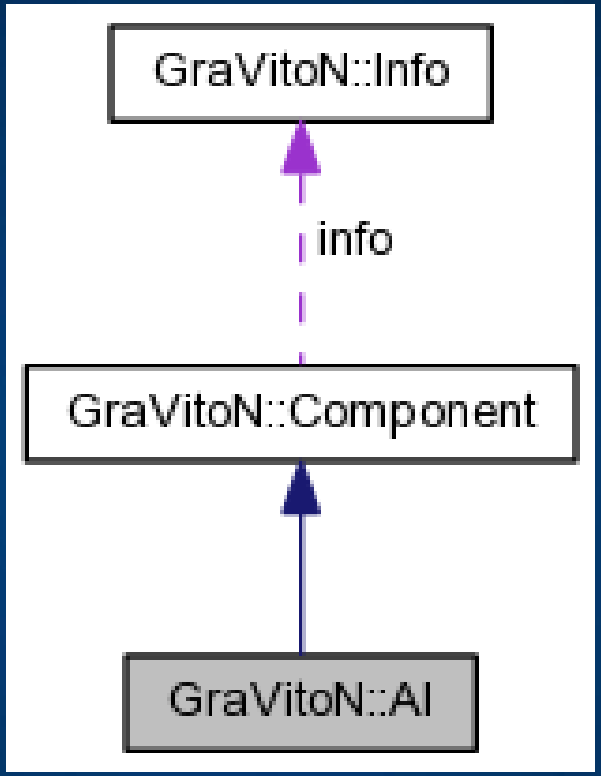
Initialize

run

AI

Definition:

Imagine GraVitoN as a missile, then AI is the program that is written inside its microprocessors, and designed to guide missile until it destroy the target!


GraVitoN::Info
info
GraVitoN::Component
GraVitoN::AI

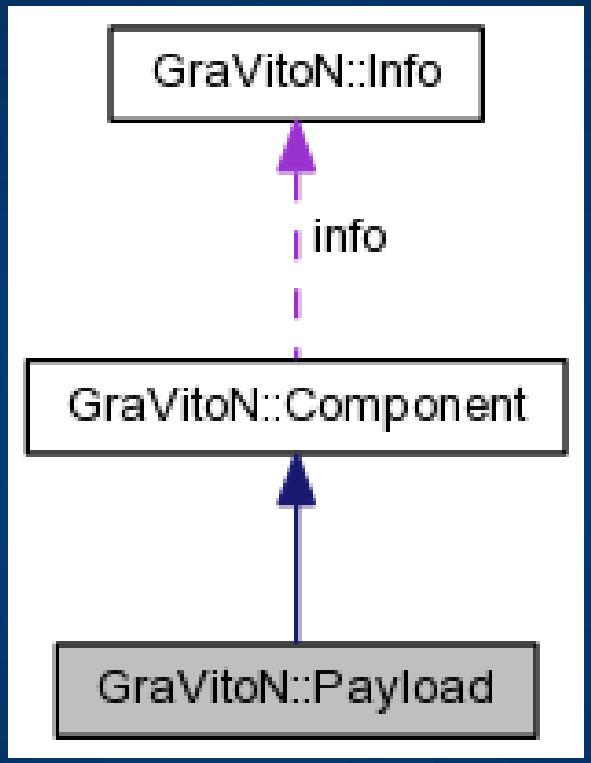
We are going to talk about it at AI Samples section of this speech.

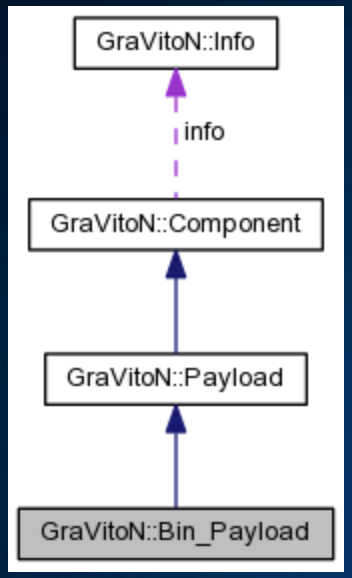
Be patient!

Payload

Definition

Malicious part of GraVitoN Code, It’s like explosive material in missile head!


GraVitoN::Info
info
GraVitoN::Component
GraVitoN::Payload



Bin_Payload

A specific type of payloads, designed to execute binary payloads (for example: shellcodes, etc.)

Let’s Go Code!

