Using Home Advantage

Combating Anti-Forensics and Linkage Blindness in Enterprise Entrenchment

“know when to hold em”

Eoghan Casey Chris Daywalt

Quick?

When an incident has been detected and analyzed, it is important to contain it before the spread of the incident overwhelms resources or the damage increases. Most incidents require containment, so it is important to consider it early in the course of handling each incident.

- NIST SP800-61 Rev. 1, page 3-19

Effective Incident Response, Part 1

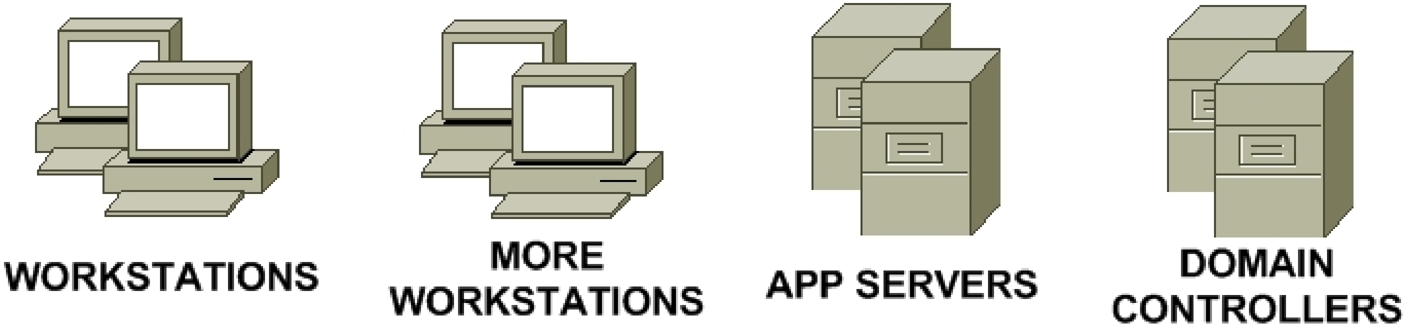
- Scope
- Scope scope scope
- Scope scope
- Scope, scopity scope scope scope

Definitions

- Linkage blindness
  - failure to recognize that crimes were committed by the same offender because they occurred in different jurisdictions
- Tandem modus operandi
  - use parallel but distinct methods of operating on compromised systems

