University of Rome “Sapienza”
Computer Science Department

A Live Digital Forensic system for Windows Networks

R. Battistoni, R. Di Pietro, A. Di Biagio, M. Formica, L.V. Mancini
(http://icsecurity.di.uniroma1.it)

IFIP-SEC 2008 – September 8th, 2008

Contributions

- **Usage of System Call interception for Computer Forensic purposes**
- Real Time System Call interception leads to *Live Digital Forensic* (LDF)
- Distributed collection of intercepted system call
- *System Call Interposition* technique on Windows NT family OS: many technical challenges
- The prototype (FOXP) is released as an open source project

Agenda

1. Computer Forensic & Live Digital Forensic
2. What’s FOXP?
3. FOXP Details
4. FOXP is FOSS
5. Future Works

Computer Forensic & Live Digital Forensic

"While the former approach is a static analysis of electronic support only after a damaging event, the latter is able to represent the state of a live system for a determined time interval"

Requirements for a Computer Forensic system

- **Completeness**: system has to collect enough information to intercept the user's activity;
- **Integrity**: nobody can modify the log without being properly authorized;
- **Authenticity**: logs have to be authenticated;
- **Non bypassable**: nobody can escape the log activity or stop the logging without authorization;
- **Transparency:** logging has to be invisible to the user;
- **Reproducibility**: knowing for every activity "who" and "what";
- **Efficiency**: minimizing the log dimension and the node overhead.

Requirements for a Live Digital Forensic system

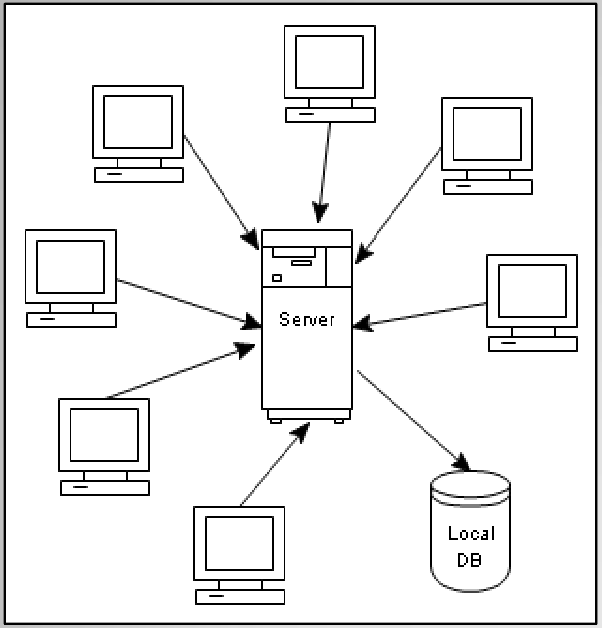
LDF has other requirements related to the "Live" term:

- **Continuity:** shutting down a system could represent a big problem in environments that cannot be stopped;
- **Real Time**: LDF intercepts activities **while the system is running** and no one knows about it; It can allow the CF expert and the Admin **to analyze in RT what happens** and to prevent malicious activities;
- **Proactivity**: In the classic Computer Forensic the approach is only "Reactive" whereas in the LDF it is "**Proactive**".

What's FOXP?

A LDF implementation: FOXP

FOXP (computer FOrensic eXPerience) : an open source Computer Forensic system for Windows network where every node has a Windows NT family OS (a closed OS that introduces a critical level of complexity)



Scenario:

- N controlled nodes, every node sends its logs to the central server
- A server node receives node logs and organizes them into a R-DBMS
- R-DBMS for data collection: is a support for a better forensic analysis