Msfpayload

Linux Fork

Intercross

Definition

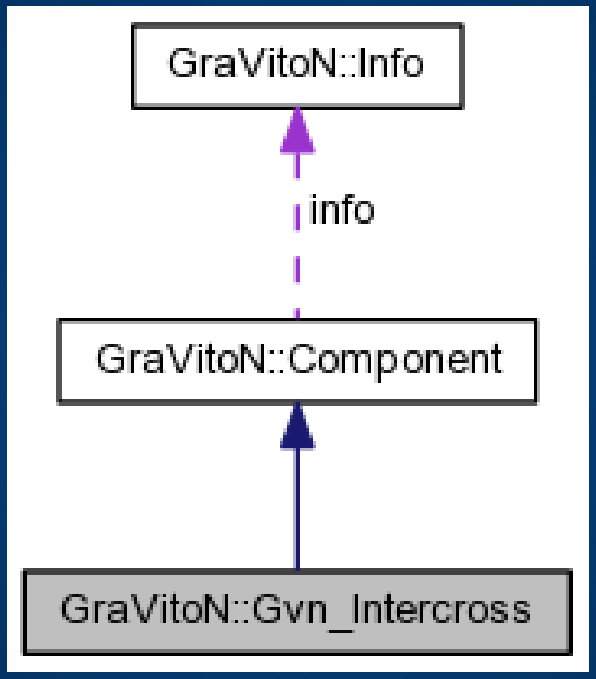
It’s a component, contains GraVitoN spread techniques.

Virus

Infects Executable

Worm

Exploitation


GraVitoN::Info
info
GraVitoN::Component
GraVitoN::Gvn_Intercross

Generic Infector

Keep It Simple, Smart!

Dark side of all executable binaries: EOF

Pick a valid executable binary file, add some bytes at the end of it, try to execute it. Operating system doesn't care of those few bytes!

Component

Gvn_Inter_EndOfFile

Metaworm

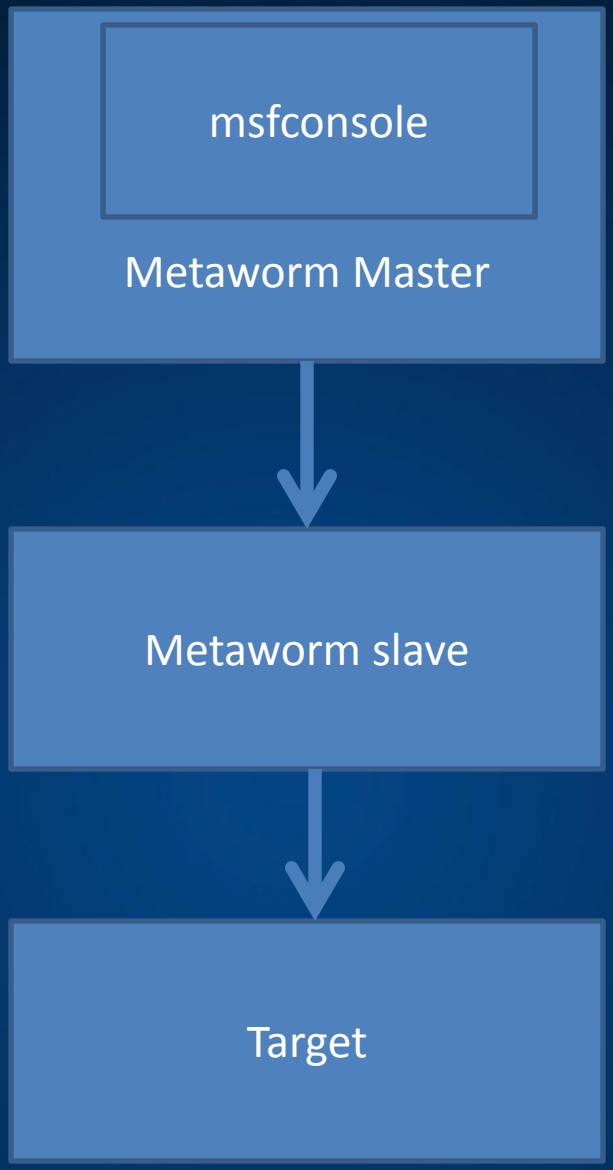
Exploit tunneling: Lunch exploits of metasploit against a target .

If exploition process was successful upload a slave to the target.

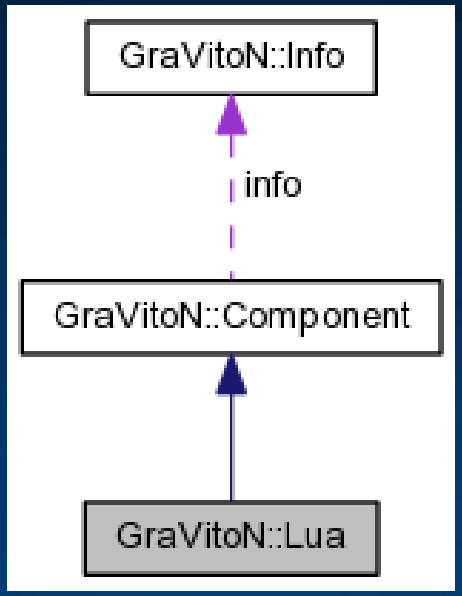
Msfpayload

Windows: download_execLinux:

Linux: exec (with wget)


msfconsole
Metaworm Master
Metaworm slave
Target

Lua



Definition

An Advanced component for advanced developers and advanced AI

Advantages

Run Lua scripts inside GraVitoN

Design dynamic AI

Upgrade your malware, by download new scripts!