These complicate scope assessment

Target Selection & Admin

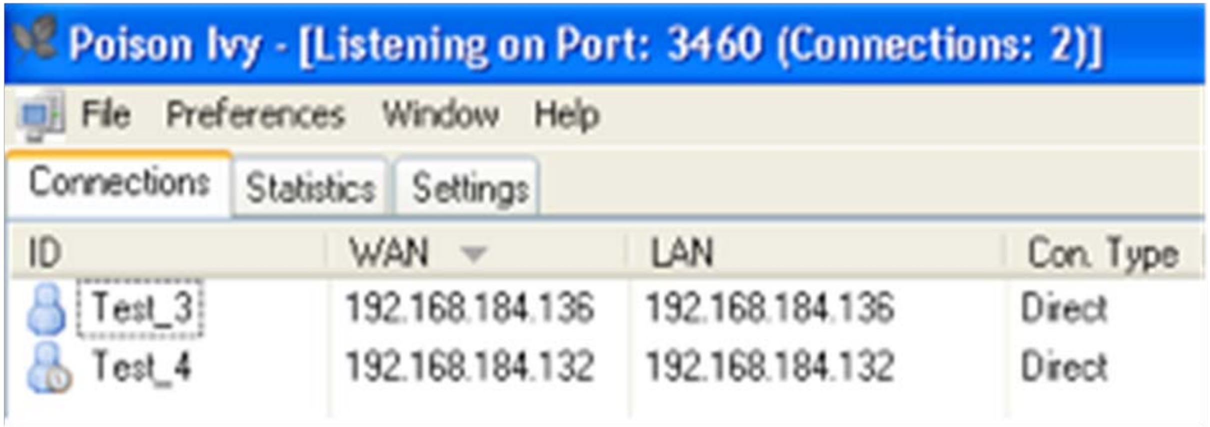


WORKSTATIONS

MORE WORKSTATIONS

APP SERVERS

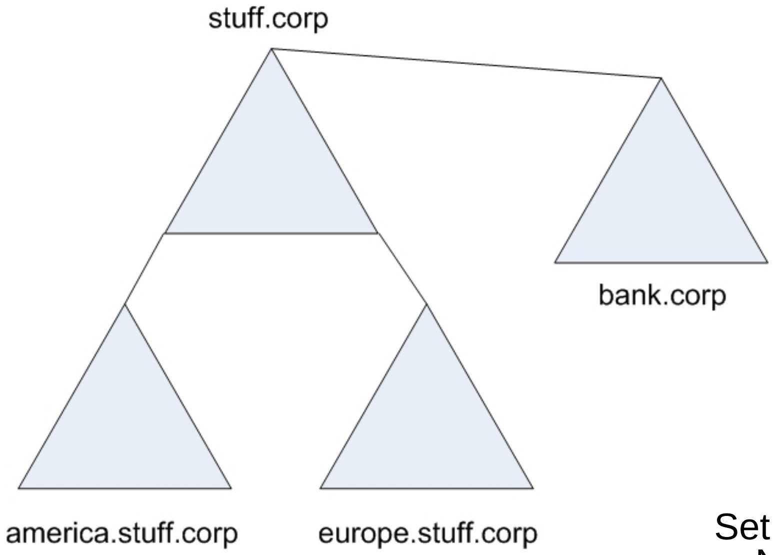
DOMAIN CONTROLLERS



Poison Ivy - [Listening on Port: 3460 (Connections: 2)]

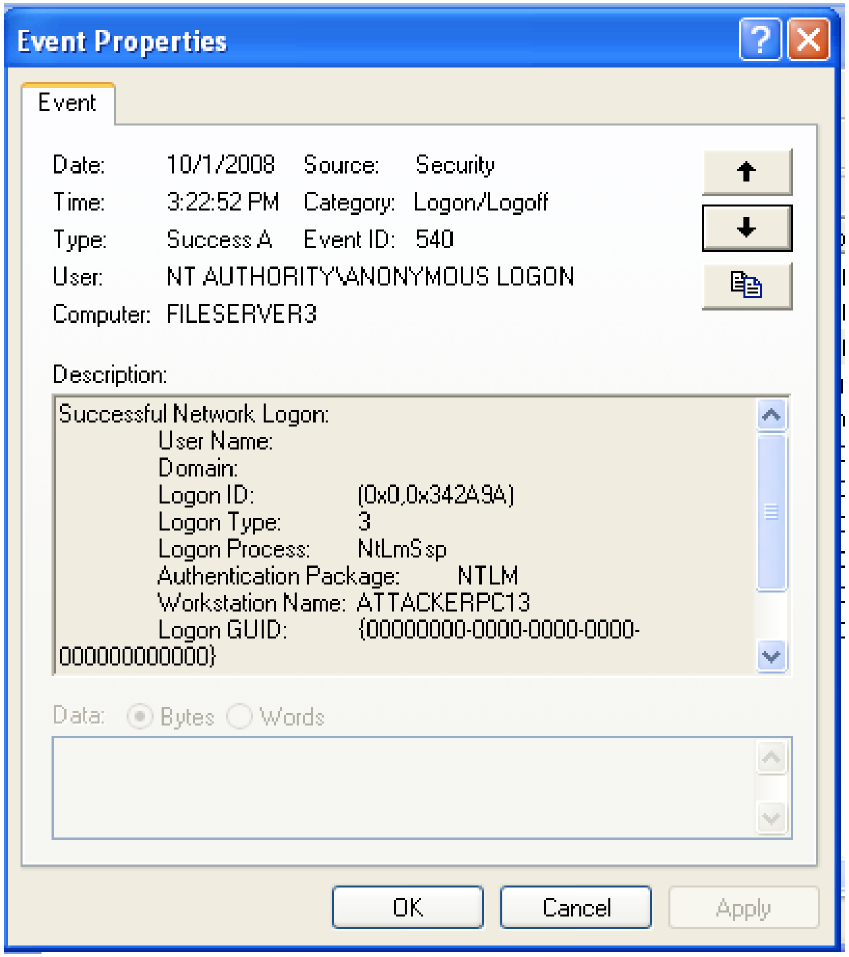
ID	WAN	LAN	Con. Type
Test_3	192.168.184.136	192.168.184.136	Direct
Test_4	192.168.184.132	192.168.184.132	Direct