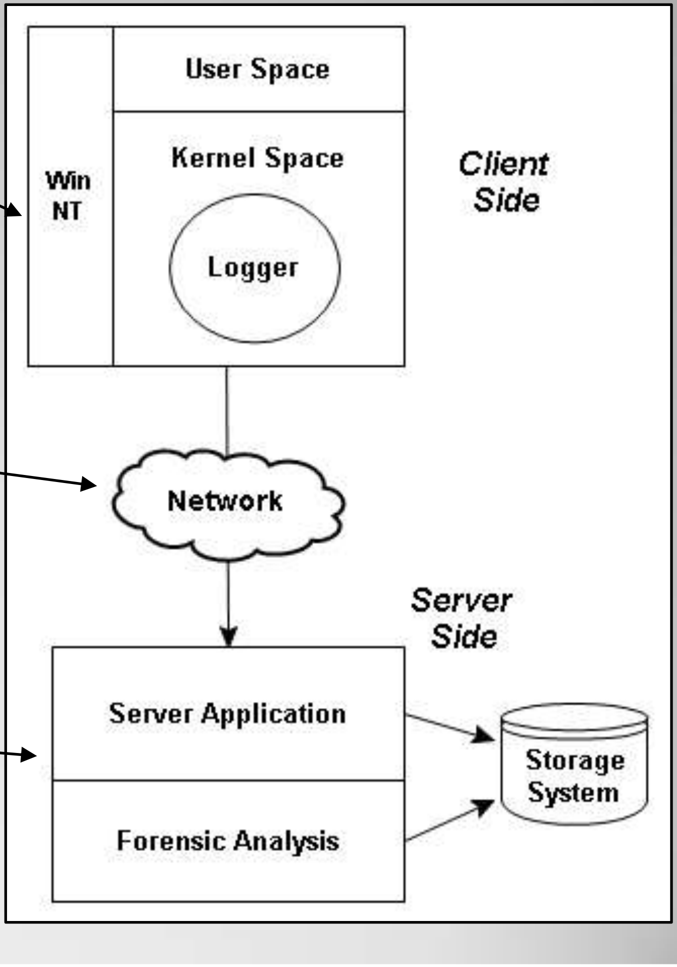
"Centralized logs collected in the collector node, allow to detect coordinated-attacks on network nodes: attacks that would not be detectable with a single node analysis"

FOXP Architecture

Client Side: logger component to collect data to send to the central server (Windows NT family OS)

Secure Communication: to provide authenticity, integrity and confidentiality (out of the scope of the paper)

Server Side: it's a server application that collects data sent from various clients; this data is available for forensic analysis

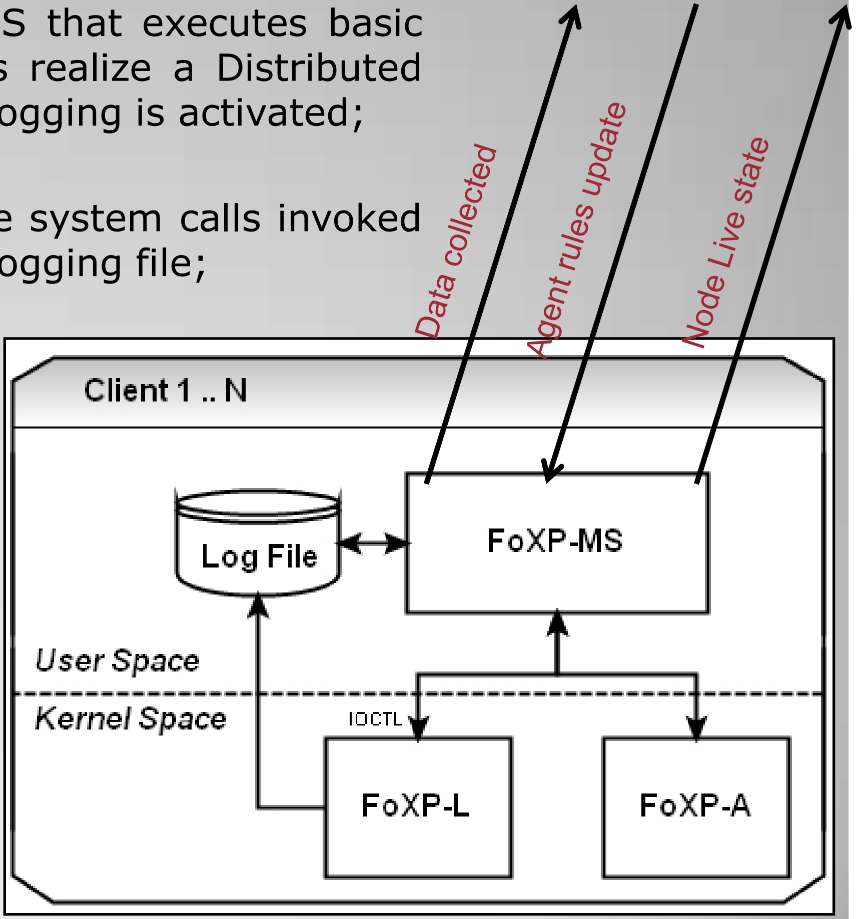


FOXP Architecture: client side

- **FOXP Agent (FOXP-A):** It is like an IDS that executes basic analysis of node activities (all the agents realize a Distributed IDS). If an anomaly is detected, than the logging is activated;