THE HACKERS CONFERENCE

Malkit

Definition

Imagine GraVitoN as a missile again! Every component that designed to improve missile functionality (for example, Gyro (Port Scanner), Laser Defense (A.V Killer), Obstacle Avoidance (IDS Evasion)) is a Malkit.

Bypass A.V

Encode/Decode

Types

1. Copy and Decode

Read your encoded payload, decode it and write decoded payload somewhere else in memory

2. In place Decoding

Read your encoded payload and write decoded payload in the same memory address.

Encode/Decode

1.Delay: Old school

Sleep

For 1 → 1000000

2.Delay: Creative Method

DNS lookup for imnotexistsonweb7357abcd.com! → Network time-out!

Do it 100 times!

Calculate last prime number lower that 2^64 (unsigned long)

Patch

Finding Nemo!

Your binary payload has a signature

Use binary search algorithm to find your AV signature

1. Fill half of your payload with \x00
2. Recompile GraVitoN
3. Check A.V
4. Do this process recursively, again!

Patch

Apply your patches

Use Jumps

Always add your extra bytes at the end/beginning of your payload

Reduces risk of wrong jumps

Old pay:
1: sub eax, 1
2: cmp eax, 0
3: jle +2
4: jmp -3
5: retn

Wrong Patched pay:
1: add ecx, eax
2: sub ecx, 1
3: mov eax, ecx
4: cmp eax, 0
5: jle +2
6: jmp -3
7: retn

Right Patched pay:
1: jmp +6
2: cmp eax, 0
3: jle +2
4: jmp -2
5: retn
6: sub eax, 1
7: jmp -5

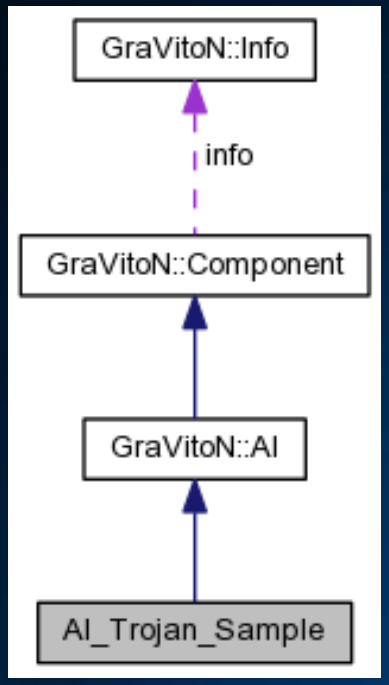
Let’s Go Code!

Target: Windows 7 pro Protected By Kaspersky Pure

AI: sample_ai_trojan

Payload: payload_meter_w32b

GraVitoN A.I: Samples



Trojan

A simple trojan has at least 2 components

1. AI
2. Payload

THE HACKERS CONFERENCE

Let’s Go Code!

A 32bit trojan against for Linux

Virus

A simple virus at least has 3 components:

1. AI
2. Payload
3. Intercross

Virus

Advanced Virus

Various Malkits

Multiple AIs managed by a master AI

Multiple Payloads

Multiple Intercross Components

THE HACKERS CONFERENCE

Let’s Go Code!

A Cross OS Virus

Future of the GraVitoN

THE HACKERS CONFERENCE

GraVer

Automated code generator

GraVitoN for 6+!

Visualizer

Drag and Drop your components and link them together

Add New Payloads

OS

Windows

Apple (OSX and IOS)

Android

Symbian

Hardware

PC

Smart Phone

ARM

New Spreading Techniques

More complicated methods

Infect windows driver files (sys files)

Different OS Support

Less AV Detection

Executable Modification Library

PE

ELF

Etc.

Sophisticated AIs

AI + Lua

Malkit

Port scanner + Banner grabber

VPN/SSL Support

Reporter Component

A valuable gift for pentesters who always are tired of writing those boring pentest reports!

Output

HTTP

SMTP

Assembly Obfuscation

An extra tool

Methods

Encode/Decode

Polymorphism

Metamorphism

Android and Apple iOS Tests

Compile GraVitoN for android and iOS

Wide community of users

Means more interesting targets for hackers

Final word

If you are a white hat…

If you are a 814(|< |-|@7…

If you are not a script kiddie…

JOIN GraVitoN Project Now!

http://www.thegraviton.org

GAME OVER