Enterprise Credential Theft/Injection



```
Set objOU = GetObject(“LDAP://OU=Any OU,dc=Domain
    Name, dc=Domain Extension”)
    Set objUser = objou.Create(“User”, “cn=User Name”)
    objUser.Put “sAMAccountName”, “User Name”
    objUser.SetInfo
    objUser.ChangePassword ‘”, “Password”
    objUser.AccountDisabled = FALSE
    objUser.SetInfo
```

Linkage Analysis: Think Global



Date: 10/1/2008 Source: Security
Time: 3:22:52 PM Category: Logon/Logoff
Type: Success A Event ID: 540
User: NT AUTHORITY\ANONYMOUS LOGON
Computer: FILESERVER3

Description:

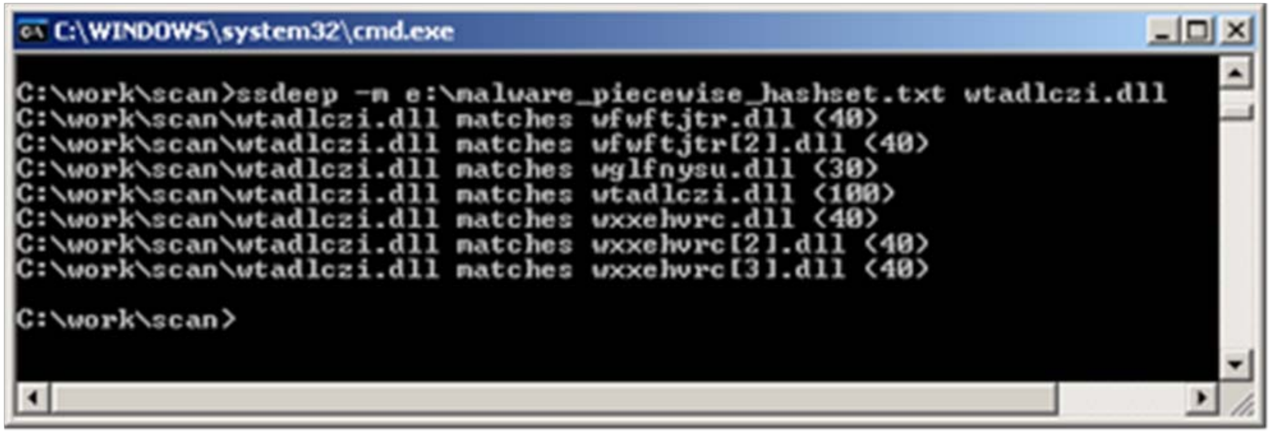
```
Successful Network Logon:
                User Name:
                Domain:
                Logon ID:               (0x0,0x342A9A)
                Logon Type:             3
                Logon Process:          NtLmSsp
                Authentication Package:         NTLM
                Workstation Name:       ATTACKERPC13
                Logon GUID:             {00000000-0000-0000-0000-
000000000000}
```

- x All Local and Network Logons

Tool Variance

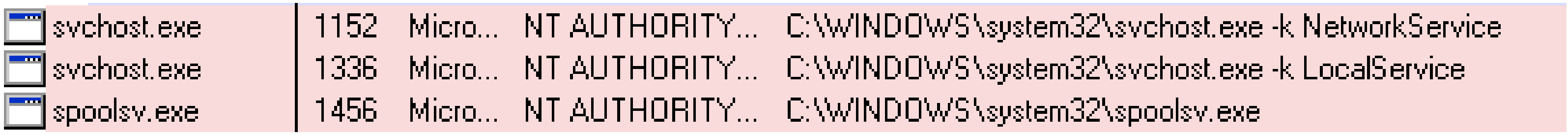
Rootkit / Backdoor Package	Victim Systems			
	1-10 Workstations	11-20 Workstations	21-30 App Servers	31-40 Domain Controllers
1A (abc.exe)	X			
1B (def.exe)		X		
1C (ghi.exe)			X	
2A (123.dll)	X			
2B (456.dll)		X		
2C (789.dll)			X	
3A (xyz123.exe)				X