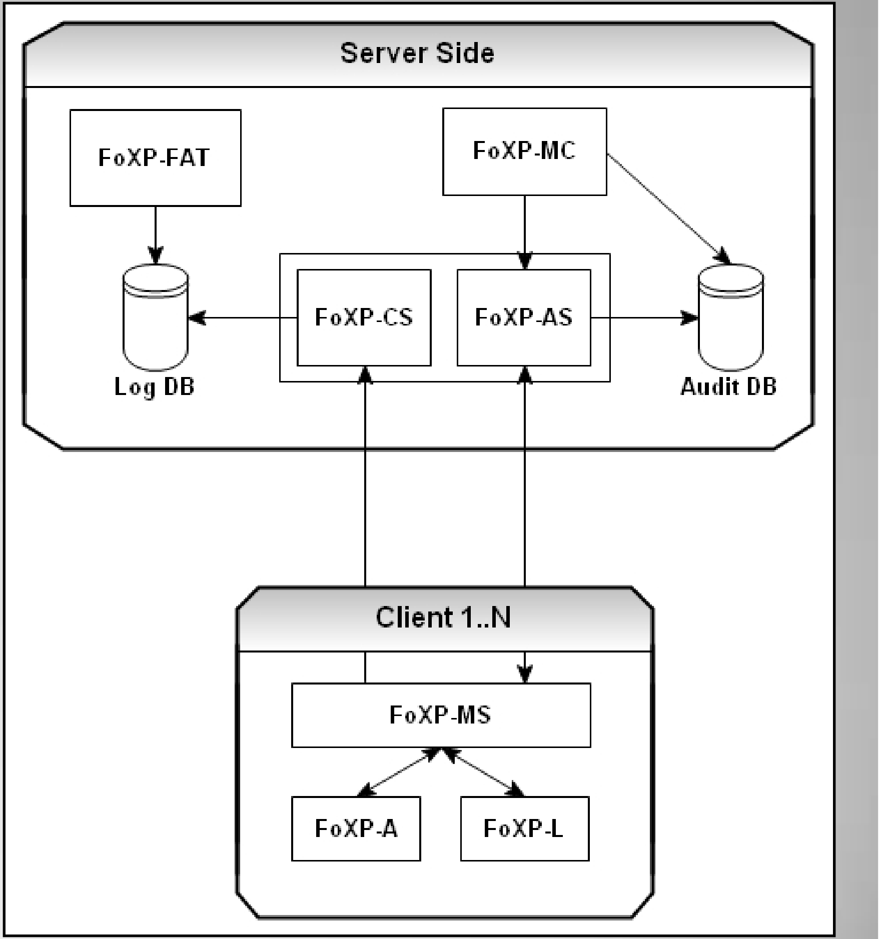
- **FOXP Logger (FOXP-L):** it intercepts the system calls invoked on the node and keeps track of them in a logging file;

- **FOXP Mgmt Service (FOXP-MS):** it manages the Agent and the Logger on every node as well as their communications with the centralized server of the architecture:
  - It receives commands from the Mgmt Console for the Agent rules update;
  - It forwards commands directly to the Logger;
  - It sends node live state to the Audit Server;
  - It receives messages from the Agent and send commands to the Logger;
  - It sends to the Collector Server the data collected from the Logger.

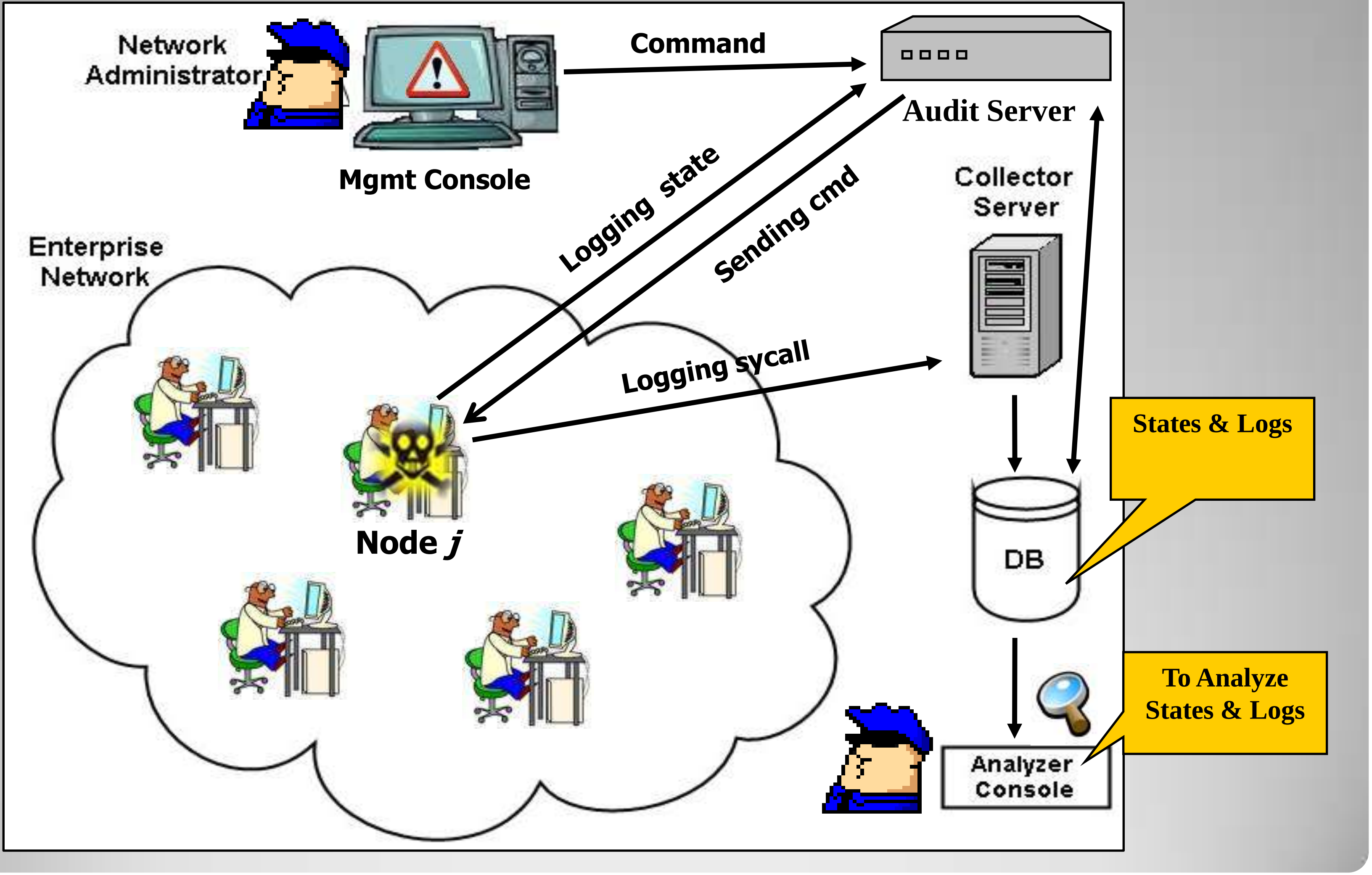


FOXP Architecture : server side

- **FOXP Collector Server (FOXP-CS):** it receives and stores logs from every network node;
- **FOXP Audit Server (FOXP-AS):** it receives and stores the state of the nodes. It receives commands from the FOXP-MC and forwards them to the FOXP-MS of the destination nodes;
- **FOXP Management Console (FOXP-MC):** it remotely manages network nodes communicating with the FOXP-MS on every node. It monitors the state of the nodes, configures and updates the Agent rules, manages the FOXP-Logger;
- **FOXP Forensic Analysis Tools (FOXP-FAT):** it executes the analysis of the collected logs and states.