Host Linkage Analysis

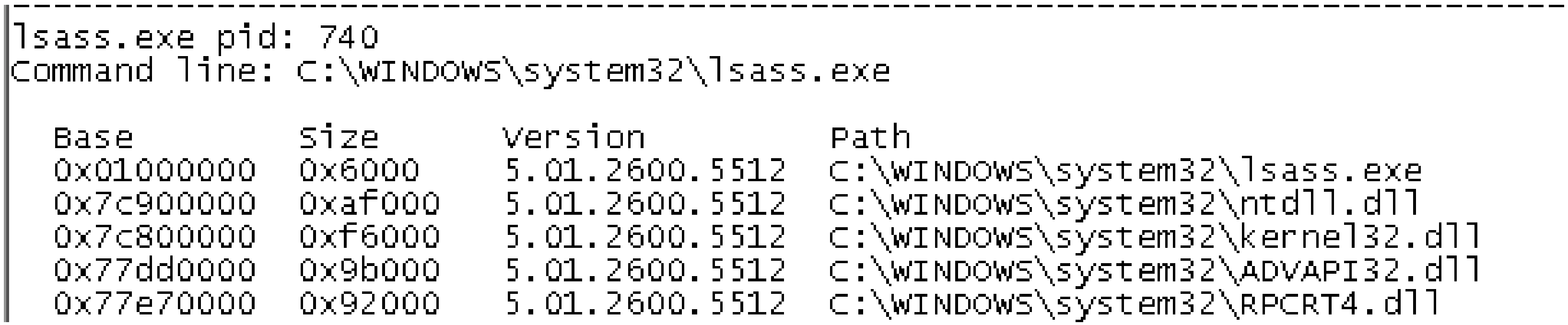


```
C:\work\scan>ssdeep -m e:\malware_piecewise_hashset.txt wtadlczi.dll
C:\work\scan\wtadlczi.dll matches wfwftjtr.dll (40)
C:\work\scan\wtadlczi.dll matches wfwftjtr[2].dll (40)
C:\work\scan\wtadlczi.dll matches wglfnysu.dll (30)
C:\work\scan\wtadlczi.dll matches wtadlczi.dll (100)
C:\work\scan\wtadlczi.dll matches wxxehwrc.dll (40)
C:\work\scan\wtadlczi.dll matches wxxehwrc[2].dll (40)
C:\work\scan\wtadlczi.dll matches wxxehwrc[3].dll (40)

C:\work\scan>
```



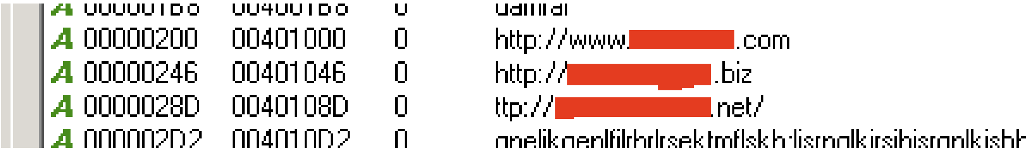
```
svchost.exe    1152  Micro...  NT AUTHORITY...  C:\WINDOWS\system32\svchost.exe -k NetworkService
svchost.exe    1336  Micro...  NT AUTHORITY...  C:\WINDOWS\system32\svchost.exe -k LocalService
spoolsv.exe    1456  Micro...  NT AUTHORITY...  C:\WINDOWS\system32\spoolsv.exe
```



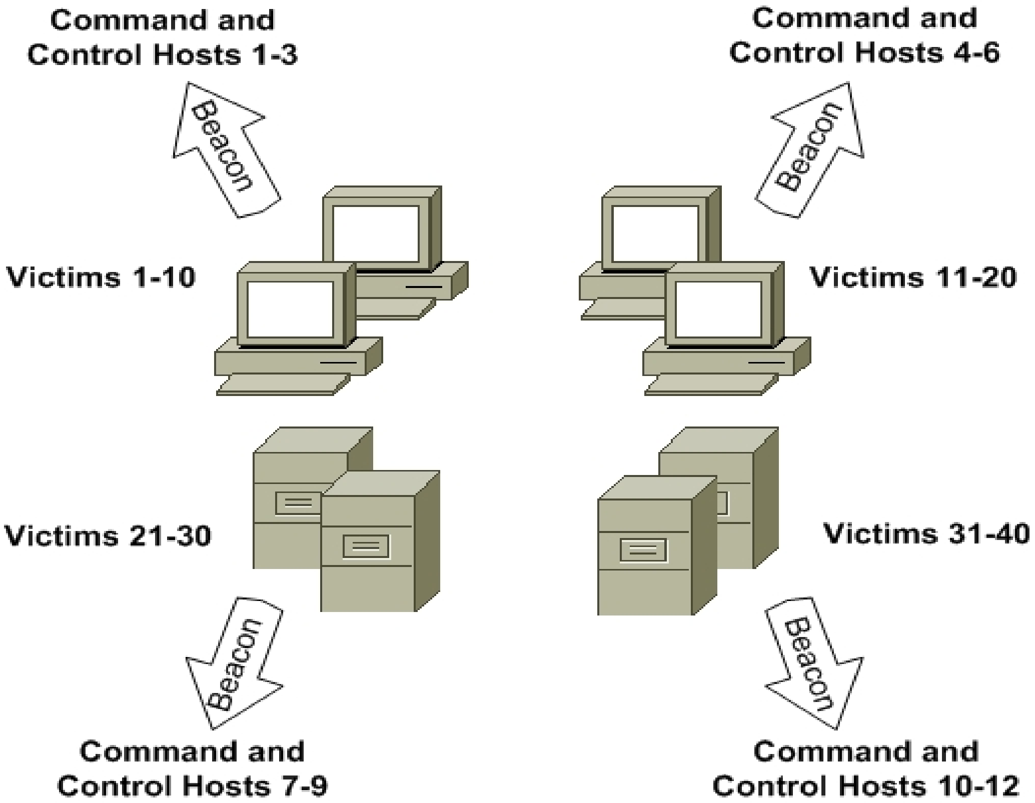
```
------------------------------------------------------------------------
lsass.exe pid: 740
Command line: C:\WINDOWS\system32\lsass.exe

  Base          Size        Version          Path
  0x01000000    0x6000      5.01.2600.5512   C:\WINDOWS\system32\lsass.exe
  0x7c900000    0xaf000     5.01.2600.5512   C:\WINDOWS\system32\ntdll.dll
  0x7c800000    0xf6000     5.01.2600.5512   C:\WINDOWS\system32\kernel32.dll
  0x77dd0000    0x9b000     5.01.2600.5512   C:\WINDOWS\system32\ADVAPI32.dll
  0x77e70000    0x92000     5.01.2600.5512   C:\WINDOWS\system32\RPCRT4.dll
```

Command & Control Variance



```
A 000001B8   004001B8   0   uamrai
A 00000200   00401000   0   http://www.[redacted].com
A 00000246   00401046   0   http://[redacted].biz
A 0000028D   0040108D   0   ttp://[redacted].net/
A 000002D2   004010D2   0   gnelikgenlfilrhdrsektmflskh:lisrnglkirsihisrnglkishh
```



Command and Control Hosts 1-3
Command and Control Hosts 4-6
Beacon
Beacon
Victims 1-10
Victims 11-20
Victims 21-30
Victims 31-40
Beacon
Beacon
Command and Control Hosts 7-9
Command and Control Hosts 10-12