FOXP Overview



States & Logs

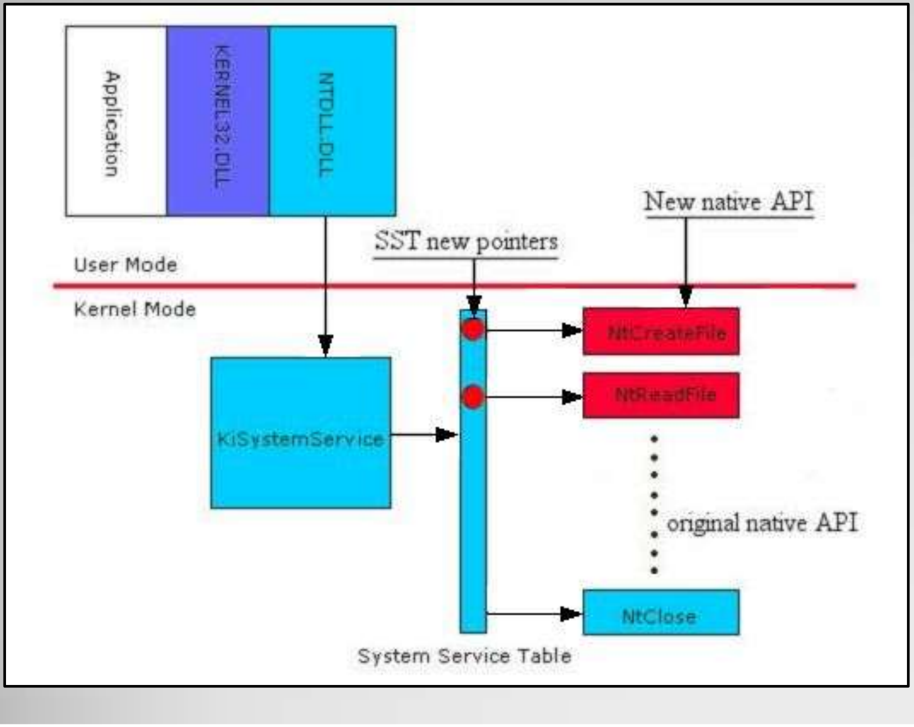
To Analyze States & Logs

FOXP Details

FOXP Logger

- It is a **kernel device driver** that uses the **system call interposition** technique;

- This technique substitutes for original pointers into the SSDT with new pointers to new system calls (**wrapper functions**);