Network Linkage Analysis

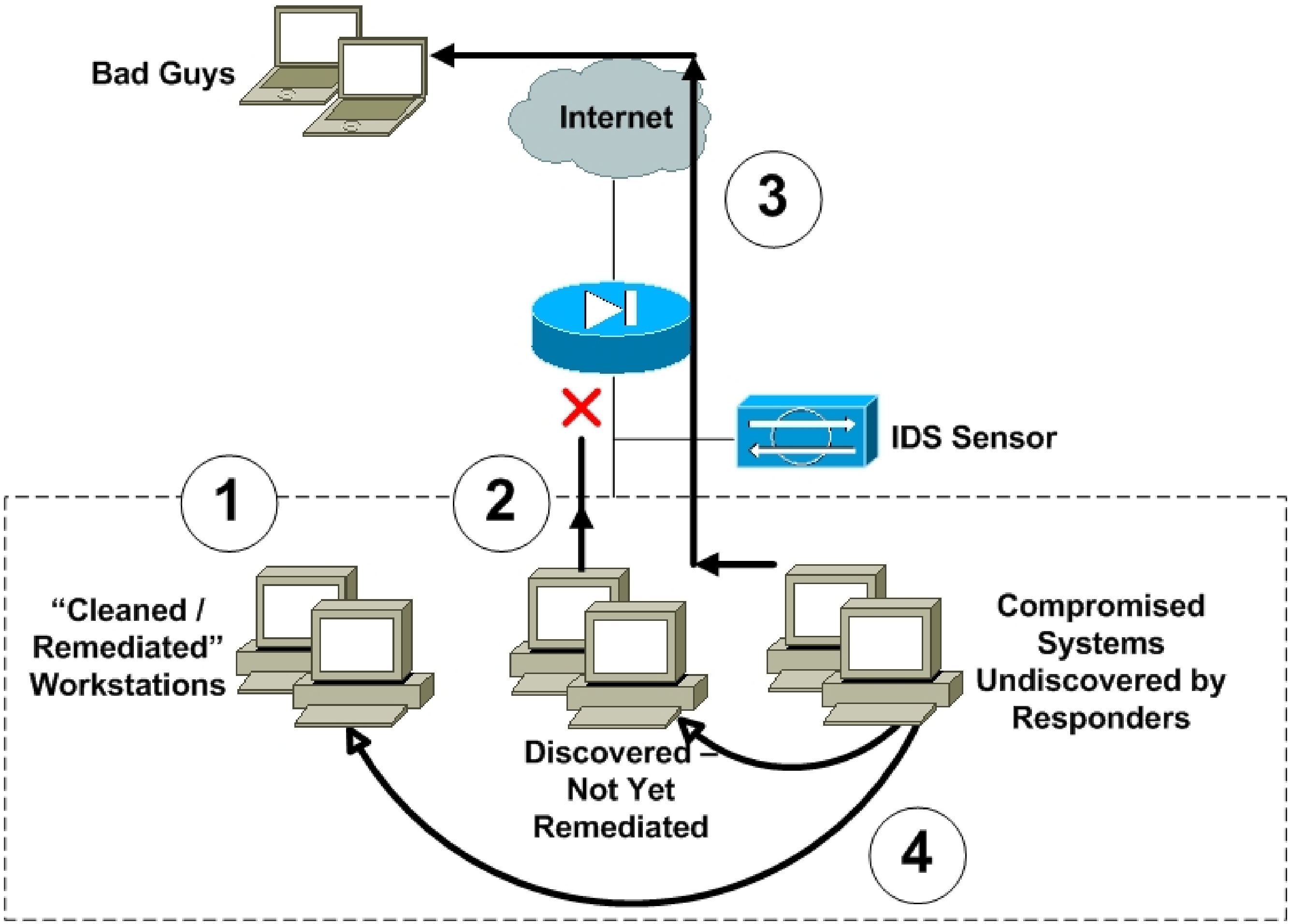
- Deep C&C traffic analysis
  - Common features in beacon packets
  - Discernible patterns in encrypted traffic
- Home Advantage
  - Deviations from normal traffic

Effective Incident Response, Part 2

NIST Incident Response Life Cycle

1. Preparation
2. Detection & Analysis
3. Containment, Eradication & Recovery
4. Post-Incident Activity

Re-infection Vectors


Bad Guys
Internet
3
IDS Sensor
1
2
"Cleaned / Remediated" Workstations
Compromised Systems Undiscovered by Responders
Discovered – Not Yet Remediated
4

Containment Strategies

CLASSIC:

- Block bad attacker IP addresses
- Block C&C domain names
- Rebuild or clean compromised systems
- Reset compromised credentials

NEW:

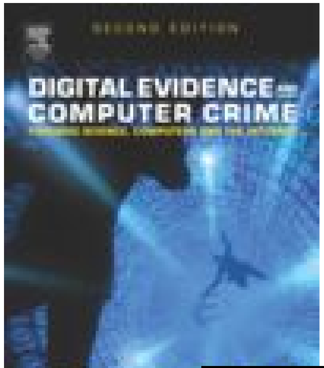
- Active directory account validation sweep
- Change critical account names
- Restrict policies
- Establish internal perimeters
- Intensified monitoring
- WHITELISTING!!!11~

Organizational Preparedness

- Team structure and training
- Windows domain isolation
- Remote forensics capabilities
- Customize IDS signature/preprocessor
- Centralized host logging
- Network logging (perimeter & internal)
- Focused monitoring of critical assets
- Tools for detecting deviations
  - Host and network abnormalities

Scope!

- Contact eoghan@jhu.edu
- Sharing the knowledge

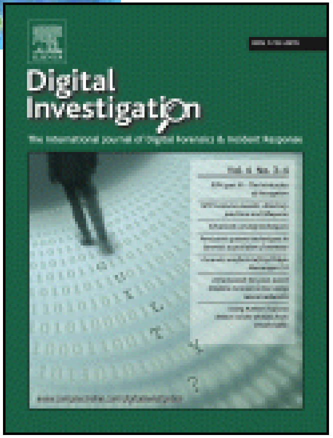


SECOND EDITION

DIGITAL EVIDENCE AND COMPUTER CRIME

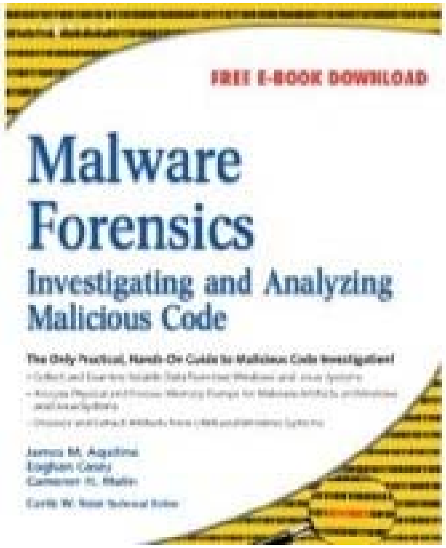
FORENSIC SCIENCE, COMPUTERS AND THE INTERNET

EOGHAN C



Digital Investigation

The International Journal of Digital Forensics & Incident Response



FREE E-BOOK DOWNLOAD

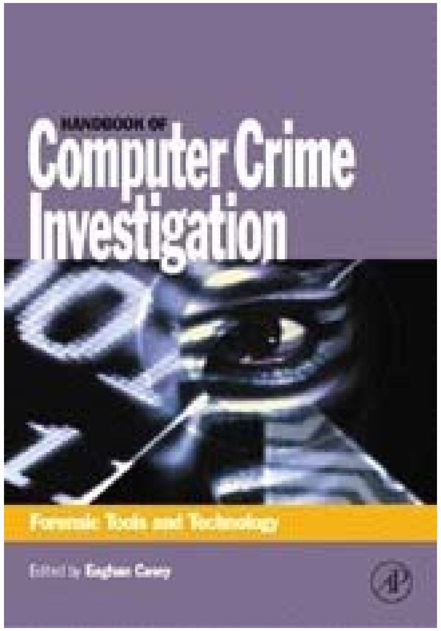
Malware Forensics

Investigating and Analyzing Malicious Code

The Only Practical, Hands-On Guide to Malicious Code Investigation!

James M. Aquilina
Eoghan Casey
Cameron H. Malin

Curtis W. Rose Technical Editor



HANDBOOK OF Computer Crime Investigation

Forensic Tools and Technology

Edited by Eoghan Casey