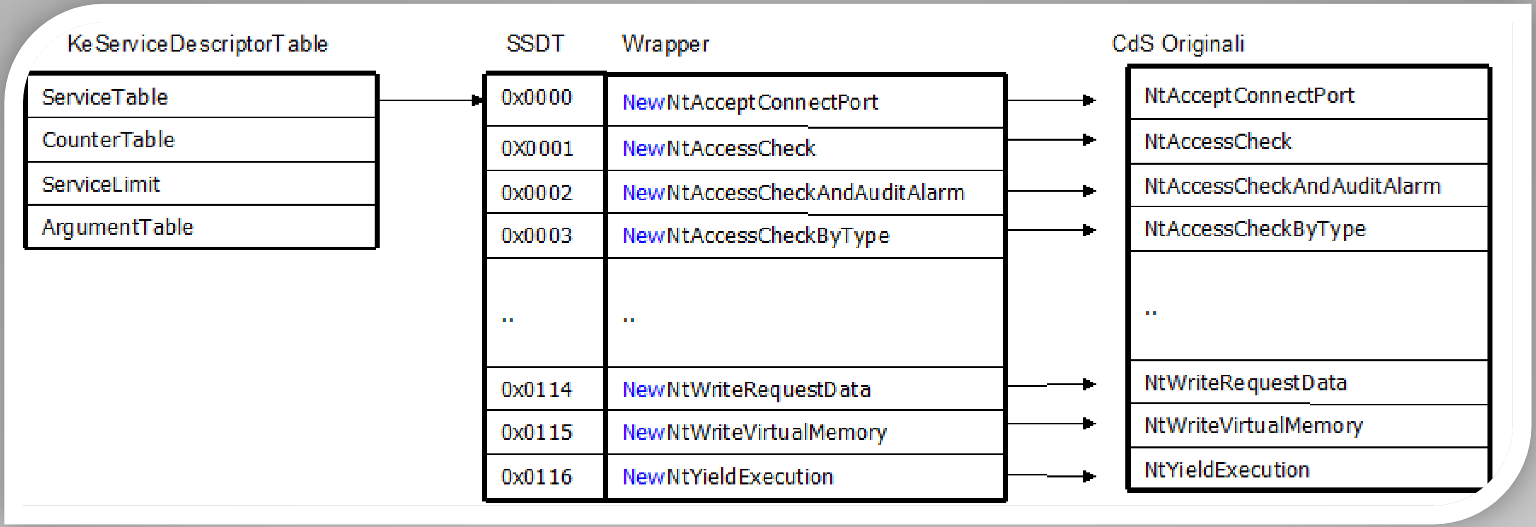


- Interception technique extended to all the **284 system calls of Windows XP**

- It uses the system call index instead of its explicit name

System Call Interposition

- System Call Interposition technique explained:



KeServiceDescriptorTable
ServiceTable
CounterTable
ServiceLimit
ArgumentTable

SSDT	Wrapper
0x0000	NewNtAcceptConnectPort
0X0001	NewNtAccessCheck
0x0002	NewNtAccessCheckAndAuditAlarm
0x0003	NewNtAccessCheckByType
..	..
0x0114	NewNtWriteRequestData
0x0115	NewNtWriteVirtualMemory
0x0116	NewNtYieldExecution

CdS Originali
NtAcceptConnectPort
NtAccessCheck
NtAccessCheckAndAuditAlarm
NtAccessCheckByType
..
NtWriteRequestData
NtWriteVirtualMemory
NtYieldExecution

FOXP Logger code

- Macro to exchange pointers in SSDT:

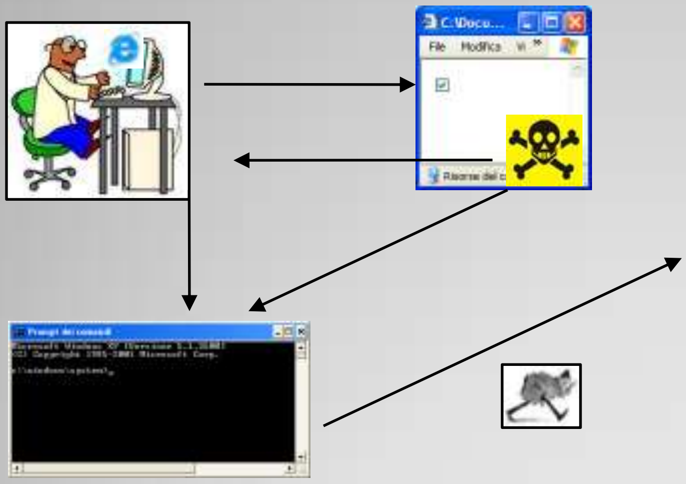
```
#define HOOK(APIName, NewAPIPtr, OldAPIPtr)
OldAPIPtr=ExchangePointers(&SSDT[Index(APIName)],NewAPIPtr)
…
HOOK( ZwOpenFile , NewZwOpenFile , OldZwOpenFile );
```

- Example of a new native API: NewZwOpenFile:

```
NewZwOpenFile(OUT PHANDLE phFile,…,IN ULONG OpenMode)
{
    doLog(“ZwOpenFile”, phFile,…, OpenMode);
    OldZwOpenFile(phFile,…,OpenMode );
}
```

Test: FOXP and Remote code exec

- Internet Explorer Remote Code Execution Exploit v 0.1



```
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\windows\system32>_
```

```
<input type="checkbox" id='a'>
<script>
        -- codice malizioso --
        var r = document.getElementById('a').createTextRange();
</script>
```

NtOpenFile

(

OUT PHANDLE phFile:34c|IN ACCESS_MASK DesiredAccess:1000a1|

IN POBJECT_ATTRIBUTES ObjectAttributes:/??/C:/WINDOWS/system32/cmd.exe|

OUT PIO_STATUS_BLOCK pIoStatusBlock:0|IN ULONG ShareMode:5|

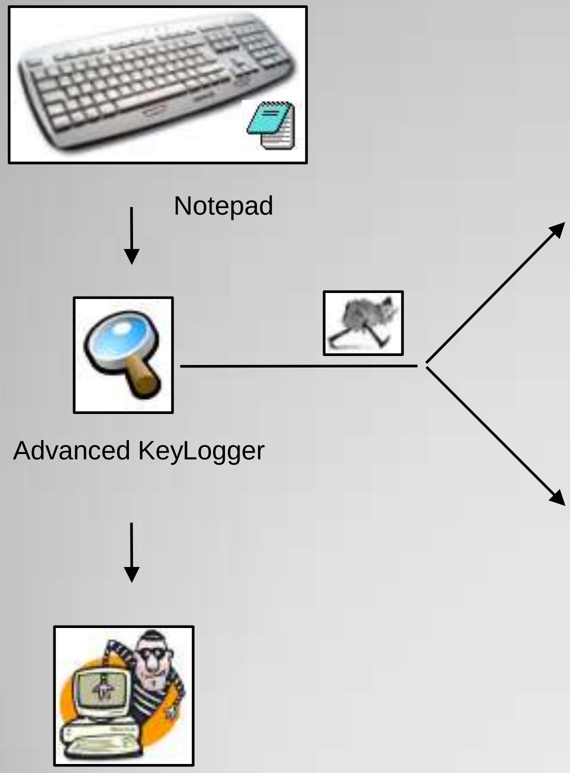
IN ULONG OpenMode:60

) ***called by:***

/Device/HarddiskVolume2/Programmi/Internet Explorer/IEXPLORE.EXE

Test: FOXP & Keylogger

- Advanced KeyLogger 1.3

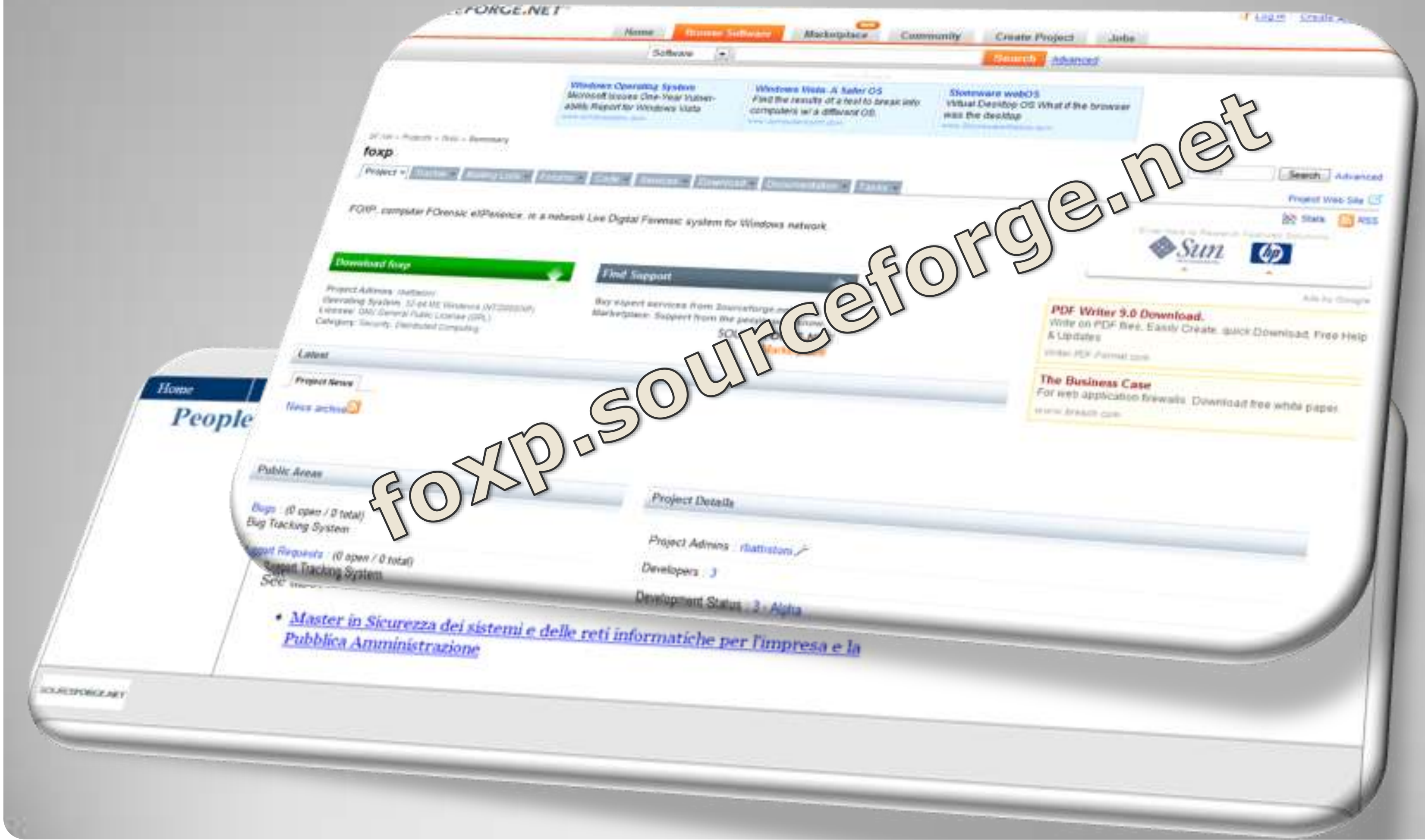


```
ZwOpenFile
(
OUT PHANDLE phFile:b4|IN ACCESS_MASK DesiredAccess:100020|
IN POBJECT_ATTRIBUTES
ObjectAttributes:/??/C:/WINDOWS/system32/TMLib.dll|
OUT PIO_STATUS_BLOCK pIoStatusBlock:0|IN ULONG ShareMode:5|
IN ULONG OpenMode:60
/Device/HarddiskVolume2/WINDOWS/system32/notepad.exe
)
called by:
/Device/HarddiskVolume2/WINDOWS/system32/notepad.exe

ZwCreateFile
(
PHANDLE FileHandle:dc|ACCESS_MASK DesiredAccess:40100080|
POBJECT_ATTRIBUTES ObjectAttributes:/??/C:/WINDOWS/ddemal.bin|
PIO_STATUS_BLOCK IoStatusBlock:0|ULONG FileAttributes:80|
ULONG ShareAccess:0|ULONG CreateDisposition:1|ULONG CreateOptions:60|
ULONG EaLength:0
) called by:
/Device/HarddiskVolume2/WINDOWS/system32/notepad.exe
```

FOXP is FOSS

FOXP on SourceForge



Windows Operating System
Microsoft Issues One-Year Vulnerability Report for Windows Vista

Windows Vista: A Safer OS
Find the results of a test to break into computers w/ a different OS

Stoneware webOS
Virtual Desktop OS What if the browser was the desktop

SF.net » Projects » foxp » Summary

foxp

FOXP, computer FOrensic eXPerience, is a network Live Digital Forensic system for Windows network

Download foxp

Project Admins: rbattistoni
Operating System: 32-bit MS Windows (NT/2000/XP)
License: GNU General Public License (GPL)
Category: Security, Distributed Computing

Find Support

Buy expert services from Sourceforge.net Marketplace. Support from the people you know.

SOURCEFORGE.NET Marketplace

PDF Writer 9.0 Download.
Write on PDF files. Easily Create, quick Download, Free Help & Updates

The Business Case
For web application firewalls. Download free white paper.
www.breach.com

Latest

Project News

News archive

Public Areas

Bugs : (0 open / 0 total)
Bug Tracking System

Support Requests : (0 open / 0 total)
Support Tracking System

Project Details

Project Admins : rbattistoni
Developers : 3
Development Status : 3 - Alpha

- Master in Sicurezza dei sistemi e delle reti informatiche per l'impresa e la Pubblica Amministrazione

foxp.sourceforge.net

Future works

Future Works

- Assessing the **efficiency and efficacy** of the FOXP system with Experimentations;
- **Classifying** the system calls according to their level of **dangerousness** (based on previous experiments);
- **Extending** our System Call Interposition technique on **VISTA** 32-bit OS;
- Communication security with authenticity and non-repudiability of collected logs, is currently under investigation and will be presented in a different paper.

Q&A

(battistoni@di.uniroma1.it - mancini@di.uniroma1.it)